Brussels, 30 August 2021

# ECSAs response to the Commission's "Have Your Say" consultation On the Proposal for a Regulation establishing a framework for a European Digital Identity



ECSA e-ID Task Force Secretariat: European Savings and Retail Banking Group, Rue Marie-Thérèse 11, B - 1000 Brussels

Tel: + 32 2 211 11 26, E-mail: matteo.mannino@wsbi-esbg.org and diederik.bruggink@wsbi-esbg.org

Transparency register: 8765978796-80

## General comments

The European Credit Sector Associations (ECSAs) welcome the Commission proposal for a regulation establishing a framework for a European Digital Identity and the high ambitions presented in the initiative as a positive development.

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 decentralised model fosters personal autonomy and increased personal data protection, giving users control over their identity attributes. The overall benefits of trusted and distributed e-ID solutions in a society are significant.

Another positive aspect is that the regulation recognises that qualified electronic attestation of attributes shall be equivalent and have the same legal effects as lawfully issued attestations in paper format in any Member State, providing legal certainty to the use of innovative technology for validating documents.

Moreover, we believe the proposal will incentivise Member States to be more expedient in developing e-ID solutions with a wide scope of usage and potentially much higher adoption rate. It also provides grounds for some attributes to be validated against public sources. This is a welcome development, particularly as regards processes where a high level of assurance is necessary, e.g., the KYC process. When acting as relying parties, banks should be aware of the chain of trust in data sharing (including actors involved) and should be able to promptly check the validity of credentials.

The COVID-19 pandemic has been a catalyst for further digitalisation. Consequently, expectations concerning both the convenience and high security for any online activity such as remotely opening a bank account or applying for a loan have matured. The European digital identity will make it possible to offer quicker onboarding processes and better user experience while ensuring the same level of security as face-to-face onboarding processes. In the end it will contribute to further adoption of digital banking services. We appreciate that the Commission recognises the special role of the financial sector, particularly regarding the AML/CFT framework.

We emphasise that cooperation between the European Institutions, Member States and the private sector, including existing e-ID schemes, is needed. To achieve this objective, Member States should cooperate within the Toolbox for a coordinated approach towards a European Digital Identity Framework (Common Toolbox), where we believe that the European Digital Identity should build on existing (and upcoming) national notified e-ID solutions and extend



ECSA e-ID Task Force Secretariat: European Savings and Retail Banking Group, Rue Marie-Thérèse 11, B - 1000 Brussels

Tel: + 32 2 211 11 26, E-mail: matteo.mannino@wsbi-esbg.org and diederik.bruggink@wsbi-esbg.org

Transparency register: 8765978796-80

the possibility for their use to the private sector, respecting current solutions and a level playing field. However, the private sector (i.e., banks) should be enabled to accept the European Digital Identity Wallet (DIW) provided that there are adequate safeguards and an in-depth assessment of the possible aspects of the measures adopted.

Even if concerned for the wide scope of use-cases and the related costs to implement it in practice, we believe that the banking sector also needs to be involved in the toolbox, as it can play the important role of partner for the EU and all Member States in building up an adoption roadmap for the success of the initiative.

It will be key to establish a common technical architecture that enables 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. If the Common 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), and investments needed from the private sectors (e.g., European players will have to adapt to all the 27 national solutions). This is especially relevant since the private sector (i.e. banks) will have to accept the European Digital Identity Wallet.

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

Finally, the combination of new technology and new principles supported by regulation can help decreasing the massive pressure from the global platform players. The distributed architecture and European approach will help all PSPs and particularly those operating at the European level, thus reducing complexity and improving customer experience.

Moreover, security and customer experience could be enhanced by using the proposed wallet on top of existing security layers, instead of existing solutions usually based just on usernames and passwords.



ECSA e-ID Task Force Secretariat: European Savings and Retail Banking Group, Rue Marie-Thérèse 11, B - 1000 Brussels

Tel: + 32 2 211 11 26, E-mail: matteo.mannino@wsbi-esbg.org and diederik.bruggink@wsbi-esbg.org

Transparency register: 8765978796-80

## Detailed comments

- **Technology and current regulation**

The proposed regulation contains many positive developments. There are however certain aspects to be highlighted in order to prevent any unforeseen negative outcomes.

There could be some challenges in terms of achieving common standards. For example, rules surrounding legal representation and power of attorney might differ between Member States, which could render standardisation difficult.

The vast majority of the needs of electronic identity and remote authentication remain with the private sector, in particular in areas like banking where the law imposes strict rules of verification of customers' identity. This evidence makes clear the need of a strict collaboration between European commission, MSs and Financial sector representatives.

Further, we believe that the difference between identification and authentication should be made clear in the proposal. We consider that identification, verification and authentication are different processes referring to different phases of the relationship between the bank and the customer. Identification is needed to confirm the identity of a certain subject, who could be unknown to the bank in order to start a continuous relationship, verification is the process of ensuring that a person is who they claim to be while authentication refers to the modality that a certain client, previously identified, uses to prove his/her identity to the bank through a remote service in order to operate a payment or other activities.

The obligation to accept ID wallets for authentication in any service where strong customer authentication is legally required (Art. 12b.2) does not consider the many special requirements for the banking industry to dynamically secure banking transactions (PSD2 RTS – Commission Delegated Regulation EU 20219/389). In case of obligation, ID wallets should include authentication mechanisms and artifacts that ensure its applicability for performing SCA -strong customer authentication- under PSD2 RTSs. This would facilitate the use of the digital wallets for payment purposes according to PSD2 requirements, as well as it would increase the security of the European digital identity wallets. Furthermore, operational aspects of ID acceptance from another Member State are unclear, as well as whether this acceptance would be made through eIDAS nodes. For this reason, we believe that the banking industry's direct participation in the activity of creation of the Toolbox is of paramount importance. We urge the Commission to include the banking sector in the process.



ECSA e-ID Task Force Secretariat: European Savings and Retail Banking Group, Rue Marie-Thérèse 11, B - 1000 Brussels

Tel: + 32 2 211 11 26, E-mail: matteo.mannino@wsbi-esbg.org and diederik.bruggink@wsbi-esbg.org

Transparency register: 8765978796-80

The physical separation and storage of ID credentials and data from other services could also pose a problem to the use of the DIW for payment services. For example, when a bank wants to become an EDIW issuer, according to the physical separation requirement, this has to be accomplished via a separate (legal) entity, which is an unnecessary burden at least for the attributes/credentials which are directly issued by the banks themselves.

Considering the unparalleled DIW experience at global level, for payments (especially cards payments) there is also the chance to impact interoperability with global standards, which will need to be updated before starting a European development. It is also unclear how the remuneration and liability for payments will be impacted, e.g. the authentication activity would now involve different actors.

For the combination of the wallet technology and new principles backed by regulation, the Digital Markets Act (DMA) has a significant impact in reducing dependency on global platform players as architecture needs to be open and free of charge for market participants. The distributed architecture and the self-determined principles can help reduce the concentration risk in the platform and ecosystem space. The distributed architecture and EU approach will help the financial sector to facilitate customer onboarding/remote access to financial services and to improve customer experience overall.

We underline the need to coordinate the eIDAS Regulation contents with other regulations that could interplay with it, such as AML, data protection, PSD2, etc. and avoid any overlaps or incongruences among them. In the banking sector, considering the different steps of an electronic identification scheme, identification and authentication do not require the same level of assurance. Identification is made at level substantial/high, whereas authentication to banking platforms during the account life cycle is under different rules, such as dynamic IT security. As foreseen by PSD2, for the authentication activity it should be possible to proceed under a risk-based approach, as suggested by the FATF, and, for specific low-risk use cases, to assist a Substantial Level of Assurance.

Moreover, a level playing field between PSD2 actors and the new wallet issuer when providing SCA for payments must be guaranteed. The same level of requirements should be applicable to both PSD2 actors and EDIW issuers when pretending to offer SCA for payments.

We express concerns about the mandatory acceptance of the DIW for payments systems, especially in cards payments, considering their impact, which could result in reducing customer experience, and also in additional investments needed from the merchant sector on the acquiring side.

In order to address Point of Sale (POS) and Point of Interaction (POI) requirements, the person must have the ability to load payment account (and credit card) attributes into their



ECSA e-ID Task Force Secretariat: European Savings and Retail Banking Group, Rue Marie-Thérèse 11, B - 1000 Brussels

Tel: + 32 2 211 11 26, E-mail: matteo.mannino@wsbi-esbg.org and diederik.bruggink@wsbi-esbg.org

Transparency register: 8765978796-80

EDIW for all their ASPSPs. This is to allow them to select the account/card attribute they wish to use for the payment.

To prevent any solution to prevail over another without leaving room for the needed competition, a principle similar to the "card application selection" as per Interchange Fee Regulation should apply: the EDIW must not recommend or prioritise account/card attributes issued by one provider over another. The person holding the EDIW must have the ability to sequence/sort their attributes for selection purposes.

In case the ID wallet acceptance by payments service providers should be considered mandatory, the banking sector raises concerns, and will need to evaluate the impact on customer journeys, on banking infrastructure and investments, as well as on the possible implementation timelines. In the meantime, it is our understanding that it will be left to the service provider and to the service user to choose which authentication systems to rely on.

Due regard should also be given to data management and to how the processing and storage of the data will be regulated where all of the data concerning a person will be routed through the wallet, under the direct control of the customer. For example, banks would be required to store certain data in their roles as credential issuers, or because the user has specifically shared it with them. This data could possibly be forwarded to third parties via the wallet. There is also need for harmonisation with AML/CFT identification data and interpretations, as well as with regards to issues of retention periods under the AML/CFT framework and storage limitation under the GDPR. Auditing costs and red tape offering eIDAS Trust Services should be minimised.

Wallet-based technologies are new and not yet widely proven. The new approach should keep favouring ID initiatives from the financial sector and not impose the discontinuation of certain existing ones that could be less secure but still fit for their purpose. Considering the wallet acceptance costs for the European banking sector (e.g., investments in IT for implementing the wallet acceptance, banking staff training, customer communications, etc.), there is a need to ensure that such investments should be acceptable from a business perspective. Therefore, the involved providers should be allowed to recover the costs incurred or be remunerated in a different way.

A DIW should allow citizens to identify themselves in order to access services and information (public as well as private), not in itself provide services or service-like functions. Hence, it is important that DIW use-cases focus strictly on providing valid personal identification credentials, and does not (unintendedly) force banks/other commercial service providers to add additional (commercial) data or services to a DIW.



ECSA e-ID Task Force Secretariat: European Savings and Retail Banking Group, Rue Marie-Thérèse 11, B - 1000 Brussels

Tel: + 32 2 211 11 26, E-mail: matteo.mannino@wsbi-esbg.org and diederik.bruggink@wsbi-esbg.org

Transparency register: 8765978796-80

From an implementation standpoint, the very wide scope also increases project and implementation risks, which may be difficult and/or costly to mitigate. In general, our recommendation would thus be to pursue an agile and stepwise implementation, for example identifying core use cases, rather than a comprehensive "big-bang" implementation, which poses significant implementation risks (and in turn costs). For legal harmonisation, identification itself should be defined as a trust service.

Finally, according to the proposal only those attributes issued by a qualified trust service provider (QTSPs) will be considered qualified. Besides those, the proposal should also include that attributes provided by the authentic sources should also be considered qualified or at least have the same legal effects attributed to the qualified ones. This would be the case for example for customers financial data attributes issued by financial institutions.

- **Scheme**

European banks, as represented by the three ECSAs, in general support having a common European e-ID architecture, since according to us having 27 (or more) substantially different solutions does not benefit consumers or our societies. However, harmonisation should not entail introducing a one-size-fits-all solution. In our view, this would not support the intentions behind the proposal, as it would likely hamper innovation. Moreover, it will probably also lead to an overly expensive and inefficient solution.

The mandatory acceptance of all offline authorisation systems for the ID wallet would have a huge impact on the whole industry (i.e., mandatory for entry control, etc.). Business cases should be clearly defined for both the national and the international levels taking into consideration the sustainability aspects. The presence of a liability framework is mandatory before an obligation to apply the ID wallets in private sector applications takes place. For payments in general, European dispute resolution mechanisms for the DIW need to be discussed in the Toolbox.

Secondly, the ambition for the DIW to use Qualified Certificates (highest assurance level) may be challenging. While in principle a positive aspect, this is not currently the standard in bank-owned e-ID solutions, could be solved with a risk-based approach in usage, as mentioned before in the section "Technology and current regulation".

These solutions are widespread, and are being used for both banking purposes and other use-cases, including also public services. Hence, private issuers will have to comply with stricter regulatory requirements, be subject to significant additional investments and operational costs, and importantly take on increased liabilities for the use/misuse of the signature in question. This must be duly considered when developing business models and fee structure



ECSA e-ID Task Force Secretariat: European Savings and Retail Banking Group, Rue Marie-Thérèse 11, B - 1000 Brussels

Tel: + 32 2 211 11 26, E-mail: matteo.mannino@wsbi-esbg.org and diederik.bruggink@wsbi-esbg.org

Transparency register: 8765978796-80

for the DIW. Being part of a European DIW should be an incentive, also for privately owned e-ID schemes.

There is a strong need to establish 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). We strongly believe this needs to be done within the Common Toolbox taking into account national experiences. Those rules should be decided at the Common Toolbox level, as setting them up at national level could result in potentially having 27 different procedures.

It should be clarified how the DIW approach will fit in the already existing EU projects, for example the ones related to the creation of a European payments scheme, or the digital euro.

- **Trust and uptake**

Overall, the proposal raises many practical questions and much of the details remain to be worked out. This might lead to delays and/or a strained process leading to a compromised outcome. A general concern would be uptake. Wallet download and usage seems to be voluntary for EU citizens, but mandatory acceptance is required for businesses. There is a risk of large investments in a product whose adoption is neither easily foreseeable nor quick enough. Many Member States have already experienced this with their identity card efforts (to note that this card is not free of charge in some Member States). European and national authorities should consider creating a sound business case for involved operators, incentives and increased publicity to promote uptake.

Another aspect to look at is the interaction with third parties. Allowing interaction with third parties (e.g., as relying parties) using the DIW will be complicated for security and legal aspects, particularly in case there is no established comprehensive liability framework that clearly defines responsibility.

To protect users from fraud and prevent the unlawful use of identity data and electronic attestations of attributes as well as to ensure that the processing of data, like financial data, Relying Parties should communicate their intent to rely on the European Digital Identity Wallets. Relying parties have also to be considered liable for the misuse of that the data received by the Financial Sector.

National authorities should work on certification/audits in a coherent and coordinated way with the financial sector. This requires creating an ecosystem of interoperability that respects the security of the end-user and the investments already made by the industry. Moreover, creating a "PCIssc like" security standardization context role for the EUid contents should be



ECSA e-ID Task Force Secretariat: European Savings and Retail Banking Group, Rue Marie-Thérèse 11, B - 1000 Brussels

Tel: + 32 2 211 11 26, E-mail: matteo.mannino@wsbi-esbg.org and diederik.bruggink@wsbi-esbg.org

Transparency register: 8765978796-80

considered to get a fully harmonised European-wide certification process, without any room for different interpretation in detail.

On the opposite side, the uptake of the proposal could be very limited unless there is a multitude of use cases/relying parties. In this context, an approach is missing to facilitate private businesses (e.g., SMEs) becoming relying parties given the obligation for relying parties to communicate to relevant Member States their intention to rely on and inform about the intended use of the European DIW (see Art. 6b of proposed regulation).

For a private actor become Relying Party, and so accepting e-ID Wallet, should be as easy as accepting a card payment, where the merchant can access the payment systems via a trusted partner, e.g. the acquirer.

The definition of "digital document archive service" should be limited, e.g. to "ID documents" or specified lists. Should this not be the case, any electronic archive could be interpreted to fall in scope of the proposal, which would clearly go beyond its intended purpose.

Also the definition of electronic ledger needs to be specified, otherwise every structured database, e.g. booking system, would be covered from the new eIDAS. The security model, as well as applied cryptography and long-term cryptographic life cycle, should include the actual development of quantum computing for mandatory lifetimes of documents.

An approach is also missing to allow SMEs to be trusted by European citizens for digital commerce activities. SMEs as legal persons could also use their "Verifiable Credentials" with prospective customers (e.g., in e-commerce transactions when using EUid) but this approach is today missing in the new Digital Identity proposal.

Furthermore, non-harmonised certification and interpretation of the regulation and certification rules due to different authorities could cause fragmentation.

Finally, we welcome the European Commission's aim to implement a European Digital Identity as soon as possible but the proposed deadline for implementation of 12 months after entry into force might be unrealistic – the timeline is ambitious and in some parts conflicting. The wallet app is supposed to appear on the market at roughly the same time its requirements are defined. An evaluation of a successful broad deployment of the ID wallets only 6 months (Art. 12b.5) after the interface specifications are provided will not be very meaningful. Discussion on the timeline based on the outcome of the Toolbox is needed, although we encourage legislators to achieve the implementation of this regulatory initiative the sooner the better.



ECSA e-ID Task Force Secretariat: European Savings and Retail Banking Group, Rue Marie-Thérèse 11, B - 1000 Brussels

Tel: + 32 2 211 11 26, E-mail: matteo.mannino@wsbi-esbg.org and diederik.bruggink@wsbi-esbg.org

Transparency register: 8765978796-80

## Final remarks

The ECSAs believe that the involvement of the financial sector in the standardisation process it is of paramount importance so that its specificities are taken into account and that a certain flexibility towards new challenges and technologies is taken into consideration.

The financial industry should play an important role in the ecosystem, in the design and implementation of the wallet.

While pursuing a neutral position on the technology used, we believe that the use of the "attributes" of eIDAS digital identities can be enabled, also using the support of innovative technologies such as DLT, to allow the subscription of new services, including banking services. The financial services sector has sound policies and regulations in place to be trusted data custodians and are capable of securely managing digital identity data attributes (proper due diligence, protect personal information, reduce the risk of misuse of personal information by criminals, and ultimately ensure financial stability). We have already developed reliable onboarding processes with the highest levels of security, and the branch network offers the necessary physical proximity for the document validation process, in case it is needed. Banks should also be allowed to provide their own wallets and integrate ID wallets into their banking apps, without the burden of a separation of data storage.

Private identity wallets which comply with requirements set in this Regulation should be recognized by Member States as European Digital Identity Wallets, and therefore accepted across the EU according to Article 12b.

Moreover, precisely because we consider Digital Identity as a catalyst for energy and investment in PSPs' processes, we recommend that the significant investments that the banking industry has made in recent years to secure processes should not be compromised by the introduction of new rules.



ECSA e-ID Task Force Secretariat: European Savings and Retail Banking Group, Rue Marie-Thérèse 11, B - 1000 Brussels

Tel: + 32 2 211 11 26, E-mail: matteo.mannino@wsbi-esbg.org and diederik.bruggink@wsbi-esbg.org

Transparency register: 8765978796-80