Eric VERHEUL

I think the eIDAS Wallet ARF is a nice document shedding light on some (but not all!) unclear issues in the eIDAS update proposal itself I identified here. It might be interesting to a make a full comparison. As a first start let met state some observations and pose some questions on the ARF:

1. In meeting the eIDAS High authentication mechanism requirements, the ARF also refers to the use of Trusted Execution Environments (TEEs). This seemingly hints that the use of the Apple Secure Enclave and Android hardware backed keystore is acceptable. As this would open the wallet for >90% of the European citizens that would be good news. However, no further light is shed on eIDAS High authentication mechanism requirements. For this the ARF simply refers to the eIDAS implementation regulation CIR 2015/1502. This is meaningless as CIR 2015/1502 does not define the fundamental notion 'resistance to attack (High) potential' apparently due to the differences among the member states. But as this needs to be resolved for the eIDAS wallet public certification scheme (Article 6c of the update), I would suggest you start the discussion here and now. It is long overdue anyway.
2. What is the difference between "PROVIDERS OF PERSON IDENTIFICATION DATA (PID)" (Section 3.3) and the (qualified) "ELECTRONIC ATTESTATION OF ATTRIBUTES PROVIDERS" (Sections 3.5, 3.6)? It seems logical to me that a PID only provides "signed" personal data without the user being able to show he/she is the owner of it, at least in a online fashion. A digital driving license would be an example of this; it is signed by a government organization (RDW in the Netherlands) including the facial image of the holder. 'Authentication' then is based on a relying party comparing the image with the person showing it. However, the text on p. 19 "Online sharing shall require the user to prove ownership of the used (Q)EAA or PID by proving access anxed control over cryptographic material linked to the (Q)EAA or PID" indicates that PIDs allow for online authentication making the difference with (Q)EAA unclear. It would be advisable to make that more clear. Also, how does a PID relate to the eIDAS update proposal itself?
3. In Footnote 15 (page 17) of the ARF it is stated: "Mutual authentication between wallets and relying parties should not be understood as mandatory for every transaction." An example would be helpful here as I have no idea what is meant here. Authentication of the relying party to user seems mandatory to me as otherwise users are susceptible to phishing. This perhaps relates to the PID discussion started above.
4. In ARF Sections 4.6.1 "User awareness component" and 4.6.2 "User authorization mechanism" the fundamental role of user consent (called reliable user confirmation in my Issue #5) is finally identified; it is lacking in the eIDAS regulation itself. What is lacking however is the level of assurance in which consent shall be implemented by the eIDAS wallet. As I argued in Issue #5 such consent is so security vital in authentication that it also should protect against attackers with 'high attack potential', i.e. the security level of the eIDAS wallet authentication mechanism itself. For instance, I don't think you want such consent to be implemented in an internet browser as then man-in-the-browser malware can fool you and let you sent sensitive data to the parties you are not aware of. That is the classical modus operandi so successfully used in internet banking fraud.
5. In ARF Section 4.8.3 "Interface towards relying parties, brokers or proxies" the role of proxies is addressed, i.e. parties sitting between the user and the relying parties providing support to the relying parties. This section only states that through the use of proxies "the reliability of the authentication mechanism shall not be affected.". As indicated in my Issue #9 also the confidentiality of the attributes traveling through the proxy shall not be affected. That is, to

protect the user privacy the proxy shall not have access to the plaintext attributes. I also sketched how Issue #9 can be easily implemented through the use of QR-codes.

Antti POIKOLA (EVERNYM)

This is a wonderful analysis of the ARF publication: https://www.evernym.com/blog/eu-digital-identity/

I copy below the main points:

[text omitted – see link above]

Andres KÜTT

The fundamental and most problematic issue of the Wallet concept is, that it uses data to authenticate a user: "... the European Digital Identity Wallets (EUDIW) shall enable the user to securely request and obtain, store, select, combine and share the necessary person identification data (PID) to authenticate online and offline in order to use online public and private services"

This approach creates a situation, where knowledge of the attributes of the person rather than knowledge of some shared secret or what-you-have/know/are is used for authentication purposes. This is problematic in two main ways:

- User data stored by all stakeholders becomes commercially useful, i.e. it can potentially be used to perform identity theft and to impersonate a user. This creates a strong incentive to breach major EU datasets greatly decreasing user privacy and significantly increasing the cost of cybersecurity in the EU
- All stakeholders intending to use the EUDIW for authentication purposes must necessarily store the user attributes or their derivatives to be able to perform authentication. This further creates datasets forming potential targets for cybercriminals

Kalev PIHL

ARF does create much needed clarity into engineering about the EUDIW legal discussions. However too little. It is focusing on using personalised wallet in interacting with services and getting new attribute and combining them in random, which I skip commenting until there is hope that it is possible to manage wallet lifecycle in a manner that is prescribed.

1. Issues with starting the service

ARF uses terms Wallet provider and Wallet issuer. In no place is it clear if these are the synonyms or the are different entities and if different then what they are responsible for.

If I just semantically try to guess, then:

- Wallet provider is someone who created a product that could be certified under ENISA's futuristic certification scheme to be compliant with EUDIW requirement.
- Wallet issuer is an entity (possibly member state) who created processes for someone to get their own wallet.

Somehow now the Figure 1 and the rest of the text is stating that PID provider is magically able to provide right personal data to the wallet and the rest of the interactions are already personalised. But who is responsible that the wallet does not get incorrect user data into it in the first place? Wallet provider, Wallet issuer or PID provider? Who is going to court in which cases?

It is not clear if person having different identity data assigned to them from several member states is able to use one wallet and link attributes from different member states, but as wallet was offered as an answer to people using services cross border that ability within wallet is crucial.

ARF text

„The EUDI Wallet shall meet the requirements set out in Article 8 of the eIDAS Regulation with regards to assurance level high, in particular as applied to the requirements for identity proofing and verification, and electronic identification means management and authentication, as defined in CIR 2015/1502.28"

Who is passing the audits for product certification, High Level of Assurance as Identity Scheme in the case of any EUDI Wallet? Here the fact that Wallet by definition in EIDAS 2.0 is not clearly a service nor product does not allow to understand the sentence.

Will I know if new wallet is created on my name in the first place? Maybe I was fooled to play a game and outcome was wallet – and in the process the contact given belong to my game host.

2. Issues with closing the service

ARF does not explain if person who has one wallet then:

- Can they have another one and could it be different from content point of view
- If they lost it are they able to restore its content to new one and make sure that no one has done interactions after their wallet was stolen
- Will I at all know if my wallet is revoked?

If we are about to create tool for hundreds of millions of EU residents then there will fraud. And repeating messages that user has great awareness from different UI's does not help if they were not the ones who saw that UI.

Mikel SANCHEZ

Section 4.8.2 "Interface towards Member States identity cards" states the following

Following Regulation 2019/115725, Member States ID cards contain attested PID in digital format, accessible through a contactless interface. The EUDI Wallet may leverage on this data in its workflows for instance in order to:

- Retrieve electronically attested PID;

- Help with the identity proofing process;

- Strengthen identification or authentication claims.

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.

Passports and national identity documents which contain electronic components may also be considered for interfaces.

In my view, it is important to clarify the relationship between the above requirement and the regulation called "REGULATION (EU) 2019/1157 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement" (see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019R1157)

This regulation came into force on August 2, 2021 and refers to the restriction of access to biometric information from the chip. Specifically it states the following in Article 11, paragraph 6.

Biometric data stored in the storage medium of identity cards and residence documents shall only be used in accordance with Union and national law, by the duly authorised staff of competent national authorities and Union agencies, for the purpose of verifying:

(a) the authenticity of the identity card or residence document;

(b) the identity of the holder by means of directly available comparable features where the identity card or residence document is required to be produced by law

For that reason, I think it is important to specify in the wallet architecture document under what conditions, access to the photo stored on the NFC chip is possible. I believe that in this use case, the competent authorities at the national level should authorize access to the photo on the NFC chip due to the following reasons.

1. To prevent fraud. Access to the photo stored on the chip allows comparing it with the photo printed on the ID card. This allows verifying that the citizen's photo has not been manipulated or altered.

2. In private conversations with different law enforcement authorities we have been informed that identity fraud based on manipulation, alteration or impersonation of the photo on the document is around 95% of the total cases. Access to the chip photo mitigates this risk.

3. Complementary to the above, the use of biometric technologies for the detection of duplicate identities is suggested. Fraud is known to occur when a person uses the same photograph in false identity documents with different personal data. To avoid this type of risk, it is possible to use 1:N facial identification techniques in which the photo of the ID document added to the wallet is compared against a state database of registered citizens, similar to the technological solutions already implemented in Mexico by the Instituto Nacional Electoral (INE) or in Peru by RENIEC.

Sebastian ELFORS

Remain technology neutral regarding repositories with attested attributes

The EU Wallet Architecture and Reference Framework (ARF) document does not yet specify what type of repositories that will be allowed/required for protection, publication and retrieval of attested attributes. There are different approaches that can be considered:

- Apply a Qualified Electronic Seal (QES) in JAdES-format to the attested attribute (Verifiable Credential), which will protect it with respect to integrity and authenticity. Such signed Verifiable Credential can be published in a HTTPS/LDAP repository, from where it can also be retrieved. A DID method can specify the creation, storage, retrieval and revocation of the Verifiable Credential. This solution will also bridge the gap between the existing eIDAS trust framework into the EU Wallet eco-system.
- Another option that has been specified by EBSI is to use a distributed ledger ("blockchain") for managing the lifecycle of Verifiable Credentials.

We recommend that the EU Wallet ARF remains technology neutral as regards to repositories for storing, protecting and resolving attested attributes.

Allow for hybrid authentication schemes

Hybrid authentication solutions and split key schemes should be allowed for the EU Wallet on LoA High. Such schemes are typically based on a combination of a client-side software app and a server-side module hosted in an HSM, which in conjunction allows for secure authentication and signature creation.

There are different types of hybrid authentication and split key protocols: The PAKE/OPAQUE protocol, the Estonian Smart-ID scheme, and the Belgian Itsme mobile eID. Such solutions can be Common Criteria certified and allow for remote qualified signature creation at a remote QSCD in an HSM.

At the eIDAS2 hearing in the EU parliament on 2022-02-03 split key schemes were addressed. The Estonian parliament member pointed this out specifically and referred to the Estonian Smart-ID scheme that is approved in Estonia on eIDAS LoA High. The eIDAS expert panel also acknowledged this as a potential solution for the EU Wallet.

There are several benefits with hybrid authentication solutions, in the sense that they combine a user-friendly mobile software app with a hardware protected key at a remote HSM. The existing Estonian and Belgian mobile eID solutions, which are currently based on such hybrid schemes, have attracted a large user group and generate far more transactions than traditional smart card based eID-cards.

Timo HOTTI

I have a general concern about the applicability of the proposed framework to the majority of the potential valuable use cases of the digital wallets.

The most common use of any wallet, analog or digital, is a trade transaction. It is without any question also the most valuable use case. It is in vast majority of the cases a multi-step process involving more than two parties. At bare minimum, the steps of a digital trade transaction are:

- The seller requesting payment from the buyer using using a verifiable credential, e.g. an invoice or other suitable request-to-pay mechanism.
- The buyer instructing, in a verifiable manner, his/her/its bank or other payment service provider to pay to the seller.
- The seller issuing a receipt (as a verifiable credential) about the completed transaction to the buyer.

More sophisticated versions of the transaction include other parties, such as logistics providers, insurers and financiers and consequently, also additional steps. It is also critical to understand, that the vast majority of such transactions have both individuals and organizations as participants.

Without going into too many details, the proposed framework makes the implementation of digital trade transactions very challenging, if not impossible.

The framework for example assumes that only organizations can issue credentials and be relying parties. This makes it impossible for individuals to issue verifiable claims to express e.g. a debt relationship or a payment authorization in the context of the transaction. The proposed framework also allows only credential exchange between two parties without any transaction context. Furthermore, the framework does not provide any guidance about establishing digital identities to legal persons, i.e. organizations. Yet further, the use cases that guide the development don't take into account the need for any value transfer between the parties of the credential exchange. Finally, the governance of parties, credentials and their use is heavily centralized into a potentially large number of registries.

The above-mentioned issues in the proposed framework make it somewhat hard for private sector to utilize the framework.

When developing a digitalisation solution for the private sector to use, it looks quite apparent, that three issues, that are currently unaddressed, need to be addressed properly in the very beginning of the private sector participation:

1. multi-party transaction contexts (e.g. trade) and the verifiable credential -based interaction of persons in those contexts,
2. digital wallets (agents) for all participants, including legal persons, and
3. integration of payment rails to the transactions and their parties to enable value transfer between parties of the transactions.

To get the digital identity journey started, it may be necessary to start from the simplified use cases with limited economic value. This is the route that seems to have been chosen. However, when going along that route, care should be taken not to impose regulation and limitations, that have unintended, even crippling consequences later on, when the scope of the journey is extended to the economically valuable use cases, especially the digital trade transactions.

I have two general recommendations:

1. **Short term scope management.**

a) Limit the scope of the wallet initially to public sector use cases only and do not impose any rules that may harm the applicability of the wallets in the private sector use cases, that may emerge later. In other words, state clearly, that the scope at this point is in use cases requiring credential exchange between EU residents and government entities.

b) Remove any mentions about private sector "non-qualified" parties, credentials or their usage from the material. It is quite probable, that the approach, that may work in the public sector domain, will not work in the private sector domain.

2. **Long-term vision and private sector participation management.**

a) Leave sufficient room for innovation for the private sector to encourage their participation. The ideas from the public sector domain may be freely "borrowed" to the private sector use cases, but they should not be made mandatory.

b) Ideally, the public and private sector domains should share technical standards, such as DID, Verifiable claims and DIDcomm. Common governance model for the domains is probably not a good idea. There is more than one possible way to e.g. establish trust within a domain. The freedom to choose the most suitable one for each domain should be maintained. Any interoperability between the domains should be made separately agreeable.

c) Establish some competitive innovation-encouraging arrangement, that has well-motivated participation from the private sector to work on the second generation of the EUDI architecture to enable the economically valuable use cases, especially the digital trade transactions.

Anna-Sophie ECKER (AUSTRIAN FEDERAL ECONOMIC CHAMBER - AUSTRIAN BANKING AND INSURANCE INDUSTRY)

The Division Bank and Insurance of the Austrian Federal Economic Chamber, as legal representative of the entire Austrian banking and insurance industry, appreciates the possibility to comment on the Architecture and Reference framework. We would like to note the following comments and remarks.

In general, the outline of the European Digital Identity Architecture and Reference Framework is welcomed by our members. Nevertheless, some clarifications regarding the framework should be considered.

We would like to raise the following questions:

The framework states that organizations, which are recognized or mandated by the member state could issue EUDI wallets. Is it correct that Member States will decide upon who can be an EUDI wallet issuer once it becomes available to the end user?

How can private industry contribute to ensure that EUDI wallets will become available on-time in each member state? (Still only half of the member states have notified an EU 910/2014 compliant eID today)

Will the PID be issued to the wallet by a member state service only or could it be introduced by utilizing an already issued (biometric) ID document (as stated in chapter 4.2)?

Figure 1 shows the role of a **wallet provider**, which issues a wallet to the end user. However, the following detailed description only refers to a role of a **wallet issuer**. Please clarify if these are two separate roles or not?

Who will be in charge of providing end user support when using the EUDI wallet (end user helpdesk?)

Could you explain the differences between an authentic source and an authoritative source?

Is there a limitation in the sense, that private institutions will only be able to issue EEA or does it depend on the certification level of the attestation provider? For example, would you describe attestations related to QEEA and EEA according the LoA model in terms of IAL / AAL and FAL, or would another ruleset be applied?

Could you provide more details regarding the roles that can be taken by different entities (public or private)?

What business opportunities (business models) can be offered for the private industries? Is there a business model available for each role in this ecosystem? Could you explain, which value chains will be available?

In Chapter 4.2 the framework refers several times to EUDI to support the LoA=High. Is it correct, that the EUDI should support LoA up to LoA=High, so that also "lower" LoA (substantial / low) will be supported?

Could you clarify the scope of online/offline authentication? To what extent is the wallet "offline" to a backend but local interfaces are still available (NFC/bluetooth) and the relying party still needs to be online to validate towards EAA provider?

Could you please define the following passage in chapter 3.10: "Relying parties are natural/legal persons"? Does this mean "service provided by a legal entity (or natural person)"?

The framework mentions using international standards to enable interoperability. Could you provide more details and please describe the interoperability principles?

For basic use cases/usage, the terms and conditions should be EU-wide standardized, otherwise, it will be difficult to switch between different wallet providers.

“EUDI Wallet Issuers would be responsible for ensuring compliance with the requirements for EUDI Wallets” page 10: Please clarify what their liabilities are.

“Authentic sources in scope of Annex VI would be required to provide interfaces to QEAA providers” page 11: Please clarify why only via providing direct verification services/interfaces? why limiting that?

“relying parties would need to inform the Member State where they are established and their intention for doing so” page 12: Will they also have to register an explicit list of attributes, they intend to query? Will these lists of attributes be made public?

“The EUDI Wallet shall 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” page 16: Does that mean enrolment can NOT be done remotely but ONLY onsite and face2face?

Please clarify, if mutual authentication between wallet and relying party, as described in chapter 4.4 and 4.4.1, is always mandatory or not. Chapter 4.4. states „...depending on the use case - EUDI wallet may authenticate itself"?

“mutual identification and authentication shall be possible both online (over the Internet) and offline” page 17: Please clarify if “offline” means

(a) DUAL offline (i.e. both parties are without internet connection) or

(b) that AT LEAST one party is offline (i.e. at least one party can have an internet connection)?

“Aiming for a common authentication protocol19 between the EUDI Wallet and third parties does not preclude the existence of different underlying solutions to provide, verify and revoke (Q)EAA and PID.” Page 20: How will it be ensured that this works cross-border? Does then each wallet have to support these different solutions?

Please clarify, if the consent procedure, as mentioned in Chapter 4.6.2, may require an additional authentication and if so, for which use cases? What other mechanisms are appropriate to express consent on what LoA?

Could you provide concepts and recommendations for providing accessibility and inclusion for the EUDI wallet?

Furthermore, we would like to point out that **the following topics/functional requirements are missing in the framework**.

Extended Data Subject Profiles

- Multiple Identity Profiles (separate work and personal lives and even pseudonymous) + Possibility for entirely anonymous usage (only for age-verification with revealing ANY personal data) for low-end use cases
- Guardianship and/or Delegation Functionality
- EU Scheme Mgmt. for Credential/Certificate standardization (syntax + semantics)

Open Infrastructure

- ("normal", not only Samsung) Smartphones as QSCDs
- Provide Functionality as SDK, not only as APP
- Mandatory possibility to use more than 1 wallet

Extended Use Cases

- Payment Functionality + Dependency to/Synergies with CBDC Wallets (!)
- Complex transactions via Countersignatures
- FULL (except Revocation) Offline capability via Credential-/Certificate-Chaining (towards root-of-trust) WITHOUT additional mandatory analogue safeguards (presenting physical ID card or similar)
- Clarification that Article 9 of Data Act Proposal does not render eID related use cases void
- Descope archiving and electronic ledger

Security

- Mandatory Relying Party Identification + Registration based on Use-Case restricted Attributes
- Mandatory Backup + Restore Functionality
- Unique Wallet and/or Unique Data Subject ID only for specific (public sector related) use-cases, otherwise allow concepts such as DIDs or similar

Özhan SAGLIK

Hello,

I would like to send my appreciation to the composer of the outline. My PhD is about preserving the trustworthiness of e-signed records. There is a perception that archiving e-signed records can be achieved by preserving the e-signature, and by this way we can maintain the trustworthiness, but it is beyond that.

In the proposal on Article 45g, it is stated that "qualified archiving service may only be provided by a qualified trust service provider". It is correct but missing.

This is one side of archiving qualified e-signed records. Archiving is not a technological issue, it is about humans. We need to establish a culture, procedures and methods for archiving e-signed records. This can be realised by national archives and other archival institutions. These institutions will define the specifications of the e-records, e.g. https://github.com/DILCISBoard/E-ARK-CSIP/blob/master/profile/E-ARK-CSI….

I recommend adding an article like "the archiving structure of the electronic records will be published by the colloquium of the Member States' national archives".

For more collaboration ozhan.saglik@gmail.com

Ronald KREUTZER

As a US-based provider of a digital identity wallet, I appreciate the well thought-out approach to this document. I echo the comments previously stated about the certification of wallet providers: ideally that it is a straightforward, low cost certification process that is done once at the EU level and not at the individual member states.

In addition, I have the following comments:

Section 2, first paragraph: consider replacing "online interactions with "online and offline interactions", to acknowledge that an identity wallet can be used in offline situations. Common offline interactions include the viewing of a document image (insurance card, membership card, etc.) on a phone for lower LOA use cases.

Section 3.11: A Member State issuing a EUDI Wallet is but one use case for how a user obtains a wallet. A more common use case is that a user downloads a wallet app from an app store and uses it for a period of time, then at some point decides to go to a government agency to have some credential verified. Consider revising "issuing a EUDI Wallet" to "issuing a EUDI Wallet, or presenting a verifiable credential to install on the user's wallet".

Section 4.3 contains the statement "authentication of the EUDI Wallet itself towards third parties" and section 5, paragraph 9 contains the statement "shall not enable the relying party to distinguish between two certified EUDI Wallets". While I don't have an issue with either statement, more thought and details need to be provided on how to implement this in a non-complex manner. Ideally, the wallet should not be required to access an outside service in order to provide proof to the relying party that "I am a certified wallet, but I won't tell you which one".

Section 4.4.1: I agree with previous comments that any revocation checks must be done at a credential level and not at the wallet level. Also consider revising ..."solution was installed" to ..."solution was installed or EUDI features enabled" to provide for multi-function identity wallet apps to be used in a limited capacity on devices without adequate security.

Irina MICHALOWITZ (TWILLO)

This comment is submitted on behalf of the company Twilio. Twilio, as both a user of public-sector identification schemes and a provider of authentication tools, takes great interest in the European Digital Identity Architecture and Reference framework and welcomes the invitation to comment.

About Twilio

Twilio is a leading b2b global cloud operator that enables other businesses, governments and nonprofits to embed communications, such as voice, text messaging, email, chat and video, into their existing web and mobile applications to enhance their engagement with their customers and constituents. Organizations have used Twilio to allow their end-users to contact their teacher or students, alert the public about an emergency, video chat with their doctor, speak with their rideshare driver, make a bank transaction, shop online, authenticate an account, and interact with elected officials, among many other activities.

Twilio provides services to more than 250,000 enterprises globally and powers more than 1,8 trillion interactions between them and their customers every year. Twilio's customers range from small and medium-sized enterprises (SMEs) to the world's largest corporations and come from a broad range of industries including financial services, health care, manufacturing, retail, education, and logistics. They include European and international brands, such as ING and Netflix. Twilio's non-profit arm, Twilio.org, supports charitable organizations to deliver their communications needs, such as the Norwegian Refugee Council, a global NGO supporting refugees worldwide. Twilio is also a technology partner and supporter of the United Nation's Vaccine Alliance GAVI. Founded in San Francisco in 2008, Twilio now has 26 offices in 16 countries - 8 of them in Europe - and the infrastructure to support communications worldwide. Trust and privacy have been core principles for Twilio since the company's founding.

Founded in San Francisco in 2008, Twilio now has 26 offices in 16 countries and the infrastructure to support communications worldwide. Trust and privacy have been core principles for Twilio since the company's founding.

Twilio acts as a provider of identification services. The company offers authentication and verification services that complement initial identification. Twilio is not formally recognized as a trust service provider under the eIDAS framework because it does not currently meet any existing eIDAS categories of trust services. However, the European Union Agency for Cybersecurity (ENISA) has listed Twilio in its overview of the technological landscape of eID solutions as part of its report on eIDAS-compliant EID solutions (March 2020).

eIDAS toolbox: clarification requests

Generally, Twilio deems it important for stakeholders to contribute to the technical development of the European Digital Identity Architecture and Reference Framework. As a leading global b2b cloud operator, Twilio has accumulated significant expertise through the offering of two authentication services; 2-factor authentication (Twilio Authy) and 'Auth token' solutions.

As a company with offices in multiple Member States, including Estonia, Germany, Ireland, Sweden and Spain, Twilio is convinced that the toolbox should

- ensure that technological neutrality is observed to clarify that 'strong user authentication' can be offered by solutions other than Biometric;

- clarify that Private Relying Parties can retain the solutions they deem most suited;
- foster the widest possible private sector uptake, explore the possibility that EUDI Wallets can be interoperable with existing, commercially available solutions.

The recommendations of the eIDAS expert group seem sufficiently broad to allow for these requests to be respected. Below, Twilio sets out a few concrete remarks on the toolbox proposals that would help clarify a number of elements:

Objectives of the EUDI Wallet (p. 6):

Twilio would appreciate some clarification around expectations of the use of the EUDI Wallet outside the Euro zone/in member states that do not take part in the Euro zone, and the technical conditions that come with this application.

Roles in the Ecosystem (p. 8):

A vendor, such as Twilio, could possibly fit many of the descriptions in the graph - most probably as a Person identification data provider, or as another type of provider. An example scenario with names of actual entities for a particular country in the EU would help contextualize this immensely.

Also, please clarify the note of a technology vendor (for instance, Twilio is a 'private' participant as opposed to a 'public' body - e.g. a driver license issuing department).

Functional requirements (p. 14 ff):

Some clarification around acceptable file formats (e.g.: upload PDFs, JPGs) or technologies (eg: QR code scans allowed?) from a government perspective would be useful.

Clarification on which of these functionalities 'shall / may' be managed in the specific Member State, Euro Zone or Internationally would be helpful (p. 15).

An example scenario with names of actual entities for a particular country in the EU would help contextualize Figure 3 (p. 22). Also, it would help to have a colour legend describing each group separately.

Non-functional requirements (p. 25):

Twilio is wondering if language capability is considered a part of accessibility, and would constitute a functional or non-functional requirement (if yes, which). Would every EU language need to be supported?

Twilio is looking forward to further engaging with the expert group and with policymakers to explore the details of the technical requirements, and to thereby help implement the framework.

Sebastian ELFORS (IDNOW)

The following questions are posted by IDnow, a German company that provides a platform for identity verification.

We welcome the EUDI Wallet Toolbox expert group's work on the Architecture Reference Framework. It is a well-written and clear document in its current version, and we are looking forward to the updates to the document and the final edition. We have a couple of questions that may be considered for the forthcoming revisions.

Questions regarding the EUDI Wallet reference application

According to the EUDI Wallet tender information day held by the EC on 2022-04-06, the EUDI Wallet reference application will be implemented Q4 2022 - Q1 2023 based on the final Architecture Reference Framework (ARF). We would like to ask the following about the use of the EUDI Wallet reference application:

Will the single EUDI Wallet reference application be mandatory for interoperability testing the different pilot solutions?

Will it be possible for each consortium to implement their own EUDI Wallet reference application based on the ARF interfaces and protocols?

Will the EUDI Wallet reference application be used also for the production phase, or is it only intended for the pilot phase?

We would also like to get an update on what date the public tender for the EUDI Wallet reference application will be published.

Questions about selective disclosure

Then we have a question about selective disclosure. If the ARF will specify any Zero Knowledge Proofs (ZKPs) such as Camenisch-Lysyanskaya signature scheme (Hyperledger Indy AnonCreds), BBS+ JSON-LD signatures (WACI-DIDcomm) or zk-SNARK, will there also be guidance on how to achieve eIDAS eID scheme LoA High if such a ZKP scheme is used? And if so, are there any plans to specify certification schemes for ZKP algorithms to be officially approved and hardware protection of ZKP keys?

Questions about the potential use of the ISO 18013-5 mobile driver's license

Finally, if the ISO 18013-5 mobile driver's license will be part of the EUDI Wallet, will it be used only for the mobile driver's license use case, or will it be used for (all) other use cases too? And will there also be guidance on how to achieve eIDAS eID scheme LoA High if the ISO mobile driver's license may be used for authentication purposes?

Giovanni BARTOLOMEO

The document is a major step forward towards the common understanding of the Wallet and its implementation. However, we believe that there are still some confusing requirements yet to be refined.

1. On the relationship between the user, her credentials and her Wallet.

Our main comment is that the document does not provide a clear understanding of the relationship between the user, her credentials (attributes) and her Wallet. In particular, it looks like there is a confusion between the user's credentials (i.e., (Q)EAA, PID) and the Wallet itself.

The sentence “the legislative proposal states that the EUDI Wallet is an electronic identification means” is a bit misleading: the Wallet should not be an electronic identification means rather it is what is contained inside a Wallet that may be an identification means. In physical life, when a wallet is found on the way by a passenger, it is not saying nothing about the user, except if the passenger opens the wallet and looks inside it.

Unfortunately, in the ARF document the widely used term Wallet “issuer” seems to foster this confusion, being perhaps more appropriate the term “provider” (sometimes used in the document too) or also the term “supplier”.

The underlying problem is not merely a terminology issue, rather we fear it may badly influence the definition of the whole EUDI Wallet ecosystem architecture.

For example, the ARF document states that the Wallet shall implement mutual authentication toward a third party: we believe that this requirement is not strictly necessary and may even represent a threat to user's privacy, especially if only one Wallet per citizen is assumed.

Wallet identification, which is needed if mutual authentication with (Q)TSP and relying parties is assumed, may allow a relying party to implement profile linkability even in transactions where users do not need or want their profiles to be linked. It may eventually lead to user re-identification.

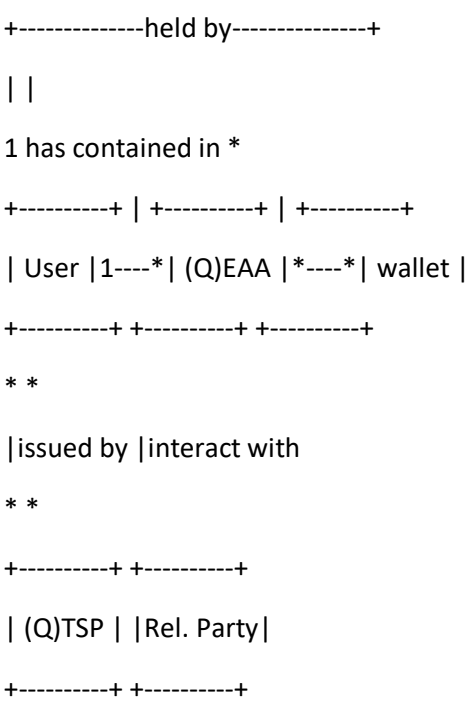
We believe that the correct requirement is to implement a mutual “authentication” between the user and the (Q)TSP and between a relying party and the (Q)EAA provided by a Wallet, rather than the Wallet itself!

Better, the essential requirement is that the Wallet proves the legitimate possession of the credentials it stores, not that it is authenticated. This problem is known in the OAuth2 community as “proof of possession” (see for example “IETF RFC 7800:Proof-of-Possession Key Semantics for JSON Web Tokens” and many other IETF drafts proposing methods to implement proof-of-possession).

We believe this design requirement may better fit the strong privacy preserving capability foreseen when a Wallet interacts with a relying party: the Wallet should not reveal anything about the user, except needed information to use the service the party provides (a concept known in crypto as “zero knowledge proof”).

For the same reason, we believe that one citizen should be able to obtain, manage and dismiss several Wallets at the same time, with different sets of (Q)EAA stored in each of them. In other words, two wallets should be able to store different sets of the same user’s credentials and the user should be able to decide which credentials have to be stored in each of her wallets and choose which wallet to use in interacting with the different relying parties.

This relationship depicted in ASCII art:



2. On derivation of user attributes

The sentence “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” is dangerous as it seems to suggest the user shall ask (Q)TSP specific attributes each time they are needed. This may lead to immediate user profiling by the (Q)TSP! We believe instead that the second suggested solution “The EUDI Wallet may have the intrinsic capability, based on the obtained PID and (Q)EAA, to selectively disclose, derivate a specific attribute and aggregate several single attributes, without the need for new PID, (Q)EAA or interactions with the PID and (Q)EAA providers'' is the very capability the Wallet should have. We highlight that such a capability is present in modern crypto schemas, such as attribute-based encryption and functional encryption.

3. On the form factors

Finally, we suggest not defining one specific form factor. We suggest defining the Wallet generically as “an electronic application running on a device with crypto capabilities” and not limiting it to one of the three forms suggested in the document.

Thanks.

Tobias JOHNSSON (FIDESMO)

Fidesmo, a European based security company, are delighted to see the focus on creating secure ID frameworks for Europeans, with the geopolitical goal of making EU countries less vulnerable to the internet and mobile OEM giants.

We would like to make a general comment on security implementation since it is regularly brought up. There is a tendency to look at what's easily available, rather than adapt the use case to the right security level. Should security be HW and/or SW based, should the wallet be available off-line and/or on-line? Well, let's first describe the use case.

Highest level of security is today based on secure elements (SE). SE:s are today in use for cards, wearables and mobile phones. They are available, and should be used when the use case so desires.

What's important for the EUDI wallet is where the root of trust resides - i.e. where the foundational secrets are. A true hardware root of trust which is certified gives assurance that the secrets cannot be simply extracted and that even nation states typically would need to do it device by device, with an expectation that extraction would likely require destruction of the hardware in the process.

A software root of trust is very vulnerable because it depends on the broader integrity of the carrier device's hardware (a general-purpose computing platform rather than something designed to secure secrets), operating system and software as well as end-user choices such as backups of the software-defined root of trust.

A software-defined root of trust requires "continued" good will of the carrier device's manufacturer to continue to secure its hardware and software, and in principle of *all* application providers with software on that device. There are scenarios in which the interest of the manufacturer or software providers are not aligned with legal principles that apply in Europe, either because they are infiltrated by criminals or because they are acting on behalf of foreign governments.

The "secrets" prove identity and that this identity was authorized. If the secret can be copied, this identity and the authority can also be copied.

Creating a trust layer based on HW root of trust is doable, by that we would be less vulnerable to the internet and mobile OEM giants.

Kind Regards

tobias.johnsson@fidesmo.com

Nick MOTHERSHAW (OPEN IDENTITY EXCHANGE)

Open Identity Exchange - Observations and Feedback

The Open Identity Exchange is a not-for-profit members organisation whose vision is a world where we can all prove our identity and eligibility anywhere, using a simple universally trusted ID. We create a community for all those involved in the ID sector to connect and collaborate. Together we create the rules, tools and confidence to support the acceptance of universally trusted IDs and eligibility information.

We bring together buyers of ID Services (Relying Parties) with ID Service organizations such as tech vendors, consultancies, along with regulators and market influencers to work together to drive adoption of ID Trust.

Our guides and papers form the bedrock of global Trust Frameworks to support the creation and use of inter-operable, universally trusted identities.

Summary

eIDAS 2.0 is certainly progressing at a pace to be applauded.

At OIX, our diverse global members have collectively reviewed the ARF in detail and provide this constructive feedback to the eIDAS Expert Group.

Our main feedback is that ARF is well thought through and aligns almost perfectly with OIX's new Trust Framework for Smart Digital ID.

Some of the terminology in the ARF is different to the terms OIX has been using, but on the roles side for instance there is almost complete alignment with OIX's view on global trust framework roles. The terms used in the ARF, such as Electronic Attribute Attestation (EAA) are clear and descriptive, and perhaps give the whole ID industry chance to move on from some semantically overloaded terms that currently cause much confusion (e.g., credential).

The ARF cements the distributed philosophy of the EU Digital Identity (EUDI) Wallet, whilst sensibly recognising that there are device-based and could-based options to achieve this.

The principle that issuers cannot see and track where the user shares their data is well enshrined. As is the fact that issuers, and then users, can restrict who can see and use data.

A Trust Registry is central to the framework, so all parties' roles can be verified. OIX, as part of its contribution to the GAIN initiative, is working on global role definitions and role permissions as part of its Global Interoperability working group. Alignment with this emerging OIX global definition would make EU-to-third-country transactions more easily verifiable in due course.

A key functionality option statement in the ARF really leapt out at us here at OIX:

Selective disclosure and combination of attestations can be handled in two different ways:

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.

the EUDI Wallet may have the intrinsic capability, based on the obtained PID and (Q)EAA, to selectively disclose, derivate a specific attribute and aggregate several single attributes, without the

need for new PID, (Q)EAA or interactions with the PID and (Q)EAA providers. For instance, specific fit for purpose signature schemes in PID and (Q)EAA could enable such capabilities.

In OIX's view the first option is "clunky" for the user and puts an undue burden on EAA providers. OIX does not recommend this option.

The second option is more appropriate for a modern Digital ID. This is a Smart Digital ID per OIX's new trust framework. The Digital ID – the EUDI Wallet – is trusted and has the capability to aggregate EEAs to derive new composite attributes to meet the needs of relying parties. It must do this in a way that allows the relying party to specify the rules, but that protects the user from needing to understand the detail of the rules. The user needs to be part of the process, and consent to any aggregations and derivations, but a Smart EUDI Wallet must help and guide them through this process.

The ARF does not cover data standards. Common data standards for each of the attributes that will be in the scope of the EUDI Wallet are required to enable interoperability across member states and with other trust frameworks around the world. OIX is currently working on a global assessment of Data Standards for Digital ID, which EU representatives would be welcome to join.

OIX would be delighted to work more closely with the eIDAS expert group to help evolve the ARF. OIX would equally encourage EU representatives to get involved in some of our current global working groups; in particular, those looking at cross-trust framework global interoperability (as part of GAIN) and global data standards in the digital ID space.

Observations and Feedback

3.0 ROLES IN THE ECOSYSTEM

- Would it help clarity to have a separate role for Authentic Sources (e.g. Bank) and having an arrow going to each of the QEAA and EAA box?
- When is a Qualified EAA required Vs a Non-qualified EAA? We assume this is use case specific. A note on when each type might be used would provide clarity.

3.3 PROVIDERS OF PERSON IDENTIFICATION DATA (PID)

- The PID is intimately tied to the requirement for 'High' LoA, and forms the trust anchor for the ID. This is good. OIX would regard the PID as another EEA, just a special one that must be present in the wallet as a pre-requisite to allow the rest of the processes. Perhaps the EU within the ARF could take a similar position?
- Is a PID mandatory? Can the EUDI Wallet function without this? If it is mandatory as the "trust anchor" for the wallet, this should be made clear in the ARF.
- Must the PID issued by a government agency, or can it be issued a third-party agent on their behalf to the stated standard?
- What is the MINIMUM and MAXIMUM data is in the scope of the PID. Is the MINIMUM core personal data: ID #, name, DoB and Address? Is the MAXIMUM everything in Regulation of the European Parliament and of the Council
- amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity Annex VI, listed as the minimum for the EUDI wallet as a whole?
- Is the PID an output of a QEAA? Must it be qualified? Or is it the trust-anchor on which qualification can be based? In which case the PID in itself is not qualified, but is highly trusted.

3.4 PROVIDERS OF REGISTRIES OF TRUSTED SOURCES

- How many Trusted Registries are envisaged? One per EUDI Wallet, one per member state or ecosystem wide. Also, to OIX DIGIF roles?
- As part of its Global Interoperability Working Group, aligned to the GAIN initiative, OIX is exploring the GLOBAL definition of ID Ecosystem Roles and their certifications (e.g. ID Providers are certified to issue a particular Level of Assurance, Proofing Providers are certified to issue Digital ID documents to a recognised (ISO) standard (such as mDL), Relying Parties are certified to manage data passed to them to a defined regulatory standard (e.g. GDPR). Representatives of the EU would be welcome to join this working group to influence this work.

3.5 QUALIFIED ELECTRONIC ATTESTATION OF ATTRIBUTES PROVIDERS

- Why are only QEAA providers are referenced as accessing Authentic Sources? Is the implication that EEA that are verified against Authentic Sources must be QEAA? This is inconsistent with the notes in the ARF role diagram.

3.6 NON-QUALIFIED ELECTRONIC ATTESTATION OF ATTRIBUTES PROVIDERS

- Once I have the PID in the EUDI Wallet, the user is trusted. There is then a difference then between whether an issuer of a EAA verifies who the user is themselves before issuing the EAA (OIX “Direct Issuer” section 10.2) or trusts the Digital ID has verified the user – which it has – has issues its EEA on that basis (OIX “Indirect Issuer” section 10.2). Does this distinction need to be recognised in the ARF?
- Must an EAA always be validated / verified by an Authentic Source? The trust value of an EAA is inherently higher when it is verified by an Authentic Source. Does this need to be clearer?

3.13 DEVICE MANUFACTURERS AND RELATED ENTITIES

- The term manufacturers implies physical / substantial devices. Should this be a) be optional? Not all EUDI wallets implementations should have to leverage device manufacturers. b) Be a more generic term to include all those who will provide technical services / tools to enable EUDI wallets. We might suggest “Tool Providers”

3.11 CONFORMITY ASSESSMENT BODIES (CAB}

- At the moment only one entity is providing conformity assessment for current iteration of EIDAS to become QTSPs. Will this stay the same? Will this same body also undertake conformity assessment for wallets?

4 FUNCTIONAL REQUIREMENTS

- Should the EUDI Wallet be shown to have a Rules Engine that determines how the attribute requests from RPs are fulfilled? See the OIX Trust Framework Digital ID model, which places a rules engine as the heart of a “SMART Digital ID.
- How does the EUDI Wallet know it’s dealing with one person ONLY? Users share their credentials. They also need to give delegated authority to act on their behalf in some circumstances.
- Must the EUDI Wallet use biometric authenticators?
- Must any biometric authenticators used be “off device” i.e. captive operating system device biometrics such as Apples Face ID are not allowed.

- The Key to the diagram should be labelled as “Key:”. Colours in the key are not aligned with the diagram.

4.1 STORE PERSON IDENTIFICATION DATA, QUALIFIED ELECTRONIC ATTESTATION OF ATTRIBUTES AND ELECTRONIC ATTESTATION OF ATTRIBUTES

- Should EUDI wallets support Self-Attested Credentials. If the user of a EUDI Wallet is always trust (level high) then their self-attested credentials are of value as they have implied trust
- Will the EUDI Wallet carrying credentials (EAAs) assured by other frameworks (e.g., third countries, health…). If so, it would be good to reference this as it will show the global interoperability intent from the EU.
- Should key EAA meta data be defined as part of the requirements: Who can use the EAA? Bound Authenticators?
- Are data standards required to enable interoperability across member states and with other trust frameworks around the world? OIX is currently working on a global assessment of Data Standards for Digital ID, which the EU would be welcome to join.

4.5 SELECTION, COMBINATION AND SHARING OF PERSON IDENTIFICATION DATA, QUALIFIED ELECTRONIC ATTESTATION OF ATTRIBUTES AND ELECTRONIC ATTESTATION OF ATTRIBUTES

“The Wallet shall leverage on a common protocol for identification and attribute sharing including verification of the integrity and authenticity of the information, irrespective of the set of attributes shared, in order to reduce the technical complexity of the solution and facilitate its deployment. This functionality will rely on QEAA and EAA, the data structures of those attestations and their sharing protocol reused for PID.”

- Does this imply a common protocol for all wallets will be defined to allow for interoperability? Will a single common protocol be defined or adopted as part of eIDAS2? Or will a variety of protocols be supported

“The EUDI Wallet shall make it impossible to collect information about the use of the wallet which are not necessary for the provision of the wallet services, nor shall it combine person identification data and any other personal data stored or relating to the use of the European Digital Identity Wallet with personal data from any other services offered by this issuer or from third-party services which are not necessary for the provision of the wallet services, unless the user has expressly requested it.”

- Would this sentence in be improved by also referencing “or necessary to meet other legal requirements”.

“The EUDI Wallet may have the intrinsic capability, based on the obtained PID and (Q)EAA, to selectively disclose, derivate a specific attribute and aggregate several single attributes, without the need for new PID, (Q)EAA or interactions with the PID and (Q)EAA providers”.

- Derived presentations of PID, QEAA, EAA result in another type of EAA. OIX calls this as Derived Credential (section 10.4), which is kept in the user’s wallet as a record of the transaction and may be re-usable (such as an over 18 Status). A Derived EAA. Should the EUDI wallet adopt the same concept?
- OIX Is pleased to see in the title of this section the term “combination”. A Smart Digital ID, by OIX’s definition, allows the combination of several credentials to create, or derive, a new derived credential that is data minimised but highly trusted. Examples of this might be: a) Deriving a Covid Safe status from a combination of Covid Vaccinations and recent Covid Tests, b) Deriving an AML KYC Assured status from evidence of ID, ID activity, risk assessment

and address proofing. This ability to derive data-minimised trust from multiple EAAs will be a key success factor for the EUDI Wallet. This ability should be made clearer in the requirements.

4.8 INTERFACES WITH EXTERNAL ENTITIES

- The key to the diagram needs to be clearer and seems incomplete. Which red line is the wallet perimeter? – the red box is used twice. Brokers, Proxies, eIDAS Nodes – should these be in the overall roles diagram and definitions in Section 3? Catalogue of attributes and EAA Schemes. Should this be on this diagram? It's used by the Relying Party for discovery.

Sara FACCHINETTI (DIZMEID)

DizmeID Foundation - legal and technical working groups (led by InfoCert): EUDI ARF outline feedbacks

The ARF outline represents an **important achievement** for providing a common and clear overview on the European Digital Identity framework described in the eIDAS revision. More specific technical guidelines are foreseen to be added in the revision expected by October 2022. These technical details will provide a common track on which to implement solutions.

The DizmeID foundation working groups have analysed in detail the ARF outline and would like to provide their comments to support a more focused technical guidelines preparation. The comments arise from the experience carried out during the last four years spent in the preparation and implementation of an ecosystem based on self-sovereign identity and eIDAS regulation.

Our feedbacks are organised with some overall recommendations to highlight key points and some comments per sections of the ARF outline.

Overall recommendations:

The governance framework shall offer standardised, high value, high integrity services between **public administrations** and **private sectors**.

Interoperability at **worldwide level** shall be preserved through the usage of standardised and global technology. The European digital identity wallet shall be able to interact with ecosystems around the world while respecting the legislative and regulatory EU needs. This can be achieved if the ecosystem is built on **open standards-based protocols** to foster a dynamic and competitive solutions market environment. The EUDI shall not be locked into specific technological layers or suppliers.

EUDI wallet shall be **easy to use** and allow for **rapid authentication** and **access control** (passwordless approach). In case of identity credentials lost (e.g. personal device) it shall be possible to securely and easily re-validate the digital identity with ecosystem services.

EU citizens shall be asked to provide the **minimum data set** of their personal information required to complete the transaction. In addition, where possible and appropriate, anonymous transactions should be enabled (e.g. eVoting).

EU citizens' confidence in the protection, disclosure and use of their personal information and identity data shall be ensured through trusted, secure and privacy-enhanced services.

Specific comments/questions on ARF sections:

<u>Section 2 objectives of the EUDI Wallet:</u>

- Overall the wallet represents the instrument provided to EU citizens to control and share, in a trusted way, their identity information. Preliminary use cases have been identified even though it is not possible to cover all potential use cases.
- Concerning the “Secure and trusted identification to access online services” use case it is very important not to limit the usage to public services but exploit it to the **private sector services** in order to leverage the digital identity impact (e.g. let’s consider how many times a citizen is required to provide some personal information to access private services).

Section 3 roles of the actors of the ecosystem:

- Overall the concepts are aligned to the Self Sovereign Identity domain. This is strongly supported and appreciated demonstrating an optimal approach. However the nomenclature is sometimes confusing. An alignment with existing **SSI nomenclature** is proposed to promote standardisation. Main roles are: Issuers (+ Trusted Issuers), Verifiers, Holders.
- It is important to clearly define **who will make use of citizens' data and how**, vetting mechanisms to "verify the verifiers" guaranteeing the identity of relying parties shall be implemented (e.g. QWAC, PSD2 process).
- Fig. 1 mentions "Device manufacturers". This part shall be better explained and further considered.
- 3.1 End users of EUDI wallets: the concept of delegation/power of attorney is missing (e.g. for minors, old people, etc.). In the Italian experience, for example, it's fundamental to set a delegation/power of attorney mechanism in order to ensure the widest dissemination of the use of online identification tools also to people affected by the digital divide. In addition the IoT concept in this paragraph is missing.
- 3.2 EUDI wallet issuers: the term "issuer" is confusing with the role of credentials issuers, it is suggested to use the term "**wallet providers**". It is of high importance to **enable private entities to provide EUDI wallet** implementations to boost the adoption and the business competition. For a legal person it's necessary to rule the change of the legal representative and the consequent access to the EUDI Wallet. A mechanism to recover the cryptographic material might be a choice (e.g. with custodian QTSP) in case the user loses the keyphrase to allow him to recover his data. In addition the EUDI Wallet Issuers shall publish the interfaces for exchanging data.
- 3.3 Providers of Person Identification data (PID): the term "**trusted issuers**" is suggested instead of "providers of PID".
- 3.4 Providers of registries of trusted sources: this role shall be better clarified and the technological choices of trusted registries shall be aligned with existing standards but not limited to proprietary solutions.
- 3.5 Qualified electronic attestation of attributes providers: the term "**trusted issuers**" is suggested. From the wallet the citizens shall be able to select the chosen QTSP for the digital certificate, this is to promote a competition policy,
- 3.6 Non-qualified electronic attestation of attributes providers: the term "**issuers**" is suggested. EEAs are highly important to exploit the EUDI potential and to maximise impact that shall not be limited only to qualified attributes. Non-qualified attributes registered on the wallet provide a huge quantity of usage scenarios. This is a key aspect for adoption. QTSP shall play a role as proxy issuer: to onboard and certify an external data provider (vetting process) enabling it to be an issuer.
- 3.8 Providers of other trust services: this paragraph is generic and more details shall be provided.
- 3.10 Relying parties: the term "**verifiers**" is suggested. It's not clear the scope of the needed information to the Member State of the established relying party, that could affect the business use of EUDI Wallet.
- 3.14 Catalogue of attributes and schemes for the attestations of attributes providers: this shall be **publicly available**. Credentials schema with the list of attributes shall be published on a ledger or a public shared repository or other technologies (not to store private information but only credential schemas). **EAAs shall not need any approval** from central

authority otherwise this will significantly limit the usage and exploitation in the private sector.

Section 4 Functional requirements:

- 4.1 Store PID, QEAAs, EAAs: **custodial** wallet versus **non-custodial** wallet is a critical point to be analysed. The citizen shall be able to choose the best solution (e.g. I keep my wallet keys and I'm conscious that I can lose it versus a trust service provider is in charge of keeping my wallet keys and can recover it for me in case of need). The solution must comply with GDPR regulation using PET (Privacy Enhanced Technology) like pseudonymization and advanced cryptographic techniques.
- 4.4 Mutual authentication: it is of utmost importance that all actors (issuers,/trusted issuers, verifiers, holders) are securely and uniquely identified to build a trusted environment. **Wallet to wallet** transaction shall be considered too (e.g. a citizen that shares information with another citizen).
- 4.5 Selection, combination and sharing of PID, QEAAs and EAAs: concepts of **selective disclosure, zero knowledge proof, AnonCreds** are key for the adoption and compliance with existing regulations, and permit the proposal to be consistent with the proposal of the Council.
- 4.6.1. User awareness component: depending on the specific application context the user will be informed of the existing rights (e.g. PSD2).
- 4.8 Interfaces with external entities: level of assurance high represents a huge constraint for the usability and the adoption in certain use cases, the **level of assurance substantial** shall be acceptable in specific contexts which do not require the high reliability (see comments on #3.6).

Section 5 Non-functional requirements:

- **Revocation** concept is fundamental and shall be fully ensured. The credential revocation is not required to be notified on the citizen wallet. This shall be available to verifiers when they require a proof of identity/information to the citizen.
- **Privacy by design** and privacy by default shall be granted under art. 25 of the GDPR. As a general statement, GDPR compliance shall be made explicit: in fact, the Regulation is recalled only in paragraph 4.6.1. in a too general statement.

Section 6 Potential building blocks of the EUDI wallet:

Our understanding is that the building blocks will be detailed during the ARF revision foreseen by October 2022 and this paragraph provides only an indicative list.

Janine BARTEN (EUROPEAN CREDIT SECTOR ASSSOCIATIONS - ECSAs)

ECSAs position on the European Digital Identity Architecture and Reference Framework

1. General Remarks

2. Suggestions

3. Detailed comments

This position was submitted on behalf of the European Credit Sector Associations (European Banking Federation, European Association of Co-operative Banks, and European Savings and Retail Banking Group). We remain at your disposal should you have any questions; please do not hesitate to reach out to janine.barten@wsbi-esbg.org).

1. General Remarks

The European Credit Sector Associations (ECSAs) welcome the Commission's efforts to strengthen the EU legislative framework on digital identity. The Commission proposal aims to provide an ecosystem of credentials leveraging a new wallet architecture of several ID solutions. The wallet architecture with its underlying principles can further increase innovation within the financial industry, primarily benefitting all European businesses and citizens.

The European Digital Identity Architecture and Reference Framework (ARF) provides more detailed information about how the EU Digital Identity Wallet (EUDIW) would be set up and it also describes the high-level specification for the ecosystem supporting the EUDIW.

Although we acknowledge that this is still a first version of the document, we highlight that there are certain areas that require careful consideration from the Common Toolbox experts.

For the EUDIW to be successful, it would be key to establish a common technical architecture enabling the private sector to integrate any wallet that can be developed within this regulatory framework without additional technical effort, regardless of where they are issued.

The ECSAs hence recommend the DIW is only accepted on a basis of a self-commitment by the financial sector for authentication purposes and particularly for payments.

In any case, the proposed integration between digital identity and payment systems cannot be separated from a rigorous analysis of the impact on risks, on the attribution of operational responsibilities and on security profiles, especially when EUDIW is used in combination with means of payment.

The assignment of roles within the new digital identity system, including the one of the wallet issuer, should be carried out according to objective criteria and with the aim of encouraging the creation of a competitive market for services relating to digital identity for the benefit of the European citizens and businesses.

If the Toolbox fails to deliver a common standard that guarantees that all national solutions are fully interoperable, the potential fragmentation in the DIW architecture could lead to increased operational costs (e.g., in case of incoherent national solutions), inefficiency (e.g., national rules to be respected), investments needed from the private sectors (e.g., European players will have to adapt to all the 27 national solutions), and poor User Experience (e.g., European citizen, Issuer, Relying Parties will have to face 27 different liability regimes).

This is especially relevant since the private sector (and banks in particular) will be mandated to accept the European Digital Identity Wallet.

In our understanding, the outcome should be a common, openly available standard that enables the development of multiple, interoperable e-ID solutions on all levels of assurance and which incentivises private sector schemes to participate. The standard should be applied by both public institutions and private companies.

There is a strong need to establish also clear rules on how to handle liability for the new wallet (e.g., procedures to allow banks and then customers to be reimbursed in case of wallet identity theft caused by phishing customer data) and a shared EU certification procedure. For all the e-ID activities, and especially when payments are involved, European dispute resolution mechanisms for the DIW need to be part of the ARF.

The ARF addresses to a certain extent the responsibility for the wallet issuer, but this should be completed with the overall responsibility framework for all the players involved in the architecture, together with a standardized procedure allowing citizens, businesses and all parties involved to activate a procedure for contestation in case of fraud or other operative issues.

Moreover, it would also be beneficial if a technical architecture would support remuneration/cost distribution model. Another attribute which could act as a possible business enabler and hence might benefit from defined technical architecture would be something similar to digital rights management, effectively enabling content owners limit usability (both time, count and application based) of the digital artefact.

The ARF also introduces the "Terms and Conditions" (T&C) for most of the players involved in the value chain which will be useful in addressing some contractual aspects.

The T&C and contestation rules should be standardized at EU level in order to:

- allow a homogeneous customer experience for citizen and RPs;
- help achieving interoperability between the 27 Member State solutions;
- minimize the compliance (setup and running) costs for all the public authorities and businesses involved in the EUDIW at European level; and
- prevent arbitrage at national level (e.g., in the certification procedure).

Maintaining the T&C and the aforementioned contestation rules as a responsibility of Member States would raise the risk of having 27 non-interoperable and non-uniform wallet solutions.

2. Suggestions

The ECSAs recommend that the Toolbox provides at least the following:

- "Deep harmonisation rules" at EU level for standards (including semantic and data syntax), liability rules and certification procedures.
- Example architectures and associated privacy and security guarantees that need to be in place, i.e., architectural difference between local, single remote wallet, diversified remote wallet and the influence on privacy, security and usability.
- A European Governance Body:
    - ensuring regulatory harmonisation and avoiding fragmentation. For example, the various national certifications related to the eIDAS levels of assurance do not necessarily allow electronic identification scheme to be fully automated. This situation leads to disparities in the context of remote customer onboarding (for

instance, whereas AML national rules mentioning the eIDAS framework refer to different level of assurance);
    - creating an EU-wide contractual framework among the involved actors (Wallet Issuer, Attribute provider, Relying Party Acquirer, Relying Party, Citizen/Customer);
    - collaborating with Member States; and
    - allowing the EUDIW to evolve daily.

In this sense, this EUDIW Governance Body at least should:

- detail the interoperability standards and certification procedures that should be enforced by Member States in setting up the EUDIW solutions;
- ensure clear and transparent rules for functional standards and business rules to be used by Member States, promote the safety and efficiency of the EUDIW, and support the objectives of relevant stakeholders at EU level;
- contribute to the development of a sound risk management framework for comprehensively managing legal, financial, operational, and other risks to be adopted by Member States;
- suggest to Member States all necessary and appropriate measures to mitigate the risks and maintain confidence in the EUDIW usage; and
- provide sufficient information to Member States to enable service providers, technical service providers and end users to reach an accurate understanding of the risks, fees and other material costs they would incur by participating in/making use of the EUDIW.

In terms of Governance, a business sustainability analysis should be conducted by Member States for national use, and by the Toolbox for the EU level, to ensure that all involved private parties would be able to cover their costs related to the service when used by natural persons and to study the viability of business models that could fit into the prospective ecosystem proposed by the Commission.

We suggest that the first elements of the aforementioned EU Governance Body will be discussed in the Common Toolbox.

In the European market today, there already are examples of governance models that are able to express at European level standards and functional service details, which could be taken in consideration for setting up a **European Identity Council** to support and follow the development of the EUDIW.

Where the Wallet Issuer is a private issuer (notified by the MS), additional safeguards should be put in place to make sure this solution is trusted by third parties.

We suggest also covering the following areas:

1. Extended Data Subject Profiles

- Multiple Identity Profiles (separate work and personal lives and even pseudonymous) + Possibility for entirely anonymous usage (e.g., only for age-verification without revealing any other personal data) for low-end use cases.
- Guardianship and/or Delegation Functionality.

2. Open Infrastructure

- Solutions should be accessible from all smartphone devices (regardless of the brand), for example for the solution of the QES: smartphone as Qualified Signature Creation Devices

(QSCDs) on high end devices, or alternatively as initiation device for remote qualified signature creation.
- Provide functionality as Software Development Toolkit (SDK) (to be integrated in existing APPs), not only as a standalone APP.
- Mandatory possibility to use more than one wallet for citizen and business.

3. Security

- Mandatory Relying Party Identification + Registration based on Use-Case restricted Attributes.
- Mandatory Backup + Restore Functionality.
- Unique Wallet and/or Unique Data Subject ID only for specific (public sector related) use-cases, otherwise allow decentralised concepts.

Our assumption is that this outline document represents only a high-level description of the architecture building blocks of the EUDIW solution.

We urge the Commission to publish details about the identified solutions in order to allow the ECSAs to produce detailed comments.

We remain ready and willing to support the Common Toolbox in designing the principles with our expertise in the European market, especially taking into account interoperability, security and neutrality. The ECSAs are already conducting an internal study on how a successful design and implementation of the EUDIW could be achieved.

3. Detailed comments

- Page 6, “Digital finance”

It is necessary that the requirements of PSD2/RTS are fulfilled for "payment authentication", i.e., in particular "binding to transaction/payment data".

To ensure positive user experience, the wallet could not only be provided via a separate App, but also be based on an SDK, which can be embedded in Banking Apps for seamless customer experience and should enable private partners (e.g., banks) to become EUDI Wallet providers.

The ECSAs’ position on the payment inclusion in the EUDIW is already public on the “Have Your Say” document and also addressed in their proposed amendments to the text of the Proposal.

- Page 8, section “Roles in the Ecosystem”

The document appears to focus on attributes, whereas in reality the wallet is likely to need to store collections of authenticated attributes together in a form usually called “credentials”. A Driving licence is not just a list of attributes, it is a combined document. A passport is similar. There are two mentions of the concept of credentials in the document but most of the focus is about how to handle attributes, not credentials.

We are also missing mechanisms on the issuing of additional attributes from private sector issuers. There should be encouragement for other parties to be able to issue credentials to the Wallet, e.g., a library card, a gym membership, a credit card. There needs to be provisions for other bodies to become issuers and to establish trust levels for these issuers that must not be abused but may not need to be as strong as for Member-State-level issuing authorities.

- Page 9, paragraph “EUDI Wallet Issuers”

There is a description about the responsibility of the wallet issuer, but it is not sufficiently clear what are their liabilities and who sets the rule for them, including on arbitration if necessary (EU or Member States).

We suggest entrusting the European Identity Council described above with such a role.

- Page 10, paragraph ‘’Providers of person identification data (PID)”

It is not clear what the pivotal data common to all existing solutions will be.

- Page 10, paragraph “Providers of registries of trusted sources”

Although a certification process to ensure trust among the participants is needed, unnecessary bureaucracy should be avoided. In fact, if permissions for all the listed roles are required, we will face the risk that the ‘network effect’ will not be achieved due to the multitude of procedures in order to create a presence in the network. For this reason, an “acquirer” for RPs could be envisaged.

- Page 11, paragraph “Non-qualified electronic attestation of attributes providers”

Analysing customer data is necessary to protect customers in the context of fraud prevention activities and other risk mitigation measures.

In this sense the provision “without having an ability to receive any information about the use of the EAA” for payment activated via the EUDIW will lower the safety of the customer and the overall payment safety.

It seems that **qualified and non-qualified electronic attestation of attributes providers will coexist** in the wallet at the same time. This is very relevant because, unlike the current eIDAS Regulation, it makes the wallet more useful for non-government use cases. This will significantly increase the adoption and use and give the new wallet a good opportunity of succeeding.

Nevertheless, we have some concerns regarding this issue: Non-qualified EAA can be provided by any trust service providers. While they would be supervised under eIDAS, it could be assumed that other legal or contractual frameworks than eIDAS would mostly govern the rules for provision, use and recognition of EAA; clarity of what “supervised under eIDAS” means and by whom is needed; and in terms of client perception, what are the differences between the two types of providers? Would the user be aware of such differences?

- Page 11, paragraph “Qualified and non-qualified certificates for electronic signature/seal providers”

It should also be clarified that the certificates used would not necessarily be eIDAS qualified.

- Page 12, paragraph “Relying Parties”

It should be ensured here that the Relying Party is always identified in the Mutual Authentication, even if other service providers are interposed. For the identification of the Relying Party, it should be clarified how the identity has to be specified. The user of the EUDIW should be able to "understand" and recognise the identity of the Relying Party.

It is advisable that the EUDI wallet can also be accessed from an app of the relying party using App2App communication.

If an aggregator role is included in the Proposal, this would require detailing the privacy rules to be applied on behalf of the relying party.

The ARF should also clarify how Relying Parties are responsible for carrying out the procedure for authenticating the attestations they receive from the EUDIW.

- Page 12, paragraph “Relying Parties”

In relation to the provision that says that “to rely on the EUDI Wallet, relying parties would need to inform the Member State where they are established and their intention for doing so”, we consider this might place a block on private sector usage as it is unclear why relying parties would need to “inform” a Member State and it could introduce potential barriers to an open and unrestricted use of a citizen’s own data. These restrictions are not in place for physical credentials and there is no reason to establish them for the digital ones.

- Page 12, paragraph “Conformity Assessment Bodies (CAB)”

CABs should respect guidelines and standards set at EU level in order to prevent fragmentation. CABs cannot be based on the Member States rules only.

We suggest entrusting the European Identity Council described above with such a role.

Page 12, paragraph “Device Manufacturers and Related Entities”

The EUDIW should be used independently from the smartphone providers. If devices are restricted too much, there is a risk that solutions cannot be used by many customers.

It is for the EU to determine the criteria to certify a device/app as a QSCD.

It will be necessary to specify the security implemented to guarantee the confidentiality of the local storage (prevent the fraudulent copying of the attributes) and the associated responsibility.

- Page 14, section “Functional requirements”

In the description under functional requirements, some aspects are missing from our point of view, which need to be considered. These include the following:

- **Revocation of attributes**: There is reference to revocation checks (under Section 4.4.1 and section 5) but has yet no details on how revocation would work.
- **Expiry for attributes:** There is no discussion of how expiry dates for attributes or credentials will be handled.
- **Recovery**: There is a need to handle situations where a device is lost, broken, stolen, or where a password is compromised or forgotten.
- **Life events & updates**: There is no discussion of how to handle updates to data, e.g., from major life events such as marriage, or other change of name or attributes.
- **Multiple users or use on behalf of another**: There is no discussion of whether one EUDI Wallet can hold multiple identities (e.g.; the Wallet bearer’s children), whether it can handle situations where one party has power of attorney over another, or how any other user such as guardian or executor of a will, or other party may access the information on behalf of another e.g., on incapacitation or death.
- **Corporate representatives**: The EUDI Wallet is described as holding data for a legal or natural person but there is no further discussion of how the EUDI Wallet works in the case of a corporate body. This may be too early, but some reference would be helpful. There are lots of questions around how this might work.

- Page 15, paragraph "Store Person Identification Data, Qualified Electronic Attestation of Attributes and Electronic Attestation of Attributes"

The benefit of a remote storage is evident. However, if such an online wallet is used, the storage should be set up in such a way that, if exposed, it would not jeopardise the user's complete set of data, e.g., diversify the locations or cloud storages where certain information is stored to in effect have multiple remote wallets to avoid a single point of compromise. We would like to stress the importance of taking the necessary measures to adequately protect off-device storage. Additionally, if remote storage is used, additional measures should be put in place to safeguard subject's privacy (prevent user profiling by the remote wallet provider).

Finally, we suggest rewording (in bold) the following sentence "The EUDI Wallet shall have either only a local storage, or a hybrid storage with at least pointers to remote **attribute** storage**s**…." as for offline use it is necessary to have local storage.

- Page 16, paragraph ''Request and obtain person identification data, qualified electronic attestation of attributes and electronic attestation of attributes''

There is nothing in the design about wallet-to-wallet interaction. Peer to peer events between EUDI wallets is a clear area of practical need in the future. In its current design the wallet only talks to registered or relying parties (which do not include individuals with wallets). This scenario needs to be at least covered in this high-level design to make sure we do not commit to a system where the network becomes too rigid.

- Page 16, paragraph "Cryptographic Functions"

To allow the customer to know who they are sending their data to, as well as to avoid "men in the middle fraud", the Relying Party needs to be clearly identified. **There is a need to define clear responsibilities** relating to each actor involved and common rules and responsibilities for fraud management.

- Page 17, paragraph "Trusted environment"

A trusted environment should be mandatory to achieve a high level of security.

- Page 17, paragraph "Mutual Authentication"

In the middle of row 4 an important "shall" is not underlined, nor made bold.

The wording online/offline is used, whilst the concept of remote or face-to-face should be considered.

More generally, we believe the document should be reviewed to add clarity to key definitions like online/offline, remote/face-to-face, among others.

The whole offline (DIW and service used) seems reserved for limited use cases depending on the risks or will have to be compensated by other complementary measures.

Example of use likely to be frequent: Offline mutual identification and authentication is a use case for kiosks, which may prove problematic in areas poorly covered by public networks. Question of the bank's liability in case of fraudulent use offline.

- Page 18, paragraph "Selection, combination and sharing of person identification data, qualified electronic attestation of attributes and electronic attestation of attributes"

The intent that information about the use of the wallet which is not necessary can only be collected, if the user had expressly requested the collection, should be further strengthened, e.g., by saying "… unless the user has expressly and **actively** requested it". It should be ensured that the tech provider cannot simply include a phrase in the Terms & Conditions saying that the user expressly requests the collection of this data. Consent management and revocation should be managed in line with the General Data Protection Regulation.

- Page 18, paragraph “Identifying and authenticating the EUDI Wallet”

It is not clear which the suitable smartphones are. The EUDIW should be independent from the smartphone vendor and the solution should rely on publicly available standards.

The concept of “revocation checks” needs to be clarified.

- Page 19, paragraph “Offline sharing”

Offline sharing does not allow for verifying “online” the source of the shared data. This should hence be considered on a case-by-case basis following an analysis and not imposed in all situations where the EUDIW is usable. The aforementioned analysis should be risk-based.

- Page 20, paragraph “User interface for user awareness and authorization mechanism’’

Beyond information, what would be the modalities of implementation?

Will there be an interoperable, European-level register?

More technical information should be obtained.

- Page 20, paragraph “User awareness component”

It is important that the relying party is identified and not the intermediary service providers (e.g., concentrators).

It should be clarified who sets the sharing policies and how a relying party could ask for a restricted attribute.

We suggest entrusting the European Identity Council described above with such a role.

- Page 21, paragraph “User authorization mechanism”

The listed criteria may conflict with the EBA RTS for strong customer authentication and common and secure open standards of communication and PSD2, because it does not take into account the application of the dynamic linking.

Consent should be an integral part of the DIW: it is the basic trust service, which guarantees compliance with the GDPR.

The ARF also states that 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: a proof of knowledge; a proof of possession; a proof of inherence. If the authentication process relies on the wallet, there will not be competition in the process because the user experience will be the same for all financial institutions. As at today the authentication process is a competitive issue.

- Page 21, paragraph “Sign by means of qualified electronic signature or seal"

It will be useful to understand how an indirect qualification will work to maintain QSCD status under SSI signature/private key.

- Page 22, paragraph “Interface towards relying parties, brokers or proxies”

The user should be able to recognise the "final" relying party to which they are passing on their data. Additional information about the identity of the brokers would be useful, but not sufficient. GDPR rules for broker and relying parties may differ, and the user should be aware who is the data controller.

- Page 24, paragraph “Trusted registries interfaces”

We suggest entrusting the European Identity Council described above with such roles. The roles and criteria should be further specified in the ARF.

- Page 24, paragraph “Device interfaces’’

‘’Offline communication channels such as Bluetooth Low Energy (BLE), WIFI Aware, Near Field Communication (NFC)’’ - Define an exchange protocol between the terminals and the DIW.

- Page 25, paragraph “Non-functional requirements of the EUDI Wallet”

It should be specified that the user does not have control over his data itself, but rather control over the use of his data. The current wording is not clear enough in this respect.

It is correctly stated that the user has to be informed of the nature of all the operations carried on with their EUDI Wallet, and to present these elements in form of a history. But the EUDIW user shall also have the possibility to delete his usage history.

The wording of the intent that the Wallet issuer shall not combine PID and any other personal data unless the user has expressly requested it, is not sufficient. The wording should be further strengthened, e.g., by saying "… unless the user has expressly and **actively** requested it". It should be ensured that the tech provider cannot simply include a phrase in the Terms & Conditions saying that the user expressly requests the collection of this data. Consent management and revocation should be managed in line with the General Data Protection Regulation.

Privacy requirements for attestation sharing in its current form do not define any tools to create feasible remuneration schemes for attribute/data sharing. Relying parties should be able to pay for usage of trusted attributes without knowing where the relied information is coming from. The current design makes this impossible.

- Page 27, paragraph ‘’Potential building blocks of the EUDI Wallet’’

We welcome the proposal for a broader spectrum than just mobile use, which makes it possible to address all customers, for the sake of fairness. With regard to “Secure Application on PC”, the cross-border interoperability of DIWs will have to be verified in the case of use on secure PCs in shared public spaces.

Diana CAMPAR (GERMAN BANKING INDUSTRY COMMITTEE – GBIC)

The German Banking Industry Committee (GBIC) fully supports the comments published by the European Credit Sector Associations (ECSAs).

We welcome the work on a European Digital Identity Architecture and Reference Framework (ARF) to operationalise the requirements of the legislative proposal for the establishment of an EU digital identity wallet and to develop common standards. ECSA's comments and proposals include GBIC's view on the state of play in the eIDAS Expert Group and highlight important aspects for the further development of a sound technical framework reflecting market needs. To make this framework work for the banking sector is an important prerequisite for a broad acceptance of EU digital identity by consumers and businesses alike.

Robert O'HALLORAN (MASTERCARD)

Mastercard welcomes the Commission's publication of the EUDI architecture and reference framework. It is encouraging to see a more detailed description of the EUDI Wallet concept, its functionalities and security aspects and detail on core use cases.

We also welcome the Commission's position of not limiting the number of European Digital Identity Wallets a Member State could or should issue. This will benefit the end user by fostering innovation. A market of competing wallet solutions is an ideal state, thereby ensuring end user freedom of choice.

More broadly, Mastercard is committed to supporting the Commission's work on digital identity and trust services in Europe. Mastercard believes that digital interactions should be privacy-enhancing, secure, intelligent, and efficient. These digital interactions should be made possible by a user-centric digital identity that is owned, managed, and controlled by the individual and that enables the individual to interact with participating organizations. A reusable digital identity service is impossible without the clear understanding, trust, and engagement of the user.

Mastercard's system model embodies privacy-by-design, is founded on user-centric principles, and requires no further aggregation of identity data or proliferation of new centralized data structures. We believe that no one organisation can deliver a globally interoperable digital identity infrastructure alone. The need for collaboration and co-operation is critical. Mastercard participates in and contributes to industry forums, such as the Trust Over IP Foundation and ID2020, as well as working with intergovernmental bodies, such as the Financial Action Task Force.

Our ID network is designed for globally interoperability in support of national and regional regulations. We recently completed accreditation against the United States' Digital Identity Guidelines, NIST-800-63, and are in process of accreditation against Australia's Trusted Digital Identity Framework (TDIF) as an Identity Provider, Credential Provider and Exchange. We recently announced a memorandum of understanding with the Thai digital identity scheme NDID. We are working with governments and partners around the world to enable digital identity and attributes that are accepted as trustworthy across borders.

We see EUDI as an opportunity to encourage principles-based solutions as well as public-private sector interoperability as the next step in the development of a digital identity ecosystem in Europe. It is also important to set the regulation in an international context: we believe that EUDI should be fully interoperable with international standards. We look forward to working with the Commission as the proposal develops. We are active in this market in Europe: Mastercard has collaborated with Macedonian Ministry of Information Society and Administration (MISA) to launch country's first remote digital identity services for Macedonian citizens.

Mastercard's white paper: https://idservice.com/~/media/digital-identity-our-vision.pdf

Aivo KALU (CYBERNETICA)

Cybernetica would like to thank European Commission for leading the work in this important topic. If this thing goes right, then we are really building a future Europe here, which is able to take a step forward in its digital single market.

Cybernetica with its quarter of a century history in providing technology for the Estonian digital ecosystem, is really concerned if EU actually does take a step forward with the new regulation and Toolbox as is the ambition of European Commission and which has always been expressed by our leaders. So we would have to be sure that ARF and regulation itself would turn out in a way as actually allowing the usage of next-generation technologies as well. Because the experience from the Baltic market is that only next-generation security technology can attract large uptake and would really allow innovation in digital identity technologies.

That all said, we would suggest change into one specific para 4.3.1 of the Architectural Reference Framework:

Current text: Supported algorithms shall be sufficiently strong in terms of cryptography to ensure confidentiality, integrity and authenticity. Such a determination may be concluded by their inclusion in e.g. the SOG-IS Catalogue. Such a determination may be concluded by their inclusion in e.g. the SOG-IS Catalogue.

Proposed text: Supported algorithms shall be sufficiently strong in terms of cryptography to ensure confidentiality, integrity and authenticity. Such a determination may be concluded by their inclusion in e.g. the SOG-IS Catalogue and/or assessing the security level of cryptographic primitives or algorithms by mathematical argumentation.

Two additional comments for explanation:

1) This version of the text would leave the door open for next-generation technologies, instead of putting its focus only on some closed reference lists.

2) Legally speaking if there is a reference made to SOG-IS Catalogue or any other reference list, then this will have to be made on the level of the regulation itself. ARF is an implementing document and it cannot bring in requirements that are not mentioned in the regulation itself.

Viky-Teodora MANAILA (TOIP FOUNDATION)

Submission from the ToIP Foundation to the EU Digital Identity Wallets Consultation Platform

The Trust Over IP (ToIP) Foundation was founded in May 2020 as a project of the Linux Foundation. Our mission is to define a complete architecture for Internet-scale digital trust that combines cryptographic assurance at the machine layers with human accountability at the business, legal, and social layers.

A critical aspect of this goal is to achieve interoperability of digital wallets, digital credentials, and the digital agents and services that issue, exchange, and verify them.

Several European members of the ToIP Foundation are already contributing to the European Digital Identity Wallets initiative in multiple ways. The purpose of this submission is to explicitly offer the assistance of the Foundation and any of our Working Groups or Task Forces in helping you achieve your interoperability objectives.

Because it is critical to our aims, we have spent the last two years deeply assessing the requirements for achieving interoperability of open standard digital wallets and verifiable credentials. We would be honored to collaborate with the European Commission and any EU Standardization Body in our mutual goal to empower citizens with trustworthy digital wallets and credentials that will interoperate around the world.

Please, find below the link to the paper approved by the ToIP Board:

https://trustoverip.org/wp-content/uploads/EU-Digital-Identity-Wallet-Consultation-Platform-Submission.pdf

Bob KRONENBURG (DUTCH .NL REGISTRY FOUNDATION & IMRA APP PROVIDER – SIDN)

On behalf of SIDN, the Dutch .nl Registry Foundation and the provider of the Dutch IRMA.app, we are grateful for the opportunity to give our feedback on the ARF. Our feedback consists of general feedback and a brief list of technical items as proposed in the descriptive parts of the ARF.

General Feedback:

This ARF as published contains a very clear architecture visual. We would like to compliment the authors.

The intensity of requirements is quite large, and if an organisation or member state would have to build a wallet given the ARF requirements may take numerous years to build. A certain degree of flexibility in terms of complying with all the requirements would reduce barriers for member states. An "implement or explained why not" policy may very well be preferred for new and current wallet providers, as there are many arguments towards decentralised SSI that reduce the need for guidelines and policies.

Open Source

By making Open-Source publication of all involved wallets in the LSP mandatory, transparency for EU citizens and observers is provided whilst different LSP projects and member states can use and learn from one another's code base and implementations. There is no reference to Open-Source policy in the ARF and we believe it should be a mandatory guiding principle that is fully aligned with the proposed legislation and the EU ID wallet's values. The principle could also be applied to other actors in the architecture, as it enhances transparency and interoperability.

Pure SSI vs Blockchain and Ledger Technology

We propose to diversify guidelines and requirements between decentralised SSI solutions vs. Distributed Ledger Technologies as the two have very different characteristics and their respective risk profiles differ substantially.

Feedback on specified sections of the ARF

- 4.4.1: "The EUDI Wallet itself shall be able to prove to the relying party the origin and integrity of the individual EUDI Wallet being used and thereby contributing to an increase in trust and security of the ecosystem."

As far as we are aware, there is no technology available with the capabilities of proving origin and integrity of the individual EUDI wallet. This has to be implemented through the (mobile) OS provider.

- 4.5.1: "The offline sharing scenario corresponds to a use case where the user share a PID, QEAA or EAA or a combination of these to a third party, which is in immediate proximity. If the electronic attestation is not linked to the EUDI Wallet, additional data out of the EUDI Wallet's scope, may be requested by the third party.

Many decentralised SSI's, where attribute and credentials are stored local only, may face difficulty complying to Offline Sharing for two very important reasons.

1. Decrypting a credential storage through a key that is solely held on the device poses a mayor threat of individual hacks and compromise, hence many SSI's operate wallets where offline and online processes combined provide security and prevent breach from decryption point of view.

2. Revocation of credentials and attributes is made difficult, for instance a drivers license that has been revoked an hour prior to a user wanting/needing to show his drivers license credentials through the app cannot be revoked from an SSI without a form of online controls.

Our suggestion would be to specify which type of credentials (for instance identity card data) is held to be displayed in offline mode, if this requirement remains in the framework. And be concise about what assurance can be given for Offline display of credentials.

- 4.5, "The Wallet **shall** leverage on a common protocol for identification and attribute sharing including verification of the integrity and authenticity of the information, irrespective of the set of attributes shared, in order to reduce the technical complexity of the solution and facilitate its deployment").

From our point of View there are currently multiple standards VC/DiD etc that may prove useful to facilitate interoperability.

All of these standards are immature and have not been properly tested, at least not on the scale of an entire continent such as the EU. We advise that the framework and LSP criteria leave room for multiple standards to be tested and evaluated as part of an interoperability work package in all the LSP proposals that will be accepted. And use the learnings and insights to specify interoperability and adjacent standards in later legislation.

Famous Last Words...

We look forward to providing the IRMA wallet (open-source) to other Member-states and consortia that apply for LSP grants. Our organisation can help member states and consortia to make their very own implementation of IRMA as well as help using the current IRMA ecosystem In multiple member states through a master- and country node scheme setup in LSP projects. The IRMA SSI source code is at the disposal of anyone who would like to use it through GitHub.

Jeremy GRANT (FIDO ALLIANCE)

These comments are submitted on behalf of the FIDO Alliance.

The Fast Identity Online (FIDO) Alliance welcomes the opportunity to comment on the EUDI Wallet Architecture and Reference Framework.

As background, the FIDO Alliance is a multi-stakeholder, public-private, industry standards development organization comprised of more than 300 companies and government agencies from around the world dedicated to the creation of standards and certification programs for Multi-Factor Authentication (MFA) and passwordless authentication, as well as remote identity verification.

Our members include leading firms in banking, payments, telecommunications, and fintech, as well as those in security, health care, and information technology. A number of government agencies from Europe, the United States, and Asia are active members as well. More on the FIDO Alliance, our members, and our work creating standards, specifications, and certification programs in the identity and authentication space is at https://fidoalliance.org/.

The launch of the FIDO Alliance in 2012 – and the subsequent creation and mass adoption of FIDO authentication standards over the eight years that have followed – has helped to transform the authentication market, addressing concerns about the problems with passwords, as well as the increasing phishability of legacy, first-generation MFA tools like One Time Passwords (OTPs) while also enabling significant improvements in the usability of MFA.

Today, the FIDO2 standards have emerged as the de-facto best choice for implementers seeking to deploy phishing-resistant authentication that is both more secure and also easier to use than legacy MFA tools.

Apple, Google, and Microsoft have all embedded support for FIDO2 at the device, operating system, and browser level, enabling new models for deployment phishing-resistant MFA to be “built in” rather than “bolted on.” The increasing ubiquity of FIDO support in commercially available smartphones, laptops and other computing devices has created new options for consumer authentication that improve security, privacy, and usability.

With regard to the EUDI Wallet Architecture and Reference Framework, FIDO authentication can be used both in local wallets, as well as wallets that are hosted remotely in the cloud. We expect that in practice, FIDO will be particularly relevant in the latter.

The most relevant portions of the Architecture and Reference Framework are Section 4.4 on Mutual Authentication, as well as Section 4.6.2, focused on User Authorization Mechanisms.

Here, we note that Section 4.4 notes: “To ensure that the EUDI Wallet can be used in a seamless way by TSPs and relying parties alike, a common authentication protocol shall be specified, ensuring interoperability at least at EU level and considering relevant European or international standards.”

Too often, strong multi-factor authentication has been “bolted on” to devices and systems rather than “built in.” This is where FIDO authentication is changing the marketplace: the FIDO2 standards – Web Authentication and Client-to-Authenticator Protocol (CTAP) – are supported today by nearly every major consumer device, browser, and cloud services. It is hard to buy a smartphone, tablet, or PC that does not support FIDO out of the box.

Given both the near-ubiquity of FIDO support and the fact that FIDO authentication is “phishing resistant” in a way that other legacy types of MFA such as OTP codes are not, we believe FIDO standards are well suited to meet the requirements of the EUDI Wallets.

FIDO can be used as an authentication standard between the following entities:

- From a mobile/desktop EUDI Wallet to the Relying Party.
- From a mobile/desktop EUDI Wallet to a remote QSCD.
- From the user’s device (app or web browser) to a web application EUDI Wallet.

We note that in the eIDAS ecosystem, FIDO is used today in Czechia in the CZ.NIC mojeID system to meet both LOA Substantial and LOA High, and will soon be used in an LOA High system in Norway as well. Other FIDO implementations are in the works across Europe.

Additionally, we note that FIDO2/WebAuthn is explicitly specified as authentication protocol by the Findy Agency in Finland for access to a web application EIUD Wallet.

FIDO Alliance welcomes the opportunity to answer any questions that the EC, the eIDAS expert group, or other EUDI stakeholders have about FIDO authentication.

Pierre-Jean VERRANDO (EUROSMART)

Eurosmart would like to thank the European Commission for the opportunity to comment on the eIDAS ARF outline. For the sake of clarity, Eurosmart compiled all its comments in a commenting table; please follow this link (https://files.eurosmart.com/s/D44X4xkxom4C9PC) to access it.

Eurosmart remains fully available for further clarification and presenting its proposals in more detail.

Some of the key messages from this table can be summarised as follows:

Level of Assurance "High"

Not all technologies mentioned in the outline allow meeting the security requirements for Level of Assurance "High", as they reach diverse levels of security. The ARF outline should clearly target level of assurance "High" and indicate what technologies enable reaching such a Level of Assurance for the Wallet.

Reliance on secure hardware solutions

The highest level of trust requires secure hardware solutions reaching the level "High". The outline should be more explicit on this point. In particular, cryptographic functions should only leverage secure hardware solutions because it is instrumental for the security and strength of the Wallet. The outline should also make clearer that Trusted Execution Environments (TEE) and Secure Elements (SE) do not provide the same level of trust – level "Substantial" for TEE and level "High" for SE.

User control

The outline refers to "full control" and "sole control" without defining these terms, especially with regards to sovereignty over data (e.g. cloud solutions), encryption keys, and the way the data are controlled by the mobile phone, SE, TEE etc. "Full" and "sole control" would deserve further explanation.

In addition, the concept of "breach of control" is introduced in the outline but not defined, while this concept does not appear in the legislative proposal.

Definitions of entities

Many entities are introduced by the outline. Some can be found in the eIDAS legislative proposal, and others are new (e.g. gateways, providers of registries, catalogues of attributes, PID providers). The outline should contain a definition clause to define all of them.

Clarify requirements

The outline should be clearer on the requirements that apply to the entities. For instance, which entities need to register?

Moreover, the responsibilities of the relying parties could be made more explicit. When relying on parties authenticate the attestations, should they verify the validity of the attestation? Should they also authenticate the PID? Another question is left unanswered: how does the relying party know that an operational phase is run at a given level of assurance (i.e. "High" or "Substantial")? These points deserve clarifications.

Mutual authentication between the Wallet and relying parties

Some details are missing for mutual authentication between the Wallet and relying parties. One missing element is the configuration and update in the Wallet of the authorisation and/or revocation list(s) of relying parties. Another missing element is the configuration of the trust anchors to be used by the Wallet to authenticate the relying parties.

Regarding the implementation of mutual authentication, the framework should leverage Qualified Website Authentication Certificates (QWACs).

In addition, mutual authentication should go beyond identification and authentication of endpoints; it should set a trusted channel whereby any subsequent communications between both parties -during the session- are protected in integrity, authenticity and confidentiality.

For further information, please consult our commenting table.

Michal TABOR

The ARF outline document is essential in establishing standard requirements for EU DI Wallet. I appreciate this document and hope for more deep down documentation on the project's next steps.

Although sometimes, I believe the missing part of all analysis is the security and usability of the transactions from the user's point of view.

The outline describes the need for an awareness interface in the wallet, but there is no information on what kind of transactions will be used with the wallet. In theory, the wallet supports Electronic Attestation of Attributes and PID presentation, but this presentation is always on request of the Relying party and in the context of the specific transaction. So the real need is that the wallet shall recognise and inform (with the use of an awareness interface) the wallet holder about the type of transactions the holder takes part in.

Wallet shall accept requests for electronic transactions from relying party. Those requests shall clearly state what is the purpose of the request and identify relying party waiting for the response.

Wallet awareness interface shall present the following data to the wallet user for acceptance:

1. Relying party identification data and level of trust (gov, trust service, bank, ...)
2. Type and text of the request - identification, authentication, acceptance
3. Attributes to be presented to relying party

In the text below, I mention the initial set of transactions to be considered as EAA/PID presentations.

Identification

Wallet presents to the selective data from PID and EAA on the request of Relying Party.

Generic scenario: Relying party requests specific data for identification, wallet presents information about relying party and what data is requested. Wallet user accepts data to be presented, wallet presents data and attributes to the relying party.

PIT Presentation type: Selective

EAA Presentation type: Selective

Level of trust to relying party: Information

Use cases:

Registration to the services,

Presentation of data to officials,

Identity proofing

Authentication

Wallet presents specified attribute on request of Relying Party. Authentication may be based on number, one attribute or wallet identifier.

Generic scenario: Relying party request authentication based on specific EAA. Wallet checks if contains specific attribute or set of attributes, presents to the user information about relying party

and what specific attribute is requested. It is possible that EAA contains data of relying party allowed to request this authentication method (unauthorised RP can't use it for authentication). Wallet makes EAA presentation after user consent.

PIT Presentation type: Not required (to be decided if PID data can be used for authentication)

EAA Presentation type: Selective

Level of trust to relying party: Information

Use cases:

Returning user authentication,

Use of key to car, hotel room, etc.

Second factor to services

Selection

Used to select an attribute of specific type (with specific data)

Generic scenario: Relying party requests attribute of specific type. Wallet presents information about relying party and list of attributes that specific type and asks to select only one to be presented. Wallet makes presentation after user consent.

PIT Presentation type: -

EAA Presentation type: One specific

Level of trust to relying party: Information

Use cases:

Presentation of covid certificate when all family certificates are on the wallet;

Service preference selection;

Corticate to be used for signing;

Payment method (card) to be selected

Acceptance

Allows to accept specific request - request is presented to the user with awareness interface.

Generic scenario: Relying party requires identification and consent of the user on specific data (short text request). Information about Relying Party and text of request is presented to the user. User explicitly accepts the text of the request and identification data to be presented to RP. Wallet after consent presents identification data and text of the consent.

NOTE: It is not electronic signature over document. Text of the consent is simple to be presented on the screen. Request is not linked to the document.

PIT Presentation type: Selective

EAA Presentation type: Selective

Level of trust to relying party: Higher

Use cases:

Terms and conditions acceptance,

GDPR acceptance,

Payment acceptance,

Data change acceptance

Signature LOCAL QSCD

Use of QSCD in singing process should be invoked in secure environment for the user - it never shall be granted on request of not authorised party for this purpose

Generic scenario: Authorised relying party to use wallet for signature creation with LOCAL QSCD request signature creation over Document TO Be Signed Representation. Wallet uses awarness interface to inform user and authenticate request. Wallet uses local QSCD for signature creation and returns the computation to authorised relying party.

NOTE: Wallet is used the same way as cryptographic card.

NOTE2: Relying party should be trusted and recognised as Signature Creation Application presenting document to be signed content

PIT Presentation type: - NO USE

EAA Presentation type: - NO USE

Level of trust to relying party: Only priorly authorised party

Use cases:

Signing with QES or Qseal using known to the wallet and wallet user Signature Creation Application

Request redirection to Signature Creation Application

Redirection to SCA may be based on Selection of EAA or wallet internal function to redirect transaction

Generic scenario: Relying party requires creation of the signature over Document To be Signed, and send request information to the wallet. Wallet presents information about relying party and asks user if he wants to initiate signature creation process. After user consent wallet presents to the Relying Party redirection token (or redirects directly) to Signature Creation Application. User finalize signature creation process with Signature Creation Application. NOTE: QES signing requires according to ETSI EN 319 102-1 presentation of the document and attributes - external app trusted to the user may be required

PIT Presentation type: - NO USE

EAA Presentation type: One specific

Level of trust to relying party: Information

Use cases:

Leasing company requests signing over document

Signature creation with remote QSCD

Use of remote QSCD in singing process should be invoked in secure environment for the user - it never shall be granted on request of not authorised party

Generic scenario: Authorised relying party to use wallet for signature creation with REMOTE QSCD request signature creation over Document TO Be Signed Representation. Wallet uses awarness interface to inform user and authenticate request. Wallet uses Remote QSCD (associated with the wallet) for signature creation and returns the computation to authorised relying party.

NOTE: This association can be done using EAA attribute of specific type and presentation of this attribute may authenticate user to the Remote QSCD

NOTE2: Relying party should be trusted and recognised as Signature Creation Application presenting document to be signed content

PIT Presentation type: - NO USE

EAA Presentation type: One specific

Level of trust to relying party: Only priorly authorised party

Use cases:

Signing with QES or Qseal using known to the wallet and wallet user Signature Creation Application

Signature creation based on identification

Wallet presents data to the TSP to issue a certificate and create one time signature (signature on the fly)

Generic scenario: TSP is relying party requesting remote identity proofing and signature creation in one process. This can be done with Acceptance function above.

PIT Presentation type: Selective

EAA Presentation type: Selective

Level of trust to relying party: Only priorly authorised party

Use cases:

Signing with QES or Qseal using known to the wallet and wallet user Signature Creation Application

Jon ØLNES

Overall impression of document is quite good. However, very few technical decisions are yet made. No technical specifications or standards are referenced. Please consider the work done by CEN (including a gap analysis for standards for wallets) and ETSI in the upcoming work.

An important comment is not directly on ARF but on the planned reference implementation. Making a reference implementation available is positive, but that must be in the same way as the building blocks developed under CEF Digital, as a voluntary offer. Making the reference implementation mandatory for all wallets, and even for all large-scale pilots, is a really bad move. This will kill innovation in wallet technology and reduce reliability since security issues will hit all implementations. Also, it will fence off interest from commercial technology providers that are already developing wallet solutions.

Opposed to the signal of a mandatory reference implementation, the ARF appears as open to different wallet technologies, which is a direction that must be kept also for future versions. The important topic is interoperability, not equal implementation, e.g. a wallet where information is stored locally can well be interoperable with a wallet storing information centrally (server-based).

The most important comment on the wallet concept is again not on the ARF but on the proposal for revised eIDAS: eID issuing, including wallet issuing, should be defined as a (qualified) trust service. That would make eID and wallet provisioning possible as a commercial offer in the internal market. And it would place the service under a firmly established and well-functioning standardisation and conformity assessment and supervision scheme, which is not the case when wallets are national and regulated under the eID part of eIDAS. Leaving wallet issuing to the individual member states puts the entire initiative at great risk. States may provide only a nominal wallet offering. To commercial actors, the incentives are limited, as market is limited to the member states that will accept wallet services from private sector, and with separate approvals for each such member state. It is an argument that identity is national and that states must be in control, but they still are by providing the identity documents that are needed as primers for wallet issuing (identity cards and passports, and even state-issued eID as an option like many states already do).

As mentioned above, defining wallet issuing as qualified trust service would mean entering a well-established conformity assessment and supervision scheme. Currently, it is not clear how this will be done for the wallet with the risk that a new scheme must be developed.

The ARF mentions wallet possessed by a legal person, but it is difficult to see how that can be a possibility. Wallet for natural person representing a legal person is however a clearly possible use case.

Regarding onboarding (identity proofing) of a user to a wallet, the approach should be to refer to the ETSI TS 119 461 standard on identity proofing for trust services as a basis and further develop this standard to include profiles for onboarding at assurance level 'high'. This work should be delegated to ETSI. Referring the standard will result in a consistent level of identity proofing across different use cases from physical presence to remote use of identity documents, eID and (qualified) signatures.

The proposed clause in eIDAS requiring national registration of relying parties is not well-founded and will hopefully be removed. There are few arguments in favour of such a bureaucratic approach, in particular because there are no rules proposed for authorisation. E.g., no clause is there for a member state to deny a relying party use of the wallet; and there is no concept of "trusted relying

parties". A standard way to authenticate relying parties must be in place (e.g. (qualified) seal and/or web-site certificates). A standard way for relying parties to declare the attributes and attestation they need, and why these are needed, is also necessary, but currently missing from the ARF.

It is very important that the ARF, as it does in current version, recognises the 'authentication gateway' (sometimes termed 'broker') role as intermediary between wallet and relying parties. The wallet will not be the only eID in the market, and relying parties will need to integrate the wallet alongside other eIDs. Services currently exist in the market to make many eIDs available over one (broker-)API, including cross-border services making eIDs from multiple states available over the same API. The need for such services will remain, and it is important, not least for uptake of wallet use, that the providers are allowed to integrate also the wallet in such a service offering.

Regarding attribute provisioning and authentic sources, the ARF needs to make a distinction and describe the two cases 'validate' (check already provided attributes for correctness against the authentic source) and 'fetch' (obtain attributes from the authentic source). In member states, these cases can be regulated differently, and in some cases, only the 'validate' model may currently be allowed.

The above is also partly related to the two models for providing attributes from wallet: Provide from wallet storage (attributes pre-fetched) or fetch on demand from attribute provider. The latter avoids issues regarding revocation but will not work if the wallet is offline (one argument for avoiding that interpretation of 'offline', see below). Both models are relevant and probably need to be provided but one or the other model may be required for different use cases.

Regarding attribute provisioning, it is not clear from the ARF if a manual "navigation" process by the wallet user is envisaged to localise an attribute attestation provider covering the desired authentic source, or if an automated "API-based" process can be used. Possibly, both alternatives are needed but API-based should be the preference if possible. The reference to the 'single digital gateway regulation' seems to indicate a manual process in the current state of that regulation.

Regarding authentic sources, many member states will lack availability of proper sources for many of the attributes specified in the annex to the proposal for revised eIDAS. This is however a problem that the ARF cannot solve.

Also related to revised eIDAS and not to the ARF directly, it is not clear how complete coverage of all authentic sources in all member states by qualified attribute attestation providers will be guaranteed. Likely no attribute attestation provider can be a "cover it all", at least not in the short term. Attestation providers will cover nationally, regionally, or sectorial (all or most authentic sources for specific attributes and attestations). A member state may be left with no qualified attestation provider covering its authentic sources.

It is very important that the ARF (and the revised eIDAS) will continue to allow non-qualified attestation of attributes. This leaves flexibility regarding the information and use cases that a wallet can cover, including specific national cases.

The business model of an attribute attestation provider is difficult. The wallet user is not supposed to pay, but the relying party, who would be the right actor to pay, shall not be known to the attestation provider. This is solvable by a carefully crafted payment scheme but is not easy and may require further trusted roles in the ecosystem.

The role of provider of 'catalogues of attributes and schemes' is introduced in the ARF (it is not in proposal for revised eIDAS) reflecting the need to navigate to find a provider for specific attributes

and attestations. It is however completely open how such services will be provided and their business model, e.g. if these will be EU owned and financed or a co-ordination of national services like the EU Trust List scheme for qualified trust services. Catalogue services may be applicable for commercial actors but then the business case must be clear.

The same is the case for the role 'provider of registries of trusted sources' where the link to a scheme like the EU Trust List may be more evident. This should likely be a national or EU-wide service provided by governments or the EU. However, the role is not present in the proposal for revised eIDAS.

Regarding qualified signature (QES), the ARF must continue to be open to different approaches. While use of devices with built-in certified QSCD should be kept as a future option, this is not going to happen in the near future. Use of an external device like an NFC-enabled smart card is relevant. However, the mainstream approach will surely be server-based signing where the wallet is used to activate a server-stored signing key with attached certificate. Note also the possibility of a 'split-key' approach where one part of the signing key is in the wallet and another part on a server. This is used e.g. by Smart-ID in the Baltic countries.

In reality, the relying party, and not the wallet user, will initiate signing, including selecting how to show the document to the user and obtaining consent to sign. From such a signing, it is virtually impossible to integrate each and every basic signing service available, considering that signing will not only be initiated from wallets, but also from other eID/signing solutions. It is therefore important the the wallet can be used "as an eID" (authentication process) to trigger issuing of qualified certificates on-the-fly for different signing services according to eIDAS article 24.1.b and the corresponding use case in ETSI TS 119 461 on identity proofing.

The requirements for 'offline' and what 'offline' means must be clarified. If this means that both wallet and relying party are without Internet connection, then the use case is really difficult regarding mutual authentication, validation of attributes etc. Potentially, a lot of validation information (trust anchors) must then be stored locally at the relying party and/or the wallet. If the relying party is required to be online, validation of presented attributes and authentication of wallet user are much easier. If the wallet is also required to be online (only communication between wallet and relying party is by other means than Internet), authentication of relying party and provisioning of attributes is also much easier. In general, the offline use case is likely exaggerated by the proposal for revised eIDAS and by the ARF given development of mobile and other network connectivity in Europe. The offline use case could likely be limited to presentation of a limited selection of information (e.g. a visual rendering of a driving license or identity document or document like a vaccination passport). Hence, the requirements for local storage by the ARF can be relaxed leaving further flexibility on technological solutions for wallet.

Wallet technologies may be possible without use of TEE on the mobile device, however this is to be further explored. This will then depend on central (server-based) hardware. Offline operation will be difficult in such a case, but depending on the definition of 'offline' (see above), this may be OK.

One or more protocols for attribute disclosure must be defined. While W3C verifiable credentials is one option, others exist, including extension of OAuth/OIDC. A strategy that specifies only one protocol has advantages but is also limiting. A strategy where a mandatory reliance on distributed ledger services is created should probably be avoided; rather if such an alternative is included, it should be one among a small number of protocols. Probably, use of at least the two protocols mentioned above should be included in the ARF specification.

OIDC should be the preferred protocol for authentication, although alternatives could be allowed (e.g. SAML).

The requirements on user control and selective disclosure need much work in further versions of the ARF. This must include protection against relying parties that ask for more information than needed, "teasing" users to approve disclosure of that information.

The non-functional requirements section raises lots of questions that must be further detailed, in particular for linkability of events and on revocation.

One clear mistake in this section is the lack of reference to the EU Web Accessibility directive and correspondingly to WCAG 2.1. These requirements must apply to a wallet implementation. This relates also to the choice of technology. For ubiquitous access to wallet, other technologies than a mobile app must be available. This may call for a cloud-based approach rather than local storage, where a wallet app, or other technologies, are front-end to the cloud-based technology. If the wallet is based on app with local storage, other technologies must be developed essentially as completely separate and parallel solutions.

Regarding linkability of events, some relying parties, notably governments but also to some extent e.g. financial service providers, may have a legal right or obligation to link certain events, while for other actors the same linking is not allowed. Making a linking function possible means it is there for possible abuse. The conditions for linking and corresponding functionality will be a difficult aspect of a wallet. Note that legislation in different member states may have different requirements.

Regarding revocation, the wallet user must have the possibility of revoking "anything". Then, there are cases where revocation must be done without the wallet user's consent. This could be the entire wallet if it is misused (e.g. used by someone else after the real user is dead) or compromised. More relevant, most attributes and attestations stored locally for a wallet must have a granular revocation functionality, including revocation checking by relying parties. This may need to be specified independently for different types of attributes and use cases.

The user must be offered means to recover from events such as lost or locked wallet (lost device). This is easier if information storage is "in the cloud" since information stored on the device will be lost. The same functionality is needed when a user switches to a new phone. A possible role in the ecosystem can be an "identity custodian" that the user trusts to provide recovery functionality including storing backup of crucial information. A custodian may also provide necessary access when the wallet user is incapable of using the wallet, e.g. deceased or unconscious. The user may e.g. appoint someone to "clean up" in such cases.

Delegation and representation are elements that are not yet addressed but that can be relevant. This can be parents on behalf of children, someone one behalf of a dement person, or otherwise, under user control or appointed otherwise. No-one else should use a person's wallet (although that can be difficult to control); delegation in that one can access information about others from ones own wallet is a better alternative.

Looking forward to the next iteration of the ARF.

Feraud ALBAN (ACN – ALLIANCE POUR LA CONFIANCE NUMERIQUE)

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 has thoroughly reviewed the ARF and prepared the following comments that you will find in the comment sheet at the following link:

https://www.confiance-numerique.fr/wp-content/uploads/2022/04/ACNs-Comments-European-Digital-Identity-ARF-04-14-2022.pdf

ACN remains at your disposal should you have any questions on these comments.

Regards

Stephane MOUY & Michael ADAMS (SGM CONSULTING + QUALI-SIGN)

QUALI-SIGN AND SGM CONSULTING COMMENTS ON ARCHITECTURE AND REFERENCE FRAMEWORK (ARF) DOCUMENT

- **Section 4.1 Store person identification data… & Section 4.4 Mutual authentication: Offline connectivity and storage interface for EUDIWs**

We support the emphasis put on offline connectivity for EUDIWs, which is needed for many use cases, and certainly critical for POS payment authorization interactions. In particular we appreciate the wording of section 4.4 Mutual authentication.

We note, however, that footnote 15 mentions that mutual authentication may not be always required but fail to understand why this should be the case given that it does not affect the customer experience nor does it imply additional costs. We only see benefits and no downsides in having mutual authentication performed for each and every interaction between EUDIWs and relying parties.

Given the focus on offline connectivity – which we fully support – we fail to understand how the EUDI Wallet storage can be meaningfully 'remote (in a cloud-based infrastructure)' as a self-sufficient alternative mentioned in the second paragraph of section 4.1. The related footnote 12 mentions 'additional challenges' in this context. To put it directly, we do not see how this could work (particularly when both the relying party and wallet are offline) and would welcome clarifications on this aspect.

Indeed, local storage using X509 certificates applying ETSI standards (notably 119 411-2) for PIDs and (Q)EAAs pointing to the wallet identity certificate (itself linked to the secure element of the smartphone) allows a secure management of identity and other attributes which can be communicated online and offline. This allows online and offline client authentication for all interactions with relying parties, root of trust verification of all certificates as well as mutual (wallet user/relying party) consent whenever needed – a essential requirement for the payment authorisation use case where legal irrevocability needs to be established.

(link to graphic description of the wallet local storage)

- **Section 4.5.1 Offline sharing**

The section contemplates a scenario where a physical ID document with biometric data is required to be presented for identity-proofing purposes of the wallet user, a situation resulting from the fact that the electronic attestation is 'not linked to the EUDI wallet'. This situation should simply not be allowed and all attestations should be linked to the EUDI wallet, and therefore the wallet user. Indeed, the link should be required irrespective of whether they are PID, QEAA or mere EAA attestations. In short, we see no rationale at all for 'unlinked' attestations. This can only weaken the trust put into EUDI wallets.

- **section 4.8.2: Interface towards Member States identity cards – treatment of facial image as an attribute**

We note, in line with other contributors, that EU regulation 2019/1157 drastically restricts access to 'biometric data stored in the storage medium of identity cards and residence documents' (including the facial image), which 'shall **only be used by duly authorized staff of competent national**

authorities and Union agencies for the purpose of verifying (a) the authenticity of the identity card or residence document and (b) the identity of the holder […] where required to be produced by law' (article 11.6). We wonder if the initial identity-proofing (binding) process implemented by providers of PID can achieve a high LoA when they are legally prevented from having access to the facial image of the holder in the card chip.

We recognise however that, as directed by GDPR requirements for biometric data, the facial image warrants enhanced protection, and would suggest either prohibiting it from being an identity attribute transferable to any relying parties – indeed this is not needed to ascertain that the person it the wallet's legitimate user – or restricting its communication to those relying parties that have a legitimate interest, such as, for example, police and customs officers. At a technical level, this can be done by requiring the relying party to first present to the wallet a dedicated electronic attestation showing that it is entitled to request the facial image (or other biometric data), meaning that no communication would be possible unless this attestation is first presented to the wallet. This can be simply achieved with X509 attribute certificates meeting ETSI standards. In our opinion, it would be beneficial to extend this approach to other 'privacy-sensitive' attributes, such as the unique identifier – see below.

- **Export of EUDI wallet interaction history for dispute resolution purposes and compliance with regulatory requirements**

We are very supportive of the requirement for the EUDI Wallet to provide the user with access to the history of their digital identity transactions (see articles 4.6.1 and 5). However, we suggest that the text be extended to explicitly state that the EUDI wallet user is always entitled to export a copy of the digital identity proof (incl. Qualified Signature) created during interactions with relying parties. The user would then be able to present this as evidence, including for compliance with regulatory requirements and court proceedings. All use cases are relevant here, but this is especially relevant for payment authorisations.

- **Legal person wallets / Identity Profiles**

We believe it is important for EUDI wallet users to be able to segregate their personal and other identity profiles (e.g., a natural person authorized to act on behalf of a legal person) within the wallet. Otherwise, requests are likely to be made to install multiple wallets on the same device in order to achieve this segregation.

With respect to export of the wallet interaction history mentioned above, we believe it is appropriate for the legal person (e.g. the employer) to be able to restrict the representative user's ability to export the proof (of potentially sensitive business-related digital identity transactions) to their personal device. Instead, the legal person must have the ability to export the proof in a secure manner and also have access to the history.

COMMENTS RELATED TO THE EIDAS 2.0 DRAFT PROPOSAL.

- **Article 11a of draft eIDAS 2.0 proposal: Privacy protection and 'Unique and Persistent Identifier'**

The ARF, and indeed the draft eIDAS 2.0 proposal, rightly emphasise the need to protect privacy, which includes ensuring that no relying party should be allowed, or indeed able, to trace the use of EUDIWs. On the other hand, we also understand the need for certain public authorities – e.g. tax authorities - to have access to a unique identifier as set out in article 11a of the draft eIDAS 2.0 proposal.

As for the facial image discussed above, an efficient way to reconcile the two requirements would be to have those relying parties authorized to request the unique identifier present a dedicated electronic attestation to this effect, which would result in no communication of the unique and persistent identifier being possible unless this attestation is first presented.

- **Article 6.bof draft eIDAS 2.0 proposal: EUDI Wallet relying parties**

We are really puzzled by article 6b, especially when requiring all relying parties to 'communicate to their member States their intention to rely on EUDI wallets and informing about the intended use of EUDI Wallets' (article 6b1). We see no clear rationale for this requirement and fear this will prevent the deployment of fully legitimate use cases for EUDI Wallets, especially for SMEs, professionals and indeed individuals who should be able to act as relying parties. Also, does this imply that non EEA/EU relying parties – who have no 'member State' – cannot rely on EUDI wallets? It strikes us that this is a major deviation from what happens in face-to-face interactions when presenting verified ID credentials, such as passports or ID cards. To take a simple example, a licenced liquor merchant does not 'notify' its member State that it is to accept national ID cards or passports to check that customers are over 18 years old.

To address this, one possible option could be to differentiate between certified relying parties (who have communicated their intention to member states) and two EUDI wallet users who wish to bilaterally conduct a digital identity transaction between their two wallets. In the latter case, we suggest that both users should be required to perform Strong User Authentication on the transaction. This approach would be applicable to P2P transactions between two wallets.

With respect to the 'common mechanism for the authentication of relying parties' (Article 6b2), we suggest that whenever relying parties (other EUDI wallets, terminals, websites etc) initiate a EUDI wallet based digital identity transaction, they must include a specific attribute attestation within their request. This attribute would include the name of the relying party, which can then be displayed by the receiving EUDI wallet to their user.

Michael ADAMS/**Quali-Sign**

Stéphane MOUY/**SGM Consulting**

Michael Adams and Stéphane Mouy are both members of the eWallet Network

Stephan ENGBERG (PRIWAY/CITIZENKEY)

Priway/CitizenKey response to the draft EU Digital Identity - Architecture and Framework.

http://blog.citizenkey.eu/public/Political/eIDAS_2_0_framework_Response…

The response is reflecting key aspects of this talk pointing towards the many problems in eIDAS 2.0 thinking.

Before we can add new credential types such as BBS+ we need to deal with the flaws and inability of eIDAS/ETSI PKI to match the requirements in both eIDAS regulation and GDPR. They key mechanism to do so is upgrading PKI to Trustworthy PKI with Non-linkable Qualified Signatures within the already standardised structures.

https://www.meetup.com/privacy-engineering-group/events/281522910/

There is a fundamental problem with the ARF document trying to put control in a hostile environment.

In a trustworthy design perspective, we would not accept any element where security depend on revocation of already deployed keys or credentials.

From a Trustworthy Design perspective, the ARF reflect an entity that cannot be considered trustworthy as it is not even aiming to be. A Virtual QSCD Interface can be provided to support a nested Wallet structure with Trustworthy structures including user wallet control intra-QSCD, but the Wallet itself is the weak point meaning trustworthiness is lost

E.g. the abuse of biometrics in paragraph 4.5.1 Offline reflect the immaturity of the thinking.

In order words, the ARF can never support an (Q)EAA level High and would rank deep in the untrustworthy in CitizenKey to the point where we must assume breech and loss of citizen control has already occured.

We warned against the blinding-at-use approach to selective disclosure that is only approach reflected in the ARF

http://blog.citizenkey.eu/index.php?post/2020/07/03/Blinding-at-use-vs…

Christian KAHLO

I got involved as an individual expert from the German civil privacy and security community, being a member of c-base e.V. and close to the CCC ("chaos") community.

That's why already adressed a few points in one of the past LIBE shadow meetings: https://vx4.net/EU%20LIBE%20EUid%2020220209.pdf.

I want to emphasize and clarify a few more things below.

Transparency disclaimer:

Besides having been invited as an individual expert I am working for adesso SE as Chief Security Architect with a main focus on "adesso ID". Additionally I've been member of the BSI eID working groups since 2009 and I'm developing with "secure elements" since the late 1990s. "adesso ID" is an eIDAS Token-based technology stack enabling flexible ID solutions combining FIDO for authentication and eID for identification and how to bring them together with everyday usage scenarios on creditcards, SIM cards, mobile phone embedded secure elements, wearables, official identity documents and so on. My comments are NOT motivated by adesso, but of course the strategy of the company relies on my views.

I am also responsible for the implementation of BSI project FIDELIO - integrating eIDAS Token-based German eID with FIDO.

And I've held a talk before OmniSecure 2020 about the prototypes of "mobile electronic IDentity" (meID) with eIDAS Token on USIM cards, wearables and embedded secure elements (text in German, but DeepL works fine).

I.) Nomenclature for security and privacy guarantees defined in the EU DI ARF

I want to point you to the paper "Terminology for Talking about Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management":

We must assure that we have the same understanding of the meaning of terms and need to define and agree on them (in written form). (Unfortunately Mr. Pfitzmann died very sudden, so work stopped at the draft but the content is neither the less valid.)

II.) We need to distinguish the use cases of the ID framework

1.) secure authentication of persons for "everyday" login into applications / web portals

A possible solution for that could be FIDO2 password-less authentication as a modern, open, already well-established industry standard and technology stack. Or any pairwise-identifier scheme.

2.) secure identification of persons for legal reasons or binding contracts between relying parties and citizen

As already stated in my feedback in the shadow meeting classical X.509 certificates are kind of obsolete because of missing crypto agility, selective disclosure, extendability, etc. eIDAS Token already addressed all those questions that been raised with the self-sovereign-identity hype many years ago.

3.) signature of data / contracts for data integrity and intended linkability to an account / profile or person during transport over public networks without the need of "person identity"

This is clearly to be handled locally by pseudonymous signatures or by using a e.g. FIDO-based signature scheme by including the hashes of the data in the FIDO client data.

4.) signature of a contract 'forever' by a person to establish a contract relationship in either eGovernment or private sector scenarios / corporate law. (i.e. with notary services)

In case of a notary service a qualified remote signature as described in BSI project 361 "REQESIDTA" may be discussed. Remote attributes and remote signature are a good extension as an "opt-in" option especially in case of notary services, but never as a default. But keep in mind custodial wallets may be hosted by providers in countries with different jurisdictions, i.e. think of Brexit and the consequences. It is not acceptable that user rights (privacy, data protection) are weakened when a state leaves the union. So, this needs to be decided very carefully.

These four scenarios and the underlying methods are often mixed up or misused for other use-cases.

III.) We need to think of "identity carriers"

An identity carrier could be the official national ID document of the member state, it could be a travel passport, a driver's license or some sheet of paper. In the digital future identity carriers are now also embedded secure elements in mobile phones, wearables containing secure elements (rings, keyfobs, ...), payment cards, SIM cards, etc.

But also trusted secure environments like "TEE" / ARM trustzone in mobile devices are being used as identity carriers when they store the cryptographic key material to authenticate / identify a user.

Authentication keys and eIDAS minimum dataset attributes must always reside in a secure and trusted environment. And especially in order to maintain sovereign control of the identity by the citizen CANNOT be uploaded and delegated into some cloud or a "custodial wallet". "Hardware wallets" or "non-custodial wallets" in form of a "personal secure device" (personal secure element) must be the anchor for an identity, the use of remote / cloud storage or custodial wallets for additional attributes should be seen as an extension option. The security of the remote attributes could also be ensured if a secure hardware wallet is in place.

IV.) Based on I.-III. we need to define security and privacy guarantees towards the users / EU citizens & visitors

I.e. the user must have the sole control of his identity and the underlying cryptographic material. And unlinkability / non-traceability (chapter 5) are important regarding the privacy rights of the citizens. This also includes unobservability (see the paper in I.) meaning a user can use her/his identity without the involvement of a (possibly tracking) third party. FIDO is a perfect example how to implement this requirement. Also relying party authentication is a "MUST HAVE" and not an option.

V.) Current problems of "secure enclaves" or trusted execution environments

Currently trusted execution environment implementations are proprietary to the manufacturers. "secure enclave" is the Apple, Inc. term for their implementation.

The difference of an (embedded) secure element (SE) and a TEE is

1.) the secure element is a separate chip with an own operating system, code and data storage and access control

2.) the SE hardware and software is specifically hardened against failures and attacks

3.) the implementation of SE hard- and software is usually evaluated according to ISO 15408 "Common Criteria" at EAL levels 5+ or even 6+.

The manufacturers (Apple, Google and the Android OEMs) currently neither implement a certifiable standard nor do they have verifiable evaluations / certifications for their implementations. That means a "secure enclave" / TEE is currently uncertified, while a secure element comes with high level certifications. This is a big difference regarding the level of trust one can put in the security stability of the chosen identity carrier.

This might change as soon as the manufacturers adopt the new (2022-03-01) BSI CC PP-0117 "Secure Sub-System in a System-on Chip" developed by EUROSMART.

VI.) Security considerations of form factors

1.) mobile app

A simple "mobile app" just storing identity data in the application storage area cannot not be implemented to be reasonably secure. This was tried with the German "id wallet" and resulted in the realization it wouldn't even reach eIDAS LoA "substantial". So it became basically useless.

Further a mobile app could leverage the platform / operating system cryptographic services, basically relying on Apple "secure enclave" or Google "keymaster HAL". As said before these implementations are neither verifiable nor evaluated or certified at the moment.

But the mobile app could make use of the internal embedded secure elements, USIM, or the NFC, Bluetooth and USB interfaces to connect to a personal secure element as it does with an identity card.

2.) web application

The problem with web applications is that their code is remotely hosted by nature. And there is an untrusted public network between the user and web server by definition. Even if TLS is used to encrypt the communication link there is no established way to verify the integrity of the code inside the web application. So if an attacker modifies the web app, the user has NO chance to detect this. That's a quite simple no go.

3.) secure app on PC

At first a "secure app on a PC" sounds like a good idea. But we have Windows, Linux, MacOS and several other operating systems out there. The basic problem is: what makes this app secure? Where shall the app store sensitive cryptographic data? Of course on Windows it is easy to make use of the TPM and modern TPMs have a wide range of sophisticated cryptographic algorithms available. But TPMs aren't built into every machine, many laptops have a TPM, but most desktops will only have a TPM when they're certified for Windows 11. And after all there is no established certification

standard for TPMs. Some TPMs may be certified to CC EAL, others are not. The average user typically can't tell certified and non-certified TPMs apart.

But again, the app on the PC could use the built-in interfaces to connect to a personal secure device. (FIDO, again, is a perfect example for this.)

-- Christian Kahlo (ck@c-base.org)

Johan NYMAN

Section 3.1

"The EUDI Wallet would enable end-users to create qualified electronic signatures and seals (QES).

We see QES signing as a crucial and important part of the wallet; a part which is often played down, while more focus is given to the identification/authentication part.

Among the main goals the wallet must be able to:

Create qualified electronic signatures

Contain and allow sharing "electronic attestations of attributes" about the person

At the same time we have all the building blocks already available and in use. We need to list existing best practices, publish them and take the wallet into use.

Our proposal

Issue 2 certificates into every wallet. First certificate for user identification that is used to verify user ID. Second certificate for qualified electronic signatures.

All the "electronic attestations of attributes" must be ASiC-E containers with machine readable and optionally human readable representations. If only machine readable data is needed the JAdES format would work too.

Machine readable part must be JSON similar to the W3C Verifiable Credential standard.

Attestation verification process must involve checking the issuer signature, trust list status and user identity using identification certificate.

Flexible trust list system must be developed. Each attestation category must have its own trust list. New category creation must be an easy and fast process.

Access to the wallet system must not be restricted. Cost of being included in the trust list as attestation issuer must be reasonable.

Further reference: https://eideasy.com/simplest-implementation-of-eu-eid-wallet-that-can-b…

Torsten LODDERSTEDT, Nat SAKEMURA & Gail HODGES (OPENID FOUNDATION – OIDF)

Dear Sir or Madam

The OpenID Foundation (OIDF) is pleased to provide the following comments on the EU Digital Wallet initiative and the Architectural Reference Framework (ARF). We are encouraged to see the EU focus on an EU Digital Identity Wallet, an initiative with the potential to offer profound benefits to EU residents, businesses, and government.

I. About the OpenID Foundation

As a global identity standards body, the OIDF's vision is to help people assert their identity wherever they choose, and our mission is to lead the global community in creating identity standards that are secure, interoperable, and privacy preserving. We achieve this through APIs that are proven, globally deployed, interoperable, agile, community developed, and certifiable. OIDF APIs currently serve 3 billion+ users and enable millions of applications. Our standards enable a broad array of use cases, and are most frequently found enabling the following use cases:

Login & Access

End user login e.g. Login with Google, Microsoft, Apple, Verizon, KDDI, GSMA Mobile Connect

Enterprise user login, e.g. Microsoft Azure, Okta/ Auth0, Ping Identity services

Online Banking & Open Data

· Enables national ecosystems to interoperate securely in: UK, Australia, Brazil, US (FDX), Russia

· In review or in development by government & private sectors globally including: Canada, Nigeria, Bahrain, Saudi Arabia, UAE, Japan, New Zealand

Health

· Sharing Medical Records in the US, UK, Norway

Anti-fraud

· Standardized sharing of signals and events in private sector used within and across digital platforms (Google, Microsoft, Amazon)

· Extensible to ecosystem-wide, and public sector identity implementations

In this context we are pleased to see that the ARF emphasized use of standards. We expect at least some of the EU Digital Identity Wallet proposals the EU will evaluate will leverage OpenID Foundation standards, and the OIDF offers its support to all entities that use our standards.

II. OIDF Standards Applicability

As the EU Digital Wallet technical committee considers standards and proposals, we would like to highlight how OIDF standards can serve the EU's Digital Wallet goals. In short, the OIDF offers the open standards for the EU Digital Wallet's interfaces to enable interoperability:

1. ARF requires interfaces between participants in a digital identity ecosystem
   - OIDF standards and profiles are mature, and fit for the EU's requirements

2. ARF requires consent-based, privacy preserving capabilities
   - OIDF standards and profiles can be configured to meet consent requirements as OpenID Connect has a mechanism to record and present the data receiver's privacy notice, and forcing consent as the lawful basis
   - Ensuring privacy-preserving ecosystems remains challenging; OIDF is keen to collaborate with the EU to close gaps

3. ARF requires support for both client-server and distributed deployment patterns
   - OIDF standards are well suited to enable both, and interoperability across them

OIDF believes implementations that focus on global standards and interoperability will be the most successful in serving the needs of the EU people (and people globally), and can deliver economy-wide benefit as a result.

III. Mapping ARF Requirements & OIDF Standards

We believe two of the foundations newer specifications are particularly well suited to the ARF requirements:

- **OpenID Connect for Identity Assurance**, a data structure to standardize communication of evidence and assurance.
  - ARF Requirements: PID Provision to Cloud Wallet, Cloud wallet to Relying Party, Conformance Testing
  - Description: A signed claims passing protocol with consent and verification meta data. The claim may be comprised of the individual's personal data such as First name, last name, date of birth, as well as metadata such as verified by whom, verified how, verified when, evidence used, and the policy followed. The individual consents to release claim(s) from a trusted entity, a signed claim object is generated, and it can be sent via a secure, interoperable protocol like OpenID Connect, Financial-Grade API, or a W3C VC/ blockchain protocol. Ecosystem participants can interoperate at scale via common interfaces, and use certification to ensure interoperation "just works."

- **OpenID Connect for Self Sovereign Identities**
  - ARF Requirement: Mobile Wallet to Relying Parties, Provision of (qualified) attribute attestations
  - Description: Standardises Self-Issued OpenID (Wallet) key exchange and authentication, and offers extensions that enable issuance and transport of verifiable credentials. As such, it is credential agnostic, such as enabling both W3C Verifiable Credentials and ISO 18013-5 Mobile Driving Licenses, and the suite of standards offer a bridge between well proven and deployed protocols like OIDC and emerging standards.

The following standards may also help address key requirements of the ARF, as follows:

- **OpenID Connect Core & Discovery**, authorization protocol that orchestrates authentication and consent
  - ARF Requirements: PID Provision to Cloud Wallet, PID Provision to Mobile Wallet, Cloud wallet to Relying Party, Mobile Wallet to Relying Party, Conformance Testing

- **Financial Grade API, specific configurations to mitigate security risks in OIDC**
  - ARF Requirements: PID Provision to Cloud Wallet, PID Provision to Mobile Wallet, Cloud wallet to Relying Party, Mobile Wallet to Relying Party, Conformance Testing
  - Description: FAPI has been selected and deployed by governments and private entities globally to enable Open Banking, Open Finance, and Open Data initiatives, such as in the UK, Brazil, Australia, US, and Russia and is in consideration in many more countries now.

- **OIDC Dynamic Client Registration**, specification that allows clients to register their meta-data including credentials and privacy notice and TOS locations for user protection.
  - ARF Requirements: PID Provision to Cloud Wallet, Cloud Wallet to Relying Party
  - Key privacy preserving capabilities embedded in the protocol.For example `policy_uri` and `tos_uri` are recommended to be included in the client registration data.They provide URIs of the privacy policy (privacy notice) and the terms of service so that the authentication server can retrieve and show/store them for the user. This also makes it possible for the server administrator to assess whether these are fair. By storing, it will also make it easier for the user to get back and hold the client accountable when they change those or misbehave.

- **OpenID for Authority,** extension that adds ability to present on-behalf-of information
  - ARF Requirements: PID Provision to Cloud Wallet

- **Shared Signals & Events**, standardized, privacy protected, secure webhooks for communicating risks & events.
  - ARF Requirements: PID Provision to Cloud Wallet, Cloud Wallet to Relying Party

- **Advanced Syntax for Claims**, extension that enables much richer data minimization
  - ARF Requirements: Cloud Wallet to Relying Party, PID Provision to Cloud Wallet

- **OIDC for Federation**, specification to enable multiple ecosystem parties to establish technical trust.
  - ARF Requirements: Entity Trust

We would be happy to speak directly about the specifications, how they could meet the ARF requirements, and address any gap closure that may be useful in the specifications or their accompanying certification test suites. More details on OIDF specifications are found on our website. (https://openid.net/developers/specs/)

IV. Feedback on Architecture & Reference Framework

This is a summary of our feedback based on topic areas, including those the ARF can highlight more clearly, and net-new additions. These comments are based on the OIDF communities lived experience of building successful, global, private and public sector ecosystems.

Primacy of the Individual

· Promote the principle of data minimization more clearly; collaborate with OIDF & others on standards & best practices

· Consider application of data portability rights, to export data from one wallet to another, while protecting data security

· Consider introducing Consumer Protection provisions

· Ensure consumer privacy & civil society groups contribute to the requirements

· Change language from a "legal person" (e.g. a company) being able to assert identity, to a natural person who can act on behalf of a "legal person" e.g. company

Interoperability

· To enable EU-wide adoption by individuals and relying parties, the ARF needs to emphasize the importance of interoperability

· EU should prioritize proposals that use interoperable standards, conformance testing, and certification

· OIDF highly recommends pursuit of standards that will enable global interoperability over time; individuals and businesses needs are global.

· Failure to enable interoperability may undermine the success of the program, as it has for identity ecosystems in the past

· A solution that leans into globally interoperable standards can benefit from accelerated acceptance and higher security, while ecosystem specific standards can slow adoption, be more exposed to attack, create a barrier to participant/ RP adoption, limit competition, and global interoperability.

Standards Lifecycle

· All standards move through an adoption curve, which can impact ecosystem success. Less mature standards will have a range of risks.

· A successful architecture & policy framework will allow for progression in standards, and ensure there is a mechanism to innovate while managing the technical, operational and cost burden of change.

Governance

· As EU moves to launch the program, there will be program and policy requirements that need to be operationalized and potentially automated, and established from the start:

· Participant roles, responsibilities, and rights

· Certification and conformance status

· Audit trail, tracking

· Metrics & reporting

Multi-protocol

· Not all standards deliver all use cases optimally

· Enabling multiple, parallel protocols can best serve ecosystem requirements

Fraud

· We recommend including anti-fraud requirements to the ARF, as signals that can be moved between the parties (in a privacy preserving manner) can enable:

· Timely mitigation against attacks and misuse

· Protect individuals & participating entities

· Reduce operational and reputation risks that undermine ecosystem trust.

Certification

· OIDF Certification test bed is open and free to use for EU entities to test their implementation deployment conforms, reducing ecosystem burden of achieving interoperability.

· Option to mandate or encourage self-certification at low cost ($1k member, $5k non-member).

· Option to partner on development and maintenance on EU specific profiles.

Proof of Concept

· Option to leverage the GAIN Proof of Concept Community Group to "prove out" interoperability of EU Digital Wallet implementation(s), with EU and global participants.

· The OIDF is a supporter of the Global Assured Identity Network, a vision for an assured identity layer to the internet. The initiative is facilitated by 5 non-profits including the OIDF. The OIDF is hosting the GAIN POC Community Group, a global group of technologists. The Community Group would welcome the opportunity to interoperably test EU Digital Wallet provider solutions against existing identity implementations using global standards.

· More information: https://openid.net/gainpoc/

V. OIDF standards are well recognized

It is worth highlighting that governments frequently select and implement OIDF standards and OIDF standards are well recognized by other leading standards bodies.

OIDF standards are commonly selected by governments, for example:

· UK, Australian, Brazilian governments selected the Financial-grade API to enable Open Banking/ Open Data implementations

· US, UK, Norway governments selected OIDC/ FAPI standards to enable movement of health records

· US government selected OIDC to enable 3rd party access to Social Security information and to enable federation of emergency response services across communication networks

Recognition from ISO, IEC and ITU-T

· OIDF is an organization with A.5 recognition meaning ITU-T can normatively refer to OIDF specifications

· OIDF is a Category A liaison organization to ISO/TC 68 and a Category C liaison organization to ISO/IEC JTC 1/SC 27/WG 5

· OIDF is underway to obtain Publicly Available Specification (PAS) submitter status with ISO/IEC

· OIDF & ISO are mutually interested in PAS status for several OIDF standards in 2022

Global Standards Alignment

· ETSI & OIDF are establishing a liaison relationship to progress OIDF standards, in line with EU Wallet requirements

· FIDO & OIDF standards are interoperable

· IETF & OIDF standards are interoperable

· W3C Verifiable Credentials are interoperable

· ISO 18013-5 Mobile Driving Licenses are interoperable with OIDC for SSI, and OpenID Connect is named in the ISO18013-5 spec as a data release method (Note: ISO eID & ICAO mPassport standards are still emerging, and could be interoperable with OIDF standards)

In service to our vision and mission, we are keen to support officials leading the EU Digital Wallet, the ART technical committee, and the EU Digital Wallet community to achieve their goals. We are happy to discuss our comments, the specifications, and opportunities to close any gaps. You may reach us at Director@oidf.org.

Sincerely,

Nat Sakimura

Chairman OpenID Foundation

Gail Hodges

Executive Director

OpenID Foundation

Helene VIGUE & Andrzej OCHOCKI (GSMA)

This position was submitted on behalf of the GSMA, specifically representing the European Mobile Network Operators involved in identity services in this instance (GSMA European Identity Group). We remain at your disposal should you have any questions.

The GSMA, specifically representing the European Mobile Network Operators involved in identity services in this instance, warmly welcomes the European Commission's initiative to revise and expand the eIDAS Regulation into the EUID framework. The consultation of private sector stakeholders in the elaboration of the Toolbox is welcome. The Architecture and Reference Framework Outline provides a solid basis for the European Digital Identity ecosystem. We recommend to expand and clarify certain aspects, as outlined below.

Section 2 OBJECTIVES OF THE EUID WALLET

Text from Framework document

"The eIDAS expert group has worked on a number of first use-case areas which include:

· Secure and trusted identification to access online services

· Mobilityanddigitaldrivinglicence

· Health

· Education / Diploma

· Digital Finance

· Digital Subscriptions"

Our analysis:

We suggest adding another first use case covering "Secure and trusted anonymous authentication to access online services" e.g. adding privacy to the well-known use case of authenticating into a website.

The digital subscription use case as mentioned in the document is a perfect example of digitising the KYC process. There are many SSI based examples in the telecommunication industry demonstrating this exact use case in governmental led projects e.g. Germany.

Section 3 ROLES IN THE ECOSYSTEM

Text from Framework document

Figure 1.

The potential roles of the EUDI Wallet ecosystem are described in Figure 1.

1 End Users of EUDI Wallets

2 EUDI Wallet Issuers

3 Person Identification Data Providers

4 Providers of registries of trusted sources

5 Qualified electronic attestation of attributes (QEAA) providers

6 Non-qualified electronic attestation of attributes (EAA) providers

7 Qualified and non-qualified certificate for electronic signature/seal providers

8 Providers of other trust services

9 Authentic sources

10 Relying parties

11 Conformity assessment bodies (CAB)

12 Supervisory bodies

13 Device manufacturers and related subsystems providers

14 Catalogue of attributes and schemes for the attestations of attribute providers

Our analysis:

For the wallet ecosystem to be a sustainable one driving innovation and economic growth across a wide range of industry actors, it is important to allow the emergence of solid business models. This requires a way for the distribution of monetary value between the different actors of a transaction while respecting the core principles set out by the European Commission (in particular security and privacy / minimization). This may require additional roles in the ecosystem.

In addition, the architecture should consider the role of Mobile Network Operators. Mobile Network Operators provide wallet authentication enablers. Mobile Network Operators also provide access to Secure Elements.

Finally, the governance entity role(s) should be considered in the architecture.

Section 3.3 PROVIDERS OF PERSON IDENTIFICATION DATA (PID)

As telecom providers we understand the PID is the identifier of the EUID wallet user. The MSISDN with its international routing characteristics should be considered as a universal way of addressing the EUID Wallet holding the PID information.

Section 3.5 QUALIFIED ELECTRONIC ATTESTATION OF ATTRIBUTES PROVIDERS

Text from Framework document

" QEAA providers would be required to provide information or the location of the services that can be used to enquire about the validity status of the QEAA, without having an ability to receive any information about the use of the attestations."

Our analysis:

Regarding the ability to receive any information about the use of the attestations, the business relationships between all the ecosystem roles e.g. attribute providers and relying parties require mechanisms that enable payments.

Section 3.6 NON-QUALIFIED ELECTRONIC ATTESTATION OF ATTRIBUTES PROVIDERS

Text from Framework document

"Depending on the domain rules, EAA providers may provide validity information about EAA, without having an ability to receive any information about the use of the EAA."

Our analysis:

Regarding the ability to receive any information about the use of the attestations, the business relationships between all the ecosystem roles e.g. attribute providers and relying parties require mechanisms that enable payments.

Section 3.7 QUALIFIED AND NON-QUALIFIED CERTIFICATES FOR ELECTRONIC SIGNATURE/SEAL PROVIDERS

Text from Framework document

"- The EUDI Wallet includes a qualified signature/seal creation device (QSCD), or

- It is a secure authentication tool as a part of a local or remote QSCD managed by a QTSP."

Our analysis:

We would like the Toolbox to clarify if the "secure authentication tool" is the EUDI wallet and if so, what the interface is between the EUDI Wallet and the QTSP.

Section 3.9 AUTHENTIC SOURCES

Text from Framework document

"The authentic sources in scope of Annex VI of the legislative proposal are sources for attributes on: address, age, gender, civil status, family composition, nationality, education and training qualifications titles and licenses, professional qualifications titles and licenses, public permits and licenses, financial and company data."

Our analysis:

Important authentic sources for relevant attributes are the mobile network operators, as the mobile operators possess the authentic information about the "mobile address" – the mobile phone number (MSISDN). Furthermore, other relevant attributes will be provided by network operators e.g. "trust indicators" based on network and device attributes which are linked to a natural person's mobile phone number (MSISDN). Location attributes are also available and could serve to protect end users against identity theft and fraud, with user consent. Attributes from mobile networks and indicators of the security of mobile devices can add another security layer to the Digital Identity ecosystem.

Section 3.10 RELYING PARTIES

Text from Framework document

"Relying parties may interact with EUDI Wallets via proxies or gateways like for example national authentication gateways or private sector authentication service providers."

Our analysis:

Proxies or gateways may create additional security and privacy issues that must be considered and therefore their role shall be scoped. For instance the revocation of an attribute may be more challenging.

Section 3.13 DEVICE MANUFACTURERS AND RELATED ENTITIES

Text from Framework document

"EUDI Wallets will have a number of interfaces with the devices they are based on, which may be for the following purposes:

• Local storage

• Online Internet access

• Sensors such as smartphone camera, IR sensors, microphones, etc.

• Offline communication channels such as Bluetooth Low Energy (BLE), WIFI Aware, Near Field Communication (NFC)

• Emitters such as screens, flashlights, speakers etc."

Our analysis:

Biometric sensors are used for access to the secure element and should be listed.

Section 4 FUNCTIONAL REQUIREMENTS

Text from Framework document

Figure 2

Our analysis:

Figure 2 should include the eID mean module such as the Secure Element (for instance SIM).

Section 4.3 CRYPTOGRAPHIC FUNCTIONS

Text from Framework document

"These functions may be used to manage:

• pseudonymous authentication of the user to relying parties."

Our analysis:

In line with our proposed change to include another first use case covering "Secure and trusted anonymous authentication to access online services" the requirement should be modified to "These functions **shall** be used to manage […].

Moreover pseudonymous authentication shall be clearly defined.

Section 4.3.2 Trusted environments

Text from Framework document

"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 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.

Identifying means to enforce a common standard to access a TEE or SE in the EUDI Wallet will be defined as it will provide higher level of trust to the whole implementation."

Our analysis:

Regarding the ability for the EUDI Wallet to rely on a TEE and SE, mobile network operators have been and are using the possibilities of the SIM and eSIM to identify the respective mobile device, its unique mobile phone number in the worldwide network and thus the user.

Moreover, we welcome the stated goal of relying on common standards to access a TEE or SE.

Section 4.4 MUTUAL AUTHENTICATION

Text from Framework document

"Additionally, this mutual identification and authentication shall be possible both online (over the Internet) and offline."

Our analysis:

We recognise the need to provide consumers with offline electronic identification and authentication, as essential services in a variety of sectors are often provided on the basis of face-to-face interaction. However, greater specification is needed concerning offline services. Some ambiguity remains as to whether offline functionality solely entails the use of a digital wallet for physical, face-to-face interactions. There is a risk that offline functionality may be interpreted as entailing that the user and/or verifier devices are not connected. We caution against such an interpretation, as authentication and identification support for non-connected devices incurs additional security risks, such as the inability to verify whether the validity of an identity has been revoked. Furthermore, the design, implementation and deployment of secure solutions for non-connected devices presents a level of challenge for multiple parties (standards, secure element makers, certification bodies, OEM, wallet developers and regulators) that is difficult considering the aim to secure a rapid widespread deployment of a compliant solution that benefits consumers.

Section 4.5 SELECTION, COMBINATION AND SHARING OF PERSON IDENTIFICATION DATA, QUALIFIED ELECTRONIC ATTESTATION OF ATTRIBUTES AND ELECTRONIC ATTESTATION OF ATTRIBUTES

Text from Framework document

"The EUDI Wallet shall make it impossible to collect information about the use of the wallet which are not necessary for the provision of the wallet services, […]

• 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."

Our analysis:

Clarification of the articulation between these two requirements shall be provided. Clarification of the second requirement vs 4.1 shall be provided.

Section 4.8 INTERFACES WITH EXTERNAL ENTITIES

Text from Framework document

Figure 3.

Our analysis:

Figure 3 should be completed with:

· Payment enabling party(ies)

· Conformity roles and responsibilities

Section 4.8.5 Device interfaces

Text from Framework document

"The EUDI Wallet will be comprised of one or several software and/or hardware components. Besides CSP (Cryptography Services Provider) components, which may provide cryptography services and storage capabilities (such as SE, SIM or appropriately evaluated software solutions), other hardware components on which the EUDI Wallet software runs, may be external to the EUDI Wallet and accessible through standardized interfaces."

Our analysis:

We support the mention of SIM, as a proven technology to provide cryptography services and storage capabilities.

Section 5 NON-FUNCTIONAL REQUIREMENTS OF THE EUDI WALLET

Text from Framework document

"As provided by the legislative proposal, EUDI Wallets **shall** be interoperable across the European Union and have externally oriented interfaces specified by common, technical standards. Certain use cases may require further international interoperability."

Our analysis:

Interoperability with international standards will ensure increased adoption. The requirements should be modified to "Certain use cases **shall** require further international interoperability". As the telecommunications industry, we can share our expertise in international interoperability.

OTHER COMMENTS

The general architecture seems to be missing a way to easily allow two wallets to interact securely upon user request. A role therefore seems to be missing for wallet discovery. As an example, with their country-based universal routing plan, MSISDNs could be used to discover wallets if they have been populated with MSISDN as a QEAA.

The necessary components for porting wallets across providers and devices shall be included in the framework.

We remain at your disposal to discuss our comments and contribute to the European Digital Identity initiative. You may reach us at identity@gsma.com

Sincerely,

Helene Vigue - Identity and Data Director, GSMA

Andrzej Ochocki - Chair of the European Identity Group, GSMA and Head of Identity, Deutsche Telekom