EUROSMART
The Voice of the Digital Security Industry

Feedback on the revision of eIDAS

Introduction

Eurosmart would like to thank the European Commission for the opportunity to comment on the proposal for a Regulation establishing a framework for a European Digital Identity[1]. Eurosmart welcomes this new proposal, which aims at providing every EU citizen with a sovereign, secure and privacy-preserving digital identity.

Eurosmart particularly appreciates the following points:

- possibility to use a European cybersecurity scheme pursuant to the Cybersecurity Act to demonstrate compliance with the cybersecurity requirements for the Wallets
- possibility to use a European cybersecurity scheme pursuant to the Cybersecurity Act instead of the peer review for (part of) electronic identification schemes
- strong focus on data protection for Wallets and attestation of attributes
- mandatory notification by Member States of at least one electronic identification scheme at Level of Assurance (LoA) High
- mandatory issuance of a European Digital Identity Wallet in every Member State
- mandatory acceptance of the Wallet by big players and key sectors
- acknowledgment and answer to the need for harmonisation of digital identities for IoT devices
- obligation for web browsers to accept and recognise the eIDAS qualified website authentication certificates

Eurosmart wishes to make the following recommendations for the proposal:

Smooth transition from eIDAS I to eIDAS 2

First, Eurosmart would like to underline that it is essential to avoid having a single point of failure within the new framework. This is one of the main strengths of the current model of nodes, which is federated and not centralised. This model should remain for the transition period at least.

[1] Proposal for a 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, 2021/0136 (COD).

Secondly, for a smooth transition, Eurosmart stresses that eIDAS players (Member States, service providers, technology providers etc.) will need time to adjust to the new framework, including for the development, setting up and issuance of a Wallet (Article 6a(1)) and the development, setting up and notification of a scheme at level "High" (Article 7). This is particularly the case if the former implementing acts are repealed and replaced by new ones. Eurosmart believes that a period of transition of at least three years is needed. The European Commission proposed a transition period of 12 months -after entry into force- for Wallet issuance, mandatory notification of an electronic identification scheme, cooperation between Supervisory Authorities. This is an extremely short amount of time. In Eurosmart's views, three years -after entry into force- would be more reasonable to put in place such a new framework.

Thirdly, Eurosmart recommends introducing in Article 51 the possibility for qualified trust service providers and qualified trust services under eIDAS 1 to remain qualified under eIDAS2 until the expiry of their validity period, starting from the moment where all the corresponding implementing acts are enacted. This would ensure that the trust service ecosystem is not disrupted during the transition period. Qualified trust service providers and qualified trust services would comply with all new requirements for the renewal of their audit (every 24 months).

Clear definition of attribute and credential

Eurosmart observes that the proposal defines attributes and credentials in Article 3 (point 43 and point 52). An attribute is "a feature, characteristic or quality of a natural or legal person or of an entity, in electronic form". A credential is "a proof of a person's abilities, experience, right or permission". Both definitions do not seem precise enough and should rely on existing standards (see Annex). Attributes and credentials are often cited together in the text, meaning that they are considered as different concepts, although unprecise. The distinction between attributes and credentials should be clarified. For the Wallet, only the concept of attribute is mentioned in Article 6a(3), not the concept of credentials, which seems missing.

Furthermore, Eurosmart notes that the relation between an attribute, a credential and personal data is unclear at this stage. Therefore, it is not clear whenever GDPR should apply. The legal definition of data and data protection should remain, GDPR should apply to attributes and credentials. Eurosmart recommends clarifying the link between attributes, credentials, and personal data in the text. Guidance from the EDPS and EDPB would also be much welcome.

Strengthened sovereignty

Electronic identification schemes

One of the key principles is that Member States should remain in control of digital identities. They have historically issued and managed proof of identity, and have put in place reliable processes and resources (e.g. birth registries etc.). Therefore, they should remain in control of notification, supervision and issuance of electronic identification schemes and Wallets.

Technology solutions should not jeopardise this sovereignty over EU digital identities. European Digital Identity Wallets are likely to rely on cloud solutions -at least to some extent. Such cloud services need to be fully trustworthy. This means that cloud services used for

Wallets should be certified at level High (pursuant to the Cybersecurity Act) and be subject to European legislation only (no extra-territorial application). Besides, cloud services shall also ensure that data are only stored and processed in EU, and not accessible in any manner to any non-EU countries.

Moreover, Eurosmart stresses that Wallets can only be a companion to physical documents issued by Member States, they should not replace them. It is absolutely crucial to keep this physical backup in case the digital system fails (e.g. because of a cyberattack) to organise resilience of secure identity.

Providers of electronic attestation of attributes

"Providers of qualified electronic attestation of attributes' services shall provide such services under a separate legal entity" (Article 45f(4), which also applies mutatis mutandis to the issuer of European Digital identity Wallet pursuant to Article 6a(7)). The wording does not seem precise enough, what does "separate" mean? Separate from what? In addition, it is not explicitly stated whether this separate legal entity shall only provide services related to the provision of qualified attestation of attributes. It could provide other services, some of them being commercial. Eurosmart also notes that this entity could be established anywhere (within or outside EU) with the current wording.

Eurosmart recommends rephrasing the provision to state that "providers of qualified electronic attestation of attributes' services shall provide such services under a legal entity that was created for the sole purpose of providing such services." This phrasing is important to ensure that providers of qualified electronic attestation of attributes' services do not use the personal data they manage for other purposes.

Moreover, another point should be added in Article 45f to stipulate that "providers of qualified electronic attestation of attributes' services shall be established in one of the EU Member States". The European place of establishment is a guarantee of sovereignty, especially if these providers have access to authentic sources provided by the Member States.

Security requirements for a trustworthy ecosystem

Electronic identification: security requirements

Eurosmart supports the mandatory notification by Member States of at least one electronic identification scheme of LoA High, and the mandatory issuance by Member States of a European Digital identity Wallet under an electronic identity scheme with a LoA High. This provision is crucial to ensure that the European Digital Identity framework is trustworthy. However, Eurosmart would like to raise concerns regarding the lack of link between the LoA High in the eIDAS Regulation and security certification at level High as defined in the Cybersecurity Act, despite their direct correspondence.

The Commission Implementing Decision 2015/1502 (on eIDAS) lays down technical specifications and procedures for assurance levels Low, Substantial and High for electronic identification means. Pursuant to this implementation decision, assurance level High, is defined as follows "[t]he electronic identification means protects against duplication and tampering as well as against attackers with high attack potential". This definition – which

implies to be resistant to attacker with high attack potential - is in line with the definition of security certification of level High pursuant to the Cybersecurity Act, where penetration testing is mandatory to ensure resistance against skilled attackers ("[…] intended to minimise the risk of state-of- the-art cyberattacks carried out by actors with significant skills and resources" Article 52(7) of the Cybersecurity Act). Therefore, there is a direct correspondence between LoA High in eIDAS and the level of certification High in the Cybersecurity Act[2]. More details on certification can be found below. Therefore, Eurosmart calls to establish an explicit link between the definition of LoA and the required level of security certification (pursuant to the Cybersecurity Act) of the electronic identity scheme. In particular, an electronic identity scheme shall only be granted LoA High provided it has been security certified at level High pursuant to the Cybersecurity Act. Likewise, a security certification of level Substantial shall be required for LoA Substantial.

For electronic identification mobile solutions, Eurosmart recommends applying to the smartphone-based identity solution the security requirements that already apply to the card-based identity solution. This would require the use of secure elements which would guarantee security to digital identity assets.

Eurosmart warns against having a European Digital Identity Wallet purely based in the cloud ("wallet on server", similar to "QSCD on server"). From our understanding, the proposed legislation does not exclude this risky possibility. A Wallet in the cloud would raise serious security concerns. Therefore, Eurosmart suggests clarifying the definition of the Wallet to state that:

- the Wallet key(s) shall only be under the user control, and stored in the user device;
- the authentication of the Wallet and the holder shall only involve the user device and the relying party. The authentication of the Wallet and the holder shall not be in any manner supported by a remote server (indeed verification of authentication will require support from a server).

Article 6a states that "Digital Identity Wallets shall, in particular: (e) ensure that the person identification data referred to in Articles 12(4), point (d) uniquely and persistently represent the natural or legal person is associated with it". Eurosmart finds this point unclear. Does this point cover the onboarding process where the Wallet/device is bound to the holder?

Particular attention should indeed be given to the level of confidence in attestation of attributes that are fed into the European Digital Identity Wallets. To ensure that attestation of attribute is of quality, the four following aspects must be extremely reliable: identity proofing, binding to the device, binding to the holder, data freshness. Eurosmart recommends relying on existing standards, such as ISO/IEC 23220 – 5.

Attributes: security requirements

Eurosmart believes that the technical requirements applicable to qualified attestation of attributes should be refined. In the current proposal (Article 45c and Annex V), a qualified attestation shall contain an advanced seal or signature. This requirement - mandating an advanced seal or signature and not a qualified seal or signature, downgrades the security of qualified attestation of attributes. Furthermore, it may lead to national fragmentation as

[2] Eurosmart, "The Cybersecurity Act: a complement to eIDAS", position paper, 1 July 2020.

interpretation of whether a signature or seal is advanced may differ between Member States, despite the envisaged implementing act defining the list of standards for which a seal is presumed to be considered "advanced". Moreover, using only an advanced seal or signature for qualified attestation of attribute may put at risk the trust relying parties can put in it. Qualified attestation of attribute, in order to meet a high level of trust, should only be created using qualified seal or signature.

Security and GDPR certification(s): level High and harmonisation as core principles

Certification of Wallets and electronic identification schemes

Eurosmart would like to reiterate its satisfaction regarding the reference to the Cybersecurity Act in Article 6c. European Digital Identity Wallets that have been certified under a European cybersecurity scheme will be presumed to be compliant with the cybersecurity requirements from the Regulation, in so far as the cybersecurity certificate or statement of conformity covers those requirements. This provision is crucial to ensure harmonised certification of the Wallets, and hence a harmonised level of trust across the EU.

Unfortunately, article 6c does not clarify the level of certification that should be applied. Yet article 6a(4)c highlights that the highest level of trust is expected from the Wallet as it shall "meet the requirements set out in Article 8 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 explained in the former section, there is a direct correspondence between a security certification of level High pursuant to the Cybersecurity Act and LoA High in eIDAS, and thus a security certification at level High should be required for electronic identity scheme claiming LoA High. The same should also apply for European Digital Identity Wallet, as it shall meet the requirements matching LoA High.

Therefore, Eurosmart strongly recommends mandating security certification at level High (pursuant to Cybersecurity Act) of European Digital Identity Wallet for all the features it provides. The level of security certification High of the Cybersecurity Act ensures that the products "have been evaluated at a level intended to minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources."[3] The evaluation activities include at least a review of the publicly know vulnerabilities, testing to demonstrate that the products correctly implement the necessary functionalities at the state of the art and assessment of their resistance to skilled attackers, using penetration testing. Given the importance of the Wallet, including the criticality of the data it contains and its use for strong customer authentication, certification at level High is indicated.

Furthermore, the Wallet should be based on the security provided by the secure hardware which is present in the device. It is the only solution to securely store and protect credentials and keys used by the Wallet so that they are tamperproof.

[3] Article 52(7), Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

Eurosmart recommends leveraging existing security certification schemes defined under the Cybersecurity Act: the EUCC scheme should be used for the security certification of secure hardware used by the European Digital Identity Wallet, the cloud service scheme, the upcoming 5G and IoT schemes. However, this will probably not be sufficient. New schemes are needed to certify not only the Wallet but also electronic identification schemes, as foreseen in Article 12a. Eurosmart has identified that the following schemes are missing, and therefore calls on the European Commission to consider requesting new certification schemes under the Cybersecurity Act:

- Security certification scheme for biometric authentication/verification, as it is instrumental to support many stages of digital identity: authentication/verification based on the face for the remote identity proofing used for instance for the issuance of qualified certificate or attestation, authentication/verification based on the face or fingerprint for the unlocking of the Wallet etc.
- Security certification scheme for the software part of the European Digital Identity Wallet when running on device (e.g. software part of the Wallet interacting between the secure hardware, the screen, the sensors, the relying party…)

With regards to technical supporting documents for the security certification, Eurosmart recommends leveraging existing standards. The standard CEN-CENELEC EN 17640 on Fixed-Time Cybersecurity Evaluation Methodology for ICT products should be used for the security certification of the software part of the European Digital Identity Wallet (e.g. software part of the Wallet interacting between the secure hardware, the screen, the sensors, the relying party…). This standard can be used for the evaluation of the software stack at level High pursuant to the Cybersecurity Act. However, despite the current drafting of an applicable technical standard at CEN-CENELEC, no security certification schemes for secure software under the Cybersecurity Act has been created so far. Eurosmart recommends the European Commission to task ENISA with the creation of such security certification scheme.

Article 6c and Article 12a still allow cybersecurity certification outside the framework of the Cybersecurity Act. Eurosmart warns about a risk of fragmentation if other schemes are used, for instance national schemes. This could lead to different levels of security and trust, and ultimately could undermine mutual trust within EU.

In addition, Eurosmart recommends exploring the possibility to have a single European certification scheme for cybersecurity AND data protection. A single scheme would bring two undeniable benefits:

1) This would avoid creating a heavy burden for the industry.
2) This would further ensure consistency in the level of cybersecurity and privacy across Member States.

Certification of trust services

Electronic attestation of attributes

Article 45f provides requirements for providers of electronic attestations of attributes regarding data protection. In the case of the personal data processing operations carried out by the issuer of the Wallet, a GDPR certification is mandated to demonstrate compliance with requirements pertaining to personal data protection (Article 6c(2)). As the issue is the same

here, the same requirement should apply, and the legislation should also mandate a GDPR certification of personal data processing operations carried out by the provider of (qualified or non-qualified) attestations of attributes.

Qualified Signature Creation Devices

The certification of qualified electronic signature creation devices (Article 30) should rely on the EUCC scheme (Cybersecurity Act), therefore an explicit mention to this security certification scheme should be included in this article. In a previous paper[4], Eurosmart explained that eIDAS is fully in line with the Cybersecurity Act when it comes to the security certification of qualified signature creation devices (QSCD).

The Commission Implementing Decision 2016/650 states that the security certification of these devices shall be carried out pursuant to the ISO/IEC 15408 – which is commonly known as Common Criteria methodology - and based on the protection profiles PP SSCD EN 419 211. However, this is not sufficient to clarify the trust recognition framework of these security certificates, and thus the trust one could put in them.

Security certificates pursuant to Common Criteria methodology could be issued within various trust recognition frameworks : within the CC-MRA (ensuring recognition up to EAL2 within members, and EAL4 under conditions), within the SOG-IS agreement (ensuring recognition up to EAL4 or EAL7 within members) or outside any trust framework, with only a certification authority testifying (1) a product meets the security requirements laid down in the protection profile(s) and (2) its evaluation was carried out in accordance with the standard ISO/IEC 15408. Clearly, the level of trust in a security certificate pursuant to Common Criteria methodology substantially depends on this trust recognition framework, and thus it is necessary to clarify it in the legal text.

When the eIDAS regulation was enacted (2014), no trust recognition framework common to the 27 Member States was available for security certificates pursuant to Common Criteria methodology, despite the SOG-IS being the natural candidate. However, today, this common trust framework for security certificates pursuant to Common Criteria methodology exists: the Cybersecurity Act (enacted in 2019) and the EUCC scheme that has been released by ENISA settle all these aspects. Therefore, Eurosmart calls the European Commission to explicitly mention in article 30(3) that security certification shall be performed in accordance with the EUCC scheme pursuant to the Cybersecurity Act.

Paragraph 3a of Article 30 states that the certification shall be valid for 5 years “conditional upon a regular 2-year vulnerabilities assessment”. This requirement is not needed if certification is done through the EUCC scheme. Vulnerability assessment is already covered as part of the continuous monitoring done by national cybersecurity certification authorities. However, for qualified signature creation devices **on server**, Eurosmart recommends maintaining the requirement of a 2-year vulnerability assessment, given the increased risks that these technologies convey, and that part of the security relies on organisational measures.

Also, Eurosmart warns about the major consequences of this provision, if kept in the final text. It would cause all QSCDs whose vulnerability assessment has been carried out more than two years ago to lose their QSCD certification once this regulation enters into force. This would

[4] Eurosmart, “The Cybersecurity Act: a complement to eIDAS”, position paper, 1 July 2020.

create a major disruption for the users of qualified electronic signature and seal. Besides, it would cause security evaluation laboratories and national cybersecurity certification authorities to face congestion before the regulation enters into force, as many QSCD providers/vendors would simultaneously apply for vulnerability assessment of their products. If this provision is kept, in order to avoid such catastrophic situation, Eurosmart recommends accompanying the implementation of this provision with transitional measures to leave time to providers/vendors of QSCDs to comply with this new requirement. In particular, this provision – if kept – shall not be applicable as soon as the text enters into force but at a later time.

Besides, it should not be possible for security certification of devices to be based on a process using "comparable security levels" (Article 30(3)(b) should be removed). Past experience has shown that this possibility could be used to counter the general spirit of Article 30 and obtain weaker security certification.

Ledgers

Eurosmart has many interrogations regarding the certification of ledgers. Such ledgers might be deployed instead of the existing eIDAS nodes. However, there are no security requirements for ledger deployment. It is not possible to certify ledgers, which would entail a problem to guarantee trustworthiness of the European Digital Identity framework.

Areas for improvement relating to electronic attestation of attribute

Conditions to act as provider

Eurosmart sees a risk of fragmentation between the Member States when it comes to the national conditions that a provider must meet to access the authentic sources (Article 45d). It seems that it remains possible for Member States to mandate qualified providers of electronic attestations of attributes to meet specific criteria prior to giving them access to authentic sources. Eurosmart recommends harmonising the required criteria to access authentic sources, to avoid a fragmentation between users within Member States providing smooth access to their authentic sources, and the others.

Likewise, it is not clear under which conditions a provider of qualified and non-qualified electronic attestation of attributes shall be allowed to interface with a European Digital Identity Wallet. From our understanding, it seems conditions may differ depending on the issuer of the European Digital Identity Wallet or the Member State, which may again create fragmentation between users.

Case of unknown value by the user

There will be cases where the user might not know the value of the attribute he/she requests. It is unclear whether the European Commission envisaged this scenario. Article 45d states "to verify by electronic means at the request of the user, the authenticity of the attribute directly against the relevant authentic source […]". It seems this provision only considers the case where the user declares the value of the attribute for which he/she wants the qualified provider to generate an attestation of attribute, meaning the user knows precisely the value of the attribute. Eurosmart recommends broadening the usage beyond simple verification and

amending as follows: “fetching or verifying at the request of the user, the attribute directly in the relevant authentic source […]”.

Standardisation: the missing mandate

The proposed Regulation includes multiple provisions on the referencing of standards. This concerns standards for trust services (including electronic attestation of attributes) but also Wallets -for which a list of standards will be established by the European Commission. The referencing of standards is foreseen 6 or 12 months after the entry into force of the Regulation. In parallel, Member States start working on a toolbox, which will contain a set of standards and technical specifications for the architecture of the Digital Identity framework.

Eurosmart highlights the importance of standardisation. In its position paper on eID standardisation[5], Eurosmart calls on the European Commission to issue a standardisation request to CEN-CENELEC and ETSI. Such a request should include a mandate to share tasks and the setup of a coordinating structure. Both entities have complementary expertise and different types of membership (membership through EU national standardisation bodies for CEN-CENELEC, direct membership of EU and non-EU companies for ETSI).

Given, the short amount of time for the referencing of standards, Eurosmart believes that this standardisation request should be issued as soon as possible. For some areas, Eurosmart recommends leveraging existing standards. For instance, the European Commission should leverage existing standards from ETSI and CEN when it comes to the security requirements applied to trust service providers (Article 19). This is preferable to laying down new requirements.

NOTE: Some of the standards of interests are developed outside the European Standardisation Organisations (ESO) and National Standardisation Organisations (NSO). For example, this is the case for W3C on verifiable credentials, 5G/6G on cellular IoT and NIST on attribute-based access control. Such standards may evolve or be withdrawn without any control of the EU, which may be problematic when these standards support implementation of a regulation, as it could create major discrepancies.

Therefore, we call on the EU to include within the European collection (CEN/CENELEC, ETSI…) any standards developed outside the European Standardisation Organisations (ESO) or National Standardisation Organisations (NSO) that may be used for the implementation of the revision of eIDAS, so that these standards remain stable and available all along the Regulation is in force.

[5] Eurosmart, “eID deserves its own standardisation mandate”, position paper, 20 April 2021.

Technological choices

Interoperability and neutrality are key

The technical architecture of the framework should allow connecting different solutions. For this purpose, the European Commission and Member States should rely on the existing standards offering the most agnostic approach for the European Digital Identity Wallet. Such design can be found in ISO/IEC 18013-5 and its correlated ISO/IEC 23220 series of standards allowing (1) for a variety of secure areas (eSE, eUICC, iSE, etc.) on board the user device, (2) for discretionary secure data storage, (3) for user consent on selective disclosure of attributes/credentials, (4) for interoperability over several mobile communication channels, (5) for online as well as offline identification and authentication, and (6) for device provisioning with high-level interoperability interfaces. Therefore, Eurosmart recommends leveraging these ISO standards (i.e. ISO/IEC 18013-5 and ISO/IEC 23220 series) that were initially designed for mobile driving licence use case, and that were enhanced to serve any other identification use case with a mobile digital wallet. These ISO standards offer a technologically neutral approach.

Besides, Eurosmart underlines that an international standard can be endorsed through the regular procedure used by CCMC and CEN-CENELEC BT whereby an international ISO/IEC standard can be transferred to a European Norm (EN).

Need for clarification on the physical separation of data

Eurosmart recommends clarifying Article 6a paragraph 7. This paragraph states the following:

> *"Personal data relating to the provision of European Digital Identity Wallets shall be kept physically and logically separate from any other data held."*

Likewise, Article 45f(3) states that:

> *"Personal data relating to the provision of qualified electronic attestation of attributes services shall be kept physically and logically separate from any other data held."*

Eurosmart understands that these two sentences primarily target storage on servers by issuers of European Digital identity Wallets and providers of qualified electronic attestation of attributes. Issuers/providers should ensure that personal data relating to the provision of the Wallets/qualified electronic attestation of attributes are stored on dedicated servers. This physical separation on the server side is much welcome for privacy reasons.

However, on the user side, if interpreted too broadly, this phrasing could exclude technological solutions whereby identity credentials and other data would be stored on the same physical support in the user device (e.g. mobile phone, eUICC), although logically separated. The current state of the art enables a logical separation to be implemented very securely. It does not seem feasible to have such a physical separation on the user side, as the user only has one mobile phone and one secure element to store the data.

Upholding Europe's security principles in an international setting

Article 14 of the proposal lays down the possibility for the European Commission to adopt implementing acts to set out the conditions under which the requirements of a third country applicable to the trust service providers established in its territory can be considered equivalent to the requirements applicable to qualified trust service providers established in the EU. Eurosmart considers that this provision does not guarantee mutual recognition by the third country at stake. The former text of eIDAS envisaged this recognition only in the framework of an agreement concluded between the EU and a third country. Eurosmart suggests reverting to the former wording of Article 14.

In any case, it should be a prerequisite for international recognition to have -at least- the same level of security requirements applicable to trust service providers in the third country at stake. For instance, trust service providers established in a third country should rely on an identity proofing process as stringent as the one performed by qualified trust service providers established in the EU. Otherwise, there would be a twofold risk. First, this international recognition would result in security risks for EU citizens using these less stringent services. Secondly, this would result in a dramatically unfair competition for qualified trust providers established in the EU. They would have to apply the more stringent security requirements in place in the EU, while competing with third-country trust service providers subject to less stringent security rules.

Unclear provisions on identification of IoT devices

The proposal defines an attribute as "a feature, characteristic or quality of a natural or legal person or of an entity, in electronic form". The impact assessment further explains that "the identification of objects and devices follows international standards, which are out of scope of eIDAS. However, scenarios where things and IoT devices need to be linked in a trusted way to owners are increasingly frequent and can be achieved by linking attributes and credentials to secure and trusted eID".[6] Therefore, the proposal intends to address the connection between IoT devices and legal or physical persons. However, the proposal itself does not give details on the linking of IoT attributes and credentials to digital identities.

It is worth noting that the IoT term can apply to devices as well as AI agents and others forms of technology. There are two main scenarios: first, the device as an extension to the user, and therefore, there is a strong need for a link between those two identities: user and device. Depending on the use case, the levels of assurance might differ. Secondly, there are devices, and in particular agents, making use of their own identity and operating semi-autonomously. This difference is key when the device is accessing trust services. It seems that the proposal only considers the first scenario and not the second one.

The standardisation of digital identities for IoT devices helps to reduce fragmentation. Fragmentation introduces inconvenience, reducing adoption, and limits the scalability of pan-European and cross border activities. It might also lead to security vulnerabilities. It is therefore desirable to have clear definitions and requirements for digital identities for IoT

[6] Commission Staff Working Document, Impact Assessment Report, Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) n° 910/2014 as regards establishing a framework for a European Digital Identity, 3 June 2021.

devices. It is also essential to define levels of assurance in the context of the use cases, as it has been defined for legal and natural persons.

Clarify the link to PSD2

Eurosmart welcomes the link to PSD2 with the mention of "strong user authentication" in Article 12b(2). Where private relying parties providing services are required by legislation to use strong user authentication for online identification, those private relying parties shall also accept the use of European Digital Identity Wallets.

Eurosmart appreciates the connection to PSD2 and Know-Your-Customer. Finance is indeed a major use case for the Wallet. This link will foster the uptake of the European Digital Identity Wallets.

However, Eurosmart notes that the definition of strong user authentication (Article 3(50)) in the proposal slightly differs from the one provided by PSD2 (Article 4(30)) as the brackets are missing:

> *"'strong customer authentication' means an authentication based on the use of two or more elements categorised as knowledge **(something only the user knows)**, possession **(something only the user possesses)** and inherence **(something the user is)** that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data"*

Eurosmart proposes to fully align the definition with PSD2.

In addition, Eurosmart observes that the introductory part of the proposal (recitals) does not give any explanation on this link between eIDAS and PSD2 and its consequences for PSD2. The introductory part should explain the principles enshrined in article 12b(2) of this Regulation:

> (1) the principle of equivalence between the usage of a European Digital Identity Wallet (as defined in the Regulation) and "strong customer authentication" as defined in other texts such as PSD2,
>
> (2) the obligation for entities required by law to perform "strong customer authentication" to accept the usage of a European Digital Identity Wallet (as defined in the Regulation).

Stability of requirements for qualified trust service providers

Article 24(2) defines the requirements to be met by qualified trust service providers providing qualified trust services. In particular, clause (fa) requires qualified trust service providers to

> *"have appropriate policies and take corresponding measures to manage legal, business, operational and other direct or indirect risks to the provision of the qualified trust service Notwithstanding the provisions of Article 18 of Directive EU XXXX/XXX [NIS2], those measures shall include at least the following:*

(i) measures related to registration and on-boarding procedures to a service;

(ii) measures related to procedural or administrative checks;

(iii) measures related to the management and implementation of services. "

Later, Article 24(6) indicates that the "Commission shall be empowered to adopt delegated acts regarding the additional measures referred to in paragraph 2(fa)". Therefore, this article empowers the Commission to expand the set of requirements pertaining to risk management applicable to qualified trust service providers providing qualified trust services by means of delegated act.

Eurosmart considers that the addition of supplemental requirements applicable to qualified trust service providers providing qualified trust services shall only be made through a regulation and not in a delegated act, as it may have substantial impacts for qualified trust service providers providing qualified trust services.

Last but not least, should this provision be nevertheless deemed necessary, the Regulation shall clearly specify the transitional measures applicable to qualified trust service providers providing qualified trust services when the Commission adopts such delegated acts. More precisely, once a delegated act was enacted, qualified trust service providers providing qualified trust services shall have enough time to (1) implement the new requirements, and (2) include them in their audit, to avoid disrupting the whole market of trust services.

Therefore, Eurosmart recommends clearly specifying in Article 24 that:

- "Delegated acts regarding the additional measures referred to in paragraph 2(fa) shall only enter into force 24 months after they have been enacted", so that technical requirements are only mandated in audit of qualified trust service providers performed 24 months after the delegated act is enacted. It aims at leaving enough time so that qualified trust service providers could implement the new requirements.
- "When a delegated act regarding the additional measures referred to in paragraph 2(fa) enters into force, qualification of trust service providers shall remain valid until their expiry." It aims at not disrupting the validity of qualification of trust service provider, and thus avoiding disruption.

ANNEX: Existing standardised definitions of the terms "attribute" and "credential" in relation with identity and identification

Organisation	Reference	Definition(s)
ISO/IEC	24670-1:2019 *IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts*	**identity, partial identity** set of attributes (3.1.3) related to an entity (3.1.1) Note 1 to entry: An entity can have more than one identity. Note 2 to entry: Several entities can have the same identity. Note 3 to entry: ITU-T X1252[13] specifies the distinguishing use of an identity. In this document, the term identifier implies this aspect. **attribute** characteristic or property of an entity EXAMPLE An entity type, address information, telephone number, a privilege, a MAC address, a domain name are possible attributes. **identifier** attribute or set of attributes (3.1.3) that uniquely characterizes an identity (3.1.2) in a domain (3.2.3) Note 1 to entry: An identifier can be a specifically created attribute with a value assigned to be unique within the domain. **identification** process of recognizing an entity (3.1.1) in a particular domain (3.2.3) as distinct from other entities Note 1 to entry: The process of identification applies verification to claimed or observed attributes. Note 2 to entry: Identification typically is part of the interactions between an entity and the services in a domain and to access resources. Identification can occur multiple times while the entity is known in the domain. **verification** process of establishing that identity information (3.2.4) associated with a particular entity (3.1.1) is correct Note 1 to entry: Verification typically involves determining which attributes are needed to recognize an entity in a domain, checking that these required attributes are present, that they have the correct syntax, and exist within a defined validity period and pertain to the entity. **identity information** set of values of attributes (3.1.3) optionally with any associated metadata in an identity (3.1.2) Note 1 to entry: In an information and communication technology system an identity is present as identity information.

		credential representation of an identity (3.1.2) for use in authentication (3.3.1) Note 1 to entry: As described in 5.4, customary embodiments of a credential are very diverse. To accommodate this wide range, the definition adopted in this document is very generic. Note 2 to entry: A credential is typically made to facilitate data authentication of the identity information pertaining to the identity it represents. Data authentication is typically used in authorization. Note 3 to entry: The identity information represented by a credential can, for example, be printed on human readable media, or stored within a physical token. Typically, such information can be presented in a manner designed to reinforce its perceived validity. Note 4 to entry: A credential can be a username, username with a password, a PIN, a smartcard, a token, a fingerprint, a passport, etc.
ISO/IEC	19286:2018 *Identification cards — Integrated circuit cards — Privacy-enhancing protocols and services*	**user attribute** quality or characteristic ascribed to someone or something [SOURCE: NIST SP 800-63-3] EXAMPLE: User name, address, date of birth or assertion about date of birth are user attributes. Note 1 to entry: Examples of user attributes that can be used to identify natural persons are given in Reference [14]. **attribute integrity** capability of an attribute (3.3) to resist to unintended or unauthorized modification **attribute provider** entity (3.13) that makes user attributes (3.3) available Note 1 to entry: An attribute provider may be an identity provider (3.18) or an entity mandated by an identity provider. **attribute statement** statement or assertion about user attributes comprising predicates over attributes (3.3) EXAMPLE: The business case age verification usually does not require information about the user attribute “date of birth” but only the verification if the age is above a specific threshold, i.e. the attribute statement over the “date of birth” saying “is over 21”. **authentication** provision of assurance in the identity (3.17) of an entity (3.13) [SOURCE: ISO/IEC 29115:2013, 3.2]

		credential set of data presented as evidence of a claimed or asserted identity and/or entitlements [SOURCE: ISO/IEC 29115:2013] **identification** process of distinguishing an entity (3.13) within a given context by the unique association of a set of descriptive parameters EXAMPLE: User attributes are descriptive parameters. **identity** set of attributes (3.3) related to an entity (3.13) [SOURCE: ISO/IEC 29115:2013, 3.13] **identity provider** trusted actor that issues and/or manages credentials (3.9) Note 1 to entry: In literature, such identity provider is often referred to as identity information provider (see ISO/IEC 24760-1) or credential service provider (see ISO/IEC 29115). **issuer** entity that is an identity provider (3.18) or attribute provider Note 1 to entry: An issuer may also issue the token (3.30).
ISO/IEC	29115:2013 Annex B	**"Characteristics of a credential"** a) A credential is data. A credential does not include any physical container or device that holds the data. Nor does it include a generator for the data that makes up the credential. Thus, a pass code generator is never part of a credential, and neither is a smart card that can sign data, software that generates digital signatures, or paper on which things might be written. b) A credential must contain data that is evidence of an identity and/or entitlements. Examples of such evidence are: 1. Something known (e.g., static password); 2. A biometric characteristic or a representation of same; or 3. Data produced by something possessed (e.g., one-time pass codes produced by a pass-code generator, data that is digitally signed by hardware or software using a private key presumed to be in the possession of an entity). c) A credential may be accompanied by other data that can be useful to the authentication and identification processes, but which do not form part of the actual credential.

		Examples of this data include the name of an entity and a public key certificate. Neither of these things is necessary as evidence of an identity or entitlements, but they are useful in authentication protocols. Associating the name of the entity with a credential confirms the identity. Associating a public key certificate with a credential provides information that assists in testing the evidence as well as possibly providing information about the identity or entitlements of an entity. d) A credential can also be a derived credential. In this case, such a derived credential can be a collection of information derived from a set of credentials, usually created and sent by an entity to authenticate to a credential verifier. For example, for some types of anonymous authentication, the entity transforms the credential issued by the CSP into a derived credential that is used for authentication. e) Not all data that comprises a credential needs to be kept secret. f) A credential can be used for authentication, identification, or authorisation of the entity, or a combination of all three. g) A credential must be verified before it can be accepted as authentic and trustworthy for its particular purpose (e.g., authentication, identification, authorization). h) A credential must go through several steps to be verified. Examples of these steps include: 1. Checking the authenticity of the credential to ensure it originated with the purported issuer; 2. Confirming the validity and trustworthiness of the credential (e.g., determining if there is a direct link to a trusted root from the credential issuer); and 3. Confirming the computational accuracy of the mathematics/cryptography. i) A credential can be authentic but not valid in all contexts (e.g., the credential held on a smart card, such as a pre-paid telephone chip card, can be authentic but may it be valid only for calls made using the facilities of the issuer).
NIST	SP 800-63-3 (June 2017) *Digital Identity Guidelines*	**Credential** An object or data structure that authoritatively binds an identity - via an identifier or identifiers - and (optionally) additional attributes, to at least one authenticator possessed and controlled by a subscriber. **Attribute** A quality or characteristic ascribed to someone or something. **Attribute Bundle** A packaged set of attributes, usually contained within an assertion. Attribute bundles offer RPs a simple way to retrieve the most relevant attributes they need from IdPs. Attribute bundles are synonymous with OpenID Connect scopes [OpenID Connect Core 1.0].

		Attribute Reference A statement asserting a property of a subscriber without necessarily containing identity information, independent of format. For example, for the attribute "birthday," a reference could be "older than 18" or "born in December." **Attribute Value** A complete statement asserting a property of a subscriber, independent of format. For example, for the attribute "birthday," a value could be "12/1/1980" or "December 1, 1980."

NOTE: The term "attribute" was used at an early stage along the US standard NIST 800-162, published for the first time in 2014. The complete name is "attribute-based access control", in short ABAC. This standard replaced the role-based access control (RBAC) standard, as defined by ANSI along 359-2004, published 10 years earlier.

Other standardisation organisations have referred the term ABAC, for example ETSI in its TS 103 532, addressing Attribute Based Encryption, published in 2018, and the German DIN in its Spec 27070 for edge connector, published in 2020, managing the Dynamic Attribute Provisioning Service in Industrial Internet of Things (IIoT).

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.

Our members

Members are designers or manufacturers of secure elements, semiconductors, smart cards, systems on chip, High Security Hardware and terminals, biometric technology providers, system integrators, secure software and application developers and issuers. Members are also involved in security evaluation as laboratories, consulting companies, research organisations, and associations.

Eurosmart members are companies (**BCA, Bureau Veritas, CYSEC**, **Fingerprint Cards**, **G+D Mobile Security**, **IDEMIA**, **IN GROUPE**, **Infineon Technologies**, **NXP Semiconductors**, **PayCert**, **Prove & Run**, **Qualcomm**, **Real Casa de la Moneda**, **Samsung**, **Sarapis**, **SGS**, **STMicroelectronics**, **Synopsys, Thales**, **Tiempo Secure, Trusted Objects, TrustCB, WISekey**, **Winbond, Xilinx**), laboratories (**Brightsight**, **Cabinet Louis Reynaud, CCLab, CEA-Leti, Jtsec, Keolabs**, **Red Alert Labs**, **Serma**), consulting companies (**Internet of Trust**), research organisations (**Fraunhofer AISEC, Institut Mines-Telecom - IMT, ISEN - Institut Supérieur de l'Électronique et du Numérique Toulon**), associations (**SCS Innovation cluster**, **Smart Payment Association**, **SPAC, Mobismart**, **Danish Biometrics**).

Eurosmart is member of several European Commission's groups of experts: Radio Equipment Directive, eCall, Multistakeholder platform for ICT standardisation, and Product Liability.

Eurosmart and its members are also active in many other security initiatives and umbrella organisations at EU-level, like CEN-CENELEC, ECIL, ECSO, ESIA, ETSI, GlobalPlatform, ISO, SIA, TCG, Trusted Connectivity Alliance and others.

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com @Eurosmart_EU @Eurosmart

Square de Meeûs 35 | 1000 Brussels | Belgium
Contact@eurosmart.com