2021/0136 (COD)

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

Rapporteur: Romana Jerković

CONSOLIDATED TEXT - COMPROMISE AMENDMENTS

(EPP, S&D, Renew, Greens, The Left)

7 February 2023

CA 1: Covers all articles and recitals, with the exception of those covered by exclusive competences of associated committees

All AMs fall, except those of associated committees related to their exclusive competences as defined by agreements endorsed by the CCC.

CHAPTER I
GENERAL PROVISIONS

Article 1

Subject matter

1. This Regulation~~s~~ aims at ***contributing towards*** ensuring the proper functioning of the internal market ~~and~~ providing an adequate level of security of electronic identification means and trust services ***used across the Union***. For these purposes, this Regulation:

(a) lays down the conditions under which Member States shall provide and recognise electronic identification means of natural and legal persons, falling under a notified electronic identification scheme of another Member State;

(b) lays down rules for trust services, in particular for electronic transactions;

(c) establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, ***non-qualified electronic delivery services and qualified*** electronic registered delivery service~~s~~, certificate services for website authentication,

and ~~electronic archiving and~~ electronic attestation of attributes, the management of remote electronic signature and seal creation devices ~~and electronic ledgers~~;

(d) lays down the conditions for the issuing***, managing and recogniting*** ~~of~~ European Digital Identity Wallets by Member States ***and for ensuring their interoperability and their cross-border use in the Union .***

(e) enables a right to participate in the digital society safe and facilitates unrestricted access to online public services throughout the Union for any natural person or legal person.

Article 2

Scope

1. This Regulation applies to electronic identification schemes that have been notified by a Member State, European Digital Identity Wallets issued ***and managed*** by Member States and to trust service providers that are established in the Union.
2. This Regulation does not apply to the provision of trust services that are used exclusively within closed systems resulting from national law or from agreements between a defined set of participants.
3. [Exclusive JURI] (text to be added for plenary tabling)

Article 3

Definitions

(1) 'electronic identification' means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person;

(2) 'electronic identification means' means a material and/or immaterial unit, including European Digital Identity Wallets or ID cards following Regulation 2019/1157, containing person identification data and which is used for authentication for an online or offline service;

(3) 'person identification data' means a set of data***, issued in accordance with national law,*** enabling the identity of a natural or legal person, or a natural person representing a legal person to be established;

(4) 'electronic identification scheme' means a system for electronic identification under which electronic identification means, are issued to natural or legal persons or natural persons representing legal ***or natural*** persons;

(4a) ***'user' means a natural or legal person, or a natural person representing a legal person using trust services, notified electronic identification means or European Digital Identity Wallets, provided according to this Regulation***;

(5) 'Authentication' means an electronic process that enables the ~~electronic~~ verification of ~~a natural or legal person, or~~ the origin and integrity of data in electronic form ~~to be confirmed;~~

(5a) 'identification' means an electronic process that establish an unequivocal relationship between a set of data and a natural or legal person.

(5b) ***'validation' means the process of verifying that an electronic signature, an electronic seal, a EDIW, an electronic identification mean, a relying party authorisation, person identification data, an electronic attestation of attributes or any electronic certificates***

for trust services provided according to this Regulation is valid and has not been revoked.

(5c) 'zero knowledge proof' means cryptographic methods by which a relying party can validate that a given statement based on the electronic attestation of attributes held in the user's European Digital Identity Wallet is true, without conveying any data related to those electronic attestation of attributes to the relying party;

(6) 'relying party' means a natural or legal person that relies upon an electronic identification ***means, including European Digital Identity Wallets,*** or a trust service***, directly or through an intermediary, in order to provide services***;

(7) 'public sector body' means a state, regional or local authority, a body governed by public law or an association formed by one or several such authorities or one or several such bodies governed by public law, or a private entity mandated by at least one of those authorities, bodies or associations to provide public services, when acting under such a mandate;

(8) 'body governed by public law' means a body defined in point (4) of Article 2(1) of Directive 2014/24/EU of the European Parliament and of the Council (15);

(9) 'signatory' means a natural person who creates an electronic signature;

(10) 'electronic signature' means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;

(11) 'advanced electronic signature' means an electronic signature which meets the requirements set out in Article 26;

(12) 'qualified electronic signature' means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures;

(13) 'electronic signature creation data' means unique data which is used by the signatory to create an electronic signature;

(14) 'certificate for electronic signature' means an electronic attestation ~~or set of attestations~~ which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person;

(15) 'qualified certificate for electronic signature' means a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I;

(16) 'trust service' means an electronic service normally provided against payment which consists of:

(a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services, electronic attestation of attributes and certificates related to those services;

(b) the creation, verification and validation of certificates for website authentication;

(c) the preservation of electronic signatures, seals or certificates related to those services;

(d) the electronic archiving of electronic documents;

(e) the management of remote electronic signature and seal creation devices;

(17) 'qualified trust service' means a trust service that meets the applicable requirements laid down in this Regulation;

(18) ‘conformity assessment body’ means a body defined in point 13 of Article 2 of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides;

(19) ‘trust service provider’ means a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider;

(20) ‘qualified trust service provider’ means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body;

(21) ‘product’ means hardware or software, or relevant components of hardware and / or software, which are intended to be used for the provision of electronic identification and trust services;

(22) ‘electronic signature creation device’ means configured software or hardware used to create an electronic signature;

(23) ‘qualified electronic signature creation device’ means an electronic signature creation device that meets the requirements laid down in Annex II;

(23a) ‘remote qualified signature creation device’ means a qualified electronic signature creation device where a qualified trust service provider generates, manages or duplicates the electronic signature creation data on behalf of a signatory;

(23b) ‘remote qualified seal creation device’ means a qualified electronic seal creation device where a qualified trust service provider generates, manages or duplicates the electronic signature creation data on behalf of a seal creator;

(24) ‘creator of a seal’ means a legal person who creates an electronic seal;

(25) ‘electronic seal’ means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter’s origin and integrity;

(26) ‘advanced electronic seal’ means an electronic seal, which meets the requirements set out in Article 36;

(27) ‘qualified electronic seal’ means an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal;

(28) ‘electronic seal creation data’ means unique data, which is used by the creator of the electronic seal to create an electronic seal;

(29) ‘certificate for electronic seal’ means an electronic attestation or set of attestations that links electronic seal validation data to a legal person and confirms the name of that person;

(30) ‘qualified certificate for electronic seal’ means a certificate for an electronic seal, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III;

(31) ‘electronic seal creation device’ means configured software or hardware used to create an electronic seal;

(32) ‘qualified electronic seal creation device’ means an electronic seal creation device that meets mutatis mutandis the requirements laid down in Annex II;

(33) ‘electronic time stamp’ means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time;

(34) ‘qualified electronic time stamp’ means an electronic time stamp which meets the requirements laid down in Article 42;

(35) ‘electronic document’ means any content stored in electronic form, in particular text or sound, visual or audiovisual recording;

(36) ‘electronic registered delivery service’ means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations;

(37) ‘qualified electronic registered delivery service’ means an electronic registered delivery service which meets the requirements laid down in Article 44;

(38) ‘certificate for website authentication’ means an ***electronic*** attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued;

(39) ‘qualified certificate for website authentication’ means a certificate for website authentication ***that links the website to the natural or legal person to whom the certificate is issued with a high level of assurance***, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV;

(40) ‘validation data’ means data that is used to validate an electronic signature or an electronic seal;

(41) ~~‘validation’ means the process of verifying and confirming that an electronic signature or a seal or person identification data or an electronic attestation of attributes is valid;~~

(42) 'European Digital Identity Wallet' is ~~a product and service that allows the user to~~ ***an electronic identification means, that securely*** stores, ***manages and validates*** identity data~~, credentials~~ and ***electronic attestations of*** attributes ~~linked to her/his identity~~, to provide them to relying parties ***and other EDIW users*** on request ~~and to use them for authentication, online and offline, for a service in accordance with Article 6a;~~, and ~~to create~~ ***enables the creation*** of qualified electronic signatures and seals;

(43) ‘attribute’ is a feature, characteristic or quality of a natural or legal person or of an entity~~, in electronic form~~;

(44) ‘electronic attestation of attributes’ means an attestation in electronic form that allows the ***presentation and*** authentication of attributes;

(45) ‘qualified electronic attestation of attributes’ means an electronic attestation of attributes, which is issued by a qualified trust service provider and meets the requirements laid down in Annex V;

(46) ‘authentic source’ is a repository or system, held under the responsibility of a public sector body or private entity, that contains attributes about a natural or legal person and is considered to be the primary source of that information or recognised as authentic in ***Union or*** national law;

(47) ‘electronic archiving’ means a service ensuring ***preservation*** ~~the receipt, storage, deletion and transmission~~ of electronic data or documents in order to guarantee their

integrity, the accuracy of their origin and legal features throughout the conservation period;

(48) 'qualified electronic archiving service' means a service that meets the requirements laid down in Article 45g;

(49) 'EU Digital Identity Wallet Trust Mark' means an indication in a simple, recognisable and clear manner that a Digital Identity Wallet has been issued in accordance with this Regulation;

(50) 'strong user authentication' means an authentication based on the use of ***at least*** two ~~or more elements~~ ***authentication factors*** categorised as user knowledge , possession and inherence that are independent, in such a way that the breach of one does not compromise the reliability of the others, and is designed in such a way to protect the confidentiality of the authentication data;

(51) 'user account' means a mechanism that allows a user to access public or private services on the terms and conditions established by the service provider;

(52) ~~'credential' means a proof of a person's abilities, experience, right or permission;~~

(53) ~~'electronic ledger' means a tamper proof electronic record of data, providing authenticity and integrity of the data it contains, accuracy of their date and time, and of their chronological ordering';~~

(54) [LIBE Exclusive] (text to be added for plenary tabling)

(55) 'identity matching' ~~'unique identification'~~ means a process where person identification data or person identification means are matched with or linked to an existing account belonging to the same person.

(55 a) 'offline service' refers to the capability for a user to electronically identify and authenticate with a third party with close proximity technologies irrespective of whether the device is connected to the internet or not in order to access a wide range of public and private services.

Article 4

Internal market principle

1. There shall be no restriction on the provision of trust services in the territory of a Member State by a trust service provider established in another Member State for reasons that fall within the fields covered by this Regulation.

2. Products and trust services that comply with this Regulation shall be permitted to circulate freely in the internal market.

Article 5

[Exclusive LIBE and JURI] (text to be added for plenary tabling)

CHAPTER II

SECTION I

Electronic identification

Article 6

[Deleted in the EC proposal]

Article 6a

European Digital Identity Wallet

1. For the purpose of ensuring that all natural and legal persons in the Union have secure, ***reliable,*** trusted and seamless access to cross-border public and private services, ***while having full control over their data,*** each Member State shall issue ***at least one*** European Digital Identity Wallet ***by ... [18*** months after the date of entry into force of ***this amending*** Regulation]

2. European Digital Identity Wallets shall be issued ***and managed in any of the following ways***:

   (a) ***directly*** by a Member State;

   (b) under a mandate from a Member State;

   (c) independently ***from a Member State*** but recognised by ***that*** ~~a~~ Member State***;***

2a. The source code used for providing European Digital Identity Wallets shall be open source, and shall be published for auditing and review.

3. European Digital Identity Wallets shall, ***in a user friendly manner,*** enable the user to:

   (a) securely request and obtain, store, select, combine and share, in a manner that is transparent to ~~and~~, traceable by ***and under the sole control of*** the user, the necessary ~~legal person~~ identification data ~~and electronic attestation of attributes~~ to ***identify and*** authenticate ***the user*** online and offline in order to use online public and private services;

   (b) securely store, select, combine and share electronic attestation of attributes;

   (c) securely issue and revoke electronic attestation of attributes issued directly by the user;

   (d) generate pseudonyms and store them encrypted and locally within it;

   (e) securely authenticate a third person's European Digital Identity Wallets or a connecting relying party, and receive and authenticate in a transparent and traceable manner the third party identity data and electronic attestation of attributes online and offline;

   (f) access a data base of all transactions done through the wallet via a common dashboard enabling the user to:

      1. view an up to date list of relying parties with whom the user has established a connection and whenever applicable all data shared;

      2. easily request to a relying party the deletion of personal data pursuant to Article 17 of the Regulation (EU) 2016/679);

      3. easily report to the competent national authority where a relying party is established if an unlawful or inappropriate request of data is received without leaving the wallet;

4. revoke any electronic attestation of attribute issued by the user;

(g) sign by means of qualified electronic ***signatures which shall be offered to all users by default and free of charge;***

(h) download all own data, electronic attestation of attributes and configurations;

(i) exercising their rights of data portability by switching to another European Digital Identity Wallet belonging to the same user.

4. ***European*** Digital Identity Wallets shall, in particular:

(a) provide ~~a~~ common ~~interface~~ ***protocols and interfaces***:

(1) to securely interact with the electronic identification means associated pursuant to Article 7 (2), for the purpose of identifying and authenticating the user;

(2) for issuers of electronic attestation of attributes to issue electronic attestation of attributes into the user's EDIW;

(3) to establish unique, private and secure peer-to peer connections between two EDIW or an EDIW and a relying party;

(4) ***for EDIW users and relying parties to request, receive, select, send, authenticate and validate electronic attestations of attributes, person identification data, the identification of relying parties, electronic signatures and electronic seals;***

(5) for EDIW users and relying parties to authenticate and validate EDIW and approved relying parties;

(6) for EDIW users or relying parties, when available, to perform a zero knowledge proof inferred from person identification data or electronic attestation of attributes;

(7) for EDIW users to transfer and request reissuance of their own electronic attestation of attributes and configurations to another European Digital Identity Wallet belonging to the same user or a device controlled by the same user;

~~(i) to qualified and non-qualified trust service providers issuing qualified and non-qualified electronic attestations of attributes or other qualified and non-qualified certificates for the purpose of issuing such attestations and certificates to the European Digital Identity Wallet;~~

~~(ii) for relying parties to request and validate person identification data and electronic attestations of attributes;~~

~~(iii) for the presentation to relying parties of person identification data, electronic attestation of attributes or other data such as credentials, in local mode not requiring internet access for the wallet;~~

~~(iv) for the user to allow interaction with the European Digital Identity Wallet and display an "EU Digital Identity Wallet Trust Mark";~~

(b) [Exclusive LIBE] (text to be added for plenary tabling)

(c) 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;

~~(d) provide a mechanism to ensure that the relying party is able to authenticate the user and to receive electronic attestations of attributes;~~

(c) ***in the case of electronic attestation of attributes with disclosure policies embedded, provide a mechanism to ensure that only the relying party or the EDIW user having the necessary electronic attestation of attribute giving permission access to it can access it;***

(d) provide a mechanism to record all digital requests received and all digital transactions in a way that is cryptographically non-repudiable;

(e) provide a mechanism to inform users, without delay, of any security breach that may have entirely or partially compromised their European Digital Identity Wallet or its content and in particular if their European Digital Identity Wallet has been suspended or revoked pursuant Article 10a.

(f) ensure that the person identification data referred to in ~~Articles~~ ***Article*** 12(4), point (d), ~~uniquely and persistently represent~~ representing the natural or legal person is associated with it.

(g) provide a mechanism allowing the user of the Wallet to act on behalf of another natural or legal person;

(h) display an "EU Digital Identity Wallet Trust Mark" for the recognition of qualified electronic attestation of attributes;

5. Member States shall provide ***free of charge*** validation mechanisms ***to*** ~~for the European Digital Identity Wallets~~:

(a) ~~to~~ ensure that ***the*** ~~its~~ authenticity and validity ***of EDIWs*** can be verified;

(b) ~~to~~ allow relying parties ***and EDIW users*** to verify that the ***electronic*** attestations of attributes are ***authentic and*** valid;

(c) ~~to~~ allow relying parties, ***EDIW users*** and qualified trust service providers to verify the authenticity and validity of attributed person identification data;

(d) ***allow EDIW users to verify the authenticity and validity of the identity of relying parties approved in accordance with Article 6b(1) ;***

5a. Member States shall provide means to revoke the validity of the European Digital Identity Wallet:

(i) upon the explicit request of the user;

(ii) when its security has been compromised;

(iii) upon the death of the user or cease of activity of the legal person.

5b. ***Member States shall raise awareness on the benefits and risks of the European Digital Identity Wallet by means of communication campaigns. They shall ensure that their citizens are well trained in its use.***

5c. Issuers of European Digital Identity Wallets shall ensure that users can easily request technical support and report technical problems or any other incidents having a negative impact on the provision of services of the European Digital Identity Wallet.

6. European Digital Identity Wallets~~,~~ shall be issued under a notified electronic identification scheme of level assurance "high". ~~The use of the European Digital Identity Wallets shall be free of charge to natural persons.~~

6a. ***The European Digital Identity Wallets shall ensure security-by-design. European Digital Identity Wallets shall provide the necessary state-of-the-art security functionalities, such us mechanisms to encrypt and store data in a way that is only accessible to and decryptable by the user and establish end-to-end encrypted exchanges with relying parties and other European Digital Identity Wallets. They shall offer resistance to skilled attackers, ensure the confidentiality, integrity and availability of their content, including person identification data and electronic attestation of attributes and request the secure, explicit and active user's confirmation of its operation.***

6b ***The issuance and use of the European Digital Identity Wallets shall be free of charge for all natural and legal persons.***

7. [LIBE exclusive] (text to be added for plenary tabling)

8. The use of the European Digital Identity Wallet by natural or legal persons shall be voluntary. Access to public and private services, access to labour market and freedom to conduct business shall not in any way be restricted or made disadvantageous for natural or legal persons not using European Digital Identity Wallets. It shall remain possible to access public and private services by other existing identification and authentication means.

~~8. Article 11 shall apply mutatis mutandis to the European Digital Identity Wallet.~~

9. Article 24(2), points (b), ***(d),*** (e), ***(f), (fa), (fb),*** (g), and (h) shall apply mutatis mutandis to Member States ***directly*** issuing and ***managing*** the European Digital Identity Wallets.

10. [IMCO exclusive] (text to be added for plenary tabling)

11. ***By … [***~~Within~~ 6 months ***after*** ~~of~~ the ***date of entry*** ~~entering~~ into force of this ***amending*** Regulation***]***, the Commission shall ~~establish technical and operational specifications and~~ reference standards for the requirements referred to in ***this Article*** ~~in paragraphs 3, 4 and~~ 5 by means of an implementing act on the implementation of the European Digital Identity Wallet. ***That*** ~~This~~ implementing act shall be adopted in accordance with the examination procedure referred to in Article 48(2).

11a. ***By ... [6 months after the date of entry into force of this amending Regulation], the Commission shall adopt a delegated act in accordance with Article 47 concerning the establishment of technical and operational specifications for the requirements referred to in this Article.***

Article 6b

European Digital Identity Wallets Relying Parties.

1. Where ***a*** relying part***y*** intend***s*** to rely upon European Digital Identity Wallets ***for the provision of public or private services it*** ~~issued in accordance with this Regulation, they~~ shall ***register in*** ~~communicate it~~ to the Member State where the relying party is established. ***The relying party's registration shall include information about the data that the relying party intends to request per each different service provided, the intended use and the reasons why such data is*** ~~***needed***~~ ***being requested. Relying parties shall notify the Member State about any change to the information notified with undue***

delay. ~~to ensure compliance with requirements set out in Union law or national law for the provision of specific services. When communicating their intention to rely on European Digital Identity wallets, they shall also inform about the intended use of the European Digital Identity Wallet.~~

1a. Relying parties that intend to process sensitive personal information, such as health or biometric data, as defined by Article 9 of the Regulation (EU) 2016/679 will need prior approval from the competent authorities in the Member State in which they intend to provide their services. Relying parties that are granted the approval shall ensure that processing of personal information is carried out in accordance with Article 6(1) of the Regulation (EU) 2016/679.

1b. Paragraph 1 and 1a is without prejudice to ex-ante approval requirements set out in Union law or national law for the provision of specific services.

1c. Member States shall make the information referred to in paragraph 1 publicly available online, together with the identity of each relying party and their contact details.

1d. Member States shall establish ex-post controls to verify that data requests are proportionate and commensurate with the declared intent and that the principle of data minimisation is respected.

1e. The EDIFB or Member States shall revoke authorisation of relying parties in the case of illegal or fraudulent use of the European Digital Identity Wallet, or suspend the authorisation until the identified irregularities have been remedied.

2. Member States shall implement a common mechanism for the ***identification and*** authentication of relying parties ***and the verification of the data sets notified referred in Article 6a(4), points (c) and (d).***

2a. Where relying parties intend to rely upon European Digital Identity Wallets issued in accordance with this Regulation, they shall authenticate and identify themselves to the user of the European Digital Identity Wallet, before any other form of transaction can take place.

3. Relying parties shall be responsible for carrying out the procedure for authenticating ***and validating*** person identification data and electronic attestation of attributes originating from European Digital Identity Wallets. ***Relying parties shall accept the use of pseudonyms, unless the identification of the user is required by Union or national law.***

3a. Intermediaries acting on behalf of relying parties are to be considered relying parties and shall not obtain data about the content of the transaction.

4. ***By*** ~~Within~~ 6 months of the entering into force of this ***amending*** Regulation, the Commission shall establish technical and operational specifications for the requirements referred to in ***this article*** ~~paragraphs 1 and 2~~ by means of ***delegated acts concerning*** ~~an implementing act on~~ the implementation of the European Digital Identity Wallets as referred to in Article 6a(~~10~~ ***11a***).

Article 6c

Certification of the European Digital Identity Wallets

1. European Digital Identity Wallets that have been certified or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to Regulation (EU)

2019/881 and the references of which have been published in the Official Journal of the European Union shall be presumed to be compliant with the cybersecurity relevant requirements set out in Article 6a ***of this Regulation*** ~~paragraphs 3, 4 and 5~~ in so far as the cybersecurity certificate or statement of conformity or parts thereof cover those requirements. ***When relevant European cybersecurity certification schemes are available, the European Digital Identity Wallet, or parts thereof, shall be certified in accordance with such schemes.***

2 [LIBE exclusive] (text to be added for plenary tabling)

2a. ***When relevant European functionality and interoperability certification schemes are available, the European Digital Identity Wallet, or parts thereof, shall be certified in accordance with such schemes. These certification schemes shall provide presumption of conformity to the functionality and interoperability requirements set out in Article 6a. In the absence of certification schemes for functionality and interoperability, standards referred to in Article 6a(10) shall apply.***

3 The conformity of European Digital Identity Wallets with the requirements laid down in article 6a ***of this Regulation*** ~~paragraphs 3, 4 and 5~~ shall be certified by ~~accredited public or private bodies designated by Member States~~ ***conformity assessment bodies in accordance with Article 60 of Regulation (EU) 2019/881 for cybersecurity requirements and by certification bodies in accordance with Article 43 of Regulation (EU) 2016/679 for personal data processing operations***.

3a ***For the purposes of this Article, European Digital Identity Wallets shall not be subject to the requirements referred to in articles 7 and 9.***

4 ***By [***~~Within~~ 6 months ***after the date of entry*** ~~of the entering~~ into force of this ***amending*** Regulation***]***, the Commission shall, by means of implementing acts, establish a list of standards, ***technical specifications, procedures and available European and national cybersecurity certification schemes pursuant to Regulation (EU) 2019/881 necessary*** for the certification of the European Digital Identity Wallets referred to in paragraphs ***2a and*** 3 ***of this Article***. ***Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2) of this Regulation.***

5 Member States shall communicate to the Commission the names and addresses of the ***conformity assessment bodies and certification bodies*** ~~public or private bodies~~ referred to in paragraph 3. The Commission shall make that information available to ***all*** Member States.

6 The Commission shall be empowered to adopt delegated acts in accordance with Article 47 concerning the establishment of specific criteria to be met by the designated bodies referred to in paragraph 3 ***of this Article***.

Article 6d

Publication of a list of certified European Digital Identity Wallets

1 Member States shall inform the Commission without undue delay of the European Digital Identity Wallets that have been issued pursuant to Article 6a and certified by the bodies referred to in Article 6c paragraph 3 They shall also inform the Commission, without undue delay where the certification is cancelled ***and the justification for it***.

2 On the basis of the information received, the Commission shall establish, publish and maintain ***an up to date machine readable*** ~~a~~ list of certified European Digital Identity Wallets.

3 ***By [*** ~~Within~~ 6 months of the entering into force of this ***amending*** Regulation***]***, the Commission shall define formats and procedures applicable for the purposes of paragraph 1. by means of an implementing act on the implementation of the European Digital Identity Wallets as referred to in Article 6a(~~10~~ ***11***).

SECTION II

Electronic identification schemes

Article 7

Eligibility for notification of electronic identification schemes

Pursuant to Article 9(1) Member States shall notify, within 12 months after the entry into force of this Regulation at least one electronic identification scheme including at least one ***electronic*** identification means ***with assurance level 'high' meeting all the following conditions***:

(a) the electronic identification means under the electronic identification scheme are issued:

(i) by the notifying Member State;

(ii) under a mandate from the notifying Member State; or

(iii) independently of the notifying Member State and are recognised by that Member State;

(b) the electronic identification means under the electronic identification scheme can be used to access at least one service which is provided by a public sector body and which requires electronic identification in the notifying Member State;

(c) the electronic identification scheme and the electronic identification means issued thereunder meet the requirements of at least one of the assurance levels set out in the implementing act referred to in Article 8(3);

(d) the notifying Member State ensures that the person identification data uniquely representing the person in question is attributed, in accordance with the technical specifications, standards and procedures for the relevant assurance level set out in the implementing act referred to in Article 8(3), to the natural or legal person referred to in point 1 of Article 3 at the time the electronic identification means under that scheme is issued;

(e) the party issuing the electronic identification means under that scheme ensures that the electronic identification means is attributed to the person referred to in point (d) of this Article in accordance with the technical specifications, standards and procedures for the relevant assurance level set out in the implementing act referred to in Article 8(3);

(f) the notifying Member State ensures the availability of authentication online, so that any relying party established in the territory of another Member State is able to confirm the person identification data received in electronic form.

For relying parties other than public sector bodies the notifying Member State may define terms of access to that authentication. The cross-border authentication shall be provided free of charge when it is carried out in relation to a service online provided by a public sector body.

Member States shall not impose any specific disproportionate technical requirements on relying parties intending to carry out such authentication, where such requirements prevent or significantly impede the interoperability of the notified electronic identification schemes;

(g) at least six months prior to the notification pursuant to Article 9(1), the notifying Member State provides the other Member States for the purposes of the obligation under Article 12(5) a description of that scheme in accordance with the procedural arrangements established by the implementing acts referred to in Article 12(7);

(h) the electronic identification scheme meets the requirements set out in the implementing act referred to in Article 12(8).

Article 8

Assurance levels of electronic identification schemes

1. An electronic identification scheme notified pursuant to Article 9(1) shall specify assurance levels low, substantial and/or high for electronic identification means issued under that scheme.

2. The assurance levels low, substantial and high shall meet respectively the following criteria:

(a) assurance level low shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a limited degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of misuse or alteration of the identity;

(b) assurance level substantial shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a substantial degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease substantially the risk of misuse or alteration of the identity;

(c) assurance level high shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a higher degree of confidence in the claimed or asserted identity of a person than electronic identification means with the assurance level substantial, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to prevent misuse or alteration of the identity.

3. By 18 September 2015, taking into account relevant international standards and subject to paragraph 2, the Commission shall, by means of implementing acts, set out minimum technical specifications, standards and procedures with reference to which assurance levels low, substantial and high are specified for electronic identification means for the purposes of paragraph 1.

Those minimum technical specifications, standards and procedures shall be set out by reference to the reliability and quality of the following elements:

(a) the procedure to prove and verify the identity of natural or legal persons applying for the issuance of electronic identification means;

(b) the procedure for the issuance of the requested electronic identification means;

(c) the authentication mechanism, through which the natural or legal person uses the electronic identification means to confirm its identity to a relying party;

(d) the entity issuing the electronic identification means;

(e) any other body involved in the application for the issuance of the electronic identification means; and

(f) the technical and security specifications of the issued electronic identification means.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 9

Notification

1. The notifying Member State shall notify to the Commission the following information and, without undue delay, any subsequent changes thereto:

   (a) a description of the electronic identification scheme, including its assurance levels and the issuer or issuers of electronic identification means under the scheme;

   (b) the applicable supervisory regime and information on the liability regime with respect to the following:

      i. the party issuing the electronic identification means; and

      ii. the party operating the authentication procedure;

   (c) the authority or authorities responsible for the electronic identification scheme;

   (d) information on the entity or entities which manage the registration of the unique person identification data;

   (e) a description of how the requirements set out in the implementing acts referred to in Article 12(8) are met;

   (f) a description of the authentication referred to in point (f) of Article 7;

   (g) arrangements for suspension or revocation of either the notified electronic identification scheme or authentication or the compromised parts concerned.

2. The Commission shall ***without undue delay*** publish in the Official Journal of the European Union a list of the electronic identification schemes which were notified pursuant to paragraph 1 of this Article and the basic information thereon.

3. The Commission shall publish in the Official Journal of the European Union the amendments to the list referred to in paragraph 2 within one month from the date of receipt of that notification.

4. A Member State may submit to the Commission a request to remove an electronic identification scheme notified by that Member State from the list referred to in paragraph 2. The Commission shall publish in the Official Journal of the European Union the

corresponding amendments to the list within one month from the date of receipt of the Member State's request.

5. The Commission may, by means of implementing acts, define the circumstances, formats and procedures of notifications under paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 10

Security breach *of electronic identification schemes for cross-border authentication*

1. Where either the electronic identification scheme notified pursuant to Article 9(1) or the authentication referred to in point (f) of Article 7 is breached or partly compromised in a manner that affects the reliability of the cross-border authentication of that scheme, the notifying Member State shall, without delay, suspend or revoke that cross-border authentication or the compromised parts concerned, and shall inform other Member States and the Commission.

2. When the breach or compromise referred to in paragraph 1 is remedied, the notifying Member State shall re-establish the cross-border authentication and shall inform other Member States and the Commission without undue delay.

3. If the breach or compromise referred to in paragraph 1 is not remedied within three months of the suspension or revocation, the notifying Member State shall notify other Member States and the Commission of the withdrawal of the electronic identification scheme. The Commission shall publish in the Official Journal of the European Union the corresponding amendments to the list referred to in Article 9(2) without undue delay.

Article 10a

Security breach of the European Digital Identity Wallets

1. Where European Digital ***Identity*** Wallets issued pursuant to Article 6a and the validation mechanisms referred to in Article 6a(5) points (a), (b) and (c) are breached or partly compromised in a manner that affects their reliability ***or the confidentiality, integrity or availability of user data,*** or the reliability of the other European Digital Identity Wallets, the issuing Member State shall, without delay, suspend the issuance and revoke the validity of the European Digital Identity Wallet and inform ***the affected users***, ***single point of contact pursuant to Article 46a***, ***the relying parties*** the other Member States and the Commission accordingly.

1a. After notification of the security breach of the European Digital Identity Wallet, the single point of contact shall liaise with the relevant national competent authorities and, when necessary, with EDIFB, EDPB, the Commission and ENISA.

2. Where the breach or compromise referred to in paragraph 1 is remedied, the issuing Member State shall re-establish the issuance and the use of the European Digital Identity Wallet and inform ***national competent authorities of*** other Member States***, affected users and relying parties, single point of contact pursuant to Article 46a*** and the Commission without undue delay.

3. If ***there has been no attempt or insufficient progress was made to remedy*** the breach or compromise referred to in paragraph 1 ~~is not remedied~~ within three months of the suspension or revocation, the Member State concerned shall withdraw the European

Digital ***Identity*** Wallet concerned and inform ***affected users***, ***single point of contact pursuant to Article 46a***, ***the relying parties*** the other Member States and the Commission on the withdrawal accordingly. Where it is justified by the severity of the breach, the European Digital Identity Wallet concerned shall be withdrawn without delay ***and the relevant decision should be justified and communicated to the Commission.***

4. The Commission shall publish in the Official Journal of the European Union the corresponding amendments to the list referred to in Article 6d without undue delay.

5. Within 6 months of the entering into force of this Regulation, the Commission shall further specify the measures referred to in paragraphs 1 and 3 by means of ***a delegated act adopted in accordance with Article 47***. ~~an implementing act on the implementation of the European Digital Identity Wallets as referred to in Article 6a(10).~~

Article 11

Liability

1. The notifying Member State shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with its obligations under points (d) and (f) of Article 7 in a cross-border transaction.

2. The party issuing the electronic identification means shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligation referred to in point (e) of Article 7 in a cross-border transaction.

3. The party operating the authentication procedure shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to ensure the correct operation of the authentication referred to in point (f) of Article 7 in a cross-border transaction.

4. Paragraphs 1, 2 and 3 shall be applied in accordance with national rules on liability.

5. Paragraphs 1, 2 and 3 are without prejudice to the liability under national law of parties to a transaction in which electronic identification means falling under the electronic identification scheme notified pursuant to Article 9(1) are used.

Article 11a

Cross-border user identification ~~Unique Identification~~

1. When ***accessing cross-border public services that requires identification of the user by Union or national law,*** ~~notified electronic identification means and the European Digital Identity Wallets are used for authentication,~~ Member States shall ensure ~~unique identification~~ ***unequivocal identity matching for natural persons using notified electronic identification means or European Digital Identity Wallets. Member States shall provide for technical and organisational measures to ensure the protection of personal data and prevent profiling of users.***

2. ***In order to identify natural persons upon their request for accessing services as described in paragraph 1,*** Member States shall ***provide a*** ~~, for the purposes of this Regulation, include in the~~ minimum set of person identification data referred to in Article 12.4.(d), ~~a unique and persistent identifier in conformity with Union law, to identify the user upon their request in those cases where identification of the user is required by law~~. ***Member States that have at least one unique identifier shall, at the request of the user,***

issue unique and persistent identifiers for cross border use. Those identifiers may be sector or relying party specific as long as they uniquely identify the user across the Union.

2a. ***Member States shall provide a single unique and persistent identifier for legal persons using electronic identification means or European Digital Identity Wallets.***

3. ***By … [***~~Within~~ 6 months of the entering into force of this ***amending*** Regulation***]***, the Commission shall ***lay down*** further ~~specify the measures referred to in paragraph 1 and 2~~ ***technical specifications that are privacy enhancing and that will ensure trustworthy, secure and interoperable cross-border authentication and identification of users*** by means of an implementing act on the implementation of the European Digital Identity Wallets as referred to in Article 6a(~~10~~***11***).

Article 12

~~Cooperation and~~ **Interoperability**

1. The national electronic identification schemes notified pursuant to Article 9(1) shall be interoperable.

2. For the purposes of paragraph 1, an interoperability framework shall be established.

3. The interoperability framework shall meet the following criteria:

   (a) it aims to be technology neutral and does not discriminate between any specific national technical solutions for electronic identification within a Member State;

   (b) it follows European and international standards, where possible;

   (c) it facilitates the implementation of data protection and security by design

   (d) it ensures that personal data is processed in accordance with Regulation (EU) 2016/679

4. The interoperability framework shall consist of:

   (a) a reference to minimum technical requirements related to the assurance levels under Article 8;

   (b) a mapping of national assurance levels of notified electronic identification schemes to the assurance levels under Article 8;

   (c) a reference to minimum technical requirements for interoperability;

   (d) a reference to a minimum set of person identification data necessary to unequivocally ~~and persistently~~ represent a natural or legal person ***available from electronic identification schemes. In general, insofar as personal data are concerned, the risks to the rights of individuals shall be assessed based on Article 25(1) of Regulation (EU) 2016/679***;

   (e) rules of procedure

   (f) arrangements for dispute resolution; and

   (g) common operational security standards.

~~5. Member States shall cooperate with regard to the following:~~

~~(a) the interoperability of the electronic identification schemes notified pursuant to Article 9(1) and the electronic identification schemes which Member States intend to notify; and~~

~~(b) the security of the electronic identification schemes.~~

~~6. The cooperation between Member States shall consist of:~~

~~(a) the exchange of information, experience and good practice as regards electronic identification schemes and in particular technical requirements related to interoperability, unique identification and assurance levels;~~

~~(b) the exchange of information, experience and good practice as regards working with assurance levels of electronic identification schemes under Article 8;~~

~~(c) peer review of electronic identification schemes falling under this Regulation; and~~

~~(d) examination of relevant developments in the electronic identification sector~~.

7. ~~By 18 March 2015, the Commission shall, by means of implementing acts, establish the necessary procedural arrangements to facilitate the cooperation between the Member States referred to in paragraphs 5 and 6 with a view to fostering a high level of trust and security appropriate to the degree of risk.~~

8. By 18 September 2015, for the purpose of setting uniform conditions for the implementation of the requirement under paragraph 1, the Commission shall, subject to the criteria set out in paragraph 3 and taking into account the results of the cooperation between Member States, adopt implementing acts on the interoperability framework as set out in paragraph 4.

9. The implementing acts referred to ~~in paragraphs 7 and~~ ***paragraph*** 8 of this Article shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 12a

Certification of electronic identification schemes

1 Conformity of notified electronic identification schemes with the requirements laid down in - Article 8 and Article 10 may be certified by ***conformity*** ~~assessment certified by public or private~~ bodies designated by Member States.

2 The peer-review of electronic identification schemes referred to in Article ***46b(5)*** ~~12(6),~~, point (c) ***of this Regulation*** shall not apply to electronic identification schemes or part of such schemes certified in accordance with paragraph 1. Member States may use a certificate or a Union statement of conformity issued in accordance with a relevant European cybersecurity certification scheme established pursuant to Regulation (EU) 2019/881 to demonstrate ***full or partial*** compliance of such schemes ***or parts of such schemes*** with the requirements set out in Article 8(2) ***of this Regulation*** regarding the assurance levels of electronic identification schemes.

2a ***The certification scheme used to demonstrate conformity pursuant to paragraph 1 shall include a two-year vulnerability assessment of the certified product and a continuous threat monitoring, unless such a certification scheme has been established pursuant to Regulation (EU) 2019/881.***

3 Member States shall notify to the Commission with the names and addresses of the ***conformity assessment bodies*** ~~public or private body~~ referred to in paragraph 1. The Commission shall make that information available to ***all*** Member States.

SECTION III

Cross-border reliance on electronic identification means

Article 12b

Cross-border reliance on European Digital Identity Wallets

1. Where Member States require an electronic identification using an electronic identification means and authentication under national law or by administrative practice to access an online service provided by a public sector body, they shall also accept European Digital Identity Wallets issued in compliance with this Regulation ***for electronic identification and authentication and they shall clearly communicate such acceptance to potential users of the service.***

2. Where private relying parties providing services are required by national or Union law, to use strong user authentication for online identification, ~~, or where strong user authentication is required by contractual obligation,~~, including in the areas of transport, energy, banking and financial services, social security, health, drinking water, postal services, digital infrastructure, ~~education or~~ telecommunications ***or education in particular with regard to the recognition of educational and professional qualifications***, private relying parties shall also ***offer and*** accept the use of European Digital Identity Wallets ***and notified electronic identification means with assurance level 'high'*** issued in ***compliance with this Regulation for identification and authentication*** ~~accordance with Article 6a~~***.***

3. Where very large online platforms as defined in Regulation [reference DSA Regulation] Article 25.1. require users to authenticate to access online services, they shall also accept, ***though not exclusively, and facilitate*** the use of European Digital Identity Wallets issued in accordance with Article 6a strictly upon voluntary request of the user and in respect of the ~~the minimum attributes necessary for the specific online service for which authentication is requested, such as proof of age~~ ***right to pseudonyms.***. ***In this case, user generated pseudonyms shall be used in connection to a European Digital Identity Wallet. Very large online platforms shall clearly indicate this possibility to users of the service. The combination of person identification data and any other personal data and identifiers linked to the European Digital Identity Wallets with personal or non-personal data from any other services which are not necessary for the provision of the authentication or use of core services, is prohibited unless the user has expressly requested it.***

4. The Commission shall ***in cooperation with the Member States, industry and the relevant stakeholders, including civil society*** encourage and facilitate the development of self-regulatory codes of conduct at Union level ('codes of conduct'), in order to contribute to wide availability and usability of European Digital Identity Wallets within the scope of this Regulation. These codes of conduct shall ensure acceptance of electronic identification means including European Digital Identity Wallets within the scope of this Regulation in particular by service providers relying on third party electronic identification services for user authentication. The Commission will facilitate the

development of such codes of conduct in close cooperation with all relevant stakeholders and encourage service providers to complete the development of codes of conduct within 12 months of the adoption of this Regulation and effectively implement them within 18 months of the adoption of the Regulation.

~~5. The Commission shall make an assessment within 18 months after deployment of the European Digital Identity Wallets whether on the basis of evidence showing availability and usability of the European Digital Identity Wallet, additional private online service providers shall be mandated to accept the use of the European Digital identity Wallet strictly upon voluntary request of the user. Criteria of assessment may include extent of user base, cross-border presence of service providers, technological development, evolution in usage patterns. The Commission shall be empowered to adopt delegated acts based on this assessment, regarding a revision of the requirements for recognition of the European Digital Identity wallet under points 1 to 4 of this article.~~

~~6. For the purposes of this Article, European Digital Identity Wallets shall not be subject to the requirements referred to in articles 7 and 9~~

Article 12c

Mutual recognition of other electronic identification means

1. Where electronic identification using an electronic identification means and authentication is required under national law or by administrative practice to access an online service provided by a public sector body in a Member State, the electronic identification means, issued in another Member State shall be recognised in the first Member State for the purposes of cross-border authentication for that online service, ***and ensuring mutual recognition*** provided that the following conditions are met:

   (a) the electronic identification means is issued under an electronic identification scheme that is included in the list referred to in Article 9;

   (b) the assurance level of the electronic identification means corresponds to an assurance level equal to or higher than the assurance level required by the relevant public sector body to access that online service in the Member State concerned, and in any case not lower than an assurance level 'substantial';

   (c) the relevant public sector body in the Member State concerned uses the assurance level 'substantial' or 'high' in relation to accessing that online service.

   Such recognition shall take place no later than 6 months after the Commission publishes the list referred to in point (a) of the first subparagraph.

2. An electronic identification means which is issued within the scope of an electronic identification scheme included in the list referred to in Article 9 and which corresponds to the assurance level 'low' may be recognised by public sector bodies for the purposes of cross-border authentication for the online service provided by those bodies.

CHAPTER III

TRUST SERVICES

SECTION 1

General provisions

Article 13

Liability and burden of proof

1. Notwithstanding paragraph 2 of this Article, trust service providers shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under this Regulation and with the cybersecurity risk management obligations under Article 18 of the Directive XXXX/XXXX [NIS2].
2. Where trust service providers duly inform their customers in advance of the limitations on the use of the services they provide and where those limitations are recognisable to third parties, trust service providers shall not be liable for damages arising from the use of services exceeding the indicated limitations.
3. Paragraphs 1 and 2 shall be applied in accordance with national rules on liability.

Article 14 [IMCO exclusive] (text to be added for plenary tabling)

Article 15 [IMCO exclusive] (text to be added for plenary tabling)

Article 16

Penalties

1. ***Without prejudice to article 31 of the Directive (EU) XXXX/XXXX [NIS2],*** Member States shall lay down the rules on penalties applicable to infringements of this Regulation. The penalties provided shall be effective, proportionate and dissuasive***, specially taking into account the SMEs status.***

2. ***Member States shall ensure that infringements by qualified trust service providers of the obligations laid down in this Regulation be subject to administrative fines of a maximum of at least 10 000 000 EUR or 2% of the total worldwide annual turnover of the undertaking to which the qualified trust service provider belongs in the preceding financial year, whichever is higher.***

3. ***Member States shall ensure that infringement by non-qualified trust service providers of the obligations laid down in this Regulation be subject to administrative fines of a maximum of at least 7 000 000 EUR or 1,4% of the total worldwide annual turnover of the undertaking to which the non-qualified trust service provider belongs in the preceding financial year, whichever is higher.***

SECTION 2
Supervision
[Deleted]

Article 17 [Deleted]
Article 18 [Deleted]
Article 19 [Deleted]

SECTION 3

Qualified trust services

Article 20

Supervision of qualified trust service providers

1. Qualified trust service providers shall be audited at their own expense at least every 24 months by a conformity assessment body. ***T***he audit shall confirm that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in this Regulation and in Article 18 of Directive (EU) XXXX/XXXX [NIS2]. ***When components of trust services have been separately certified in accordance with this regulation, the conformity assessment body responsible for certifying the trust service shall not conduct additional audits of these components. Instead, conformity assessment bodies shall ensure that the interactions between the various components do not impede the trust service's compliance with the requirements outlined in this paragraph***. Qualified trust service providers shall submit the resulting conformity assessment report to the supervisory body within three working days of receipt.

2. Without prejudice to paragraph 1, the supervisory body may at any time audit or request a conformity assessment body to perform a conformity assessment of the qualified trust service providers, at the expense of those trust service providers, to confirm that they and the qualified trust services provided by them fulfil the requirements laid down in this Regulation. [last sentence **LIBE exclusive]** [(text to be added for plenary tabling)...].

3. Where the qualified trust service provider fails to fulfil any of the requirements set out by this Regulation, the supervisory body shall require it to provide a remedy within a set time limit, if applicable.

   where that provider does not provide a remedy and, where applicable within the time limit set by the supervisory body, the supervisory body, taking into account in particular, the extent, duration and consequences of that failure, ***shall*** ~~may~~ withdraw the qualified status of that provider or of the service concerned which it provides and, request it, where applicable within a set time limit, to comply with the requirements of Directive XXXX/XXXX[NIS2]. The supervisory body shall inform the body referred to in Article 22(3) for the purposes of updating the trusted lists referred to in Article 22(1).

   The supervisory body shall inform the qualified trust service provider of the withdrawal of its qualified status or of the qualified status of the service concerned.

4. Within 12 months of the entering into force of this regulation, the Commission shall, by means of implementing acts, establish reference number for the following standards:

   (a) the accreditation of the conformity assessment bodies and for the conformity assessment report referred to in paragraph 1;

   (b) the auditing requirements for the conformity assessment bodies to carry out their conformity assessment of the qualified trust service providers as referred to in paragraph 1, carried out by the conformity assessment bodies;

   (c) the conformity assessment schemes for carrying out the conformity assessment of the qualified trust service providers by the conformity assessment bodies and for the provision of the conformity assessment report referred to in paragraph 1.

   Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 21

Initiation of a qualified trust service

1. Where trust service providers, without qualified status, intend to start providing qualified trust services, they shall submit to the supervisory body a notification of their intention together with a conformity assessment report issued by a conformity assessment body.

2. The supervisory body shall verify whether the trust service provider and the trust services provided by it comply with the requirements laid down in this Regulation, and in particular, with the requirements for qualified trust service providers and for the qualified trust services they provide.

   In order to verify the compliance of the trust service provider with the requirements laid down in Article 18 of Dir XXXX [NIS2], the supervisory body shall request the competent authorities referred to in Dir XXXX [NIS2] to carry out supervisory actions in that regard and to provide information about the outcome within three days from their completion.

   Where the supervisory body concludes that the trust service provider and the trust services provided by it comply with the requirements referred to in the first subparagraph, the supervisory body shall grant qualified status to the trust service provider and the trust services it provides and inform the body referred to in Article 22(3) for the purposes of updating the trusted lists referred to in Article 22(1), not later than three months after notification in accordance with paragraph 1 of this Article.

   Where the verification is not concluded within three months of notification, the supervisory body shall inform the trust service provider specifying the reasons for the delay and the period within which the verification is to be concluded.

3. Qualified trust service providers may begin to provide the qualified trust service after the qualified status has been indicated in the trusted lists referred to in Article 22(1).

4. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, define the formats and procedures of the notification and verification for the purposes of paragraphs 1 and 2 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 22

Trusted lists

1. Each Member State shall establish, maintain***, regularly update*** and publish trusted lists, including information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them.

2. Member States shall establish, maintain and publish, in a secured manner, the electronically signed or sealed trusted lists referred to in paragraph 1 in a form suitable for automated processing.

3. Member States shall notify to the Commission, without undue delay, information on the body responsible for establishing, maintaining and publishing national trusted lists, and

details of where such lists are published, the certificates used to sign or seal the trusted lists and any changes thereto.

3a. ***The Commission in coordination with Member States and where relevant ENISA shall develop a harmonised reporting mechanism for qualified trust service providers as well as other interested third parties to appeal in a transparent and duly-justified manner the decision of a Member State in respect to inclusion and removal of a qualified trust service provider from the trust list.***

4. The Commission shall make available to the public, through a secure channel, the information referred to in paragraph 3 in electronically signed or sealed form suitable for automated processing.

5. By 18 September 2015 the Commission shall, by means of implementing acts, specify the information referred to in paragraph 1 and define the technical specifications and formats for trusted lists applicable for the purposes of paragraphs 1 to 4. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

5a. By...[6 months of the entering into force of this amending Regulation] the Commission shall, by means of implemented acts lay down further details on the process referred to in paragraph 3a.

Article 23

EU trust mark for qualified trust services

1. After the qualified status referred to in the second subparagraph of Article 21(2) has been indicated in the trusted list referred to in Article 22(1), qualified trust service providers may use the EU trust mark to indicate in a simple, recognisable and clear manner the qualified trust services they provide.

2. When using the EU trust mark for the qualified trust services referred to in paragraph 1, qualified trust service providers shall ensure that a link to the relevant trusted list is made available on their website.

2a. Paragraph 1 and 2 shall also apply to trust service providers established in third countries and to the services they provide, provided that they have been recognised in the Union in accordance with Article 14.

3. By 1 July 2015 the Commission shall, by means of implementing acts, provide for specifications with regard to the form, and in particular the presentation, composition, size and design of the EU trust mark for qualified trust services. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 24

Requirements for qualified trust service providers

1. When issuing a qualified certificate or a qualified electronic attestation of attributes for a trust service, a qualified trust service provider shall verify the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate or the qualified electronic attestation of attribute is issued.

The information referred to in the first subparagraph shall be verified by the qualified trust service provider, either directly or by relying on a third party, in any of the following ways:

(a) by means of a notified electronic identification means which meets the requirements set out in Article 8 with regard to the assurance level ~~levels 'substantial' or~~ 'high'

(b) by means of ~~qualified electronic attestations of attributes or~~ a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a), (c) or (d)

(c) by using other identification methods which ensure the identification of the natural person with a high level of confidence, the conformity of which shall be confirmed by a conformity assessment body;

(d) through the physical presence of the natural person or of an authorised representative of the legal person by appropriate procedures and in accordance with national laws if other means are not available.

1a. Within 12 months after the entry into force of this Regulation, the Commission shall by means of ***delegated*** ~~implementing~~ acts, set out minimum technical specifications, standards and procedures with respect to the verification of identity and attributes in accordance with paragraph 1, point c. ~~Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).~~

2. A qualified trust service provider providing qualified trust services shall:

(a) inform the supervisory body of any change in the provision of its qualified trust services and an intention to cease those activities;

(b) employ staff and, if applicable, subcontractors who possess the necessary expertise, reliability, experience, and qualifications and who have received appropriate training regarding security and personal data protection rules and shall apply administrative and management procedures which correspond to European or international standards;

(c) with regard to the risk of liability for damages in accordance with Article 13, maintain sufficient financial resources and/or obtain appropriate liability insurance, in accordance with national law;

(d) before entering into a contractual relationship, inform, in a clear, comprehensive and easily accessible manner, in a publicly accessible space and individually any person seeking to use a qualified trust service of the precise terms and conditions regarding the use of that service, including any limitations on its use;

(e) use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them;

(f) use trustworthy systems to store data provided to it, in a verifiable form so that:

(i) they are publicly available for retrieval only where the consent of the person to whom the data relates has been obtained,

(ii) only authorised persons can make entries and changes to the stored data,

(iii) the data can be checked for authenticity;

(fa) 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.

(fb) notify the supervisory body and, where applicable, other relevant bodies of any linked breaches or disruptions in the implementation of the measures referred to in paragraph (fa), points (i), (ii) and, (iii) that has a significant impact on the trust service provided or on the personal data maintained therein.

(g) take appropriate measures against forgery, theft or misappropriation of data or, without right, deleting, altering or rendering data inaccessible;

(h) record and keep accessible for as long as necessary after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service provider, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. Such recording may be done electronically;

(i) have an up-to-date termination plan to ensure continuity of service in accordance with provisions verified by the supervisory body under point (i) of Article 17(4);

(k) in case of qualified trust service providers issuing qualified certificates, establish and keep updated a certificate database.

3. If a qualified trust service provider issuing qualified certificates decides to revoke a certificate, it shall register such revocation in its certificate database and publish the revocation status of the certificate in a timely manner, and in any event within 24 hours after the receipt of the request. The revocation shall become effective immediately upon its publication.

4. With regard to paragraph 3, qualified trust service providers issuing qualified certificates shall provide to any relying party information on the validity or revocation status of qualified certificates issued by them. This information shall be made available at least on a per certificate basis at any time and beyond the validity period of the certificate in an automated manner that is reliable, free of charge and efficient.

4a. Paragraph 3 and 4 shall apply accordingly to the revocation of electronic attestations of attributes.

5. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, establish reference numbers of standards for the requirements referred to in paragraph 2. compliance with the requirements laid down in this Article shall be presumed, where trustworthy systems and products meet those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

6. The Commission shall be empowered to adopt delegated acts regarding the additional measures referred to in paragraph 2(fa).

SECTION 4

Electronic signatures

Article 25

Legal effects of electronic signatures

1. An electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures.
2. A qualified electronic signature shall have the equivalent legal effect of a handwritten signature.
3. A qualified electronic signature based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic signature in all other Member States.

Article 26

Requirements for advanced electronic signatures

An advanced electronic signature shall meet the following requirements:

(a) it is uniquely linked to the signatory;

(b) it is capable of identifying the signatory;

(c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and

(d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

Article 27

Electronic signatures in public services

1. If a Member State requires an advanced electronic signature to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic signatures, advanced electronic signatures based on a qualified certificate for electronic signatures, and qualified electronic signatures in at least the formats or using methods defined in the implementing acts referred to in paragraph 5.
2. If a Member State requires an advanced electronic signature based on a qualified certificate to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic signatures based on a qualified certificate and qualified electronic signatures in at least the formats or using methods defined in the implementing acts referred to in paragraph 5.
3. Member States shall not request for cross-border use in an online service offered by a public sector body an electronic signature at a higher security level than the qualified electronic signature.
4. The Commission may, by means of implementing acts, establish reference numbers of standards for advanced electronic signatures. Compliance with the requirements for advanced electronic signatures referred to in paragraphs 1 and 2 of this Article and in Article 26 shall be presumed when an advanced electronic signature meets those

standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

5. By 18 September 2015, and taking into account existing practices, standards and Union legal acts, the Commission shall, by means of implementing acts, define reference formats of advanced electronic signatures or reference methods where alternative formats are used. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 28

Qualified certificates for electronic signatures

1. Qualified certificates for electronic signatures shall meet the requirements laid down in Annex I.

2. Qualified certificates for electronic signatures shall not be subject to any mandatory requirement exceeding the requirements laid down in Annex I.

3. Qualified certificates for electronic signatures may include non-mandatory additional specific attributes. Those attributes shall not affect the interoperability and recognition of qualified electronic signatures.

4. If a qualified certificate for electronic signatures has been revoked after initial activation, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.

5. Subject to the following conditions, Member States may lay down national rules on temporary suspension of a qualified certificate for electronic signature:

   (a) if a qualified certificate for electronic signature has been temporarily suspended that certificate shall lose its validity for the period of suspension;

   (b) the period of suspension shall be clearly indicated in the certificate database and the suspension status shall be visible, during the period of suspension, from the service providing information on the status of the certificate.

6. Within 12 months after the entry into force of this Regulation, the Commission shall, by means of implementing acts, establish reference numbers of standards for qualified certificates for electronic signature. Compliance with the requirements laid down in Annex I shall be presumed where a qualified certificate for electronic signature meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 29

Requirements for qualified electronic signature creation devices

1. Qualified electronic signature creation devices shall meet the requirements laid down in Annex II.

1a. Generating, managing and duplicating ***qualified*** electronic signature creation data on behalf of the signatory may only be done by a qualified trust service provider providing a qualified trust service for the management of a remote electronic qualified signature creation device.

2. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified electronic signature creation devices. Compliance with the requirements laid down in Annex II shall be presumed where a qualified electronic signature creation device meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 29a

Requirements for a qualified service for the management of remote electronic signature creation devices

1. The management of remote qualified electronic signature creation devices as a qualified service may only be carried out by a qualified trust service provider that:

(a) Generates or manages electronic signature creation data on behalf of the signatory;

(b) notwithstanding point (1)(d) of Annex II, duplicates the electronic signature creation data only for back-up purposes provided the following requirements are met:

(i) the security of the duplicated datasets must be at the same level as for the original datasets;

(ii) the number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service.

(c) complies with any requirements identified in the certification report of the specific remote qualified signature creation device issued pursuant to Article 30.

2. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, establish technical specifications and reference numbers of standards for the purposes of paragraph 1.

Article 30

Certification of qualified electronic signature creation devices

1. Conformity of qualified electronic signature creation devices with the requirements laid down in Annex II shall be certified by appropriate public or private bodies designated by Member States.

2. Member States shall notify to the Commission the names and addresses of the public or private body referred to in paragraph 1. The Commission shall make that information available to Member States.

3. The certification referred to in paragraph 1 shall be based on one of the following:

(a) a security evaluation process carried out in accordance with one of the standards for the security assessment of information technology products included in the list established in accordance with the second subparagraph; or

(b) a process other than the process referred to in point (a), provided that it uses comparable security levels and provided that the public or private body referred to in paragraph 1 notifies that process to the Commission. That process may be used only in the absence of standards referred to in point (a) or when a security evaluation process referred to in point (a) is ongoing.

The Commission shall, by means of implementing acts, establish a list of standards for the security assessment of information technology products referred to in point (a). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

3a. The certification referred to in paragraph 1 shall be valid for 5 years, conditional upon a regular 2 year vulnerabilities assessment. Where vulnerabilities are identified and not remedied, the certification shall be withdrawn.

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 47 concerning the establishment of specific criteria to be met by the designated bodies referred to in paragraph 1 of this Article.

Article 31

Publication of a list of certified qualified electronic signature creation devices

1. Member States shall notify to the Commission without undue delay and no later than one month after the certification is concluded, information on qualified electronic signature creation devices that have been certified by the bodies referred to in Article 30(1). They shall also notify to the Commission, without undue delay and no later than one month after the certification is cancelled, information on electronic signature creation devices that are no longer certified.

2. On the basis of the information received, the Commission shall establish, publish and maintain a list of certified qualified electronic signature creation devices.

3. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, define formats and procedures applicable for the purpose of paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 32

Requirements for the validation of qualified electronic signatures

1. The process for the validation of a qualified electronic signature shall confirm the validity of a qualified electronic signature provided that:

   (a) the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I;

   (b) the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing;

   (c) the signature validation data corresponds to the data provided to the relying party;

   (d) the unique set of data representing the signatory in the certificate is correctly provided to the relying party;

   (e) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;

   (f) the electronic signature was created by a qualified electronic signature creation device;

   (g) the integrity of the signed data has not been compromised;

(h) the requirements provided for in Article 26 were met at the time of signing.

Compliance with the requirements laid down in the first sub-paragraph shall be presumed where the validation of qualified electronic signatures meet the standards referred to in paragraph 3.

2. The system used for validating the qualified electronic signature shall provide to the relying party the correct result of the validation process and shall allow the relying party to detect any security relevant issues.

3. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, establish reference numbers of standards for the validation of qualified electronic signatures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 33

Qualified validation service for qualified electronic signatures

1. A qualified validation service for qualified electronic signatures may only be provided by a qualified trust service provider who:

   (a) provides validation in compliance with Article 32(1); and

   (b) allows relying parties to receive the result of the validation process in an automated manner, which is reliable, efficient and bears the advanced electronic signature or advanced electronic seal of the provider of the qualified validation service.

2. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified validation service referred to in paragraph 1. Compliance with the requirements laid down in paragraph 1 shall be presumed where the validation service for a qualified electronic signature meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 34

Qualified preservation service for qualified electronic signatures

1. A qualified preservation service for qualified electronic signatures may only be provided by a qualified trust service provider that uses procedures and technologies capable of extending the trustworthiness of the qualified electronic signature beyond the technological validity period.

2. Compliance with the requirements laid down in the paragraph 1 shall be presumed where the arrangements for the qualified preservation service for qualified electronic signatures meet the standards referred to in paragraph 3.

3. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, establish reference numbers of standards for the qualified preservation service for qualified electronic signatures. Those implementing acts shall be adopted in accordance with the examination procedure referred to In Article 48(2).

SECTION 5

Electronic seals

Article 35

Legal effects of electronic seals

1. An electronic seal shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic seals.
2. A qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked.
3. A qualified electronic seal based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic seal in all other Member States.

Article 36

Requirements for advanced electronic seals

An advanced electronic seal shall meet the following requirements:

(a) it is uniquely linked to the creator of the seal;

(b) it is capable of identifying the creator of the seal;

(c) it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and

(d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.

Article 37

Electronic seals in public services

1. If a Member State requires an advanced electronic seal in order to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic seals, advanced electronic seals based on a qualified certificate for electronic seals and qualified electronic seals at least in the formats or using methods defined in the implementing acts referred to in paragraph 5.
2. If a Member State requires an advanced electronic seal based on a qualified certificate in order to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic seals based on a qualified certificate and qualified electronic seal at least in the formats or using methods defined in the implementing acts referred to in paragraph 5.

2a. Compliance with the requirements for advanced electronic seals referred to in Article 36 and in paragraph 5 of this Article shall be presumed where an advanced electronic seal meets the standards referred to in paragraph 4.

3. Member States shall not request for the cross-border use in an online service offered by a public sector body an electronic seal at a higher security level than the qualified electronic seal.
4. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, establish reference numbers of standards for advanced electronic seals. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

5. By 18 September 2015, and taking into account existing practices, standards and legal acts of the Union, the Commission shall, by means of implementing acts, define reference formats of advanced electronic seals or reference methods where alternative formats are used. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 38

Qualified certificates for electronic seals

1. Qualified certificates for electronic seals shall meet the requirements laid down in Annex III. Compliance with the requirements laid down in Annex III shall be presumed where a qualified certificate for electronic seal meets the standards referred to in paragraph 6.
2. Qualified certificates for electronic seals shall not be subject to any mandatory requirements exceeding the requirements laid down in Annex III.
3. Qualified certificates for electronic seals may include non-mandatory additional specific attributes. Those attributes shall not affect the interoperability and recognition of qualified electronic seals.
4. If a qualified certificate for an electronic seal has been revoked after initial activation, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.
5. Subject to the following conditions, Member States may lay down national rules on temporary suspension of qualified certificates for electronic seals:
   (a) if a qualified certificate for electronic seal has been temporarily suspended, that certificate shall lose its validity for the period of suspension;
   (b) the period of suspension shall be clearly indicated in the certificate database and the suspension status shall be visible, during the period of suspension, from the service providing information on the status of the certificate.
6. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, establish reference numbers of standards for qualified certificates for electronic seals. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 39

Qualified electronic seal creation devices

1. Article 29 shall apply mutatis mutandis to requirements for qualified electronic seal creation devices.
2. Article 30 shall apply mutatis mutandis to the certification of qualified electronic seal creation devices.
3. Article 31 shall apply mutatis mutandis to the publication of a list of certified qualified electronic seal creation devices.

Article 39a

Requirements for a qualified service for the management of remote electronic seal creation devices

Article 29a shall apply mutatis mutandis to a qualified service for the management of remote electronic seal creation devices.

Article 40

Validation and preservation of qualified electronic seals

Articles 32, 33 and 34 shall apply mutatis mutandis to the validation and preservation of qualified electronic seals.

SECTION 6

Electronic time stamps

Article 41

Legal effect of electronic time stamps

1. An electronic time stamp shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic time stamp.
2. A qualified electronic time stamp shall enjoy the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound.
3. A qualified electronic time stamp issued in one Member State shall be recognised as a qualified electronic time stamp in all Member States.

Article 42

Requirements for qualified electronic time stamps

1. A qualified electronic time stamp shall meet the following requirements:
   (a) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably;
   (b) it is based on an accurate time source linked to Coordinated Universal Time; and
   (c) it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method.

1a. Compliance with the requirements laid down in paragraph 1 shall be presumed where the binding of date and time to data and the accurate time source meet the standards referred to in paragraph 2.

2. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, establish reference numbers of standards for the binding of date and time to data and for accurate time sources. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

SECTION 7

Electronic registered delivery services

Article 43

Legal effect of an electronic registered delivery service

1. Data sent and received using an electronic registered delivery service shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic registered delivery service.

2. Data sent and received using a qualified electronic registered delivery service shall enjoy the presumption of the integrity of the data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt indicated by the qualified electronic registered delivery service.

Article 44

Requirements for qualified electronic registered delivery services

1. Qualified electronic registered delivery services shall meet the following requirements:

   (a) they are provided by one or more qualified trust service provider(s);

   (b) they ensure with a high level of confidence the identification of the sender;

   (c) they ensure the identification of the addressee before the delivery of the data;

   (d) the sending and receiving of data is secured by an advanced electronic signature or an advanced electronic seal of a qualified trust service provider in such a manner as to preclude the possibility of the data being changed undetectably;

   (e) any change of the data needed for the purpose of sending or receiving the data is clearly indicated to the sender and addressee of the data;

   (f) the date and time of sending, receiving and any change of data are indicated by a qualified electronic time stamp.

   In the event of the data being transferred between two or more qualified trust service providers, the requirements in points (a) to (f) shall apply to all the qualified trust service providers.

1a. Compliance with the requirements laid down in paragraph 1 shall be presumed where the process for sending and receiving data meets the standards referred to in paragraph 2.

2. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, establish reference numbers of standards for processes for sending and receiving data. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

SECTION 8

Website authentication

Article 45

Requirements for qualified certificates for website authentication

1. ***Qualified certificates for website authentication shall allow the authentication and identification of the natural or legal person to whom the certificate was issued with a high level of assurance.*** Qualified certificates for website authentication shall ***also*** meet the requirements laid down in Annex IV. Qualified certificates for website authentication shall be deemed compliant ***with this paragraph and*** the requirements laid down in Annex IV where they meet the standards referred to in paragraph 3.
2. Qualified certificates for website authentication referred to in paragraph 1 shall be recognised by web-browsers. ***Web browsers shall not be prevented from taking measures that are both necessary and proportionate to address substantiated risks of breaches of security, user's privacy and loss of integrity of certificates provided such measures are duly justified. In such a case the web browser shall notify without delay of any measure taken to the Commission, to ENISA and to the qualified trust service provider that issued that certificate or set of certificates. This recognition means that*** ~~For those purposes~~ web-browsers shall ensure that the ***relevant*** identity data ***and electronic attestation of attributes*** provided is displayed in a user friendly manner***, where possible, consistent manner, that reflects state of the art regarding accessibility, user awareness and cybersecurity according to best industry standards***. Web-browsers shall ensure support and interoperability with qualified certificates for website authentication referred to in paragraph 1, with the exception of enterprises, considered to be microenterprises and small enterprises in accordance with Commission Recommendation 2003/361/EC in the first 5 years of operating as providers of web-browsing services.
3. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, provide the specifications and reference numbers of standards for qualified certificates for website authentication referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

SECTION 9

Electronic attestation of attributes.

Article 45a

Legal effects of electronic attestation of attributes

[JURI Exclusive] (text to be added for plenary tabling)

Article 45b

Electronic attestation of attributes in public services

When an electronic identification using an electronic identification means and authentication is required under national law to access an online service provided by a public sector body, person identification data in the electronic attestation of attributes shall not substitute electronic identification using an electronic identification means and authentication for electronic identification unless specifically allowed by the Member State or the public sector body. In

such a case, qualified electronic attestation of attributes from other Member States shall also be accepted.

Article 45c

Requirements for qualified *electronic* attestation of attributes

1. Qualified electronic attestation of attributes shall meet the requirements laid down in Annex V. A qualified electronic attestation of attributes shall be deemed to be compliant with the requirements laid down in Annex V, where it meets the standards referred to in paragraph 4.

2. ***Without prejudice to its content,*** qualified electronic attestations of attributes shall not be subject to any mandatory ***technical*** requirement in addition to the requirements laid down in Annex V.

3. Where a qualified electronic attestation of attributes has been revoked after initial issuance, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted. ***Only relying parties the user has shared this attribute with shall be able to link the revocation to those attributes.***

4. ***By*** 6 months of the entering into force of this ***amending*** Regulation, the Commission shall establish reference numbers of standards for qualified electronic attestations of attributes by means of an implementing act on the implementation of the European Digital Identity Wallets as referred to in Article 6a(~~10~~**11**).

Article 45d

Verification of attributes against authentic sources

1. Member States shall ensure that, at least for the attributes listed in Annex VI, wherever these attributes rely on authentic sources within the public sector, measures are taken to allow qualified providers of electronic attestations of attributes to verify ***free of charge*** by electronic means at the request of the user, the authenticity of the attribute directly against the relevant authentic source at national level or via designated intermediaries recognised at national level in accordance with national or Union law.

1a. Authentic sources may issue non-qualified electronic attestation of attributes at the request of the user.

2. ***By … [***~~Within~~ 6 months of the entering into force of this ***amending*** Regulation***]***, taking into account relevant international standards, the Commission shall ***by means of implementing acts*** set out the minimum technical specifications, standards and procedures with reference to the catalogue of attributes and schemes for the attestation of attributes and verification procedures for qualified electronic attestations of attributes by means of an implementing act on the implementation of the European Digital Identity Wallets as referred to in Article 6a(10).

Article 45e

Issuing of electronic attestation of attributes to the European Digital Identity Wallets

1. Providers of qualified electronic attestations of attributes shall provide an interface with the European Digital Identity Wallets issued in accordance in Article 6a.

1a. Public registers shall provide qualified electronic attestation of attributes to the user of a European Digital Identity Wallet at the request of the user.

1b. Non-qualified attestation of attributes can be issued by any trust service provider, an authentic source or directly through a European Digital Identity Wallet.

1c. Providers of electronic attestations of attributes established in a Member State other than the Member State that issued user's European Digital Identity Wallet, shall provide to that user the possibility to request, obtain, store and manage the electronic attestation of attributes in an easy manner, with no additional technical, administrative or procedural requirements in the Wallet issued and managed by the Member State of origin.

Article 45f

Additional rules for the provision of electronic attestation of attributes services

[Exclusive LIBE] (text to be added for plenary tabling)

SECTION 10

Qualified electronic archiving services

Article 45fa

Legal effects of an electronic archiving service

1. The legal effect and the admissibility of data and documents archived using an electronic archiving service as legal evidence shall not be refused on the sole grounds that this service is in an electronic form or does not fulfil the requirements of a qualified electronic archiving service.

2. The data and documents archived using a qualified electronic archiving service shall benefit from a presumption regarding the integrity of the archived data and documents, their availability, their traceability, their accuracy and their origin as well as the identification of users.

Article 45g

Qualified electronic archiving services

1. A qualified electronic archiving service for electronic documents may only be provided by a qualified trust service provider ***which implements*** ~~that uses~~ procedures and ***uses*** technologies ***that ensure that all the requirements for a qualified electronic archiving service are met***. ~~capable of extending the trustworthiness of the electronic document beyond the technological validity period.~~

2. Within ~~12~~ ***24*** months after the entry into force of this Regulation, the Commission shall, by means of implementing acts, establish reference numbers of standards for electronic

archiving services. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 45ga

Requirements for electronic archiving services

1. Qualified electronic archiving services shall meet the following requirements:

(a) they are created or maintained by a qualified trust service provider;

(b) they ensure the integrity and the accuracy of their origin and legal features throughout the conservation period;

(c) they ensure the accuracy of the date and time of the archiving process;

2. Compliance with the requirements laid down in paragraph 1 shall be presumed where an electronic archiving service meets the standards referred to in paragraph 3.

3. The Commission may, by means of implementing acts, establish reference numbers of standards for the processes of reception, storing, deletion and transmission of electronic data or documents. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

~~SECTION 11~~

~~**Electronic ledgers**~~

~~*Article 45h*~~

~~**Legal effects of electronic ledgers**~~

~~1. An electronic ledger shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic ledgers.~~

~~2. A qualified electronic ledger shall enjoy the presumption of the uniqueness and authenticity of the data it contains, of the accuracy of their date and time, and of their sequential chronological ordering within the ledger.~~

~~*Article 45i*~~

~~**Requirements for qualified electronic ledgers**~~

~~1. Qualified electronic ledgers shall meet the following requirements:~~

~~(a) they are created by one or more qualified trust service provider or providers;~~

~~(b) they ensure the uniqueness, authenticity and correct sequencing of data entries recorded in the ledger;~~

~~(c) they ensure the correct sequential chronological ordering of data in the ledger and the accuracy of the date and time of the data entry;~~

~~(d) they record data in such a way that any subsequent change to the data is immediately detectable.~~

~~2. Compliance with the requirements laid down in paragraph 1 shall be presumed where an electronic ledger meets the standards referred to in paragraph 3.~~

~~3. The Commission may, by means of implementing acts, establish reference numbers of standards for the processes of execution and registration of a set of data into, and the creation, of a qualified electronic ledger. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).~~

CHAPTER IV

ELECTRONIC DOCUMENTS

Article 46

Legal effects of electronic documents

An electronic document shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form.

CHAPTER IVa

Governance

Article 46a

National competent authorities and single point of contact

1. Each Member State shall establish one or more new national competent authorities to carry out the tasks assigned to them under Article 46b or designate and existing body for that purpose.

2. Each Member State shall designate one national single point of contact on European digital identity framework (single point of contact). Where a Member State designates only one competent authority, that competent authority shall also be the single point of contact for that Member State.

3. Each single point of contact shall exercise a liaison function to ensure cross-border cooperation of its Member State's authorities with the relevant authorities in other Member States, and, where appropriate, the Commission and ENISA, as well as to ensure cross-sectorial cooperation with other national competent authorities within its Member State.

4. Member States shall ensure that the competent authorities referred to in paragraph 1 have the necessary powers and adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them and thereby to fulfil the objectives of this Regulation. Member States shall ensure effective, efficient and secure cooperation of the designated representatives in the European Digital Identity Framework Board referred to in Article 46c.

5. Each Member State shall notify to the Commission, without undue delay, the designation of the competent authority referred to in paragraph 1 and single point of contact referred to in paragraph 3, their tasks, and any subsequent change thereto. Each Member State shall make public their designation. The Commission shall publish the list of the designated single points of contacts.

Article 46b

Tasks of the national competent authorities

1. *The national competent authorities shall carry the following tasks:*

   (a) *to monitor and enforce the application of this Regulation;*

   (b) *to supervise issuers of European Digital Identity Wallets established in its territory through ex ante and ex post supervisory activities, ensuring that those issuers of European Digital Identity Wallet meet the requirements laid down in this Regulation and to take corrective actions when they fail to do so;*

   (c) *to supervise allegedly unlawful or inappropriate behaviours of relying parties established in its territory, in particular when such behaviours have been reported through European Digital Identity Wallets and apply corrective actions if necessary;*

   (d) *to supervise qualified trust service providers established in the territory of the designating Member State through ex ante and ex post supervisory activities, that those qualified trust service providers and the qualified trust services that they provide meet the requirements laid down in this Regulation;*

   (e) *to take action if necessary, in relation to non-qualified trust service providers established in the territory of the designating Member State, through ex post supervisory activities, when informed that those non-qualified trust service providers or the trust services they provide allegedly do not meet the requirements laid down in this Regulation;*

   (f) *to analyse the conformity assessment reports referred to in Articles 20(1) and 21(1);*

   (g) *to inform the relevant national competent authorities of the Member States concerned, designated pursuant to Directive (EU) XXXX/XXXX [NIS2], of any significant breaches of security or loss of integrity they become aware of in the performance of their tasks and, in the case of a significant breach of security or loss of integrity which concerns other Member States, to inform the single point of contact of the Member State concerned designated pursuant to Directive (EU) XXXX/XXXX (NIS2);*

   (h) *to report to the Commission about its main activities in accordance with paragraph 2;*

   (i) *to carry out audits or request a conformity assessment body to perform a conformity assessment of the qualified trust service providers in accordance with Article 20(2);*

   (j) *to cooperate with supervisory authorities established under Regulation (EU) 2016/679, in particular, by informing them without undue delay, about the results of audits of qualified trust service providers where personal data protection rules have been breached and about security breaches which constitute personal data breaches;*

   (k) *to grant qualified status to trust service providers and to the services they provide and to withdraw this status in accordance with Articles 20 and 21;*

(l) to inform the body responsible for the national trusted list referred to in Article 22(3) about its decisions to grant or to withdraw qualified status, unless that body is also the national competent authority ;

(m) to verify the existence and correct application of provisions on termination plans in cases where the qualified trust service provider ceases its activities, including how information is kept accessible in accordance with Article 24(2), point (h);

(n) to require that trust service providers and issuers of EDIW's remedy any failure to fulfil the requirements laid down in this Regulation;

(o) to cooperate with other national competent authorities and provide them with assistance in accordance with Article 46c.

2. By 31 March each year, each national competent authority shall submit to the Commission a report on its main activities during the previous calendar year.

3. The Commission shall make the annual reports referred to in paragraph 2 available to the European Parliament and the Council and the public.

4. By … [12 months of the entering into force of this amending Regulation], the Commission shall, by means of implementing acts, define the formats and procedures for the report referred to in paragraph 1, point (h). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

5. By … [12 months of the entering into force of this amending Regulation], the Commission shall adopt a delegated act in accordance with Article 47 to further specify the tasks of the national competent authorities referred to in paragraph 1.

Article 46c

The European Digital Identity Framework Board

1. The European Digital Identity Framework Board (the 'EDIFB') shall be established.

2. The EDIFB shall be composed of national competent authorities and the Commission.

3. Stakeholders and all relevant third parties may be invited to attend meetings of the EDIFB and to participate in its work.

4. ENISA shall be invited when issues regarding cyber threats, notification of breaches, cybersecurity certificates or standards or other issues pertaining to the security are discussed.

5. The EDIFB shall have the following tasks:

(a) assist the Commission in the preparation of legislative proposals and policy initiatives in the field of digital wallets, electronic identification means and trust services;

(b) assist and cooperate with the Commission on the preparation of implementing and delegated acts pursuant to this Regulation;

(c) support the consistent application of this Regulation, among other for the purpose of:

(i) exchanging good practices and information regarding the application of the provisions of this Regulation;

(ii) examining the relevant developments in the digital wallet, electronic identification and trust services sectors;

(iii) organising regular joint meetings with relevant interested parties from across the Union to discuss activities carried out by the Board and gather input on emerging policy challenges;

(iv) issuing common guidelines on the implementation of the Regulation;

(v) with the support of ENISA, exchanging information, experience and good practice as regards to all cybersecurity aspects of the European Digital Identity Wallet, the electronic identification schemes and trust services;

(vi) national competent authorities under this Regulation and national competent authorities under Directive (EU) XXXX/XXXX of the European Parliament and of the Council [NIS2] shall cooperate to ensure the continuation of current practices and to build on the knowledge and experience gained in the application of the eIDAS Regulation. In addition, they shall collaborate as to ensure a coherent implementation of the Directive (EU) XXXX/XXXX of the European Parliament and of the Council [NIS2];

(vii) providing guidance in relation to the development and implementation of policies on notification of breaches, coordinated vulnerability disclosure and common measures as referred to in Articles 10 and 10a;

(viii) exchanging best practices and information in relation to the cybersecurity measures of this Regulation and on Directive (EU) XXXX/XXXX of the European Parliament and of the Council [NIS2] as regards to trust services, in relation to cyber threats, incidents, vulnerabilities, awareness raising initiatives, trainings, exercises and skills, capacity building, standards and technical specifications capacity as well as standards and technical specifications;

(ix) carrying out coordinated security risk assessments in cooperation with ENISA;

(x) peer review of notified electronic identification schemes falling under this Regulation.

6. In the framework of the EIDB, Member States may seek mutual assistance:

(a) upon receipt of a justified request from a national competent authority, EIDB shall provide that national competent authority with assistance so that it can be carried out in a consistent manner, which may cover, in particular, information requests and supervisory measures, such as requests to carry out inspections related to the conformity assessment reports as referred to in Articles 20 and 21 regarding the provision of trust services;

(b) where appropriate, Member States may authorise their respective national competent authorities to carry out joint investigations in which staff from other Member States' competent national authority is involved. The arrangements and procedures for such joint actions shall be agreed upon and established by the Member States concerned in accordance with their national law.

7. By … [6 months after the date of entry into force of this amending Regulation] and every two years thereafter, the EIDB shall establish a work programme in respect of actions to be undertaken to implement its objectives and tasks.

8. The Commission may adopt implementing acts laying down procedural arrangements necessary for the functioning of the EIDB. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

CHAPTER V

DELEGATIONS OF POWER AND IMPLEMENTING PROVISIONS

Article 47

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.
2. The power to adopt delegated acts referred to in ~~Article~~ ***Articles 6a(11a), 6c(6), 24 (1a), 24(6),*** 30(4) ***and 46b(5)*** shall be conferred on the Commission for an indeterminate period of time from 17 September 2014.
3. The delegation of power referred to in ~~Article~~ ***Articles 6a(11a), 6c(6), 24 (1a), 24(6),*** 30(4) ***and 46b(5)*** may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.
4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.
5. A delegated act adopted pursuant to ~~Article~~ ***Articles 6a(11a), 6c(6), 24 (1a), 24(6),*** 30(4) ***and 46b(5)*** shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Article 48

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

Article 48a

Reporting requirements

1. Member States shall ensure the collection of statistics in relation to the functioning of the European Digital Identity Wallets and the qualified trust services.
2. The statistics collected in accordance with paragraph 1, shall include the following:
   (a) the number of natural and legal persons having a valid European Digital Identity Wallet;
   (b) the type and number of services accepting the use of the European Digital ***Identity*** Wallet ***and the number and justifications of rejection of application of service providers aiming to become a relying party;***
   (ba) ***the number of user complaints and consumer protection or data protection incidents relating to relying parties and qualified trust services;***
   (c) ***the type and number of*** incidents and down time of the infrastructure at national level preventing the use of European Digital Identity Wallet ~~Apps~~ ;
   (ca) ***the type and number of security incidents, suspected data breaches and affected users of European Digital Identity Wallet or qualified trust services;***
3. The statistics referred to in paragraph 2 shall be made available to the public in an open and commonly used, machine-readable format.
4. By March each year, Member States shall submit to the Commission a report on the statistics collected in accordance with paragraph 2.

CHAPTER VI

FINAL PROVISIONS

Article 49

Review

1. The Commission shall review the application of this Regulation and shall report to the European Parliament and to the Council within 24 months after its entering into force. The Commission shall evaluate in particular whether it is appropriate to modify the scope of this Regulation or its specific provisions taking into account the experience gained in the application of this Regulation, as well as technological, market and legal developments. Where necessary, that report shall be accompanied by a proposal for amendment of this Regulation.
2. The evaluation report shall include an assessment of the availability***, security*** and usability of the identification means including European Digital Identity Wallets in scope of this Regulation and assess whether all online private service providers relying on third party electronic identification services for users authentication, shall be mandated to accept the use of notified electronic identification means and European ***Digital Identity Wallet.***
3. In addition, the Commission shall submit a report to the European Parliament and the Council every four years after the report referred to in the first paragraph on the progress towards achieving the objectives of this Regulation.

Article 50

Repeal

1. Directive 1999/93/EC is repealed with effect from 1 July 2016.
2. References to the repealed Directive shall be construed as references to this Regulation.

Article 51

Transitional measures

1. Secure signature creation devices of which the conformity has been determined in accordance with Article 3(4) of Directive 1999/93/EC shall continue to be considered as qualified electronic signature creation devices under this Regulation until [date – OJ please insert period of four years following the entry into force of this Regulation].
2. Qualified certificates issued to natural persons under Directive 1999/93/EC shall continue to be considered as qualified certificates for electronic signatures under this Regulation until [date – PO please insert a period of four years following the entry into force of this Regulation].

Article 52

Entry into force

1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.
2. This Regulation shall apply from 1 July 2016, except for the following:
   (a) Articles 8(3), 9(5), 12(2) to (9), 17(8), 19(4), 20(4), 21(4), 22(5), 23(3), 24(5), 27(4) and (5), 28(6), 29(2), 30(3) and (4), 31(3), 32(3), 33(2), 34(2), 37(4) and (5), 38(6), 42(2), 44(2), 45(2), and Articles 47 and 48 shall apply from 17 September 2014;
   (b) Article 7, Article 8(1) and (2), Articles 9, 10, 11 and Article 12(1) shall apply from the date of application of the implementing acts referred to in Articles 8(3) and 12(8);
   (c) Article 6 shall apply from three years as from the date of application of the implementing acts referred to in Articles 8(3) and 12(8).
3. Where the notified electronic identification scheme is included in the list published by the Commission pursuant to Article 9 before the date referred to in point (c) of paragraph 2 of this Article, the recognition of the electronic identification means under that scheme pursuant to Article 6 shall take place no later than 12 months after the publication of that scheme but not before the date referred to in point (c) of paragraph 2 of this Article.
4. Notwithstanding point (c) of paragraph 2 of this Article, a Member State may decide that electronic identification means under electronic identification scheme notified pursuant to Article 9(1) by another Member State are recognised in the first Member State as from the date of application of the implementing acts referred to in Articles 8(3) and 12(8). Member States concerned shall inform the Commission. The Commission shall make this information public.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, xxxxx.

For the Parliament	For the Council
The President	The President

Recitals

(1) The Commission Communication of 19 February 2020, entitled "Shaping Europe's Digital Future"[1] announced a revision of Regulation (EU) No 910/2014 of the European Parliament and of the Council with the aim of improving its effectiveness, extend its benefits to the private sector and promote trusted digital identities for all Europeans.

(2) In its conclusions of 1-2 October 2020[2], the European Council called on the Commission to propose the development of a Union-wide framework for secure public electronic identification, including interoperable digital signatures, to provide people with control over their online identity and data as well as to enable access to public, private and cross-border digital services.

(2a) ***The Digital Decade Policy Programme 2030 sets the objective and digital target of a Union framework which, by 2030, leads to wide deployment of a trusted, voluntary, user-controlled digital identity, that will be recognised throughout the Union and allow each user to control their data and presence in online interactions.***

(3) ~~The Commission Communication of 9 March 2021 entitled "2030 Digital Compass: the European way for the Digital Decade" sets the objective of a Union framework which, by 2030, leads to wide deployment of a trusted, user-controlled identity, allowing each user to control their own online interactions and presence.~~

(3a) The Commission Declaration of 26 January 2022 entitled "European Declaration on Digital Rights and Principles for the Digital Decade" underlines every citizen's right to access digital technologies, products and services that are safe, secure, and privacy-protective by design. This includes ensuring that all Europeans are offered an accessible, secure and trusted digital identity that enables access to a broad range of online and offline services, protected against all cyberthreats, including identity theft or manipulation. The Commission Declaration also states that everyone has the right to the protection of their personal data online. That right encompasses the control on how the data is used and with whom it is shared.

(3b) ***Union citizens should have the right to a digital identity that is under their sole control and that enables them to exercise their rights as citizens in the digital environment and to participate in the digital economy. A European digital identity should be legally recognised throughout the Union.***

(4) A more harmonised approach to digital identification should reduce the risks and costs of the current fragmentation due to the use of divergent national solutions ***or, in some Member States, lack thereof*** and will strengthen the Single Market by allowing citizens, other residents as defined by national law and ~~businesses~~ ***legal entities*** to identify ***and authenticate*** online ***and offline*** in a ***safe, trustworthy, user friendly,*** convenient, ***accessible and harmonised*** ~~and uniform~~ ***way,*** across the Union. Everyone should be able to securely access public and private services relying on an improved ecosystem for trust services and on verified proofs of identity and electronic attestations of attributes, such as ***academic qualifications,*** university ~~degree~~ ***degrees or other educational or professional attainments*** legally recognised and accepted everywhere in the Union, ***or a license or a mandate to represent a company , whilst creating an uniform set of rules for providers of electronic attestations that ensures a level playing field.*** The framework for a European Digital Identity aims to achieve a shift from the reliance on national digital

---

1 COM/2020/67 final

2 https://www.consilium.europa.eu/en/press/press-releases/2020/10/02/european-council-conclusions-1-2-october-2020/

identity solutions only, to the provision of electronic attestations of attributes valid ***and legally recognised across the Union*** ~~at European level~~**.** Providers of electronic attestations of attributes should benefit from a clear and uniform set of rules and public administrations should be able to rely on electronic documents ~~in a given format~~ ***that are highly secured and accepted across the Union. With regards to electronic identification for public services with very high security identification requirements, Member States should be allowed to enable notaries and other professionals entrusted with special powers in the public interest to rely on additional remote identity controls, set out in accordance with the principle of proportionality through national legislation.***

(5) To support the competitiveness of European businesses, online ***and offline*** service providers should be able to rely on digital identity solutions recognised across the Union, irrespective of the Member State in which they have been issued, thus benefiting from a harmonised European approach to trust, security and interoperability. Users and service providers alike should be able to benefit from the same legal value provided to electronic attestations of attributes across the Union. ***Harmonised digital identity framework has the potential to create economic value by providing easier access to goods and services, by significantly reducing operational costs linked to identification and authentication procedures, for example during the on-boarding of new customers, by reducing damages related to cybercrimes, such as identity theft, data theft and online fraud, and by promoting digital transformation of the Union's micro, small and medium sized enterprises (SMEs).***

(5a) ***A fully harmonised digital identity framework would contribute to the creation of a more digitally integrated Union, taking down the digital barriers between Member States and empower the Union citizens and Union residents to enjoy the benefits of digitalization while increasing transparency and the protection of their rights.***

(5b) In order to encourage digitalisation of the Member States' public sector services and to ensure wide up-take of the European digital identity framework and the European Digital Identity Wallets, this Regulation should support the use of the 'once only' principle in order to reduce administrative burden, to support cross-border mobility of citizens and businesses, and to foster development of interoperable e-government services across the Union. The cross-border application of the 'once only' principle should result in citizens and businesses not having to supply the same data to public authorities more than once, and that it should also be possible to use those data only at the request of the user for the purposes of completing cross border online procedures. The implementation of this Regulation and of the 'once-only' principle should comply with all applicable data protection rules, including the principle of data minimisation, accuracy, storage limitation, integrity and confidentiality, necessity, proportionality and purpose limitation. The application of the 'once-only' principle should be done with the explicit consent of the user.

(6) [LIBE exclusive] (text to be added for plenary tabling)

(6a) ***The European Digital Identity Wallet should have the function of a privacy management dashboard embedded into the design, in order to ensure a higher degree of transparency and control of the users over their data. This function should provide an easy, user friendly interface with an overview of all relying parties with whom the user has shared data, including attributes, and the type of data shared with each relying party. It should allow the user to track all transactions executed through the wallet, with at least the following data: the time and date of the transaction, the counterpart identification, the data requested and the data shared. That information should be***

stored even if the transaction was not concluded. The information contained in the transaction history should be non repudiable for any legal purpose. Such a function should be active by default. It should allow users to easily request to a relying party the immediate deletion of personal data pursuant Article 17 of the GDPR and to easily report to the competent national authority where a relying party is established if an unlawful or inappropriate request of data is received without leaving the wallet;

(6b) Zero Knowledge Proof (ZKP) allows verification of a claim without revealing the data that proves it, based on cryptographic algorithms. The European Digital Identity Wallet should allow for verification of claims inferred from personal data identification or attestation of attributes without having to provide the source data, to preserve the privacy of the user of the European Digital Identity Wallet.

(7) It is necessary to set out the harmonised conditions for the establishment of a framework for European Digital Identity Wallets to be issued ***directly*** by a Member State***, under a mandate from a Member State or recognised by a Member State,*** which should empower all Union citizens and other residents as defined by national law to ***securely request, receive, store, combine and selectly*** share ~~securely~~ data related to their identity ***and request deletion of their personal data*** in a user-friendly ~~and convinient~~ way ***and*** under the sole control of the user. ***The selective disclosure of electronic attestation of attributes should be without any setting by default. All data should be stored by default on the user's device unless the user explicitly choses otherwise. This Regulation should reflect shared values and uphold fundamental rights, strong ethical aspects, legal safeguards and liability, thus protecting our democratic societies and citizens.*** Technologies used to achieve those objectives should be developed aiming towards the highest level of ***privacy and*** security, user convenience, ***accessibility,*** and wide usability ***and seamless interoperability***. Member States should ensure equal access to ***and voluntary use of*** digital identification to all their nationals and residents. ***Member States should not, directly or indirectly, limit access to public services or public-funded services to natural or legal persons deciding not to use the European Digital Identity Wallet and should develop and ensure free availability of alternative solutions for such individuals. Private relying parties using the European Digital Identity Wallet to provide services should not deny those services or create disadvantageous conditions to consumers not using the European Digital Identity Wallet to access their services.***

(7a) EDIW issued directly by a Member State means that a competent authority of the Member State is directly responsible for the issuance and management of the Wallet using their own resources. EDIW issued under a mandate from a Member State means that the competent authority of the Member State has authorized a specific organisation to issue and manage the wallet on their behalf on the basis of a public procurement procedure based on transparent, open and fair competition process in which all interested parties have the opportunity to participate and the best candidate is selected based on specific objective criteria and evaluation process. EDIW issued and managed independently but recognised by a Member State means that the competent authority of the Member State has selected a specific organisation who has already developed a EDIW that complies with the requirements of this Regulation. The issuer and the manager of a EDIW does not necessarily need to be the same entity.

(8) In order to ensure compliance within Union law or national law compliant with Union law, ***relying parties*** ~~service providers~~ should ***register*** ~~communicate~~ their intent to rely on

the European Digital Identity Wallets ***in the*** ~~to~~ Member ***State*** ~~States~~ ***where they are established***. That will allow Member States 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 sensitive data, like health data, can be verified by relying parties in accordance with Union law or national law. ***The registration and approval processes should be cost-effective and proportional to the risk. The registration should include the data the relying party intend to request, the intended use and the justification of the need of such data, per each different category of services provided by the relying party. Relying parties should justify that their request complies with data minimisation principles.***

(9) All European Digital Identity Wallets should ***enable*** ~~allow~~ users to electronically identify and authenticate online and offline across borders for accessing a wide range of public and private services. Without prejudice to Member States' prerogatives as regards the identification of their nationals and residents, Wallets can also serve the institutional needs of public administrations, international organisations and the Union's institutions, bodies, offices and agencies. Offline use would be important in many sectors, including in the health sector where services are often provided through face-to-face interaction and ePrescriptions should be able to rely on QR-codes or similar technologies to verify authenticity. Relying on the level of assurance "high" ***for identity proofing***, the European Digital Identity Wallets should benefit from the potential offered by tamper-proof solutions such as secure elements, to comply with the security requirements under this Regulation. ***When on-boarding into the European Digital Identity Wallet, users should obtain the qualified electronic signature, free of charge and by default, without having to go through any additional administrative or technical procedures.*** ~~The European Digital Identity Wallets should also allow users to create and use qualified electronic signatures and seals which are accepted across the EU~~ To achieve simplification and cost reduction benefits to persons and businesses across the ***Union*** ~~EU~~, including by enabling powers of representation and e-mandates, Member States should issue European Digital Identity Wallets relying on common standards ***and technical specifications*** to ensure seamless interoperability and ***to adequately increase the IT*** ~~and a high level of~~security, ***strengthen robustness against cyber-attacks and thus significantly reduce the potential risks of ongoing digitalisation for citizens and businesses***. Only Member States' competent authorities can provide a high degree of confidence in establishing the identity of a person and therefore provide assurance that the person claiming or asserting a particular identity is in fact the person he or she claims to be. It is therefore necessary ***for issuing*** ~~that~~ of the European Digital Identity Wallets to rely on the legal identity of citizens, other residents or legal entities. ***The reliance on the legal identity should not hinder the possibility of the users of the EIDW to access services through the use of pseudonyms, where there is no legal requirement for legal identity for authentication*** Trust in the European Digital Identity Wallets would be enhanced by the fact that issuing ***and managing*** parties are required to implement appropriate technical and organisational measures to ensure ***the highest*** level of security ***that is*** commensurate to the risks raised for the rights and freedoms of the natural persons, in line with Regulation (EU) 2016/679.

(9a) ***European Digital Identity Wallets should include a functionality to generate freely chosen and user managed pseudonyms, as a form of authentication to access online services provided, including services provided by very large online platforms as defined in Regulation (EU) 2022/... of the European Parliament and of the Council on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2020/0361(COD)reference to DSA].***

(9b). ***Member States should develop harmonised approaches to enable the technical possibility for persons with limited legal capacity, such as minors and for persons with no legal capacity, to use European Digital Identity Wallets, trust services and end-user products.***

(9c). ***Natural and legal persons should be able to give permission to a third natural or legal person's European Digital Identity Wallet to perform certain actions on their behalf. Uses cases would include powers of attorney, delegation of authority for specific transactions to specific employees or subcontractors in case of a company or parents acting on behalf of minor children.***

(10) In order to achieve a high level of security and trustworthiness, this Regulation establishes the requirements for European Digital Identity Wallets. The conformity of European Digital Identity Wallets with those requirements should be certified by accredited public or private sector bodies designated by Member States. Relying on a certification scheme based on the availability of commonly agreed standards with Member States should ensure a high level of trust and interoperability. Certification should in particular rely on the relevant European cybersecurity certifications schemes established pursuant to Regulation (EU) 2019/881[3]. Such certification should be without prejudice to certification as regards personal data processing pursuant to Regulation (EC) 2016/679

(10a) Transparency of European Digital Identity Wallets and accountability of their issuers are key elements to create social trust on the framework. All issuers of European Digital Identity Wallets should make the source code available to the public for its scrutiny, in particular for privacy and security. Issuers and managers of European Digital Identity Wallets should be subject to similar controls and liabilities as Qualified Trust Services Providers.

(11) European Digital Identity Wallets should ensure the highest level of security for the personal data used for ***identification and*** authentication irrespective of whether such data is stored locally***, in decentralised ledgers*** or on cloud-based solutions, ***and*** taking into account the different levels of risk. Using biometrics to ***identify and*** authenticate ***should not be a precondition for using European Digital Identity Wallet, notwithstanding the requirement for strong user authentication. Biometric data used for the purpose to authenticate a natural person in the context of this Regulation should not be stored in the cloud without the explicit consent of the user. Using biometrics*** is one of the identifications methods providing a high level of confidence, ~~in particular~~when used in combination with '***what you know' factor***~~other elements of authentication~~. Since biometrics represents a unique characteristic of a person, the use of biometrics ***should not be obligatory. Furthermore the use of biometric data should be limited to specific scenarios pursuant to Article 9 of Regulation (EU) 2016/679, and*** requires organisational and security measures, commensurate to the risk that such processing may entail to the rights and freedoms of natural persons and in accordance with Regulation 2016/679. ***Storing information from the European Digital Identity Wallet in the cloud should be an optional feature only active after the user has given explicit consent. Where the European Digital Identity Wallet is issued on a personal electronic device***

---

[3] 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), OJ L 151, 7.6.2019, p. 15

of the user its cryptographic material should be, when technologically possible, stored in the secure elements of the device.

(11a) European Digital Identity Wallets should be secure-by-design. They should implement advanced security features to protect against identity theft, data theft, denial of service and any other cyberthreat. This includes state of the art encryption and storage methods that are only accessible to and decryptable by the user, and establishing end-to-end encrypted communication with other wallets and relying parties. Additionally, the wallet should require secure explicit, and active use confirmation for operations.

(11b) The use of the European Digital Identity Wallets as well as discontinuation of their use is a right and a choice of users. Member States should develop a simple, user friendly, speedy and secure procedure for the users to request immediate revocation of validity of the European Digital Identity Wallets. For the situations when users are in possession of the device, this functionality should be designed as an integrated feature of the Wallet. A user friendly and speedy remote mechanism should be established for the cases when users do not hold the device in possession, such as theft or loss. Upon death of the user or cease of activity of a legal person, a mechanism should be established to enable the authority responsible for settling the succession of the natural person or assets of the legal person to request the immediate termination of the Wallet.

(11c) In order to promote uptake of the European Digital Identity Wallet and the use of digital identity more broadly, Member States should not only show the benefits of the relevant services, but also, in cooperation with the private sector, researchers and academia, develop training programmes aimed at strengthening the digital skills of their citizens and residents, in particular for vulnerable groups such as persons with disabilities, elderly or persons lacking digital skills.

(12) To ensure that the European Digital Identity framework is open to innovation, technological development and future-proof, Member States should be encouraged to ~~set up~~ jointly ***set-up*** sandboxes to test innovative solutions in a controlled, ***time limited*** and secure environment in particular to improve the functionality, protection of personal data, security and interoperability of the solutions and to inform future updates of technical references and legal requirements. This environment should foster the inclusion of European Small and Medium Enterprises, start-ups and individual innovators and researchers ***as well as relevant industry stakeholders while improving compliance and preventing the placing on the market of solutions which infringe Union law on data protection and IT security***.

(13) Regulation (EU) No 2019/1157[4] strengthens the security of identity cards with enhanced security features by August 2021. Member States should consider the feasibility of notifying them under electronic identification schemes to extend the cross-border availability of electronic identification means.

(14) The process of notification of electronic identification schemes should be ***improved*** ~~simplified~~and accelerated to promote the access to convenient, trusted, secure and innovative authentication and identification solutions and, where relevant, to encourage private identity providers to offer electronic identification schemes to Member State's

[4] Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement (OJ L 188, 12.7.2019, p. 67).

authorities for notification as national electronic identity card schemes under Regulation 910/2014.

(15) Streamlining of the current notification and peer-review procedures will prevent heterogeneous approaches to the assessment of various notified electronic identification schemes and facilitate trust-building between Member States. New, simplified, mechanisms should foster Member States' cooperation on the security and interoperability of their notified electronic identification schemes.

(16) Member States should benefit from new, flexible tools to ensure compliance with the requirements of this Regulation and of the relevant implementing acts. This Regulation should allow Member States to use reports and assessments performed by accredited conformity assessment bodies or voluntary ICT security certification schemes, such as certification schemes to be established at Union level under Regulation (EU) 2019/881, to support their claims on the alignment of the schemes or of parts thereof with the requirements of the Regulation on the interoperability and the security of the notified electronic identification schemes.

(17) Service providers use the identity data provided by the set of person identification data available from electronic identification schemes pursuant to Regulation (EU) No 910/2014 in order to match users from another Member State with the legal identity of that user. However, despite the use of the eIDAS data set, in many cases ensuring an accurate match requires additional information about the user and specific unique identification procedures at national level. ***In order to ensure a high-level of trust and security of personal data of natural persons, different technical solutions should be considered, including*** the use ***or combination of various cryptographic techniques, such as cryptographically verifiable identifiers***. To further support the usability of electronic identification means ***and implementation of 'once-only' principle,*** this Regulation should require Member States to take specific measures to ensure a correct identity match in the process of electronic identification. ***exclusively for the cross-border access of public services that requires the identification of the user by law. Specifically, this requirement should not be read as a call for a centralized identity register in the Union for natural persons and reliance would be placed on decentralized national registers. The use of person identification data or a combination of person identification data, including the use of unique and persistent identifiers issued by Member States or generated by the European Digital Identity Wallet is important for ensuring that the identity of the user can be verified. Member State law should be able to require the use of sector- or relying party specific unique and persistent identifiers. The European Digital Identity Wallet should be capable of storing those identifiers and disclosing them where requested by the user.*** For the same purpose, this Regulation should ~~also~~ extend the mandatory minimum data set and require the use of a unique and persistent electronic identifier ***for legal persons*** in conformity with Union law~~ in those cases where it is necessary to legally identify the user upon his/her request in a unique and persistent way~~.

(17a) ***When accessing public and private services cross-borders, authentication and identification of a user of the Wallet should be possible. The receiving Member States should be able to unequivocally identify the user upon their request in those cases where identification of the user is required by law and proceed to identity matching. In order to ensure high-level of trust and security of personal data, different technical solutions should be considered, including the use or combination of various cryptographic techniques, such as cryptographically verifiable identifiers, unique***

user-generated digital pseudonyms, self-sovereign identities and domain specific identifiers using state of the art encryption technology.

(18) [IMCO exclusive] (text to be added for plenary tabling)

(19) This Regulation should not cover aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form laid down by national or Union law. In addition, it should not affect national form requirements pertaining to public registers, in particular commercial and land registers.

(20) The provision and use of trust services are becoming increasingly important for international trade and cooperation. International partners of the EU are establishing trust frameworks inspired by Regulation (EU) No 910/2014. Therefore, in order to facilitate the recognition of such services and their providers, implementing legislation may set the conditions under which trust frameworks of third countries could be considered equivalent to the trust framework for qualified trust services and providers in this Regulation, as a complement to the possibility of the mutual recognition of trust services and providers established in the Union and in third countries in accordance with Article 218 of the Treaty.

(21) ***Issuers of European Digital Identity Wallets may need access to specific hardware and software features of smartphones, such as parts of the operating system, secure hardware (secure element, SIM etc.), NFC, Bluetooth, Wi-Fi Aware and biometric sensors. Such features are under the control of operating system and equipment manufacturers. Therefore t***his Regulation should build on Union acts ensuring contestable and fair markets in the digital sector. In particular, it builds on ***Article 6(7) of*** the Regulation ***2022/1925*** (Digital Markets Act), which ***requires the*** ~~introduces rules for~~ providers of core platform services designated as gatekeepers ~~to require business users to use, offer or interoperate with an identification service of the gatekeeper in the context of services offered by the business users using the core platform services of that gatekeeper. Article 6(1)(f) of the Regulation XXX/XXXX [Digital Markets Act] requires gatekeepers~~ to allow business users and ***alternative*** providers of ~~ancillary~~ services ***provided together with, or in support of, core platform services, free of charge, effective*** ~~access to and~~ interoperability with***, and access for the purposes of interoperability to,*** the same operating system, hardware or software features ***, regardless of whether those features are part of the operating system, as*** ~~that~~ are available ***to*** or used ***by that*** ~~in the provision by the~~ gatekeeper ***when providing such*** ~~of any ancillary~~ services. ~~According to Article 2 (15) of [Digital Markets Act] identification services constitute a type of ancillary services. Business users and providers of ancillary services should therefore be able to access such hardware or software features, such as secure elements in smartphones, and to interoperate with them through the European Digital Identity Wallets or Member States' notified electronic identification means.~~

(21a) ***This Regulation seeks to facilitate creation, choice and switching between different European Digital Identity Wallets. In order to avoid lock-in effects, the issuers of the European Digital Identity Wallets should at the request of the user of the Wallet, provide for effective portability of data, including provisions of continuous and real-time access to services, and not be allowed to use contractual, economic or technical barriers to prevent or to discourage effective switching between different European Digital Identity Wallets.***

(22) In order to streamline the cybersecurity obligations imposed on trust service providers, as well as to enable these providers and their respective competent authorities to benefit

from the legal framework established by Directive XXXX/XXXX (NIS2 Directive), trust services are required to take appropriate technical and organisational measures pursuant to Directive XXXX/XXXX (NIS2 Directive), such as measures addressing system failures, human error, malicious actions or natural phenomena in order to manage the risks posed to the security of network and information systems which those providers use in the provision of their services as well as to notify significant incidents and cyber threats in accordance with Directive XXXX/XXXX (NIS2 Directive). With regard to the reporting of incidents, trust service providers should notify any incidents having a significant impact on the provision of their services, including such caused by theft or loss of devices, network cable damages or incidents occurred in the context of identification of persons. The cybersecurity risk management requirements and reporting obligations under Directive XXXXXX [NIS2] should be considered complementary to the requirements imposed on trust service providers under this Regulation. Where appropriate, established national practices or guidance in relation to the implementation of security and reporting requirements and supervision of compliance with such requirements under Regulation (EU) No 910/2014 should continue to be applied by the competent authorities designated under Directive XXXX/XXXX (NIS2 Directive). Any requirements pursuant to this Regulation do not affect the obligation to notify personal data breaches under Regulation (EU) 2016/679.

(23) Due consideration should be given to ensure effective cooperation between the NIS and eIDAS authorities. In cases where the supervisory body under this Regulation is different from the competent authorities designated under Directive XXXX/XXXX [NIS2], those authorities should cooperate closely, in a timely manner by exchanging the relevant information in order to ensure effective supervision and compliance of trust service providers with the requirements set out in this Regulation and Directive XXXX/XXXX [NIS2]. In particular, the supervisory bodies under this Regulation should be entitled to request the competent authority under Directive XXXXX/XXXX [NIS2] to provide the relevant information needed to grant the qualified status and to carry out supervisory actions to verify compliance of the trust service providers with the relevant requirements under NIS 2 or require them to remedy non-compliance.

(24) It is essential to provide for a legal framework to facilitate cross-border recognition between existing national legal systems related to electronic registered delivery services. That framework could also open new market opportunities for Union trust service providers to offer new pan-European electronic registered delivery services and ensure that the identification of the recipients is ensured with a higher level of confidence than the identification of the sender.

(25) ~~In most cases, citizens and other residents cannot digitally exchange, across borders, information related to their identity, such as addresses, age and professional qualifications, driving licenses and other permits and payment data, securely and with a high level of data protection.~~

(26) It should be possible to issue and handle trustworthy digital attributes and contribute to reducing administrative burden, empowering citizens and other residents to use them in their private and public transactions. Citizens and other residents should be able, for instance, to demonstrate ownership of a valid driving license issued by an authority in one Member State, which can be verified and relied upon by the relevant authorities in other Member States, to rely on their social security credentials or on future digital travel documents in a cross border context.

(27) [JURI exclusive] (text to be added for plenary tabling)

(28) Wide availability and usability of the European Digital Identity Wallets require their acceptance ***and trust*** by ***both private individuals*** and private service providers. Private relying parties providing services in the areas of transport, energy, banking and financial services, social security, health, drinking water, postal services, digital infrastructure, education or telecommunications should accept the use of European Digital Identity Wallets for the provision of services where strong user authentication for online identification is required by national or Union law ~~or by contractual obligation~~. ***The information requested from the user via the European Digital Identity Wallet has to be necessary and proportionate for the intended use case of the relying party and follow the principle of data minimisation, ensuring transparency over what data is shared and for what purposes***.Where very large online platforms as defined in Article 25.1. of Regulation [reference DSA Regulation] require users to authenticate to access online services, those platforms should be mandated to accept the use of European Digital Identity Wallets upon voluntary request of the user. Users should be under no obligation to use the wallet to access private services ***and should not be restricted or hindered on account of not using the Wallet***, but if ***users*** wish to do so, ***very*** large online platforms should accept the European Digital Identity Wallet for this purpose while respecting the principle of data minimisation ***and the right of the users to use freely chosen pseudonyms***. Given the importance of very large online platforms, due to their reach, in particular as expressed in number of recipients of the service and economic transactions this is necessary to increase the protection of users from fraud and secure a high level of data protection. Self-regulatory codes of conduct at Union level ('codes of conduct') should be developed in order to contribute to wide availability and usability of electronic identification means including European Digital Identity Wallets within the scope of this Regulation. The codes of conduct should facilitate wide acceptance of electronic identification means including European Digital Identity Wallets by those service providers which do not qualify as very large platforms and which rely on third party electronic identification services for user authentication. They should be developed within 12 months of the adoption of this Regulation. ~~The Commission should assess the effectiveness of these provisions for the availability and usability for the user of the European Digital Identity Wallets after 18 months of their deployment and revise the provisions to ensure their acceptance by means of delegated acts in the light of this assessment.~~

(29) [Exclusive LIBE] (text to be added for plenary tabling)

(30) Attributes provided by the qualified trust service providers as part of the qualified attestation of attributes should be verified against the authentic sources either directly by the qualified trust service provider or via designated intermediaries recognised at national level in accordance with national or Union law for the purpose of secure exchange of attested attributes between identity or attestation of attributes' service providers and relying parties.

(31) Secure electronic identification and the provision of attestation of attributes should offer additional flexibility and solutions for the financial services sector to allow identification of customers and the exchange of specific attributes necessary to comply with, for example, customer due diligence requirements under the Anti Money Laundering Regulation, [reference to be added after the adoption of the proposal], with suitability requirements stemming from investor protection legislation, or to support the fulfilment of strong customer authentication requirements for account login and ***for*** initiation of transactions in the field of payment services.

(31a) ***This Regulation should establish the principle that an electronic signature should not be denied legal effect on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic signature. However, it is for national law to define the legal effect of electronic signatures, except for the requirements provided or in this Regulation according to which a qualified electronic signature should have the equivalent legal effect of a handwritten signature. In determining the legal effects of signatures Member States should take into account the principle of proportionality between the judicial value of a document to be signed and level of security and cost that an electronic signature requires. To increase the accessibility and use of electronic signatures Member States are encouraged to consider the use of advanced electronic signatures in the day to day transactions for which they provide a sufficient level of security and confidence. The use of qualified electronic signatures should be mandated only when the highest level of security and confidence is required.***

(32) Website authentication services provide users with ***a high level of*** assurance ***of the identity of the*** ~~that there is a genuine and~~ entity standing behind the website. Those services contribute to the building of trust and confidence in conducting business online, as users will have confidence in a website that has been authenticated. The use of website authentication services by websites is voluntary. However, in order for website authentication to become a means to increasing trust, providing a better experience for the user and furthering growth in the internal market, this Regulation lays down minimal security and liability obligations for the providers of website authentication services and their services. To that end, web-browsers should ensure support and interoperability with qualified certificates for website authentication pursuant to Regulation (EU) No 910/2014. They should recognise and display qualified certificates for website authentication to provide a high level of assurance, allowing website owners to assert their identity as owners of a website and users to identify the website owners with a high degree of certainty. To further promote their usage, public authorities in Member States should consider incorporating Qualified certificates for website authentication in their websites. ***Web browsers should be able to take measures in case of security breaches that should be proportional to the risk. The web browsers should notify to the Commission immediately any security breach as well as the measures taken to remedy them related to a single certificate or a set of them.***

(33) Many Member States have introduced national requirements for services providing secure and trustworthy digital archiving in order to allow for the long term preservation of electronic documents and associated trust services. To ensure legal certainty and trust, it is essential to provide a legal framework to facilitate the cross border recognition of qualified electronic archiving services. That framework could also open new market opportunities for Union trust service providers.

~~(34) Qualified electronic ledgers record data in a manner that ensures the uniqueness, authenticity and correct sequencing of data entries in a tamper proof manner. An electronic ledger combines the effect of time stamping of data with certainty about the data originator similar to e-signing and has the additional benefit of enabling more decentralised governance models that are suitable for multi-party co-operations. For example, it creates a reliable audit trail for the provenance of commodities in cross-border trade, supports the protection of intellectual property rights, enables flexibility markets in electricity, provides the basis for advanced solutions for self-sovereign identity and supports more efficient and transformative public services. To prevent fragmentation of the internal market, it is important to define a pan-European legal framework that allows~~

~~for the cross-border recognition of trust services for the recording of data in electronic ledgers.~~

~~(35) The certification as qualified trust service providers should provide legal certainty for use cases that build on electronic ledgers. This trust service for electronic ledgers and qualified electronic ledgers and the certification as qualified trust service provider for electronic ledgers should be notwithstanding the need for use cases to comply with Union law or national law in compliance with Union law. Use cases that involve the processing of personal data must comply with Regulation (EU) 2016/679. Use cases that involve crypto assets should be compatible with all applicable financial rules for example with the Markets in Financial Instruments Directive , the Payment Services Directive and the future Markets in Crypto Assets Regulation .~~

(36) In order to avoid fragmentation and barriers, due to diverging standards and technical restrictions, and to ensure a coordinated process to avoid endangering the implementation of the future European Digital Identity framework, a process for close and structured cooperation between the Commission, Member States***, civil society, academics*** and the private sector is needed. To achieve this objective, Member States should cooperate ~~within the framework set out in the Commission Recommendation XXX/XXXX [Toolbox for a coordinated approach towards a European Digital Identity Framework] to identify a Toolbox for a European Digital Identity framework. The Toolbox should include~~. ***The Member States should agree on*** a comprehensive technical architecture and reference framework, a set of common standards and technical references ***including recognised existing standards,*** and a set of guidelines and descriptions of best practices covering at least all aspects of the functionalities and interoperability of the European Digital Identity Wallets including eSignatures and of the qualified trust service ***providers*** for attestation of attributes as laid out in this regulation. In this context, Member States should also reach agreement on common elements of a business model and fee structure of the European Digital Identity Wallets, to facilitate take up, in particular by ***SMEs in a cross-border context*** ~~small and medium sized companies in a cross-border context. The content of the toolbox should evolve in parallel with and reflect the outcome of the discussion and process of adoption of the European Digital Identity Framework~~.

(36a) ***In order to ensure wide usability and availability, additional financial support measures should be envisaged to support Member States in issuing and managing the European Digital Identity Wallets. To this end, the Commission should asses the availability of additional Union funds to be made available for the Member States that would request support in the development, deployment and management of European Digital Identity Wallets.***

(36b) In order to ensure a wider use and applicability of the European Digital Identity Wallets across the Union, the Commission should build on and leverage the framework of this Regulation when developing sectoral Union instruments, such as the European Social Security Pass and the common European data spaces. The coordination with the European Social Security Pass should enable the digital portability of citizens' social security rights across borders and the verification of their entitlements and validity of documents. For the common European data space, the European Digital Identity Wallets should enable a higher degree of transparency and control of the users over their data.

(37) The European Data Protection Supervisor has been consulted pursuant to Article 42 (1) of Regulation (EU) 2018/1525 of the European Parliament and of the Council[5].

(38) Regulation (EU) 910/2014 should therefore be amended accordingly,

[5] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

ANNEX I

REQUIREMENTS FOR QUALIFIED CERTIFICATES FOR ELECTRONIC SIGNATURES

Qualified certificates for electronic signatures shall contain:

(a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic signature;

(b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least, the Member State in which that provider is established and:

– for a legal person: the name and, where applicable, registration number as stated in the official records,

– for a natural person: the person's name;

(c) at least the name of the signatory, or a pseudonym; if a pseudonym is used, it shall be clearly indicated;

(d) electronic signature validation data that corresponds to the electronic signature creation data;

(e) details of the beginning and end of the certificate's period of validity;

(f) the certificate identity code, which must be unique for the qualified trust service provider;

(g) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;

(h) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge;

(i) the information, or the location of the services that can be used to enquire, about the validity status of the qualified certificate;

(ia) an indication, in a form suitable for automated processing, showing what identity verification method listed in paragraph 1 of Article 24 was used during issuance of the certificate.

(j) where the electronic signature creation data related to the electronic signature validation data is located in a qualified electronic signature creation device, an appropriate indication of this, at least in a form suitable for automated processing.

ANNEX II

REQUIREMENTS FOR QUALIFIED ELECTRONIC SIGNATURE CREATION DEVICES

1. Qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that at least:

(a) the confidentiality of the electronic signature creation data used for electronic signature creation is reasonably assured;

(b) the electronic signature creation data used for electronic signature creation can practically occur only once;

(c) the electronic signature creation data used for electronic signature creation cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery using currently available technology;

(d) the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others.

2. Qualified electronic signature creation devices shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing.

ANNEX III

REQUIREMENTS FOR QUALIFIED CERTIFICATES FOR ELECTRONIC SEALS

Qualified certificates for electronic seals shall contain:

(a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic seal;

(b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least the Member State in which that provider is established and:

– for a legal person: the name and, where applicable, registration number as stated in the official records,

– for a natural person: the person's name;

(c) at least the name of the creator of the seal and, where applicable, registration number as stated in the official records;

(d) electronic seal validation data, which corresponds to the electronic seal creation data;

(e) details of the beginning and end of the certificate's period of validity;

(f) the certificate identity code, which must be unique for the qualified trust service provider;

(g) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;

(h) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge;

(i) the information, or the location of the services that can be used to enquire, about the validity status of the qualified certificate;

(j) ***an indication, in a form suitable for automated processing, showing what identity verification method listed in paragraph 1 of Article 24 was used during issuance of the seal.***

(k) where the electronic seal creation data related to the electronic seal validation data is located in a qualified electronic seal creation device, an appropriate indication of this, at least in a form suitable for automated processing.

ANNEX IV

REQUIREMENTS FOR QUALIFIED CERTIFICATES FOR WEBSITE AUTHENTICATION

Qualified certificates for website authentication shall contain:

(a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for website authentication;

(b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least the Member State in which that provider is established and:

- for a legal person: the name and, where applicable, registration number as stated in the official records,
- for a natural person: the person's name;

(c) for natural persons: at least the name of the person to whom the certificate has been issued ***with a high level of assurance***, or a pseudonym. If a pseudonym is used, it shall be clearly indicated; ~~for legal persons: at least the name of the legal person to whom the certificate is issued and, where applicable, registration number as stated in the official records;~~

(ca) for legal persons: at least the name of the legal person to whom the certificate is issued and, where applicable, registration number as stated in the official records with a high level of assurance;

(d) elements of the address, including at least city and State, of the natural or legal person to whom the certificate is issued and, where applicable, as stated in the official records;

(e) the domain name(s) operated by the natural or legal person to whom the certificate is issued;

(f) details of the beginning and end of the certificate's period of validity;

(g) the certificate identity code, which must be unique for the qualified trust service provider;

(h) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;

(i) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (h) is available free of charge;

(j) the information, or the location of the certificate validity status services that can be used to enquire, about the validity status of the qualified certificate.

ANNEX V

REQUIREMENTS FOR QUALIFIED ELECTRONIC ATTESTATION OF ATTRIBUTES

Qualified electronic attestation of attributes shall contain:

(a) an indication, at least in a form suitable for automated processing, that the attestation has been issued as a qualified electronic attestation of attributes;

(b) a set of data unambiguously representing the qualified trust service provider issuing the qualified electronic attestation of attributes including at least, the Member State in which that provider is established and:

(c) for a legal person: the name and, where applicable, registration number as stated in the official records,

(d) for a natural person: the person's name;

(e) a set of data unambiguously representing the entity to which the attested attributes is referring to; if a pseudonym is used, it shall be clearly indicated;

(f) the attested attribute or attributes, including, where applicable, the information necessary to identify the scope of those attributes;

(g) details of the beginning and end of the attestation's period of validity;

(h) the attestation identity code, which must be unique for the qualified trust service provider and if applicable the indication of the scheme of attestations that the attestation of attributes is part of;

(i) the ***qualified*** electronic signature or ***qualified*** electronic seal of the issuing qualified trust service provider;

(j) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (f) is available free of charge;

(k) the information or location of the services that can be used to enquire about the validity status of the qualified attestation.

ANNEX VI

MINIMUM LIST OF ATTRIBUTES

Further to Article 45d, Member States shall ensure that measures are taken to allow qualified providers of electronic attestations of attributes to verify by electronic means at the request of the user, the authenticity of the following attributes against the relevant authentic source at national level or via designated intermediaries recognised at national level, in accordance with national or Union law and in cases where these attributes rely on authentic sources within the public sector:

1. Address;

2. Date of birth~~Age~~;

3. Gender;

4. Civil status;

5. Family composition;

6. Nationality ***or nationalities***;

6a. Citizenship or citizenships;

7. Educational qualifications, titles and licenses;

8. Professional qualifications, titles and licenses;

8a. Documents proving the activation of a protection regime and name of the authorised party designated to act on behalf of the natural person;

9. Public permits and licenses;

10. ~~Financial and c~~Company data;