EUROSMART
The Voice of the Digital Security Industry

European digital identity framework

Eurosmart's recommendations on Council's general approach for the interinstitutional discussions

The Council of the European Union announced, on 6 December 2022, the adoption of its general approach on the Proposal for a Regulation amending Regulation (EU) No 910/2014 as regards Establishing a Framework for a European Digital Identity.

Ahead of the interinstitutional discussions (Trilogues), Eurosmart shares its policy and technical position to initiate an active debate between the co-legislators.

The European Digital Security industry is pleased that the legislative process is progressing. The current Council's position constitutes a real improvement; however, it falls short of addressing some of the concerns shared between different stakeholders represented by Eurosmart.

Executive summary

Eurosmart calls upon the co-legislators to carefully review some essential provisions with regards to

1. *EU digital wallet's level of assurance*

   Eurosmart supports the interaction of the wallet with national electronic identification schemes and means. This approach allows the wallet to rely on electronic identification means (e.g. electronic identity document) to carry out an electronic authentication with the strength matching the level of assurance "high". Moreover, Eurosmart welcomes the generic principle whereby the on-boarding of a wallet with a level of assurance "high" could be achieved using an electronic identification means of level of assurance "high" or "substantial".

2. *Security Certification*

   Eurosmart recommends requesting as soon as possible new security certification schemes to ENISA under the Cybersecurity Act (Regulation 2019/881) covering, security certification of software, biometric technologies, services, and process.

3. *Access to hardware and software features including the Secure Element*

   To ensure consistency, Eurosmart considers that the exemption decided by the Member States for relying parties to authenticate to the wallet should be subject to an implementing act. The rules for exemption should also match the requirements for data protection (decided by the Member State where the wallet is issued).

4. *Notification of relying parties*

   Eurosmart recommends adding providers of electronic identification means as business users of gatekeepers within the meaning of the respective definition in the Digital Market Act. Moreover, additional provisions should be included to avoid gatekeepers claiming unjustified potential security risks to refuse access to virtual assistants, software components, hardware components and operating systems.

5. *The alternate possibilities to issue electronic attestation of attributes by public bodies*

   Eurosmart welcomes the possibility that electronic attestation of attributes, with the same legal effects as a qualified electronic attestation of attributes, may be issued to the Wallet directly by the public sector body responsible for the authentic source or by a designated public sector body on behalf of a public sector body responsible for an authentic source.

6. *Record Matching*

   The proposed definition of record matching in article 3(55) remains unclear and introduces substantial ambiguities. Eurosmart recommends using the following definition: "Record matching means a process where person identification data or unique and persistent identifier are matched with or linked to an existing account belonging to the same person."

1. EU digital wallet's level of assurance

Eurosmart very much welcomes the following provisions introduced by the Council in its General Approach:

- In provision 6b, the Council has introduced the possibility for Member States to provide additional functionalities in the wallet. Eurosmart supports this approach. This provision will allow including within the wallet "add-on", for instance, to:
  - **Interact with national electronic identification schemes and electronic identification means** in order to leverage on the existing infrastructure deployed under eIDAS 1. In particular, it allows the wallet to rely on electronic identification means (e.g. electronic identity document such as an electronic identity card) to carry out an electronic authentication with the strength matching the level of assurance "high" where the electronic identification means securely stores the authentication key and the wallet uses the cryptographic services of the electronic identification means to carry out the authentication at level of assurance "high". For instance, this could be achieved with a mobile phone using an electronic identity card through NFC.
  - **Interact with an electronic identity document** (electronic identity card, electronic passport...) to carry out the holder identity verification in the course of the wallet onboarding. This stage makes use of the holder's portrait securely stored in the electronic identity document, which is read by the wallet/mobile phone using NFC.
- In provision 11a, the Council has introduced a generic principle whereby the on-boarding of a wallet with a level of assurance "high" could be achieved using an electronic identification means of level of assurance "high" or "substantial" with additional remote on-boarding procedures that together meet the requirements of level of assurance "high". This positive provision will definitely support a massive adoption and uptake of the wallet by relying on existing notified electronic identification schemes, which are mostly at level of assurance "substantial" or "high". Eurosmart very much welcomes this approach. However, Eurosmart would like to highlight that unlike other similar provisions in the text requiring the European Commission to establish specifications through implementing act, this one does not set any timeline for establishing such specifications. As for the other similar provisions relating to the wallet implementation, these specifications should be established within 6 months of entering into force of this Regulation as they are instrumental for implementing and deploying the wallet.

2. Security Certification

As proposed in article 6c, the security certification approach should acknowledge a concentric approach for security. In particular, it shall be required that all the critical security functions of the wallet, including cryptographic algorithms as well as cryptographic key storage and management, be security certified at the highest level, i.e., "high" pursuant to the Regulation (EU) No 2019/881 (Cybersecurity Act) using EU CC scheme with assurance component AVA_VAN.5.

Besides, the security certification of the wallet will require several European Cybersecurity certification schemes issued under the Cybersecurity Act. The wallet will indeed be a combination of (1) different technologies (e.g. software, hardware, cloud, biometry...), (2) services (e.g. provision of qualified signature) and (3) processes (e.g. for on-boarding). Currently, only two security certification schemes should be made available soon: EUCC (Common Criteria) and EUCS (cloud), which are insufficient to address the wallet's needs.

> *Eurosmart recommends requesting as soon as possible new security certification schemes to ENISA under the Cybersecurity Act (Regulation 2019/881) covering in particular, security certification of software, biometric technologies, services and process.*

3. Access to hardware and software features including the Secure Element

The Council general approach has included an explicit articulation with the Digital Market Act (DMA) (Regulation (EU) 2022/1925) to ensure access to hardware and software features as part of core platform services provided by gatekeepers. The Council has provided new elements:

- Article 12b, clarifies that providers of Wallets and issuers of notified electronic identification means acting in a commercial or professional capacity are business users of gatekeepers within the meaning of the respective definition in the DMA.
- New Recital 20 specifies that gatekeepers should be required to ensure, free of charge, effective interoperability with, and access for the purposes of interoperability to, the same operating system, hardware or software features that are available or used in the provision of its own complementary and supporting services.

Eurosmart considers that these elements are not sufficient. First, this provision is paramount not only for wallet issuers but also for providers of wallet (the ones that develop the technical solutions). Likewise, it should also apply to providers of electronic identification means, which must be guaranteed the benefits of the DMA during the development of the electronic identification means. This approach also implies that the developer of electronic identification means should enjoy this provision BEFORE its notification, as the capacity to develop the electronic identification mean is a prerequisite to its notification. In addition, these provisions should also apply to (1) qualified trust service providers and (2) providers of Qualified Signature Creation Devices (QSCD) and (3) providers of Qualified Seal Creation Devices (QSCD). Therefore, the text should be reworded as follows:

> *"Issuers of European Digital Identity Wallets, issuers of electronic identification means, providers of European Digital Identity Wallets, providers of electronic identification means, providers of qualified signature creation device, providers of qualified trust services acting in a commercial or professional capacity and using core platform services as defined in Article 2(2) of Regulation (EU) 2022/1925 for the purpose of, or in the course of, providing European Digital Identity Wallet services, electronic identification means, or qualified trust services to end-users are business users in accordance with Art.2(21) or Regulation (EU) 2022/1925."*

4. Access to hardware and software features including the Secure Element

The Council general approach has included an explicit articulation with the Digital Market Act (DMA) (Regulation (EU) 2022/1925) to ensure access to hardware and software features as part of core platform services provided by gatekeepers. The Council has provided new elements:

- Article 12b, clarifies that providers of Wallets and issuers of notified electronic identification means acting in a commercial or professional capacity are business users of gatekeepers within the meaning of the respective definition in the DMA.
- New Recital 20 specifies that gatekeepers should be required to ensure, free of charge, effective interoperability with, and access for the purposes of interoperability to, the same operating system, hardware or software features that are available or used in the provision of its own complementary and supporting services.

Eurosmart considers that these elements are not sufficient. First, this provision is paramount not only for wallet issuers but also for providers of wallet (the ones that develop the technical solutions). Likewise, it should also apply to providers of electronic identification means, which must be guaranteed the benefits of the DMA during the development of the electronic identification means. This approach also implies that the developer of electronic identification means should enjoy this provision BEFORE its notification, as the capacity to develop the electronic identification mean is a prerequisite to its notification. In addition, these provisions should also apply to (1) qualified trust service providers and (2) providers of Qualified Signature Creation Devices (QSCD) and (3) providers of Qualified Seal Creation Devices (QSCD). Therefore, the text should be reworded as follows:

> *"Issuers of European Digital Identity Wallets, issuers of electronic identification means, providers of European Digital Identity Wallets, providers of electronic identification means, providers of qualified signature creation device, providers of qualified trust services acting in a commercial or professional capacity and using core platform services as defined in Article 2(2) of Regulation (EU) 2022/1925 for the purpose of, or in the course of, providing European Digital Identity Wallet services, electronic identification means, or qualified trust services to end-users are business users in accordance with Art.2(21) or Regulation (EU) 2022/1925."*

Besides, article 6(7) of the DMA clarifies under which conditions a gatekeeper may refuse or limit access to core platform services, "[t]he gatekeeper shall not be prevented from taking strictly necessary and proportionate measures to ensure that interoperability does not compromise the integrity of the operating system, virtual assistant, hardware or software features provided by the gatekeeper, provided that such measures are duly justified by the gatekeeper". Security is an essential aspect of integrity requirements.

Nevertheless, gatekeepers shall not use potential security risks as a pretext to refuse access to virtual assistants, software components, hardware components and operating systems. In the past, some gatekeepers invoked potential security issues to deny access to hardware or software features (related to mobile payment solutions). After a preliminary investigation, the European Commission concluded that the security risk was not demonstrated. Pursuant to eIDAS, European Digital Identity Wallets, electronic identification means, qualified signature creation devices and qualified trust services have to meet a high level of security and undergo security certification. **Therefore, they shall be presumed as not compromising the security** – and thus integrity – of the operating system, virtual assistant, hardware or software features provided by the gatekeeper. Should a gatekeeper claim that security risks exist, it shall provide reasonable evidence to the European Commission. Therefore, the following provisions should also be inserted in this article:

> *"Gatekeepers, as defined in Article 2(2) of Regulation (EU) 2022/1925, shall not prevent organisations providing European Digital Identity Wallets, electronic identification means, qualified signature creation devices and qualified trust services from accessing*

> *operating systems, virtual assistants, hardware and software features on security grounds, unless they present reasonable evidence to the European Commission."*

5. Alternate possibilities to issue electronic attestation of attributes by public bodies

The Council general approach introduced the possibility that electronic attestation of attributes, with the same legal effects as a qualified electronic attestation of attributes, may be issued to the Wallet directly by the public sector body responsible for the authentic source or by a designated public sector body on behalf of a public sector body responsible for an authentic source.

Eurosmart considers introducing this new type of attestation by the Council as a very positive headway. It allows the public sector responsible for authentic sources to issue attestations of attributes contained in these authentic sources. In addition, these attestations have the same legal value as qualified electronic attestations of attributes and lawfully issued attestations in paper format.

This new possibility brings three main benefits:

- It allows Member States to directly issue by themselves attestations with a high level of trust to their citizens, which could be considered as a form of public service in some Member States;
- It gives the possibility for Member States to ensure a high level of protection of authentic sources (which may be very sensitive) by restricting their access to the public sector only, and limiting private providers of qualified electronic attestations of attributes to have access to them;
- It acknowledges that for some specific types of attestations, only Member States shall be allowed to issue them. It is especially the case for those representing an authorisation or right recognised by laws.

Besides, this new kind of attestation brings a higher level of trust than qualified electronic attestations of attributes as the former is based on an attribute which has been verified against an authentic source, which is not necessarily the case for qualified electronic attestations of attributes: the issuance of a qualified electronic attestation of attributes does not require to verify the said attribute in the authentic source.

Consequently, as the issuance of qualified electronic attestations of attributes does not require to verify the attribute(s) in an authentic source - or even to have access to the said authentic source, it may be very useful for relying parties accepting qualified electronic attestations of attributes to know (1) whether the attribute has been verified in an authentic source or not, as well as (2) the identification of the authentic source to assess the level of trust to put in the attribute and ultimately carry out their own risk analysis and management. For that purpose, annex V should be amended accordingly to include the following field: "field indicating (1) whether the attribute(s) has/have been verified within an authentic source as well as (2) a unique identification of the authentic source(s) where the attribute(s) has/have been verified".

6. Record Matching

The proposed definition of record matching in article 3(55) remains unclear and introduces substantial ambiguities:

- First, it introduces the term “person identification means”, which is undefined. What does it refer to?
- Secondly, the proposed definition mixes up the nature of the data used to carry out record matching (e.g., person identification data) and the technical shape of the data (qualified attestations and attestations). Having a definition of “record matching” that refers to both the nature of the data and the technical shape creates confusion, as it does not clearly identify the very nature of the data at stake to carry out record matching. In that regard, it would be advisable to rely only on the very nature of the data, not its technical shape. The definition should be clarified by leveraging the concept of “unique and persistent identifier” as introduced in article 3(55a) and rewritten as follows:

  > *“Record matching means a process where person identification data or unique and persistent identifier are matched with or linked to an existing account belonging to the same person.”*

Moreover, article 11a, dealing with record matching, also raises some questions regarding the implementation of record matching and unique identification.

- Pursuant to 1, when acting as relying party, (any) Member States shall ensure record matching when a wallet is used for authentication. The statement applies to any Member State;

- Pursuant to 2, at least one unique and persistent identifier shall be included in the PID stored in the wallet. The purpose of the unique and persistent identifier is to allow record matching;

- Pursuant to 2aa, the unique and persistent identifier in the wallet may be changed upon user request;

If the unique and persistent identifier stored in the person identification data in the wallet is updated as provided in 2aa) during the lifetime of the wallet, it may hamper the capacity of Member States which are not the ones in charge of ensuring unique identification of individual to carry out record matching, as they would not be able to reconcile old unique and persistent identifier and new unique and persistent identifier. This situation creates a significant hurdle to effective record matching.

In addition, provision 1 requires Member States, when acting as relying parties to ensure record matching. Experience has demonstrated that it is not always possible to achieve record matching using electronic identification means defined by Regulation (EU) No 910/2014 (eIDAS I). Therefore, it is likely that this requirement entails changes in the existing electronic identity schemes and electronic identification means on the field, which may (1) break backward compatibility and (2) require to change electronic identification means.

About us

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

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com
@Eurosmart_EU
@Eurosmart

Square de Meeûs 35 | 1000 Brussels | Belgium
Tel +32 2 895 36 56 | mail Contact@eurosmart.com