COUNCIL OF THE EUROPEAN UNION

Brussels, 31 October 2013

15531/13

Interinstitutional File: 2012/0146 (COD)

TELECOM 276
MI 942
DATAPROTECT 154
EJUSTICE 85
CODEC 2418

NOTE

from:	Presidency
to:	Delegations
No. Cion prop.:	10977/12 TELECOM 122 MI 411 DATAPROTECT 73 CODEC 1576
No prev. doc. :	13890/13 TELECOM 239 MI 783 DATAPROTECT 130 EJUSTICE 66 CODEC 2076
Subject:	Proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market - *Consolidated text*

1. In its conclusions of 25 October 2013 the European Council[1] has requested the adoption of the above mentioned proposal under the end of the current legislature. In order to achieve this, the Presidency's intention is to engage in negotiations with the European as soon as possible, with the first trialogue planned for November.

2. As already indicated at the last WP TELE meeting, the first trialogue should concentrate on the most developed and discussed part of the text, i.e. the first 19 Articles. The modifications[2] introduced in the text in Annex focus therefore exclusively on this part of the proposal.

[1] EUCO 169/13

[2] For easier reference, the changes as compared to the Commission proposal are in **bold** (and deletion in **~~strikethough~~**). The latest changes introduced by the Presidency are **underlined**.

3. The revised text reflects the following orientations, most of them being already well established in the previous versions:

For cluster 1

- The scope of mutual recognition is limited to cross-border access to services provided by public service bodies (or private entities mandated by such bodies).
- Private e-ID means may also be notified.
- Recognised e-ID means should correspond to assurance levels equal to or higher than national assurance levels.
- Assurance levels are to be defined in an implementing act with inspiration taken from STORK.
- Notified e-ID schemes should be interoperable.
- A cooperation process will support the operation of an interoperability framework.
- While data protection is paramount, this Regulation does not add requirements on top of what is already foreseen in EU legislation.

For cluster 2:

- There is a broad agreement that while cluster 2 should cover both qualified and non-qualified trust service providers (TSPs), the requirements for non-qualified TSPs should be much lighter (so called 'light-touch' approach), in particular with regard to the following:
    - Both qualified and non-qualified TSPs should be subject to the liability provision but the reversed burden of proof should only apply to qualified TSPs.
    - While full supervision applies to qualified TSPs, the supervisory body should take action with regard to non-qualified TSPs only when informed of non-compliance.
- Audits of qualified trust service providers should be carried out by a conformity assessment body (Regulation 765/2008).
- The provision of qualified trust services should be subject to prior verification of the compliance with the Regulation by the supervisory body.

4. In order to further progress with the examination, the attached text also contains the EP amendments[3] (concerning the operative part of the proposal only) adopted on 14 October 2013 by the ITRE committee. Those amendments also include certain amendments by the IMCO committee (voted in July 2013) that has exclusive competence over some provisions of the proposal.

5. At the WP TELE of 5 November, delegations will be invited to express their positions with regard to the revised text of the first 19 Articles, the broad orientations listed above and, possibly, the acceptability of the EP amendments.

_____

.

[3] The EP amendments are grey-shaded. Please note that the text of the amendments is based on a provisional version of the adopted amendments; final changes, if any, will be communicated later.

ANNEX

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on electronic identification and trust services for electronic transactions in the internal market

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national Parliaments,

Having regard to the opinion of the European Economic and Social Committee[4],

After consulting the European Data Protection Supervisor[5],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) Building trust in the online environment is key to economic development. Lack of trust makes consumers, businesses and administrations hesitate to carry out transactions electronically and to adopt new services.

(2) This Regulation seeks to enhance trust in electronic transactions in the internal market by enabling secure and seamless electronic interactions to take place between businesses, citizens and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union.

4 OJ C , , p. .
5 OJ C, , p. .

(3) Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures[6], essentially covered electronic signatures without delivering a comprehensive cross-border and cross-sector framework for secure, trustworthy and easy-to-use electronic transactions. This Regulation enhances and expands the *acquis* of the Directive.

(4) The Commission's Digital Agenda for Europe[7] identified the fragmentation of the digital market, the lack of interoperability and the rise in cybercrime as major obstacles to the virtuous cycle of the digital economy. In its Citizenship Report 2010 the Commission further highlighted the need to solve the main problems which prevent European citizens from enjoying the benefits of a digital single market and cross-border digital services[8].

(5) The European Council invited the Commission to create a digital single market by 2015[9] to make rapid progress in key areas of the digital economy and to promote a fully integrated digital single market[10] by facilitating the cross-border use of online services, with particular attention to facilitating secure electronic identification and authentication.

(6) The Council invited the Commission to contribute to the digital single market by creating appropriate conditions for the mutual recognition of key enablers across borders, such as electronic identification, electronic documents, electronic signatures and electronic delivery services, and for interoperable eGovernment services across the European Union[11].

(7) The European Parliament stressed the importance of the security of electronic services, especially of electronic signatures, and of the need to create a public key infrastructure at pan-European level, and called on the Commission to set up a European validation authorities gateway to ensure the cross-border interoperability of electronic signatures and to increase the security of transactions carried out using the internet[12].

---

6 OJ L 13, 19.1.2000, p. 12

7 COM(2010) 245 final/2

8 EU Citizenship Report 2010: Dismantling obstacles to EU citizens' rights, COM(2010) 603 final, point 2.2.2, page 13.

9 4/2/2011: EUCO 2/1/11

10 23/10/2011: EUCO 52/1/11

11 Council Conclusions on the European eGovernment Action Plan 2011-2015, 3093rd Transport, Telecommunications and Energy Council meeting, Brussels, 27 May 2011.

12 European Parliament resolution of 21.9.2010 on completing the internal market for e-commerce, 21.9.10, P7_TA(2010)0320, and European Parliament resolution of 15.6.2010 on internet governance: the next steps, P7_TA(2010)0208.

(8) Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market[13] requests Member States to establish 'points of single contact' (PSC) to ensure that all procedures and formalities relating to access to a service activity and to the exercise thereof can be easily completed, at a distance and by electronic means, through the appropriate point of single contact and with the appropriate authorities. Many online services accessible through PSCs require electronic identification, authentication and signature.

(9) In most cases service providers from another Member State cannot use their electronic identification to access these services because the national electronic identification schemes in their country are not recognised **~~and accepted~~** in other Member States. This electronic barrier excludes service providers from enjoying the full benefits of the internal market. Mutually recognized **~~and accepted~~** electronic identification means will facilitate cross-border provision of numerous services in the Internal Market and enable businesses to go cross-border without facing many obstacles in interactions with public authorities

(10) Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare[14] sets up a network of national authorities responsible for eHealth. To enhance safety and the continuity of cross-border healthcare, the network is required to produce guidelines on cross-border access to electronic health data and services, including by supporting '*common identification and authentication measures to facilitate transferability of data in cross-border healthcare*'. Mutual recognition **~~and acceptance~~** of electronic identification and authentication is key to make cross border healthcare for European citizens a reality. When people travel for treatment, their medical data needs to be accessible in the country of treatment. This requires a solid, safe and trusted electronic identification framework.

(11) One of the objectives of this Regulation is to remove existing barriers to the cross-border use of electronic identification means used in the Member States to access at least public services. This Regulation does not aim at intervening on electronic identity management systems and related infrastructures established in the Member States. The aim of this Regulation is to ensure that for the access to cross-border online services offered by the Member States, secure electronic identification and authentication is possible.

---

13 OJ L 376, 27.12.2006, p. 36

14 OJ L 88, 4.4.2011, p. 45

(12) Member States should remain free to use or introduce means, for electronic identification purposes, for accessing online services. They should also be able to decide whether to involve the private sector in the provision of these means. Member States should not be obliged to notify their electronic identification schemes. The choice to either notify all, some or none of the electronic identification schemes used at national level to access at least public online services or specific services is up to the Member States.

(13) Some conditions need to be set in the Regulation with regard to which electronic identification means have to be **recognised** ~~**accepted**~~ and how the schemes should be notified. These should help Member States to build the necessary trust in each other's electronic identification schemes and to mutually recognise ~~**and accept**~~ electronic identification means falling under their notified schemes. The principle of mutual recognition ~~**and acceptance**~~ should apply if the notifying Member State meets the conditions of notification and the notification was published in the Official Journal of the European Union. However**, the principle of mutual recognition should only relate to authentication for a service online. T**the access to these online services and their final delivery to the applicant should be closely linked to the right to receive such services under the conditions set by national legislation.

(13a) The obligation to recognise electronic identification means relates only to those means the identity assurance level of which corresponds to the level~~s~~ equal to or higher than the level required for the service online in question ~~defined by this Regulation~~. Member States should remain free, in accordance with Union law, to recognise electronic identification means having lower identity assurance levels.

(14) Member States should be able to decide to involve the private sector in the issuance of electronic identification means and to allow the private sector the use of electronic identification means under a notified scheme for identification purposes when needed for online services or electronic transactions. The possibility to use such electronic identification means would enable the private sector to rely on electronic identification and authentication already largely used in many Member States at least for public services and to make it easier for businesses and citizens to access their online services across borders. In order to facilitate the use of such electronic identification means across borders by the private sector, the authentication possibility provided by the Member States should be available to relying parties without discriminating between public or private sector.

(14a) This Regulation provides for the liability of the notifying Member State, the party issuing the electronic identification means and the party operating the authentication procedure for failing to comply with the relevant obligations under this Regulation. However, it should be applied in accordance with national rules on liability. Therefore, it does not affect those rules, for example, on definition of damages or on relevant applicable procedural rules.

(15) The cross border use of electronic identification means under a notified scheme requires Member States to cooperate in providing technical interoperability. This rules out any specific national technical rules requiring non-national parties for instance to obtain specific hardware or software to verify and validate the notified electronic identification. Technical requirements on users, on the other hand, stemming from the inherent specifications of whatever token is used (e.g. smartcards) are inevitable.

(16) Cooperation of Member States should serve the technical interoperability of the notified electronic identification schemes with a view to foster a high level of trust and security appropriate to the degree of risk. The exchange of information and the sharing of best practices between Member States with a view to their mutual recognition should help such cooperation.

(17) This Regulation should also establish a general legal framework for the use of electronic trust services. However, it should not create a general obligation to use them. In particular, it should not cover the provision of services based on voluntary agreements under private law. Neither should it cover aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form prescribed by national or Union law.

(18) In order to contribute to the general cross-border use of electronic trust services, it should be possible to use them as evidence in legal proceedings in all Member States.

(19) Member States should remain free to define other types of trust services in addition to those making part of the closed list of trust services provided for in this Regulation, for the purpose of recognition at national level as qualified trust services.

(20) Because of the pace of technological change, this Regulation should adopt an approach which is open to innovations.

(21) This Regulation should be technology-neutral. The legal effects it grants should be achievable by any technical means provided that the requirements of this Regulation are met.

(22) To enhance people’s trust in the internal market and to promote the use of trust services and products, the notions of qualified trust services and qualified trust service provider should be introduced with a view to indicating requirements and obligations to ensure high-level security of whatever qualified trust services and products are used or provided.

(23) In line with the obligations under the UN Convention on the Rights of Persons with Disabilities that has entered into force in the EU, persons with disabilities should be able to use trust services and end user products used in the provision of those services on equal bases with other consumers. **Therefore, where feasible, trust services provided and end user products used in the provision of those services should be made accessible for persons with disabilities. The feasibility assessment should include technical and economical considerations.**

(24) A trust service provider is a controller of personal data and therefore has to comply with the obligations set out in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[15]. In particular the collection of data should be minimised as much as possible taking into account the purpose of the service provided.

(24a) Member States should designate a supervisory body or supervisory bodies to carry out the supervisory activities under this Regulation. Member States should be also able to decide, upon a mutual agreement with another Member State, to designate a supervisory body in the territory of that other Member State.

(25) Supervisory bodies should cooperate and exchange information with data protection authorities to ensure proper implementation of data protection legislation by service providers. The exchange of information should in particular cover security incidents and personal data breaches.

(26) It should be incumbent on all trust service providers to apply good security practice appropriate to the risks related to their activities so as to boost users' trust in the single market.

(27) Provisions on the use of pseudonyms in certificates should not prevent Member States from requiring identification of persons pursuant to Union or national law.

(28) All Member States should follow common essential supervision requirements to ensure a comparable security level of qualified trust services. To ease the consistent application of these requirements across the Union, Member States should adopt comparable procedures and should exchange information on their supervision activities and best practices in the field.

(28a) All trust service providers should be subject to requirements of this Regulation, in particular on security and liability to ensure due diligence, transparency and accountability of their operations and services. However, taking into account the type of services provided by trust service providers, it is appropriate to distinguish as far as those requirements are concerned between qualified and non-qualified trust service providers.

[15] OJ L 281, 23.11.1995, p. 31

(28b) Establishing a supervisory regime for all trust service providers should ensure a level playing fied for the security and accountability of their operations and services, thus contributing to protection of users and to the good functioning of the internal market. Non-qualified trust service providers should be subject to a light-touch and reactive ex-post supervisory activities justified by the nature of their services and operations. The supervisory body should therefore have no general obligation to supervise non-qualified service providers. The supervisory body should only take action when it is clearly informed (for example by the non-qualified trust service provider itself , by another supervisory body, by a notification from a user or a business partner or on the basis of its own investigation) that a non-qualified trust service provider does not to comply with the requirements of the Regulation.

(28c) This Regulation provides for the liability of all trust service providers. In particular, it establishes the liability regime under which all trust service providers should be liable for damage caused to any natural or legal person due to failure to comply with the obligations under this Regulation. It allows trust service providers to limit, under certain conditions, the liability. However, this Regulation should be applied in accordance with national rules on liability. Therefore, it does not affect those rules, for example, on definition of damages, fault, negligence, on relevant applicable procedural rules.

(29) Notification of security breaches and security risk assessments is essential with a view to providing adequate information to concerned parties in the event of a breach of security or loss of integrity.

(30) To enable the Commission and the Member States to assess the effectiveness of the breach notification mechanism introduced by this Regulation, supervisory bodies should be requested to provide summary information to the Commission and to European Network and Information Security Agency (ENISA).

(31) To enable the Commission and the Member States to assess the impact of this Regulation, supervisory bodies should be requested to provide statistics on and the use of qualified trust services.

(32) To enable the Commission and the Member States to assess the effectiveness of the enhanced supervision mechanism introduced by this Regulation, supervisory bodies should be requested to report on their activities. This would be instrumental in facilitating the exchange of good practices between supervisory bodies and would ensure the verification that essential supervision requirements are implemented consistently and efficiently in all Member States.

(33) To ensure sustainability and durability of qualified trust services and to boost users' confidence in the continuity of qualified trust services, supervisory bodies should ensure that the data of qualified trust service providers are preserved and kept accessible for an appropriate period of time even if a qualified trust service provider ceases to exist.

(34) To facilitate the supervision of qualified trust services providers, for example when a provider is providing its services in the territory of another Member State and is not subject to supervision there, or when the computers of a provider are located in the territory of another Member State than the one where it is established, a mutual assistance system between supervisory bodies in the Member States should be set up.

(35) It is the responsibility of trust service providers to meet the requirements set out in this Regulation for the provisioning of trust services, in particular for qualified trust services. Supervisory bodies have the responsibility to supervise how trust service providers meet these requirements.

(36) In order to allow an efficient initiation process, which should lead to the inclusion of qualified trust service providers and the qualified trust services they provide into trusted lists, preliminary interactions between prospective qualified trust service providers and the competent supervisory body should be encouraged with the view of facilitating the due diligence leading to the provisioning of qualified trust services.

(37) Trusted lists are essential elements to build trust among market operators as they indicate the qualified status of the service provider at the time of supervision, on the other hand they are not a prerequisite for achieving the qualified status and providing qualified trust services which results from respecting the requirements of this Regulation.

(38) Once it has been subject to a notification, a qualified trust service cannot be refused for the fulfilment of an administrative procedure or formality by the concerned public sector body, for not being included in the trusted lists established by the Member States. For the present purpose a public sector body refers to any public authority or other entity entrusted with the provision of eGovernment services such as online tax declaration, request for birth certificates, participation to electronic public procurement procedures, etc.

(39) While a high level of security is needed to ensure mutual recognition of electronic signatures, in specific cases, such as in the context of Commission Decision 2009/767/EC of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the 'points of single contact' under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market[16], electronic signatures with a lower security assurance should also be accepted.

[16] OJ L 274, 20.10.2009, p. 36

(40) It should be possible to entrust qualified electronic signature creation devices to the care of a third party by the signatory, provided that appropriate mechanisms and procedures are implemented to ensure that the signatory has sole control over the use of his electronic signature creation data, and the qualified signature requirements are met by the use of the device.

(41) To ensure legal certainty on the validity of the signature it is essential to detail which components of a qualified electronic signature must be assessed by the relying party carrying out the validation. Moreover, defining the requirements of qualified trust service providers that can provide a qualified validation service to relying parties not willing or unable to carry out themselves the validation of qualified electronic signatures, should stimulate the private or public sector to invest in such services. Both elements should make qualified electronic signature validation easy and convenient for all parties at Union level.

(42) When a transaction requires a qualified electronic seal from a legal person, a qualified electronic signature from the authorised representative of the legal person should be equally acceptable.

(43) Electronic seals should serve as evidence that an electronic document was issued by a legal person, ensuring certainty of the document's origin and integrity.

(44) This Regulation should ensure the long-term preservation of information, i.e. the legal validity of electronic signature and electronic seals over extended periods of time, guaranteeing that they can be validated irrespective of future technological change.

(45) In order to enhance the cross-border use of electronic documents this Regulation should provide for the legal effect of electronic documents which should be considered as equal to paper documents dependent on the risk assessment and provided the authenticity and integrity of the documents are ensured. It also important for further development of cross-border electronic transactions in the internal market that original electronic documents or certified copies issued by relevant competent bodies in a Member State under their national law are accepted as such also in other Member States. This Regulation should not affect Member States' right to determine what constitutes an original or a copy at a national level but ensures that these can be used as such also across borders.

(46) As competent authorities in the Member States currently use different formats of advanced electronic signatures to sign their documents electronically, it is necessary to ensure that at least a number of advanced electronic signature formats can be technically supported by Member States when they receive documents signed electronically. Similarly, when competent authorities in the Member States use advanced electronic seals, it would be necessary to ensure that they support at least a number of advanced electronic seal formats.

(47) In addition to authenticating the document issued by the legal person, electronic seals can be used to authenticate any digital asset of the legal person, e.g. software code, servers.

(48) Making it possible to authenticate websites and the person owning them would make it harder to falsify websites and thus reduce fraud.

(48a) The concept of 'legal persons', according to the Treaty provisions on establishment, leaves operators free to choose the legal form which they deem suitable for carrying out their activity. Accordingly, 'legal persons', within the meaning of the Treaty, means all entities constituted under, or governed by, the law of a Member State, irrespective of their legal form.

(49) In order to complement certain detailed technical aspects of this Regulation in a flexible and rapid manner, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission in respect of interoperability of electronic identification; security measures required of trust service providers; recognised independent bodies responsible for auditing the service providers; trusted lists; requirements related to the security levels of electronic signatures; requirements of qualified certificates for electronic signatures their validation and their preservation; the bodies responsible for the certification of qualified electronic signature creation devices; and the requirements related to the security levels of electronic seals and to qualified certificates for electronic seals; the interoperability between delivery services. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level.

(50) The Commission, when preparing and drawing up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and to the Council.

(51) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission, in particular for specifying reference numbers of standards which use would give a presumption of compliance with certain requirements laid down in this Regulation or defined in delegated acts. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers[17].

(52) For reasons of legal certainty and clarity, Directive 1999/93/EC should be repealed.

[17] OJ L 55, 28.2.2011, p. 13

(53) To ensure legal certainty to the market operators already using qualified certificates issued in compliance with Directive 1999/93/EC, it is necessary to provide for a sufficient period of time for transitional purposes. It is also necessary to provide the Commission with the means to adopt the implementing acts and delegated acts before that date.

(54) Since the objectives of this Regulation cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective, especially regarding the Commission's role as coordinator of national activities,

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter

1. **With a view to ensuring the proper functioning of the internal market** ~~T~~this Regulation**:**

- lays down **conditions under which Member States shall recognise electronic identification means of natural and legal persons falling under a notified electronic identification scheme of another Member State,**

- lays down rules for ~~**electronic identification and**~~ electronic trust services for electronic transactions ~~**with a view to ensuring the proper functioning of the internal market**~~ **and**

- establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, ***[electronic documents, electronic delivery services and website authentication].***

1. This Regulation lays down rules for ***cross-border*** electronic identification and trust services for electronic transactions with a view to ensuring the proper functioning of the internal market.

~~**2. This Regulation lays down the conditions under which Member States shall recognise and accept electronic identification means of natural and legal persons falling under a notified electronic identification scheme of another Member State.**~~

~~**3. This Regulation establishes a legal framework for electronic signatures, electronic seals, electronic time stamps,** ***[electronic documents, electronic delivery services and website authentication].***~~

~~**4. This Regulation ensures that trust services and products which comply with this Regulation are permitted to circulate freely in the internal market.**~~

4. This Regulation ensures that ***qualified and non-qualified*** trust services and products which comply with this Regulation are permitted to circulate freely in the internal market.

Article 2

Scope

1. This Regulation applies to electronic identification **schemes notified** ~~**provided by, on behalf or under the responsibility of a mandate from or recognised**~~ **by a** Member State~~**s,**~~ and to trust service providers established in the Union.

1. This Regulation applies to ***notified*** electronic identification ***schemes mandated, recognised or issued*** by ***or*** on behalf of Member Sates, and to trust service providers established in the Union.

2. This Regulation does not apply to the provision of electronic trust services ~~**based on voluntary agreements under private law**~~ **used exclusively within closed systems resulting from agreements between a** ~~**specified number**~~ **defined set of participants**.

2. ***This Regulation applies to both qualified and non-qualified trust service providers established in the Union.*** This Regulation does not apply to the trust services ***which are provided to a closed group of parties and which are used exclusively within that group***.

3. This Regulation does not ~~**apply to aspects**~~ **affect national or Union law** related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form prescribed by national or Union law.

Article 3

Definitions

For the purposes of this Regulation, the following definitions shall apply:

(1) 'electronic identification' means the process of using person identification data in electronic form ~~**unambiguously**~~ representing a natural or legal person **or natural person representing a legal person**;

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

(a) to fully identify a person

(b) or to confirm only those identification data necessary to grant access to a specific service.

(2) 'electronic identification means' means a material **and/**or immaterial unit containing **person identification** data ~~**as referred to in point 1 of this Article**~~, and which is used ~~**to access**~~ **for authentication for** services online ~~**as referred to in Article 5**~~;

(2) ‘electronic identification means’ means a material or immaterial unit containing data as referred to in point 1 of this Article, and which is used to access ***electronic*** services as referred to in Article 5;

(2a) ‘person identification data’ means a set of data enabling to establish the identity of natural or legal person, or natural person representing a legal person;

(3) ‘electronic identification scheme’ means a system for electronic identification under which electronic identification means are issued to persons as referred to in point 1 of this Article;

(4) ‘authentication’ means an electronic process that allows the **~~validation~~ attestation** of the electronic identification of a natural or legal person; or of the origin and integrity of an electronic data;

(4) ‘authentication’ means an electronic process that allows the validation of the electronic identification of a natural or legal person; or of the origin and integrity of electronic data;

(4a) 'relying party' means a natural or legal person to whom the holder of an electronic authentication means verifies attributes;

(4a) ‘public sector body’ means the State, regional or local authorities, bodies governed by public law and associations 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;

(4b) ‘body governed by public law’ means any body:

(a) established for the specific purpose of meeting needs in the general interest, not having an industrial or commercial character; and

(b) having legal personality; and

(c) financed, for the most part by the State, or regional or local authorities, or other bodies governed by public law; or subject to management supervision by those bodies; or having an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional or local authorities or by other bodies governed by public law.

(5) ‘signatory’ means a natural person who creates an electronic signature;

(6) ‘electronic signature’ means data in electronic form which are attached to or logically associated with other electronic data and which are used by the signatory to sign;

(7) ‘advanced electronic signature’ means an electronic signature which meets the following requirements:

(a) it is uniquely linked to the signatory;

(b) it is capable of identifying the signatory;

(b) it is ***capable of guaranteeing the legal validity of the identity of*** the signatory;

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

(c) it is created using ***an*** electronic signature creation ***device*** that the signatory can use under his sole control; 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;

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

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

(8) 'qualified electronic signature' meansan advanced electronic signature which is created by a qualified electronic signaturecreation device, and which is based on a qualified certificate for electronic signatures ***issued by a qualified trust provider***;

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

(10) 'certificate **for electronic signature**' means an electronic attestation which links electronic signature ~~**or seal**~~ validation data ~~**of**~~**to** a natural ~~**or a legal**~~ person ~~**respectively to the certificate**~~ and confirms ~~**those data**~~ **the name or the pseudonym** of that person;

(10) 'certificate' means an electronic attestation which links electronic signature or seal validation data ***with the identification data of an entity, or*** a natural or a legal person respectively and confirms those data of that person;

(11) 'qualified certificate for electronic signature' means ~~**an attestation which is used to support**~~ **a certificate for** electronic signatures**, that** is issued by a qualified trust service provider and meet**s** the requirements laid down in Annex I;

(11) 'qualified certificate for electronic signature' means ***a certificate*** which isused to support electronic signatures, isissued by a qualified trust service providerand meet the requirements laid down in Annex I;

(12) 'trust service' means ~~**any**~~ electronic service**s** consisting in**:**

- the **creation of certificates or the**~~,~~ verification**,** ~~**and**~~ validation~~**, handling and preservation**~~ of electronic signatures, electronic seals~~**, or**~~ electronic time stamps, ~~**electronic documents,**~~ ***[****electronic delivery* ~~***services***~~*, website authentication,]* ~~**and**~~ **or**
- **the preservation of electronic signatures, seals or** certificates~~**, including certificates for electronic signature and for electronic seals**~~;

(12) 'trust service' means ***an*** electronic service consisting in the creation, verification, validation ***or*** preservation of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic delivery services, website authentication, and electronic certificates, including certificates for electronic signature and for electronic seals;

(13) 'qualified trust service' means a trust service that meets the requirements provided for in this Regulation;

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

(**13a) 'conformity assessment body' in point 13 of Regulation 765/2008;**

(14) 'trust service provider' means **a natural or a legal person who provides one or more trust services. There are qualified and non-qualified trust service providers**;

(14) 'trust service provider' means a natural or a legal person who provides one or more trust services ***as defined in this regulation***;

~~**(14a) 'non-qualified trust service provider' means a natural or a legal person who provides one or more trust services;**~~

(15) '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** ~~**meets the requirements laid down in this Regulation**~~;

(16) 'product' means hardware or software, or relevant components thereof, which are intended to be used for the provision of trust services;

(17) 'electronic signature creation device' means configured software or hardware used to create an electronic signature;

(18) 'qualified electronic signature creation device' means an electronic signature creation device which meets the requirements laid down in Annex II;

(19) 'creator of a seal' means a legal person who creates an electronic seal;

(19) 'creator of a seal' means a ***natural or*** legal person who creates an electronic seal;

(20) 'electronic seal' means data in electronic form which are attached to or logically associated with other electronic data to ensure the origin and the integrity of the associated data;

(20) 'electronic seal' means data in electronic form which are attached to or logically associated with other electronic data to ensure the ***authenticity*** and the integrity of the associated data;

(21) ‘advanced electronic seal’ means an electronic seal which meets 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

(c) it is created using ***an*** electronic seal creation ***device*** 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;

(d) it is linked to the data ***the origin and integrity of*** which it ***attests*** in such a way that any subsequent change in the data is detectable;

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

22) ‘qualified electronic seal’ means an advanced electronic seal which is created by a qualified electronic seal creation device, and which is based on a qualified certificate for electronic seal ***issued by a qualified trust service provider***;

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

(23a) ‘certificate for electronic seal’ means an electronic attestation which links electronic seal validation data to a legal person and confirms the name of that person;

(24) ‘qualified certificate for electronic seal’ means ~~**an attestation which is used to support** a~~**n certificate for** electronic seal, **that** is issued by a qualified trust service provider and meet**s** the requirements laid down in Annex III;

(24a) ‘electronic seal creation device’ means configured software or hardware used to create an electronic seal;

(24b) ‘qualified electronic seal creation device’ means an electronic seal creation device which meets the requirements laid down in Annex III;

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

(26) ‘qualified electronic time stamp’ means an electronic time stamp which meets the requirements laid down in Article 33;

[(27) 'electronic document' means a document in any electronic format;

(27) 'electronic document' means ***a separate set of structured data*** in any electronic format;

(28) 'electronic delivery service' means a service that makes it possible to transmit data by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending or receiving the data, and which protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations;

(29) 'qualified electronic delivery service' means an electronic delivery service which meets the requirements laid down in Article 36;

(30) 'qualified certificate for website authentication' means an attestation which makes it possible to authenticate a website and links the website to the person to whom the certificate is issued, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV;]

(31) 'validation data' means data which are used to validate an electronic signature**, ~~or~~** an electronic seal**, an electronic time stamp or electronic delivery service;**

(31a) 'validation' means the process of checking the validation data to confirm that the electronic signature, ~~or~~ seal , an electronic time stamp or electronic delivery service is valid.

(31a) 'breach of security' means asecurity incident leading to the accidentalor unlawful destruction, loss, alteration,unauthorised disclosure of, or access to,data transmitted, stored or otherwiseprocessed.

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 States for reasons which fall within the fields covered by this Regulation.

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 States for reasons which fall within the fields covered by this Regulation. ***Member States shall ensure that trust services originating from another Member States are admissible as evidence in legal proceedings.***

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

2. Products which comply with this Regulation shall circulate freely ***and securely*** in the internal market.

Article 4a

Data processing and protection

1. Processing of personal data shall be carried out in accordance with Directive 95/46/EC. *[Such processing shall be strictly limited to the minimum data needed to issue and maintain a certificate or to provide trust service]*[18].

~~**2. Confidentiality and integrity of data shall be guaranteed.**~~

3. Without prejudice to the legal effect given to pseudonyms under national law, the use of pseudonyms in electronic transaction shall not be prohibited.

[18] The Presidency noted the wish of a number of delegations to delete this sentence. It should however be noted that such deletion would render this paragraph declaratory. This provision could be completed to cover the entire Regulation (for example to include the monitoring and supervising activities of the supervisory bodies; Chapter II on electronic identification should also be reflected).

CHAPTER II

ELECTRONIC IDENTIFICATION

Article 5

Mutual recognition ~~and acceptance~~

Mutual recognition

1. When an electronic identification using an electronic identification means and authentication is required under national legislation or administrative practice to access **cross-border** a service **provided by a public sector body** online **in one Member State**, **~~any~~ the** electronic identification means issued in another Member State **~~falling under a scheme included in the list published by the Commission pursuant to the procedure referred to in Article 7,~~** shall be recognised **~~and accepted~~ in the first Member State** for the purposes of **~~accessing~~authentication for ~~this~~ that** service **online, ~~not later than six months after the list, including that scheme, is published.~~ provided that the following conditions are met:**

a. that electronic identification means is issued under an electronic identification scheme included in the list published by the Commission pursuant to Article 7;

b. the assurance level of that electronic identification means corresponds to ~~one of the assurance levels set out in Annex 0~~ an assurance level equal to or higher than the assurance level required by the relevant public sector body to access that service online in the first Member States.

Such recognition shall take place no later than 12 months after the list published by the Commission pursuant to Article 7, including the scheme referred to in point (a) of the previous subparagraph, is published.

~~2. Notwithstanding point (b) of paragraph 1, a specific assurance level set out in Annex 0 may be required for the electronic identification means to accessfor authentication for online services defined in accordance with Article 8(2b).~~

When an electronic identification using an electronic identification means and authentication is required under ***Union or*** national legislation or administrative practice to access a service online ***in one Member State or provided online by Union institutions, bodies, offices and agencies, this*** electronic identification means issued in another Member State ***or by Union institutions, bodies, offices and agencies*** under a scheme included in the list published by the Commission pursuant to Article 7, ***and with a security level equal to or higher than the security level required to access the service***, shall be ***recognised in the Member State or by Union institutions, bodies, offices and agencies*** for the purposes of accessing ***that*** service ***online, not later than six months after the list, including that scheme, is published***.

Article 6

Conditions ~~of~~for notification of electronic identification schemes

1. An ~~E~~electronic identification scheme**~~s~~** shall be eligible for notification pursuant to Article 7**(1)** if all the following conditions are met:

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

(i) by**~~, on behalf of, or under the responsibility of~~** 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;

(a) the electronic authentication means are ***either*** issued by ***the Member State, or issued by another entity as mandated by the Member State or issued independently but recognised by*** the notifying Member State;

(b) the electronic identification means **under that scheme** can be used to access at least **one service provided by a** public **~~services~~ sector body** requiring electronic identification in the notifying Member State;

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

(ba) that scheme and the electronic identification means issued thereunder meet the requirements of one of the assurance levels set out in ~~Annex 0~~ the implementing act referred to in Article 6a;

(ba) the electronic identification scheme meets the requirements of the interoperability model under Article 8,

(c) the notifying Member State ensures that the **unambiguous** person identification data are attributed **~~unambiguously~~** to the natural or legal person referred to in **point 1 of** Article 3 **~~point1~~ at the time of issuance of the electronic identification means under that scheme**;

(cb) the party issuing the electronic identification means under that scheme ensures that electronic identification means is attributed to the person referred to in point (c) in accordance with the requirements for the relevant assurance level set out in ~~Annex 0~~ the implementing act referred to in Article 6a;

(d) the notifying Member State ensures the availability of ~~an~~ authentication ~~possibility~~ online, ~~at any time and free of charge~~ so that any relying party **established ~~outside of the territory of that~~in the territory of another Member State** can validate the person identification data received in electronic form. **Such cross border authentication shall be provided free of charge ~~when accessing a service online provided by a public sector body~~[19].** Member States shall not **unduly** impose any specific technical requirements on relying parties ~~established outside of their territory~~ intending to carry out such authentication~~. When either the notified identification scheme or authentication possibility is breached or partly compromised, Member States shall suspend or revoke without delay the notified identification scheme or authentication possibility or the compromised parts concerned and inform the other Member States and the Commission pursuant to Article 7~~;

(d) the notifying Member State ensures the availability of an authentication possibility online, at any time and, ***in case of access to a service online provided by a public sector body,*** free of charge so that any relying party ***established outside the territory of that member state*** can validate the person identification data received in electronic form. Member States shall not impose ***disproportionate*** technical requirements on relying parties established outside of their territory intending to carry out such authentication. When either the notified identification scheme or authentication possibility is breached or partly compromised, Member States shall suspend or revoke without delay the notified identification scheme or authentication possibility or the compromised parts concerned and inform the other Member States and the Commission pursuant to Article 7;

(da) at least six months prior to notification pursuant to Article 7(1), the notifying Member State provides to other Member States for the purposes of the obligation under Article 8(1c) a description of that scheme in accordance with the procedural modalities referred to in Article 8(1d).

(db) that scheme meets the requirements of the implementing act referred to in Article 8(2a).

~~**(e) the notifying Member State takes liability for:**~~

~~**(i) the unambiguous attribution of the person identification data referred to in point (c), and**~~

~~**(ii) the authentication possibility specified in point (d).**~~

[19] This text has been deleted following the amendment in Article 5 restricting the scope to services provided by public sector bodies.

(e) the notifying Member State takes liability for:

- (i) the attribution of the person identification data referred to in point (c), and

- (ii) the authentication possibility specified in point (d).

~~**2. Point (e) of paragraph 1 is without prejudice to the liability of parties to a transaction in which electronic identification means falling under the notified scheme are used.**~~

2. Point (e) of paragraph 1 is without prejudice to the liability of parties to a transaction in which electronic identification means falling under the notified scheme are used.

~~**3. For the purposes of taking into account relevant developments in the electronic identification sector, subject to the criteria set out in point 1 of Annex 0 and taking into account the results of the cooperation between Member States, the Commission shall be empowered to adopt delegated acts in accordance with Article 38 to amend that Annex, with the exception of point 1.**~~

Article 6a

Assurance levels of electronic identification schemes

1. An electronic identification scheme notified in accordance with Article 7 shall specify the assurance levels for electronic identification means issued under that scheme.

2. Subject to the second subparagraph, the Commission shall set out, by means of implementing acts, minimum technical requirements for three assurance levels for electronic identification schemes notified in accordance with Article.

The three assurance levels referred to in the previous subparagraph shall correspond to the headings: 'low', 'substantial' and 'high'. Those levels shall be established by assessing the reliability and quality of:

(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, in which the natural or legal person uses the electronic identification means to attest its identity to a relying party.

(d) the entity issuing electronic identification means;

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

(f) the technical aspects of the issued electronic identification means.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

Article 7

Notification

1. **The notifying** Member State**~~s which notify an electronic identification scheme~~** shall forward to the Commission the following information and without undue delay, any subsequent changes thereof:

(a) a description of the notified electronic identification scheme**, including its assurance level~~s~~, ~~and~~ the issuer(s) of electronic identification means under that scheme and the applicable supervisory and liability regime**;

(a) a description of the notified electronic identification scheme ***and its security assurance level***;

(b) the authority **or authorities** responsible for the notified electronic identification scheme;

(c) information on **the entity or entities ~~by whom~~ which manages** the registration of the unambiguous person identifi**~~ers~~cation data ~~is managed~~**;

(c) information on ***which entity or entities*** the registration of the ***appropriate attributes*** identifiers is managed;

(ca) a description of how the requirements of the implementing act referred to in Article 8(2a) are met;

(ca) a description of how the requirements of the interoperability framework referred to in Article 8 are met;

(d) a description of the authentication ~~**possibility**~~ **referred to in point (d) of Article 6(1)**;

(d) a description of the authentication possibility ***and any technical requirements imposed on relying parties***;

(e) arrangements for suspension or revocation of either the notified identification scheme or authentication ~~**possibility**~~ or the compromised parts concerned.

(e) arrangements for suspension or revocation of either the notified authentication ***scheme*** or the compromised parts concerned.

2. [**Six**] ~~**Twelve**~~ months after the ~~**entry into force**~~ **date of application** of the Regulation, the Commission shall publish in the *Official Journal of the European Union* the list of the electronic identification schemes which were notified pursuant to paragraph 1 and the basic information thereon.

2. Six months after the entry into force of the Regulation, the Commission shall publish in the Official Journal of the European Union ***as well as on a publicly available website*** the list of the electronic identification schemes which were notified pursuant to paragraph 1 and the basic information thereon.

3. If the Commission receives a notification after the period referred to in paragraph 2 **has** expired, it shall ***publish in the Official Journal of the European Union*** **the** amend**ments to** the list **referred to in paragraph 2** within ~~**three**~~ **two** months **from the date of receipt of that notification**.

3. If the Commission receives a notification after the period referred to in paragraph 2 expired, it shall amend the list within three months.

3a. A Member State may submit to the Commission a request to remove the 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 in the list within one month from the date of receipt of the Member State's request.

4. The Commission may, by means of implementing acts, define the circumstances, formats and procedures of the notification referred to in paragraph~~s~~ 1 ~~**and 3**~~. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

4. The Commission may, by means of implementing acts, define the formats of the notification referred to in paragraphs 1 and 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

Article 7a

Security breach

1. When either the electronic identification scheme notified pursuant to Article 7(1) or the authentication referred to in point (d) of Article 6(1) 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 suspend or revoke without delay that cross border authentication or the compromised parts concerned and 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 3 months of the suspension or revocation, the notifying Member State shall notify the withdrawal of the electronic identification scheme to other Member States and to the Commission. The Commission shall publish without undue delay in the *Official Journal of the European Union* the corresponding amendments to the list referred to in Article 7(2).

Article 7a

Security breach

1. When either the electronic identification scheme notified pursuant to Article 7(1) or the authentication referred to in point (d) of Article 6(1) is breached or partly compromised in a way that would affect the reliability of that scheme for cross-border transactions, the notifying Member State shall without undue delay suspend or revoke the crossborder function of that electronic identification scheme or that authentication or the compromised parts concerned and inform other Member States and the Commission thereof.

2. When the breach or compromise referred to in paragraph 1 has been remedied, the notifying Member State shall re-establish the authentication and shall inform other Member States and the Commission as soon as possible.

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 the withdrawal of the electronic identification scheme to other Member States and to the Commission. The Commission shall publish without undue delay in the Official Journal of the European Union the corresponding amendments to the list referred to in Article 7(2).

Article 7b

Liability

1. The notifying Member State shall be liable for damage caused to any natural or legal person for failing in a cross border transaction to comply with its obligations under points (c) and (d) of Article 6(1).

2. The party issuing the electronic identification means shall be liable for damage caused to any natural or legal person for failing in a cross border transaction to comply with the obligation referred to in point (cb) of Article 6(1).

2a. The party operating the authentication procedure shall be liable for damage caused to any natural or legal person for failing to ensure in a cross border transaction the correct operation of the authentication referred to in point (d) of Article 6(1).

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

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

Article 7a

Liability

1. The notifying Member State shall be liable with regard to electronic identification means issued by it or on its behalf for any direct damage caused by non-compliance with obligations under Article 6, unless it can show that it has not acted negligently.

2. The issuer of an electronic identification means recognized and notified by a Member State pursuant to the procedure referred to in Article 7 shall be liable for failure to ensure

– (i) the unambiguous attribution of the person identification data, and

– (ii) the authentication possibility, unless he can show that he has not acted negligently.

Article 8

~~Coordination~~ Cooperation and interoperability

Coordination ***and interoperability***

1. **~~Member States shall cooperate in order to ensure the interoperability of electronic identification means falling under a notified scheme and to enhance their security.~~**

The national electronic identification schemes notified in accordance with Article 7 shall be interoperable.

1. Member States shall cooperate in order to ensure the interoperability of electronic identification means. ***The interoperability between national electronic identification infrastructures shall be ensured through an interoperability model.***

1.a. The national electronic identification schemes notified pursuant to Article 7 shall be interoperable.

1aa. For the purposes of the requirement under paragraph 1, the interoperability framework shall be established.

1a. The interoperability framework shall meet the following criteria:

1b. The interoperability framework shall meet the following criteria:

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

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

(b) it shall follow European and international standards, when possible;

(c) it shall facilitate the implementation of the principle of privacy by design;

(b) it shall facilitate the implementation of the principle of privacy by design.

(d) it shall ensure that personal data is processed in accordance with Directive 95/46/EC.

1b. The interoperability framework shall consist of:

(a) reference to minimum technical requirements related to the assurance levels defined in ~~Annex 0~~ the implementing act referred to in Article 6a;

(b) a mapping of national assurance levels of notified electronic identification schemes into the assurance levels defined in ~~Annex 0~~ the implementing act referred to in Article 6a;

(c) reference to minimum technical requirements for interoperability;

(ca) reference to a minimum set of person identification data available from electronic identification schemes;

(d) rules of procedure[20];

(e) arrangements for dispute resolution.

1.b. Member States and the commission shall in particular prioritize interoperability for such e-services with the greatest cross-border relevance by:

(a) exchanging best practices concerning the electronic identification means falling under a notified scheme;

(b) providing and regularly update best practices on trust and security of the electronic identification means;

(c) providing and regularly update on the promotion of the use of electronic identification means.

1c. Member States shall cooperate with regard to the following:

- the interoperability of the electronic identification schemes notified pursuant to Article 7(1) and the electronic identification schemes which Member States intend to notify;

- the security of the electronic identification schemes.

1d. The cooperation between Member States shall consists of :

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

(b) exchange of information, experience and good practice on working with assurance levels of electronic identification schemes referred to in ~~Annex 0~~ the implementing act referred to in Article 6a and on categories of services requiring a specific assurance level;

---

20 The rules of procedures would define the governance principles, mechanisms and rules for the interoperability framework. As such, they would facilitate all phases and activities of the interoperability framework: from conception to implementation; from cooperation of experts to application of standards; etc. A possible example can be the ISA interoperability Framework for Public Administration (see: http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf

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

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

2. The Commission shall, by means of implementing acts, establish the necessary **procedural** modalities to facilitate the cooperation between the Member States referred to in paragraph**s** 1**c and 1d** with a view to fostering a high level of trust and security appropriate to the degree of risk. ~~**Those implementing acts shall concern, in particular, the exchange of information, experiences and good practice on electronic identification schemes, the peer review of notified electronic identification schemes and the examination of relevant developments arising in the electronic identification sector by the competent authorities of the Member States.**~~

2. The Commission shall, by means of implementing acts, establish the necessary modalities to facilitate the cooperation between the Member States referred to in paragraph 1 with a view to fostering a high level of trust and security appropriate to the degree of risk. Those implementing acts shall concern, in particular, the exchange of information, experiences and good practice on electronic identification schemes, the ***independent, third-party auditing*** of notified electronic identification schemes and the examination of relevant developments arising in the electronic identification sector by the competent authorities of the Member States. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

2a. By [*insert the date*], for the purpose of setting uniform conditions for the implementation of the requirement under paragraph 1, the Commission, subject to the criteria set out in paragraph 1a and taking into account the results of the cooperation between Member States, shall adopt implementing acts on the interoperability framework as defined in paragraph 1b.

~~**2b. When public policy or public security or protection of personal data justifies it, the Commission, taking into account the results of the cooperation between Member States, may adopt implementing acts to establish categories of services for which a specific assurance level referred to in Annex 0 may be required, provided that the following conditions are met:**~~

~~**(a) analysis of the requirement for a specific assurance level has shown the appropriatness of such a requirement;**~~

~~**(b) the requirement for a specific assurance level shall be proportionate to the objective of public policy, public security or protection of special categories of personal data within the meaning of Article 8(1) of Directive 95/46/EC;**~~

~~**(c) there is a high risk that accepting a lower assurance level would expose a fundamental interest of society to threats.**~~

3.~~ Those i~~Implementing acts **referred to in paragraphs 2~~,~~ and 2a ~~and 2b~~ of this Article** shall be adopted in accordance with the examination procedure referred to in Article 39(2).

~~**3. The Commission shall be empowered to adopt delegated acts in accordance with Article 38 concerning the facilitation of cross border interoperability of electronic identification means by setting of minimum technical requirements.**~~

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 38 concerning the facilitation of cross border interoperability of electronic identification means by setting ***technologically neutral*** minimum ***requirements for the different security levels which shall not require changes to the fundamental design of national electronic identification schemes.***

3a. With regard to the cross-border exchange of personal data necessary to ensure interoperability of electronic identification means, the provisions ofArticle 11(2) shall apply mutatis mutandis.

CHAPTER III

TRUST SERVICES

Section 1

General provisions

Article 9

Liability and burden of proof[21]

1. ~~**A**~~ **Without prejudice to paragraph 2, t**rust service provider**s** shall be liable for ~~**any direct**~~ damage caused to any natural or legal person due to failure to comply with the obligations ~~**laid down in Article 15(1)**~~ **under this Regulation if that damage is due to fault or neglect of the trust service provider**~~**., unless the trust service providers can prove that he has not acted negligently**~~. ~~**Qualified trust service provider shall not be liable if it proves that it has not acted negligently.**~~

The burden of proving fault or neglect of a non-qualified trust service provider shall lie with a natural or legal person claiming the damage referred to in the first subparagraph.

The fault or neglect of a qualified trust service provider shall be presumed unless a qualified trust service provider proves that the damage referred to in the first subparagraph occurred without the fault or neglect of that qualified trust service provider.

~~**This provision shall be applied in accordance with national rules on liability.**~~

1. A trust service provider shall be liable for direct damage caused to any natural or legal person due to failure to comply with the obligations laid down in Article 15(1), unless the trust service provider can prove that he has not acted negligently.

~~**2. A qualified trust service provider shall be liable for any direct damage caused to any natural or legal person due to failure to meet the requirements laid down in this Regulation, in particular in Article 19, unless the qualified trust service provider can prove that he has not acted negligently.**~~

2. Where trust service providers duly inform their customers in advance about the limitations on the use of the services they provide and those limitations are recognisable to third parties, ~~they~~ trust service providers shall not be liable for damages arising from the use of services exceeding the indicated limitations.

---

21 This Article deals exclusively with the liability of TSPs and QTSPs. Obligations or responsibilities of users, clients and relying parties are left to national law.

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

2a. The law applicable to trust services, particularly with regard to disputes, shall be that of the Member State in which the person receiving the service is established unless otherwise jointly agreed by the service provider and recipient.

Article 10

~~Trust services providers from third countries~~ International aspects

Qualified trust services providers from third countries

1. Qualified trust services **~~and qualified certificates~~** provided by qualified trust service providers established in a third country shall be **~~accepted~~ recognised** as **legally equivalent to** qualified trust services **~~and qualified certificates~~** provided by **~~a~~** qualified trust service providers established in **~~the territory of~~** the Union if the qualified trust services **~~or qualified certificates~~** originating from the third country are recognised under an agreement **concluded** between the Union and third countries or international organisations in accordance with Article 218 **~~TFUE~~TFEU**.

1. Qualified trust services and qualified certificates provided by qualified trust service providers established in a third country shall be accepted as qualified trustservices and qualified certificates providedby a qualified trust service ***provider*** established in the territory of the Union if:

(a) the qualified trust service provider fulfils the requirements laid down in this Regulation and has been accredited under an accreditation scheme established in a Member State; or

(b) the qualified trust service provider established within the Union which fulfilsthe requirements laid down in thisRegulation guarantees the compliancewith the requirements laid down in thisRegulation; or

(c) the qualified trust services or qualifiedcertificates originating from a thirdcountry are recognised under anagreement between the Union and thatthird country or internationalorganisation in accordance with Article218 TFEU.

2. **~~With reference to paragraph 1, such a~~A**greements **referred to in paragraph 1** shall ensure**, in particular,** that**:**

- the requirements applicable to qualified trust service**s ~~and qualified certificates provided by qualified trust service~~** providers established in **~~the territory of~~** the Union **and the qualified trust services they provide** are met by the trust service providers in the third countries or international organisations **with which agreements are concluded, and by services they provide~~especially with regard to the protection of personal data, security and supervision.~~;**

- the qualified trust services provided by qualified trust services providers established in the Union are recognised as legally equivalent to trust services provided by trust service providers in the third country or international organisation with which agreements are concluded.

2. With reference to paragraph 1, such agreements shall ensure that the requirements applicable to qualified trust services and qualified certificates provided by qualified trust service providers established in the territory of the Union aremet by the trust service providers in the third countries or international organisations, especially the security of the trust services provided and the supervision of qualified trust service providers.

The third country in question shall afford adequate protection of personal data, in accordance with Article 25(2) of Directive 95/46/EC.

~~***Article 11***~~

~~**Data processing and protection**~~

~~**1. Trust service providers and supervisory bodies shall ensure fair and lawful processing process personal data in accordance with [Directive 95/46/EC] when processing personal data.**~~

~~**2. Trust service providers shall process personal data according to Directive 95/46/EC. Such Personal data processing shall be strictly limited to the minimum data needed to issue and maintain a certificate or to provide a trust service.**~~

~~**3. Trust service providers shall guarantee ensure the confidentiality and integrity of data related to a person to whom the trust service is provided.**~~

~~**4. Without prejudice to the legal effect given to pseudonyms under national law, Member States shall not prevent trust service providers from indicating in electronic signature certificates a pseudonym instead of the signatory's name in certificates.**~~

Article 11

Data processing and protection

1. Trust service providers and supervisory bodies shall ensure fair and lawful processing in accordance with Directive 95/46/EC ***and applicable national law*** when processing personal data.

2. Trust service providers shall process personal data according to Directive 95/46/EC. Such processing shall be strictly limited to the minimum data needed to issue and maintain a certificate or to provide a trust service.

3. Trust service providers shall guarantee the confidentiality and integrity of data related to a person to whom the trust service is provided, ***in particular by ensuring that the data used for trust service generation cannot be tracked.***

4. Without prejudice to the legal effect given to pseudonyms under national law, Member States shall not prevent trust service providers indicating in electronic signature certificates a pseudonym instead of the signatory's name.

4 a. Processing of personal data by or on behalf of the trust service provider, where strictly necessary to ensure network and information security for the purpose ofcomplying with the requirements of Articles 11, 15, 16 and 19, shall be considered a legitimate interest in the meaning of point (f) of Article 7 of Directive 95/46/EC.

Article 12

Accessibility for persons with disabilities

Where feasible[22]**,** ~~**T**~~**t**rust services provided and end user products used in the provision of those services shall be made accessible for persons with disabilities ~~**whenever possible**~~.

Trust services provided and end user products used in the provision of those services shall be made accessible for persons with disabilities ***in accordance with union law.***

1a. The Commission shall establish and award trust mark to distinguish products and services accessible for persons with disabilities.

1b. EU standards organizations areresponsible for development of assessmentcriteria for products and servicesaccessible for persons with disabilities.

[22] See amended recital 23.

Section 2

Supervision

Article 13

Supervisory body

1. Member States shall designate ~~**an appropriate**~~ **a supervisory** body[23] established in their territory or, upon mutual agreement ~~**in**~~ **with** another Member State, **a supervisory body established in that other Member State**, **which body shall be** ~~**under the responsibility of**~~ **responsible for supervisory tasks in** the designating Member State.

Supervisory bodies shall **be given** ~~**have**~~ **all the necessary** ~~**supervisory and investigatory**~~ **powers and adequate** ~~**human and financial**~~ **resources** for the exercise of their tasks.

1. Member States shall designate ***a supervisory*** body established in their territory or, upon mutual agreement, in another Member State under the responsibility of the designating Member State. ***The name and address of the supervisory body shall be communicated to the Commission.*** Supervisory bodies shall be given ***adequate resources and powers*** necessary for the exercise of their tasks.

1a. Member States shall notify to the Commission the names and the addresses of their respective designated supervisory bodies.

2. The **role of the** supervisory body shall be **the following:** ~~**responsible for the performance of the following tasks:**~~

2. The supervisory body shall ***perform*** the following tasks:

(a) ~~**monitoring**~~ **to supervise qualified** trust service providers established in the territory of the designating Member State to ensure**, through ex ante and ex post supervisory activities,** that they **and the qualified trust services they provide** ~~**fulfil**~~ **meet** the requirements laid down in **this Regulation** ~~**Article 15;**~~

(a) ***undertaking supervision of*** trust service providers ***and qualified trust service providers*** established in the territory of the designating Member State ***in order*** to ensure that they ***meet the*** requirements laid down in ***this Regulation***;

[23] See new recital 24a.

(b) ~~**undertaking supervision of qualified to monitor**~~ **to take action in relation to non-qualified** trust service providers established in the territory of the designating Member State ~~**and of the qualified trust services they provide to verify, whenever needed and**~~ **through ex post supervisory activities, when informed** ~~**in order to ensure**~~ that they and the ~~**qualified**~~ trust services ~~**provided by them**~~ **they provide** ~~**qualified trust service providers**~~ **do not** meet the ~~**applicable**~~ requirements laid down in this Regulation**. The supervisory body has no general obligation to supervise non-qualified trust service providers;**

(b) Deleted

~~**(c) ensuring that relevant information and data referred to in point (g) of Article 19(2), and recorded by qualified trust service providers are preserved and kept accessible after the activities of a qualified trust service provider have ceased, for an appropriate time with a view to guaranteeing continuity of the service.**~~

(c) ensuring that relevant information and data referred to in point (g) of Article 19(2), and recorded by qualified trust service providers are preserved and kept accessible after the activities of a qualified trust service provider have ceased, for an appropriate time***, in particular considering the validity period of the services,*** with a view to guaranteeing continuity of the service.

2a. For the purposes of paragraph 2 and subject to the limitations provided therein, the tasks of the supervisory body, shall include in particular:

(a) to cooperate with other supervisory bodies and provide those bodies with assistance in accordance with Article 14;

(b) to analyse the conformity assessment reports referred to in Articles 16(1) and 17(1);

(c) to inform other supervisory bodies and the public about breaches of security or loss of integrity in accordance with Article 15(2);

(d) to report to the Commission about its main activities in accordance with paragraph 3 of this Article;

(e) to carry out audits or request a conformity assessment body to perform a conformity assessment of qualified trust service providers in accordance with Article 16(2);

(ea) to inform the data protection authorities about the results of audits of qualified trust service providers, where personal data protection rules appear to have been breached;

(f) to grant the qualified status to ~~non-qualified~~ trust service providers and to the services they provide and to withdraw this status in accordance with Articles 16 and 17;

(g) to inform the body responsible for the national trusted list referred to in Article 18(3) about its decisions to grant or to withdraw the qualified status, unless this body is the supervisory body itself;

(h) to ~~adopt~~ verify existence and correct application of provisions on termination plans in cases where the qualified trust service providers cease their activities;

(i) to require that trust service providers remedy any failure to fulfil the requirements of this Regulation.

2b. Member States may provide that supervisory body shall establish, maintain and update a trust infrastructure according to the conditions set by national law.

3. **Annually, by the 31st March, ~~E~~e**ach supervisory body shall submit **to the Commission** a ~~**yearly**~~ report on **its previous ~~the last~~** calendar year's ~~**supervisory**~~ **main** activities ~~**to the Commission and Member States by the end of the first quarter of the following year. It shall include at least:**~~

3. Each supervisory body shall ***make publically available*** a yearly report on the last calendar year's supervisory activities by the end of the first quarter of the following year. It shall include at least:

~~**(a) information on its supervisory activities;**~~

(a) Information on its supervisory activities;

~~**(b)**~~ **together with** a summary of breach notifications received from trust service providers in accordance with Article 15(2)~~**;**~~**. Where appropriate,~~T~~the Commission may communicate that summary to the European Network and Information Security Agency (ENISA).**

(b) a summary of ***all*** breach notifications received from trust service providers in accordance with Article 15(2);

~~**(c) statistics on the market and usage of qualified trust services, including information on qualified trust service providers themselves, the qualified trust services they provide, the products they use and the general description of their customers.**~~

(c) Deleted

3a. The Commission shall make the annual report referred to in paragraph 3 available to Member States.

~~**4. Member States shall notify to the Commission and other Member States the names and the addresses of their respective designated supervisory bodies.**~~

4. Deleted

~~**5. The Commission shall be empowered to adopt delegated acts, in accordance with Article 38, concerning the definition of procedures applicable to the tasks referred to in paragraph 2.**~~

5. Deleted

6. The Commission may, by means of implementing acts, define the ~~**circumstances,**~~ formats and procedures for the report referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

6. The Commission may, by means of implementing acts, define the formats for the report referred to in paragraph 3. ***The Commission shall ensure, that stakeholder input is duly considered.*** Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

Article 13a

Cooperation with data protection authorities

Member States shall provide that the supervisory bodies referred to in Article 13 shall cooperate with Member States' data protection authorities designated pursuant to Article 28 of Directive 95/46/EC in order to enable them to ensure compliance with national data protection rules adopted pursuant to Directive 95/46/EC.

Article 14

Mutual assistance

1. Supervisory bodies shall cooperate with a view to exchange good practice~~**. and provide each other, within the shortest possible time, with relevant information and**~~ **A supervisory body shall, upon a justified request from another supervisory body, provide that body with** ~~**mutual**~~ assistance so that **their** activities can be carried out in a consistent manner. Mutual assistance ~~**shall**~~ **may** cover, in particular, information requests and supervisory measures, such as requests to carry out inspections related to the ~~**security audits**~~ **conformity assessment reports** as referred to in Articles 15, 16 and 17.

1. Supervisory bodies shall cooperate with a view to ***exchanging*** good practice. ***They shall*** provide each other, within the shortest possible time, with relevant information, and ***upon justified requests, provide each other*** mutual assistance so that activities can be carried out in a consistent manner. ***Requests for*** mutual assistance ***may*** cover, in particular, information requests and supervisory measures, such as requests to carry out inspections related to the security audits as referred to in Articles 15, 16 and 17.

2. A supervisory body to which a request for assistance is addressed may ~~**not**~~ refuse **that request** ~~**to comply with it unless**~~ **under any of the following conditions**:

2. A supervisory body to which a request for assistance is addressed may refuse ***that request under any of the following conditions***:

(a) ~~**it**~~ **the supervisory body** is not competent to ~~**deal with the request**~~ **provide the requested assistance**; ~~**or**~~

(a) ***The supervisory body*** is not competent to deal with the request; or

(aa) the requested assistance is not proportionate to standard supervisory activities of the supervisory body;

(b) ~~**compliance with**~~ **providing** the request**ed assistance** would be incompatible with this Regulation.

(b) ***if the requested assistance*** would ***go beyond the tasks and powers of the supervisory body set out in*** this Regulation ***and applicable legislation***.

3. Where appropriate, **Member States may authorise their respective** supervisory bodies ~~**may**~~ **to** carry out joint investigations in which staff from other Member States' supervisory bodies is involved. **The arrangements and procedures for such joint investigations shall be agreed and established by the Member States concerned in accordance with their national laws.**

3. Where appropriate, supervisory bodies may carry out joint ***actions***.

~~**The supervisory body of the Member State where the investigation is to take place, in compliance with its own national law, may devolve investigative tasks to the assisted supervisory body's staff. Such powers may be exercised only under the guidance and in the presence of staff from the host supervisory body. The assisted supervisory body's staff shall be subject to the host supervisory body's national law. The host supervisory body shall assume responsibility for the assisted supervisory body staff's actions.**~~

The supervisory body of the Member State where the investigation is to take place, in compliance with its own national law, may devolve investigative tasks to the assisted supervisory body's staff. Such powers may be exercised only under the guidance and in the presence of staff from the host supervisory body. The assisted supervisory body's staff shall be subject to the host supervisory body's national law. The host supervisory body shall assume responsibility for the assisted supervisory body staff's actions.

~~4. The Commission may, by means of implementing acts, specify the formats and procedures for the mutual assistance provided for in this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).~~

4. Deleted

Article 15

Security requirements applicable to trust service providers

1. **Qualified and non-qualified ~~T~~t**rust service providers **~~who are established in the territory of the Union~~** shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. Having regard to **~~state of the art~~ the latest technological developments**, these measures shall ensure that the level of security is **~~appropriate~~ commensurate** to the degree of risk. In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of **the** adverse effects of any incidents.

1. Trust service providers who are established in the territory of the Union shall take appropriate technical and organisational measures in accordance with existing industry best practise to manage the risks posed to the security ***and resilience*** of the trust services they provide. Having regard to ***the technological development,*** these measures shall ***fully respect the data protection rights and ensure a*** level of security appropriate to the degree of risk. In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders, of adverse effects of any incidents. ***Trust service providers must also take appropriate measures to remedy any new security risks and restore the normal security level of the service.***

~~Without prejudice to Article 16(1), any trust service providers may submit the report of a security audit carried out by a recognised independent body to the supervisory body to confirm that appropriate security measures have been taken.~~[24]

[24] Deleted as overlapping with article 16(1).

Without prejudice to Article 16(1), any trust service provider ***shall, without undue delay and not later than 6 months following the commencement of its activities,*** submit the report of a ***compliance*** audit carried out by an independent body ***whose competence to carry out the audit has been demonstrated*** to confirm that appropriate security measures have been taken.

2. **Qualified and non-qualified ~~T~~t**rust service providers shall, without undue delay ~~**and where feasible not later than**~~ **but in any case within [**24**]** hours after having become aware of it, notify the ~~**competent**~~ supervisory body **and**, **where ~~appropriate~~ applicable, other relevant bodies, such as** the competent national body for information security ~~**and other relevant third parties such as**~~ **or the** data protection authorit**y~~ies~~,** of any breach of security or loss of integrity that has a significant impact[25] on the trust service provided ~~**and**~~ **or** on the personal data maintained therein.

2. Trust service providers shall without undue delay and where feasible not later than 24 hours after having become aware of it, notify the competent supervisory body and, ***where appropriate,*** other relevant ***bodies*** such as ***the competent national body for information security or the*** data protection authorities of any breach of security or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained therein. ***Where such notification cannot be made within 24 hours, an explanation of the reasons for the delay should accompany the notification.***

When the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the trust service provider shall also notify the natural or legal person of the breach or loss of integrity without undue delay.

Where appropriate, in particular if a breach of security or loss of integrity concerns two or more Member States, the **notified** supervisory body ~~**concerned**~~ shall inform **the** supervisory bodies in other Member States **concerned** ~~**and the European Network and Information Security Agency (ENISA)**~~.

Where appropriate, in particular if a breach of security or loss of integrity concerns two or more Member States, the supervisory body concerned shall inform supervisory bodies in ***these*** Member States and the European Network and Information Security Agency (ENISA).

The **notified** supervisory body ~~**concerned may**~~ **shall ~~also~~** inform the public or require the trust service provider to do so, where it determines that disclosure of the breach **of security or loss of integrity** is in the public interest.

The supervisory body concerned, ***in consultation with the trust service provider, shall*** inform the public or require the trust service provider to do so, where it determines that disclosure of the breach is in the public interest ***in order to allow them to take the necessary precautions***. ***Publication shall normally be as soon as reasonably practical; however the trust service provider may request a delay so that vulnerabilities can be fixed. If the supervisory body grants this, it may be for no longer than 45 days.***

[25] Explanatory recital could clarify the meaning of 'significant impact'.

~~**3. The supervisory body shall provide to ENISA and to the Commission once a year with a summary of breach notifications received from trust service providers.**~~

3. The supervisory body shall provide to ***the European Network and Information Security Agency*** (ENISA) and to the Commission once a year with a summary of breach notifications received from trust service providers.

~~**4. In order to implement paragraphs 1 and 2, the competent supervisory body shall have the power to issue binding instructions to trust service providers.**~~[26]

4. In order to implement paragraphs 1 and 2, the competent supervisory body shall have the power to issue binding instructions to trust service providers. ***The supervisory body should coordinate these binding instructions with other relevant regulatory bodies that supervise the trust service provider's activities other than the trust service provision. All such instructions must be published.***

~~**5. The Commission shall be empowered to adopt delegated acts, in accordance with Article 38, concerning the further specification of the measures referred to in paragraph 1.**~~

5. Deleted

6. The Commission may, by means of implementing acts, define**:**

- further specification of the measures referred to in paragraph 1, and

- the ~~**circumstances,**~~ formats and procedures, including deadlines, applicable for the purpose of paragraph~~**s 1 to 3**~~ **2**.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

6. The Commission may, by means of implementing acts, define the ***further specification of the measures referred to in paragraph 1 and*** formats applicable for the purpose of paragraphs 1 to 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

[26] Deleted as already covered by article 13(1).

Article 16

Supervision of qualified trust service providers

1. **Qq**ualified trust service providers shall be audited, **at least every 24 months, at their own expense** by a ~~**recognised independent**~~ **conformity assessment** body ~~**once a year**~~ **in order** to confirm that they and the qualified trust services provided by them fulfil the requirements set out in this Regulation, and **they** shall submit the resulting ~~**security audit**~~ **conformity assessment** report to the supervisory body **within three working days after receiving it**.

1. Qualified trust service providers shall be audited ***annually*** by ***an*** independent body ***whose competence to carry out the audit has been demonstrated*** to confirm that they and the qualified trust services provided by them fulfil the requirements set out in this Regulation, and shall submit the resulting ***compliance*** audit report to the supervisory body. ***Such audit shall also be carried out following any significant technological or organizational changes. If, after three years, the annual audit reports raise no concerns, the audits referred to in this paragraph shall be carried out every two years only.***

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 to confirm that they and the qualified trust services provided by them ~~**still**~~ meet the conditions set out in this Regulation~~**, either on its own initiative or in response to a request from the Commission**~~. **Where personal data protection rules appear to have been breached, T**~~**t**~~he supervisory body shall inform the data protection authorities of the results of its audits~~**, in case personal data protection rules appear to have been breached**~~.

2. Without prejudice to paragraph 1, the supervisory body may at any time audit the qualified trust service providers to confirm that they and the qualified trust services provided by them meet the conditions set out in this Regulation. ***Where personal data protection rules as set out in Directive 95/46/EC appear to have been breached,*** the supervisory body shall inform the data protection authorities of the results of its audits.

~~**3. The supervisory body shall have the power to issue binding instructions to qualified trust service providers to remedy any failure to fulfil the requirements indicated in the security audit report.**~~[27]

3. The supervisory body shall have the power to issue binding instructions to qualified trust service providers to remedy any failure to fulfil the requirements ***set out in this Regulation***.

[27] Included as a task in article 13(2)(i).

4. ~~**With reference to paragraph 3, if**~~ **Where the supervisory body requires the qualified trust service provider to remedy ~~any~~ failure to fulfil requirements under this Regulation and ~~the qualified trust service~~ that** provider does not ~~**remedy any such failure**~~ **act accordingly, if applicable~~,~~** within a time limit set by the supervisory body, ~~**it**~~ **the supervisory body, taking into account in particular the extent, duration and consquences of that failure, may ~~shall~~ ~~lose its~~ withdraw ~~its~~ the** qualified status **of that provider** and ~~**be informed by the supervisory body that its status will be changed accordingly in**~~ **inform the body referred to in Article 18(3) for the purposes of updating** the trusted lists referred to in Article 18. **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.** [28]

4. With reference to paragraph 3, if the qualified trust service provider does not remedy any such failure within a time limit ***and in accordance with the procedure specified*** set by the supervisory body, it shall lose its qualified status and be informed by the supervisory body that its status will be changed accordingly in the trusted lists referred to in Article 18.

~~**5. The Commission shall be empowered to adopt delegated acts in accordance with Article 38 concerning the specification of the conditions under which the independent body carrying out the audit referred to in paragraph 1 of this Article and in Article 15(1) and in Article 17(1) shall be recognised.**~~

5. Deleted

~~**6. The Commission may, by means of implementing acts, define the circumstances, procedures and formats applicable for the purpose of paragraphs 1, 2 and 4. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).**~~

6. The Commission may, by means of implementing acts, define the formats applicable for the purpose of paragraphs 1, 2 and 4. ***The Commission shall ensure, that stakeholder input is duly considered, in form of an impact assessment, when defining standards to be used for the purpose of this Regulation.*** Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

[28] Article 16(4) is re-drafted taking into account the deletion of article 16(3).

Article 16a

Supervision of trust service providers

In order to facilitate supervision by the supervisory body referred to in point (a) of Article 13(2), trust service providers shall notify the supervisory body of their intention to start offering a trust service and shall inform it of the technical and organisational measures they have taken to manage the risks linked to the security of the trust services they provide in accordance with Article 15(1).

Article 16a

Penalties

Member States shall lay down the rules on penalties applicable to infringements of this Regulation. The penalties provided for shall be effective, proportionate and dissuasive.

Article 17

Initiation of a qualified trust service

1. ~~**Qualified**~~ **Where** trust service providers**, without qualified status, intend to start providing qualified trust services, they** shall ~~**notify**~~ **submit to** the supervisory body **a notification** of their intention ~~**to start providing a qualified trust service and shall submit to the supervisory body a security audit**~~ **together with a conformity assessment** report ~~**carried out**~~ **issued** by a ~~**recognised independent**~~ **conformity assessment** body~~**, as provided for in Article 16(1)**~~. ~~**Qualified trust service providers may start to provide the qualified trust service after they have submitted the notification and security audit report to the supervisory body.**~~

1. Qualified trust service providers shall notify the supervisory body of their intention to ***provide*** a qualified trust service and shall submit to the supervisory body a security audit report carried out by ***an*** independent body ***whose competence to carry out the audit has been demonstrated***, as provided for in Article 16(1). Qualified trust service providers may start to provide the qualified trust service after they have submitted the security audit report to the supervisory body***, and only once obtained the qualified status***.

~~**2. Once the relevant documents are submitted to the supervisory body according to paragraph 1, the qualified service providers shall be included in the trusted lists referred to in Article 18 indicating that the notification has been submitted.**~~

2. Once the relevant documents are submitted to the supervisory body according to paragraph 1 ***and the supervisory body confirms compliance*** the qualified service providers shall be included in the trusted lists referred to in Article 18 indicating that the ***qualified status*** has been ***confirmed***.

3. The supervisory body shall verify the compliance of the **~~qualified~~** trust service provider **referred to in paragraph 1** and of the **~~qualified~~** trust services provided by it with the requirements of th**~~is~~e** Regulation**, in particular, with the requirements provided for qualified trust services providers**. **If the supervisory body concludes that the trust service provider and the trust services provided by it comply with those requirements, ~~T~~t**he supervisory body shall **~~indicate~~ grant** the qualified status **~~of~~ to** the **~~qualified~~ trust** service provider**~~s~~** and the **~~qualified~~** trust services **~~they~~ it** provide**s and inform the body referred to in Article 18(3) for the purposes of updating ~~in~~** the trusted lists **referred to in Article 18 ~~after the positive conclusion of the verification~~**, not later than **~~one~~ three** month**s** after **~~the~~** notification **~~has been done~~** in accordance with paragraph 1.

3. The supervisory body shall verify the compliance of the qualified trust service provider and of the qualified trust services provided by it with the requirements of the Regulation.

The supervisory body shall indicate the qualified status of the qualified service providers and the qualified trust services they provide in the trusted lists after the positive conclusion of the verification ***process without undue delay and not later than 1 month***.

If the verification is not concluded within **~~one~~ three** month**s**, the supervisory body shall inform the **~~qualified~~** trust service provider specifying the reasons **~~of~~ for** the delay and the period **~~by~~ within** which the verification shall be concluded.

If the verification is not concluded within one month, the supervisory body shall inform the qualified trust service provider specifying the reasons of the delay and the period by which the verification shall be concluded. ***Provided that the trust service provider has supplied the relevant documents, the verification may not exceed three months.***

~~4. A qualified trust service which has been subject to the notification referred to in paragraph 1 cannot be refused for the fulfilment of an administrative procedure or formality by the concerned public sector body for not being included in the lists referred to in paragraph 3.~~

4. Deleted

4. Qualified trust service providers may start to provide the qualified trust service after the status referred to in paragraph 3 has been indicated in the trusted lists.

5. The Commission may, by means of implementing acts, define the **~~circumstances,~~** formats and procedures for the purpose of paragraphs 1**~~, 2~~** and 3.Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

5. The Commission may, by means of implementing acts, define the formats for the purpose of paragraphs 1, 2 and.3 Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

Article 18

Trusted lists

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

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

2. Member States shall establish, maintain and publish, in a secure manner, electronically signed or sealed trusted lists provided for in paragraph 1 in a form suitable for automated processing ***of both the list itself as well as the individual certificates.***

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 certificate**s** used to sign or seal the trusted lists and any changes thereto.

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. The Commission shall be empowered to adopt delegated acts in accordance with Article 38 concerning the definition of the information referred to in paragraph 1.**~~

5. Deleted

6. The Commission may, 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 39(2).

6. The Commission may, by means of implementing acts, ***specify the information referred to in paragraph and*** define the technical specifications and formats for trusted lists applicable for the purposes of paragraphs 1 to 4. ***The Commission shall ensure, that stakeholder input is duly considered, in form of an impact assessment, when defining standards to be used for the purpose of this Regulation.*** Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

Article 18a

EU trustmark for qualified trust services

1. Qualified trust service providers may use an EU trustmark to present and advertise the qualified trust services they offer that meet the requirements laid down in this Regulation.

2. By using the EU trustmark for qualified trust services referred to in paragraph 1, qualified trust service providers shall be responsible for ensuring that the services meet all applicable requirements laid down in this Regulation.

3. By means of implementing acts, the Commission shall lay down specific, binding criteria relating to the presentation, composition, size and design of the EU trustmark for qualified trust services. The Commission shall ensure, that stakeholder input is duly considered, preferably in form of an impact assessment, when defining standards to be used for the purpose of this Regulation. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

Article 19

Requirements for qualified trust service providers

1. When issuing a qualified certificate **for a trust service**, a qualified trust service provider shall verify, by appropriate means ~~[~~and in accordance with national law~~]~~, the identity and, if applicable, any specific attributes of the natural or legal person to whom a qualified certificate is issued.

~~**Such**~~ **The** information **referred to in the previous subparagraph** shall be verified by the qualified **trust** service provider or by ~~**an authorised**~~ **a trusted** third party ~~**acting under the responsibility of the qualified trust service provider**~~:

(a) by a physical appearance of the natural person or of an authorised representative of the legal person, or

(b) remotely, using electronic identification means **when during prior issuance of the qualified certificate, a physical appearance of the natural person or of an authorised representative of the legal person was ensured and it is trusted by the issuer under national law or**

(ba) a certificate of a qualified electronic signature or ~~an~~ of a qualified electronic seal ~~under a notified scheme~~ issued in compliance with point (a) **or (b)~~, or~~**

~~**(c) by using other electronic identification means recognised at national level**~~**.**

2. Qualified trust service providers providing qualified trust services shall:

(aa) inform the supervisory body of any change in provision of qualified trust services, including of the intention to cease its activities;

(a) 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 ~~**and have received appropriate training regarding security and personal data protection rules**~~;

(b) ~~**bear**~~ **with regard to** the risk of liability for damages **in accordance with Article 9,** ~~**by**~~ maintain~~**ing**~~ sufficient financial resources **and/**or ~~**by**~~ **obtain** ~~**an**~~ appropriate liability insurance ~~**scheme**~~;

(c) before entering into a contractual relationship, inform**, in a clear and comprehensive manner,** any person seeking to use a qualified trust service of the precise terms and conditions regarding the use of that service**, including any limitation on its use**;

(c) before entering into a contractual relationship, inform any person seeking to use a qualified trust service of the precise terms and conditions regarding the use of that service ***as well as the liability limits, in a clear and transparent manner***;

(d) use trustworthy systems and products which are protected against modification and **guarantee ensure** the technical security and reliability of the process supported by them;

(d) use systems and products which are protected against ***unauthorized*** modification and guarantee the technical security and reliability of the process supported by them;

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

(e) use systems to store data provided to them, in a verifiable form so that:

- they are publicly available for retrieval only where the consent of the person to whom the data ~~**has been issued**~~ **relates** has been obtained,

– they are publicly available for retrieval only where ***national or Union law allows for this and where*** the consent of the person to whom the data has been issued has been obtained,

- only authorised persons can make entries and changes **to the stored data**,

- ~~**information**~~ **the data** can be checked for authenticity;

(f) take **appropriate** measures against forgery and theft of data;

(g) record **and keep accessible** for an appropriate period of time[29]**, including 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, in particular 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;

(g) record for an appropriate period ***of time, regardless of whether the qualified trust service provider has ceased to provide qualified trust services,*** relevant information concerning data issued and received by the qualified trust service provider, in particular for the purpose of providing evidence in legal proceedings. ***The retention of this information shall be strictly limited to the time period necessary***. Such recording may be done electronically;

(h) have an up-to-date termination plan to ensure continuity of service**, where applicable,** in accordance with ~~**arrangements issued**~~ **provisions adopted** by the supervisory body under ~~**point (c) of**~~ Article 13(2**a**);

(i) ensure lawful processing of personal data in accordance with ~~**Article 11**~~ **Directive 95/46/EC**~~.~~;

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

3. **When ~~Q~~q**ualified trust service providers issuing qualified certificates **decide to revoke a certificate, they** shall register **such revocation** in their certificate database **and publish** the revocation **status** of the certificate **in timely manner, but in any case** within ~~**ten minutes**~~ **24 hours**[30] **after the receipt of the request** ~~**of the decision to revoke being taken**~~. ~~**s**~~**S**uch revocation ~~**has taken effect**~~ **shall become effective immediately upon its** ~~**registration in the certificate database**~~ **publication**.

3. Qualified trust service providers issuing qualified certificates shall register in their certificate database the revocation of the certificate ***without undue delay***.

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 any time **and beyond the certificate validity period** at least on a certificate basis in an automated manner which is reliable, free of charge and efficient.

---

29 The length of an "appropriate period of time" should be assessed by the trust service providers by taking into utmost account the type and nature services being provided as well as the administrative, financial, operational and legal obligations applicable at national level.

30 This timing is in line with the European Norm written by ETSI - EN 319411, part 2

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 any time at least on a certificate basis in an automated manner.

5. The Commission may, by means of implementing acts, establish reference numbers of standards for trustworthy systems and products**, which comply with the requirements under paragraph 2, points (d) and (e), of this Article** . Compliance with the requirements laid down in Article 19 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 39(2). ~~**The Commission shall publish those acts in the *Official Journal of the European Union*.**~~

5. The Commission may, by means of implementing acts, establish reference numbers of standards for systems and products. ***The Commission shall ensure, that stakeholder input is duly considered, in form of an impact assessment, when defining standards to be used for the purpose of this Regulation.*** Compliance with the requirements laid down in Article 19 shall be ***achieved through the compliance of*** systems and products ***with*** those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2). The Commission shall publish those acts in the Official Journal of the European Union.

Section 3

Electronic signature

Article 20

Legal effects ~~and acceptance~~ 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**:**

(a) in an electronic form**;**

(b) not an advanced electronic signature,

(c) not based upon a qualified certificate for electronic signature, or

(d) not created by a qualified electronic signature creation device.

1. An electronic signature shall have legal effect and ***may be admissible*** as evidence in legal proceedings. ***It shall be taken into account that the qualified electronic signature offers a higher level of security than other types of*** electronic ***signatures***.

2. A qualified electronic signature shall have the equivalent legal effect of a handwritten signature.

2. A qualified electronic signature ***shall satisfy*** the legal ***requirements of a signature in relation to data in electronic form in the same manner as a*** handwritten signature ***satisfies those requirements inrelation to paper-based data***;

2a. A valid qualified electronic signature shall serve as prima facie evidence for the authenticity and integrity of the electronic document associated with it.

3. **A ~~Q~~q**ualified electronic signature**~~s~~** shall be recognised **~~and accepted~~ as a qualified one** in all Member States.

3. Qualified electronic signatures shall be recognised and accepted in Member ***States and institutions of the Union***.

4. If an electronic signature with a security assurance level below qualified electronic signature is required, in particular by a Member State for accessing a service online offered by a public sector body on the basis of an appropriate assessment of the risks involved in such a service, all electronic signatures matching at least the same security assurance level shall be recognised and accepted.

4. If an electronic signature with a security assurance level below qualified electronic signature is required, by a Member State ***or by institutions, bodies, offices and agencies of the Union*** for ***completing a transaction*** offered by a public sector body on the basis of an appropriate assessment of the risks involved in such a service, all electronic signatures matching at least the same security assurance level shall be recognised and accepted ***for access to that online service***.

5. Member States shall not request for cross-border access to a service online offered by a public sector body an electronic signature at a higher security assurance level than qualified electronic signature.

5. Member States shall not request for cross-border access to a service online offered by a public sector body an electronic signature at a higher security level than qualified electronic signature.

6. The Commission shall be empowered to adopt delegated acts in accordance with Article 38 concerning the definition of the different security levels of electronic signature referred to in paragraph 4.

6. ***deleted***

7. The Commission may, by means of implementing acts, establish reference numbers of standards for the security levels of electronic signature. Compliance with the security level defined in a delegated act adopted pursuant to paragraph 6 shall be presumed when an electronic signature meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2). ~~**The Commission shall publish those acts in the *Official Journal of the European Union*.**~~

7. The Commission may, by means of implementing acts, establish reference numbers of standards for the security levels of electronic signature. ***The Commission shall ensure, that stakeholder input is duly considered, preferably in form of an impact assessment, when defining standards to be used for the purpose of this Regulation.*** Compliance with the security level defined in a delegated act adopted pursuant to paragraph 6 shall be presumed when an electronic signature meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2). The Commission shall publish those acts in the Official Journal of the European Union.

Article 21

Qualified certificates for electronic signature

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

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

3. If a qualified certificate for electronic signature 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 ~~**by renewing its validity**~~.

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 38 concerning the further specification of the requirements laid down in Annex I.

4. ***deleted***

5. The Commission may, 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 39(2). ~~**The Commission shall publish those acts in the *Official Journal of the European Union*.**~~

5. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified certificates for electronic signature. ***The Commission shall ensure, that stakeholder input is duly considered, preferably in form of an impact assessment, when defining standards to be used for the purpose of this Regulation.*** 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 39(2). The Commission shall publish those acts in the Official Journal of the European Union.

Article 22

Requirements for qualified electronic signature creation devices

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

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 39(2). ~~**The Commission shall publish those acts in the *Official Journal of the European Union*.**~~

2. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified electronic signature creation devices***. The Commission shall ensure, that stakeholder input is duly considered, preferably in form of an impact assessment, when defining standards to be used for the purpose of this Regulation***. 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 39(2). The Commission shall publish those acts in the *Official Journal of the European Union*.

Article 23

Certification of qualified electronic signature creation devices

1. Qualified electronic signature creation devices ~~**may**~~**shall** be certified by appropriate public or private bodies designated by Member States**.** ~~**provided that they have been submitted to**~~

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

2a. The certification referred to in paragraph 1 shall be based on a security evaluation process carried out in accordance with one of the standards for the security assessment of information technology products included in a list that shall be established by the Commission by means of implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2). ~~**The Commission shall publish those acts in the *Official Journal of the European Union*.**~~

1. Qualified electronic signature creation devices ***shall*** be certified by appropriate public or private bodies designated by Member States provided that they have been submitted to a security evaluation process carried out in accordance with one of the standards for the security assessment of information technology products included in a list that shall be established by the Commission by means of implementing acts. ***The Commission shall ensure, that stakeholder input is duly considered, preferably in form of an impact assessment, when defining standards to be used for the purpose of this Regulation.*** Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2). The Commission shall publish those acts in the Official Journal of the European Union.

~~**2. Member States shall notify to the Commission and other Member States the names and addresses of the public or private body designated by them as referred to in paragraph 1.**~~

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 38 concerning the establishment of specific criteria to be met by the designated bodies referred to in paragraph 1.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 38 concerning the establishment of specific criteria to be met by the designated bodies referred to in paragraph 1 ***for the purpose of carrying out the certification under paragraph 1***.

Article 24

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 1 month after the certification is concluded**, information on qualified electronic signature creation devices which have been certified by the bodies referred to in Article 23. They shall also notify to the Commission, without undue delay **and no later than 1 month after the certification is canceled**, information on electronic signature creation devices that would no longer be 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. The Commission may, by means of implementing acts, define circumstances, 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 39(2).

3. The Commission may, 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 39(2).

Article 25

Requirements for the validation of qualified electronic signatures

1. **The process for the validation of ~~A~~a** qualified electronic signature **~~shall be considered as valid~~ shall confirm the validity of a qualified electronic signature** provided that **~~it can be established with a high level of certainty, that at the time of signing~~**:

(a) the certificate, that supports the signature**~~, is~~ was, at the time of signing** a qualified electronic signature certificate complying with the provisions laid down in Annex I;

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

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

(d) the set of data **~~unambiguously~~** representing the signatory is correctly provided to the relying party;

(e) the use of any pseudonym is clearly indicated to the relying party if a pseudonym **~~is~~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 3 point 7 **~~are~~were** met **at the time of signing**;

~~(i)~~ 1a. ~~t~~The system used for validating the **electronic** signature **shall** provide**~~s~~** to the relying party the correct result of the validation process and **shall** allow**~~s~~** the relying party to detect any security relevant issues.

2. The Commission shall be empowered to adopt delegated acts in accordance with Article 38 concerning the further specification of the requirements laid in down in paragraph 1.

3. The Commission may, by means of implementing acts, establish reference numbers of standards for the validation of qualified electronic signatures. Compliance with the requirements laid down in paragraph 1 shall be presumed where the validation of qualified electronic signatures meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2). **~~The Commission shall publish those acts in the *Official Journal of the European Union*.~~**

3. The Commission may, by means of implementing acts, establish reference numbers of standards for the validation of qualified electronic signatures. ***The Commission shall ensure, that stakeholder input is duly considered, preferably in form of an impact assessment, when defining standards to be used for the purpose of this Regulation.*** Compliance with the requirements laid down in paragraph 1 shall be presumed where the validation of qualified electronic signatures meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2). The Commission shall publish those acts in the *Official Journal of the European Union*.

Article 26

Qualified validation service for qualified electronic signatures

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

(a) provides validation in compliance with Article 25(1), and

(b) allows relying parties to receive the result of the validation process in an automated manner which is reliable, efficient and bearing 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 ~~**point (b) of**~~ paragraph 1 shall be presumed where the validation service for qualified electronic signature meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2). ~~**The Commission shall publish those acts in the *Official Journal of the European Union*.**~~

2. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified validation service referred to in paragraph 1. ***The Commission shall ensure, that stakeholder input is duly considered, preferably in form of an impact assessment, when defining standards to be used for the purpose of this Regulation***. Compliance with the requirements laid down in point (b) of paragraph 1 shall be presumed where the validation service for qualified electronic signature meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2). The Commission shall publish those acts in the *Official Journal of the European Union*.

Article 27

Preservation of qualified electronic signatures

1. A qualified electronic signature preservation service ~~**shall**~~**may only** be provided by a qualified trust service provider who uses procedures and technologies capable of extending the trustworthiness of the qualified electronic signature ~~**validation data**~~ beyond the technological validity period.

2. The Commission shall be empowered to adopt delegated acts in accordance with Article 38 concerning the further specification of the requirements laid down in paragraph 1.

3. The Commission may, by means of implementing acts, establish reference numbers of standards for the preservation of qualified electronic signatures. Compliance with the requirements laid down in paragraph 1 shall be presumed where the arrangements for the preservation of qualified electronic signatures meet those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2). ~~**The Commission shall publish those acts in the *Official Journal of the European Union*.**~~

3. The Commission may, by means of implementing acts, establish reference numbers of standards for the preservation of qualified electronic signatures. ***The Commission shall ensure, that stakeholder input is duly considered, preferably in form of an impact assessment, when defining standards to be used for the purpose of this Regulation***. Compliance with the requirements laid down in paragraph 1 shall be presumed where the arrangements for the preservation of qualified electronic signatures meet those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2). The Commission shall publish those acts in the *Official Journal of the European Union*.

Section 4

Electronic seals

Article 28

Legal effects of electronic seal

1. An electronic seal shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is**:**

(a) in an electronic form**;**

(b) not an advanced electronic seal,

(c) not based upon a qualified certificate for electronic seal, or

(d) not created by a qualified electronic seal creation device.

2. A qualified electronic seal shall enjoy the legal presumption of ensuring the origin and integrity of the data to which it is linked.

2. A ***valid*** qualified electronic seal shall ***serve at least as prima facie evidence for the authenticity and integrity of the electronic document associated with it. This shall be without prejudice to national provisions on power of attorney and representation.***

3. A qualified electronic seal shall be recognised ~~**and accepted**~~ **as a qualified one** in all Member States.

3. A qualified electronic seal shall be recognised in all Member States.

4. If an electronic seal security assurance level below the qualified electronic seal is required, in particular by a Member State for accessing a service online offered by a public sector body on the basis of an appropriate assessment of the risks involved in such a service, all electronic seals matching at a minimum the same security assurance level shall be accepted.

4. If an electronic seal security level below the qualified electronic seal is required, in particular by a Member State for accessing a service online offered by a public sector body on the basis of an appropriate assessment of the risks involved in such a service, all electronic seals matching at a minimum the same security assurance level shall be accepted ***for access to that online service***.

5. Member States shall not request for accessing a **cross-border** service online offered by a public sector body an electronic seal with higher security assurance level than qualified electronic seals.

5. Member States shall not request for ***cross-border access to*** a service online offered by a public sector body an electronic seal with higher security level than qualified electronic seals.

6. The Commission shall be empowered to adopt delegated acts in accordance with Article 38 concerning the definition of different security assurance levels of electronic seals referred to in paragraph 4.

6. deleted

7. The Commission may, by means of implementing acts, establish reference numbers of standards for the security assurance levels of electronic seals. Compliance with the security assurance level defined in a delegated act adopted pursuant to paragraph 6 shall be presumed when an electronic seal meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2). ~~**The Commission shall publish those acts in the *Official Journal of the European Union*.**~~

7. The Commission may, by means of implementing acts, establish reference numbers of standards for the security assurance levels of electronic seals. ***The Commission shall ensure, that stakeholder input is duly considered, preferably in form of an impact assessment, when defining standards to be used for the purpose of this Regulation.*** Compliance with the security assurance level defined in a delegated act adopted pursuant to paragraph 6 shall be presumed when an electronic seal meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2). The Commission shall publish those acts in the Official Journal of the European Union.

Article 29

Requirements for qualified certificates for electronic seal

1. Qualified certificates for electronic seal shall meet the requirements laid down in Annex III.

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

2. Qualified certificates for electronic seal ***for cross-border use*** shall not be subject to any mandatory requirements exceeding the requirements laid down in Annex III.

3. 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 ~~**by renewing its validity**~~.

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 38 concerning the further specification of the requirements laid down in Annex III.

5. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified certificates for electronic seal. Compliance with the requirements laid down in Annex III shall be presumed where a qualified certificate for electronic seal meet those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2). ~~**The Commission shall publish those acts in the *Official Journal of the European Union*.**~~

5. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified certificates for electronic seal ***The Commission shall ensure, that stakeholder input is duly considered, preferably in form of an impact assessment, when defining standards to be used for the purpose of this Regulation.*** Compliance with the requirements laid down in Annex III shall be presumed where a qualified certificate for electronic seal meet those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2). The Commission shall publish those acts in the Official Journal of the European Union.

Article 30

Qualified electronic seal creation devices

1. Article 22 shall apply *mutatis mutandis* to requirements for qualified electronic seal creation devices.

1. Article 22 shall apply mutatis mutandis to requirements for qualified electronic seal ***and/or stamp*** creation devices.

2. Article 23 shall apply *mutatis mutandis* to the certification of qualified electronic seal creation devices.

2. Article 23 shall apply mutatis mutandis to the certification of qualified electronic seal ***and/or stamp*** creation devices.

3. Article 24 shall apply *mutatis mutandis* to the publication of a list of certified qualified electronic seal creation devices.

3. Article 24 shall apply mutatis mutandis to the publication of a list of certifiedqualified electronic seal ***and/or stamp*** creation devices.

Article 31

Validation and preservation of qualified electronic seals

Articles 25, 26 and 27 shall apply *mutatis mutandis* to the validation and preservation of qualified electronic seals.

Articles 25, 26 and 27 shall apply mutatis mutandis to the validation and preservation of qualified electronic seals ***and/or stamps***.

Section 5

Electronic time stamp

Article 32

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**:**

(a) in an electronic form**;**

(b) not signed using an advanced electronic signature or an advanced electronic seal, or

(c) not a qualified electronic time stamp.

2. Qualified electronic time stamp shall enjoy a legal presumption of ~~**ensuring**~~ **the accuracy of the date and** the time it indicates and the integrity of the data to which the time is bound.

2. ***A qualified*** electronic time stamp ***shall constitute at least prima facie evidence of the correctness of*** the time it indicates and the integrity of the ***document with which it is associated.***

3. A qualified electronic time stamp shall be recognised ~~**and accepted**~~ **as a qualified one** in all Member States.

Article 33

Requirements for qualified electronic time stamps

1. A qualified electronic time stamp shall meet the following requirements:

(a) it is accurately linked to Coordinated Universal Time (UTC) in such a manner as to preclude any possibility of the data being changed undetectably;

(b) it is based on an accurate time source;

(c) it is issued by a qualified trust service provider;

(d) 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.

(d) it is signed using an advanced electronic signature or an advanced electronic seal of the qualified trust service provider.

2. The Commission may, by means of implementing acts, establish reference numbers of standards for the accurate linkage of time to data and an accurate time source. Compliance with the requirements laid down in paragraph 1 shall be presumed where an accurate linkage of time to data and an accurate time source meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2). ~~**The Commission shall publish those acts in the *Official Journal of the European Union*.**~~

2. The Commission may, by means of implementing acts, establish reference numbers of standards for the accurate linkage of time to data and an accurate time source. ***The Commission shall ensure, that stakeholder input is duly considered, preferably in form of an impact assessment, when defining standards to be used for the purpose of this Regulation.*** Compliance with the requirements laid down in paragraph 1 shall be presumed where an accurate linkage of time to data and an accurate time source meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

The Commission shall publish those acts in the *Official Journal of the European Union*.

[Section 6

Electronic documents

Article 34

Legal effects and acceptance of the electronic documents

1. An electronic document shall be considered as equivalent to a paper document and admissible as evidence in legal proceedings, having regard to its assurance level of authenticity and integrity.

1. 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 format***.

2. A document bearing a qualified electronic signature or a qualified electronic seal of the person who is competent to issue the relevant document, shall enjoy legal presumption of its authenticity and integrity provided the document does not contain any dynamic features capable of automatically changing the document.

2. A document bearing a qualified electronic signature or a qualified electronic seal, ***shall have the equivalent legal effect of a paper document bearing a handwritten signature or a physical seal, where this exists under national law, provided the document does not contain*** any dynamic features capable of automatically changing the document.

3. When an original document or a certified copy is required for the provision of a service online offered by a public sector body, at least electronic documents issued by the persons who are competent to issue the relevant documents and that are considered to be originals or certified copies in accordance with national law of the Member State of origin, shall be accepted in other Member States without additional requirements.

3. deleted

4. The Commission may, by means of implementing acts, define formats of electronic signatures and seals that shall be accepted whenever a signed or sealed document is requested by a Member State for the provision of a service online offered by a public sector body referred to in paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

4. deleted

Section 7

Qualified electronic delivery service

Article 35

Legal effect of an electronic delivery service

1. Data sent or received using an electronic delivery service shall be admissible as evidence in legal proceedings with regard to the integrity of the data and the certainty of the date and time at which the data were sent to or received by a specified addressee.

1. Data sent or received using an electronicdelivery service shall be admissible as evidence in legal proceedings.

2. Data sent or received using a qualified electronic delivery service shall enjoy legal presumption of the integrity of the data and the accuracy of the date and time of sending or receiving the data indicated by the qualified electronic delivery system.

2. Data sent or received using a qualified electronic delivery service shall ***constitute at least prima facie evidence of the authenticity*** of the data and the ***correctness*** of the date and time of sending or receiving the data indicated by the qualified electronic delivery system.

2a. This Article shall be without prejudice to Regulation (EC) No 1348/2000.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 38 concerning the specification of mechanisms for sending or receiving data using electronic delivery services, which shall be used with a view to fostering interoperability between electronic delivery services.

3. deleted

Article 36

Requirements for qualified electronic delivery services

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

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

(b) they must allow the unambiguous identification of the sender and if appropriate, the addressee;

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

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

(e) the date of sending, receipt and any change of data must be indicated by a qualified electronic time stamp;

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

2. The Commission may, by means of implementing acts, establish reference numbers of standards for processes for sending and receiving data. Compliance with the requirements laid down in paragraph 1 shall be presumed where the process for sending and receiving data meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2). The Commission shall publish those acts in the Official Journal of the European Union.

2. The Commission may, by means of implementing acts, establish reference numbers of standards for processes for sending and receiving data. ***The Commission shall ensure, that stakeholder input is duly considered, preferably in form of an impact assessment, when defining standards to be used for the purpose of this Regulation.*** Compliance with the requirements laid down in paragraph 1 shall be presumed where the process for sending and receiving data meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2). The Commission shall publish those acts in the *Official Journal of the European Union*.

Section 8

Website authentication

Article 37

Requirements for qualified certificates for website authentication

1. Qualified certificates for website authentication shall meet the requirements laid down in Annex IV.

2. Qualified certificates for website authentication shall be recognised and accepted in all Member States.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 38 concerning the further specification of the requirements laid down in Annex IV.

4. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified certificates for website authentication. Compliance with the requirements laid down in Annex IV shall be presumed where a qualified certificate for website authentication meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2). The Commission shall publish those acts in the Official Journal of the European Union.

4. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified certificates for website authentication. ***The Commission shall ensure, that stakeholder input is duly considered,preferably in form of an impact assessment, when defining standards to be used for the purpose of this Regulation.*** Compliance with the requirements laid down in Annex IV shall be presumed where a qualified certificate for website authentication meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2). The Commission shall publish those acts in the Official Journal of the European Union. *]*

CHAPTER IV

DELEGATED ACTS

Article 38

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 Articles 8(3), 13(5), 15(5), 16(5), 18(5), 20(6), 21(4), 23(3), 25(2), 27(2), 28(6), 29(4), 30(2), 31, 35(3) and 37(3) shall be conferred on the Commission for an indeterminate period of time from the entry into force of this Regulation.

2. The power to adopt delegated acts referred to in Articles 8(3), 20(6), 21(4), 23(3), 25(2), 27(2), 28(6), 29(4), 30(2), 31, 35(3) and 37(3) shall be conferred on the Commission for ***a*** period of ***five years beginning on date*** of the entry into force of this Regulation. ***The Commission shall draw up a report in respect of the delegation of power not later than six months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.***

3. The delegation of power referred to in Articles 8(3), 13(5), 15(5), 16(5), 18(5), 20(6), 21(4), 23(3), 25(2), 27(2), 28(6), 29(4), 30(2), 31, 35(3) and 37(3) 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.

3. The delegation of power referred to in Articles 8(3), 20(6), 21(4), 23(3), 25(2), 27(2), 28(6), 29(4), 30(2), 31, 35(3) and 37(3) 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.

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council. ***The Commission may not adopt a delegated act subject to this Regulation without prior consultation with relevant stakeholders.***

5. A delegated act adopted pursuant to Articles 8(3), 13(5), 15(5), 16(5), 18(5), 20(6), 21(4), 23(3), 25(2), 27(2), 28(6), 29(4), 30(2), 31, 35(3) and 37(3) 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.

5. A delegated act adopted pursuant to Articles 8(3), 20(6), 21(4), 23(3), 25(2), 27(2), 28(6), 29(4), 30(2), 31, 35(3) and 37(3) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of ***three*** 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.

CHAPTER V

IMPLEMENTING ACTS

Article 39

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.

(1a) Implementing acts subject to this Regulation may not be adopted without prior consultation of industry and relevant stakeholders.

2. Where reference is made to this paragraph, Article 5 of Regulation 182/2011 shall apply.

2. Where reference is made to this paragraph, Article ***4*** of Regulation 182/2011 shall apply.

CHAPTER VI

FINAL PROVISIONS

Article 40

Report

The Commission shall report to the European Parliament and to the Council on the application of this Regulation. The first report shall be submitted no later than four years after the entry into force of this Regulation. Subsequent reports shall be submitted every four years thereafter.

The Commission shall report to the European Parliament and to the Council on the application of this Regulation. The first report shall be submitted no later than ***two*** years after the entry into force of this Regulation. Subsequent reports shall be submitted every four ***y***ears thereafter ***accompanied, if necessary by appropriate legislative proposals***.

1a. The report should evaluate whether the scope of this Regulation needs to be changed for the purposes of adaptation to developments in technology, in the market and in the legal context in the Member States and internationally; generally, the report must indicate whether the Regulation has made it possible to attain its stated objectives with regard to building trust in the online environment.

Article 41

Repeal

1. Directive 1999/93/EC is repealed.

2. References to the repealed Directive shall be construed as references to this Regulation.

3. Secure signature creation devices of which the conformity has been determined in accordance with Article 3(4) of Directive 1999/93/EC shall be considered as qualified signature creation devices under this Regulation.

4. Qualified certificates issued under Directive 1999/93/EC shall be considered as qualified certificates for electronic signatures under this Regulation until they expire, but for no more than five years from the entry into force of this Regulation.

Article 42

Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall apply from (.....).

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

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*

Annex 0.

Identity aAssurance levels of electronic identification schemes and of electronic identification means issued thereunder

1. The criteria to establish a identity assurance level of an electronic identification scheme and of the electronic identification means issued under that scheme shall be established by assesing the reliability of the following phases:

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

(b) reliability of the process to the issueance of the requested electronic identification means;

(c) the authentication mechanism, in which the natural or legal person uses the electronic identification means to attest its identity to a relying party.

In addition, the reliability of the following aspects of an electronic identification scheme shall be assessed:

(cd) the quality of the entity issuing electronic identification means;

(de) types and robustness the technical quality of the issued electronic identification means.

(e) security of the authentication mechanism.

2. An electronic identification scheme and the electronic identification means issued under that scheme with 'high'[31] identity assurance level shall fulfill all the following requirements:

(a) The identity of the natural or legal persons applying for the issuance of electronic identification means is must be verified, in accordance with national law, by appropriate means similar to the verification performed for the issuance of official documents such as passports or identity cards, by the issuer of the electronic identification means or by an authorised third party based on a government identity document which must be checked against the official registers.

[31] This level corresponds to level 4 of STORK.

~~The verification of the identity referred to in the previous subparagraph requires the physical appearancepresence of the natural person or of an authorised representative of the legal person is required during the process of issuing the electronic identification means the application or the issuance phase or on a prior occasion, if this prior verification is trusted by the issuer under national law.~~

~~(b) the electronic identification means is delivered after the identity of the natural or legal person has been verified with very high level of confidence, for example in the following manner:~~

~~– it is directly given to the person after validation of his/her identity, or~~

~~– it is sent to the person and then activated after validation of his/her identity.~~

~~(cc) the authentication process offers state of art protection against attacks threats to the use of the electronic identification means~~

~~(cd) the issuer of the electronic identification means~~

~~– is a public sector body or~~

~~– meets the requirements in Article 19 (2) applied *mutatis mutandis*;~~

~~(d) the electronic identification means is based on or logically linked to a qualified certificate or a qualified signature creation device;~~

~~(e) the electronic identification means *mutatis mutandis* complies with Annex II and contains data compliant with Annex I.~~

3. An electronic identification scheme and the electronic identification means issued under that scheme with 'substantial'[32] identity assurance level shall fulfill all the following requirements or the corresponding requirements laid down in paragraph 2:

(a) the identification of the natural or legal persons applying for the issuance of electronic identification means meets one of the following conditions:

- **it requires a physical presence, and the person identification data are validated against a public register, or**

- **it is remote, and the person identification data are validated by using trusted means under national law.**

(b) the electronic identification means is issued as followsdelivered after the identity of the natural or legal person has been verified with high level of confidence, for example in the following manner:

- **it is directly given to the person after validation of his/her identity, or**

- **it is sent by registered mail after prior validation of the address against an official identity database, or**

- **it is downloaded on the Internet after the request is signed by the person with a qualified electronic signature, or**

- **it is downloaded directly by the person applying for the issuance of electronic identification means after entering a private password which was given physically to that person during the course of a registration fulfilling the requirements of point (a) of this paragraph.**

(cc) the authentication process offers protection against most type of attacks threats to the use of the electronic identification means.

(cd) the issuer of the electronic identification means meets the requirements in Article 19 (2) applied *mutatis mutandis* is supervised or accredited by the notifying Member State according to national law;

(e) the electronic identification means is based on a hard certificate or a soft at least contains a certificate or is a one-time password device token or a qualified soft certificate;

---

[32] This level corresponds to level 3 of STORK.

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) ~~**a set of data unambiguously representing the signatory to whom the certificate is issued including at least**~~ the name of the signatory**,** or a pseudonym**.,** ~~**which shall be identified as such**~~ **If a pseudonym is used, it shall be clearly indicated**;

(d) electronic signature validation data which correspond 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 location of the ~~**certificate validity status**~~ services that can be used to enquire about the validity status of the qualified certificate;

(j) where the electronic signature creation data related to the electronic signature validation data are 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 signature creation devices

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

(a) the secrecy of the electronic signature creation data used for electronic signature **~~generation~~creation** is assured;

(b) the electronic signature creation data used for electronic signature **~~generation~~creation** can occur only once;

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

(c) the electronic signature creation data used for electronic signature generation cannot be derived and the electronic signature is protected against forgery using currently available technology;

(d) the electronic signature creation data used for electronic signature **~~generation~~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.

3. Generating or managing electronic signature creation data on behalf of the signatory shall be done by a qualified trust service provider.

4. Qualified trust service providers managing electronic signature creation data on behalf of the signatory may duplicate the electronic signature creation data **only** for back-up purposes provided the following requirements are met:

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

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

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: person's name;

(new) Sensitive data within the meaning of Article 8 of Directive 95/46/CE shall notbe processed.

(c) ~~**a set of data unambiguously representing the legal person to whom the certificate is issued, including at least name**~~ **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 correspond 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 location of the certificate validity status services that can be used to enquire the validity status of the qualified certificate;

(j) where the electronic seal creation data related to the electronic seal validation data are 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 registration number as stated in the official records,*
- *for a natural person: person's name;*

(new) Sensitive data within the meaning of Article 8 of Directive 95/46/CE shall notbe processed.

(c) a set of data unambiguously representing the legal person to whom the certificate is issued, including at least name and registration number as stated in the official records;

*(c) a set of data unambiguously representing the **natural or** legal person to whom the certificate is issued, including at least name and registration number **as the case may be**, as stated in the official records;*

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

*(d) elements of the address, including at least city and Member State, of the **natural or** legal person to whom the certificate isissued as stated in the official records;*

(e) the domain name(s) operated by the 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 location of the certificate validity status services that can be used to enquire the validity status of the qualified certificate.]