COUNCIL OF THE EUROPEAN UNION

Brussels, 23 September 2013

13890/13

Interinstitutional File: 2012/0146 (COD)

TELECOM 239
MI 783
DATAPROTECT 130
EJUSTICE 66
CODEC 2076

NOTE

from:	Presidency
to:	Delegations
No. Cion prop.:	10977/12 TELECOM 122 MI 411 DATAPROTECT 73 CODEC 1576
No prev. doc. :	11741/13 TELECOM 186 MI 593 DATAPROTECT 85 EJUSTICE 56 CODEC 1638
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 order to provide a better overview of the work done so far on the above mentioned proposal and to facilitate its further examination, the Presidency has put together a consolidated version of the text, containing all six clusters. On the basis of the latest discussions on clusters 1 and 2 and on the written contributions received in early 2013 on clusters 3, 4 and 5, the Presidency introduced further changes in the text[1] and also identified a number of concerns that the Presidency intends to address at the WP TELE meeting of 26 September. The changes/issues to be discussed are outlined below.

[1] 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 **<u>underlined</u>**.

Cluster 1: Electronic identification

2. Based on the discussion held at the informal attaches meeting of 9 September, it is clear that that the scope of cluster 1 has to be limited to services provided by public sector bodies[2]. However, the Presidency believes that the extent of this limitation still needs to be clarified since two options are available:

   - to limit the scope of the whole Chapter II: This would in particular mean that eID schemes of private providers could not be notified (Art. 6(1)(iii) would have to go out) and that they could not benefit from the interoperability framework.

   - to limit the obligation to recognise foreign eID means in Article 5: This would mean that only public sector bodies would have an obligation to recognise foreign eID means, while private schemes fulfilling the conditions could still be notified (if a Member States so decides) and could participate in the interoperability framework.

   The Presidency would therefore like to know which of the options above delegations could support.

   Since some delegations would like to exclude private services completely from the scope and others could not support an automatic extension to private services, the Presidency would suggest to accompany the provision limiting the scope by a review clause calling on the Commission, while carrying out the review, to assess in particular the possibility of extension of the scope to private services.

3. At the request of several delegations, the word 'access' has been replaced by 'authentication' in Article 5 in order to clarify that the obligation to recognise notified eID means does not imply an obligation to give full access to the service concerned. This principle is also expressed in the last sentence of recital 13.

[2] In order to address concerns of some delegations that this would exclude private entities mandated to provide public services by a Member State, the definition of public sector body in Art. 3(4a) could be extended to cover such cases.

4. The deadline for recognition in Article 5(1) second subparagraph has been extended, at a request of many delegations, from 6 to 12 months. Some of these also asked to delete Article 6(1)(da) concerning the information obligation prior to the notification. The Presidency believes, however, that this point represents an important part of the cooperation mechanism and would allow Member States to engage early in this process and save time later on.

   The Presidency would therefore like to outline the steps necessary for the recognition obligation to set in:

   - A Member State intending to notify informs other Member States at least **6 months** prior to notification (Art. 6(1)(da)).
   - Member States cooperate (Art. 8(1c) first indent).
   - The scheme to be notified must become interoperable (obligation of Art. 6(1)(db)).
   - The notification takes place.
   - The Commission publishes **2 months** after the notification (Art. 7(3)). Please note that, according to the current text, the first publication will occur **6 months** after the date of application of the Regulation.
   - The notified scheme must be recognised in other Member States **12 months** following the publication (Art. 5(1) second subparagraph).

   Delegations are certainly aware that before the whole process outlined above can start, the Regulation must enter into force and into application and all the necessary implementing acts (in particular those on cooperation - Art. 8(2) and on interoperability - Art. 8(2a)) must be in place. For further considerations on the overall time-line for the Regulation please refer to paragraph 18 of this note.

5. Some delegations did not agree with the introduction of Article 5(2) and 8(2b) on the list of categories of services where a specific assurance level may be required. The Presidency would like to stress that this represents an additional option and not an obligation. Member States, as well as providers would remain free not to require that specific level. Moreover, the implementing act listing the categories would be based on the cooperation between Member States.

6. The provisions of Annex 0 on assurance levels has been amended to align them as much as possible with STORK. The term 'assurance level' is now used throughout the text of cluster 1 instead of 'identity assurance level'.

Cluster 2: Trust service general provisions and supervision

7. At the meeting of the WP TELE of 18 July, many delegations expressed support for the Commission suggestion to provide for a 'light touch' approach to non-qualified trust service providers (TSPs). To address this issue, the Presidency has introduced the following modifications:

    - Article 9 on liability now provides for liability for all TSPs but the reversed burden of proof only applies to QTSPs.

    - Article 13(2) sets a framework for the supervision of QTSPs (ex ante and ex post) and for the monitoring of TSPs (ex post only).

    - The tasks of the supervisory body listed (in a non-exhaustive list) in Art. 13(2a) have therefore to be interpreted in the light of Article 13(2).

    - Article 15(1) on appropriate technical and organisational measures and Art. 15(2) on notification of security breaches applies to all TSPs.

    - In addition, recitals 28a and 28b explain the different approach to QTSPs and non-QTSPs.

8. With regard to Article 10 on international aspects, the Presidency noted that most delegations were not in favour of including additional options from Article 7 of the eSignature Directive and thus no further substantial changes have been made in this respect.

Cluster 3: Electronic signatures and Cluster 4: Other trust services

9. Since the latest discussions on Clusters 3 and 4 were held in early 2013, the Presidency has not introduced many changes at this stage. The main changes include the following:

    - Articles 20(1), 28(1) and 32(1) have been amended to correspond to Article 5(2) of the current eSignatures Directive.

    - The certification of qualified electronic signature creation devices in Article 23 has been made mandatory. This is an important issue that should be discussed further.

    - Article 25(1) on the requirements for the validation of qualified electronic signatures has been clarified with regard to 'the time of signing'.

10. Among others, the Presidency noted the following concerns of delegations with regard to the legal effects of electronic signatures (Article 20):

    - usage of security levels below 'qualified'

    - uncertainty whether the provisions would apply to private providers

    - the reference to 'access to a service online' which causes confusion with electronic identification (Art. 20(4))

    - delegated acts on different security levels (Art. 20(6)).

The Presidency is considering to replace paragraphs 4 to 7 of Article 20 by a new text that would aim to address those issues (please see footnote[3]). Delegations are invited to indicate if this proposal seems to be in the right direction and/or provide further drafting suggestions. Since very similar comments were raised for the corresponding provisions concerning the other trust services, once the text of Article 20 is more or less stable, a similar approach could be applied to those sections as well.

11. Many delegations raised the issue of suspension of qualified certificates (Art. 21 and 29) which is not addressed in the text while some of them argued that the possibility of suspension of certificates could lead to uncertainties when validating electronic signatures or seals. Delegations are therefore invited to indicate whether they would wish to provide for the suspension in the text.

12. Articles 30 and 31 on electronic seals stipulate that Articles 22 to 27 on electronic signatures shall apply *mutatis mutandis*. Can delegations agree to this or would they prefer to include the full text of the respective provisions in the section on electronic seals?

3

Article 20a

Electronic signatures in public services

1. If an advanced electronic signature is required by a Member State , or a Union legal act, for the usage in a publicly available service online offered by or on behalf of a public sector body on the basis of an appropriate assessment of the risks involved in such a service, advanced electronic signatures based on a qualified certificate for electronic signatures and qualified electronic signatures shall also be accepted

2. If an advanced electronic signature based on a qualified certificate for electronic signatures is required by a Member State, or a Union legal act, for the usage in a publicly available service online offered by or on behalf of a public sector body on the basis of an appropriate assessment of the risks involved in such a service, qualified electronic signatures shall also be accepted

3. Member States shall not request for the cross-border usage in a publicly available service online offered by a public sector body an electronic signature at a higher security level than qualified electronic signature

4. The Commission may, by means of implementing acts, establish reference numbers of standards for advanced electronic signatures. Compliance with the requirements for advanced electronic signatures referred to in paragraphs 1 and 2 shall be presumed when an advanced electronic signature meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

13. Moreover, delegations expressed doubts with regard to the added value of provisions on electronic documents, electronic delivery service and website authentication. The Presidency would therefore like to know whether delegations can support the deletion of these three sections, which would facilitate an earlier conclusion of the examination of the proposal.

Cluster 5: General provisions; Final provisions, including delegated and implementing acts

14. Articles 1 and 2 on the subject matter and scope have been slightly amended with the aim to simplify those provisions and/or to avoid unnecessary duplications.

15. Modifications have been suggested also in Article 3 on definitions and some new definitions have been added (Article 3(4a), (4b),(13a), (23a) and (31a). Further work will however be needed as the discussions on various parts of the proposal will progress. The Presidency invites delegations to provide drafting suggestions and to indicate what new definitions they wish to include.

16. The Presidency continues working on the data protection issue. New Article 4a has been provisionally included. The Presidency however wishes to recall that, as noted already in paragraph 5 of doc.11741/13, this matter needs to be carefully considered in order to avoid possible contradictions, overlaps or duplications with the existing data protection legislation. Delegations' views and drafting suggestions would be welcome on this issue.

17. The Presidency believes that the issue of delegated acts should be discussed once the text of the relevant provisions is more advanced. In many places, delegations indicated that an implementing act should be used instead or that the relevant details should be specified in the Regulation. Drafting suggestions in this respect would be welcome. At the same time, the Presidency noticed that many provisions on delegated acts (such as Art. 21(4), 25(3), 27(3) and others) refer to 'further specifications of the requirements'. The Presidency would like to invite the Commission to provide more information on what is to be addressed by those delegated acts.

18. The time-line for the Regulation should be subject to a specific consideration. Until now delegations raised a number of concerns in relation to the date of entry into force of this Regulation, underlining the necessity to provide for an appropriate period for the Member States and the operators to prepare for the application of this Regulation.

    Based on those discussions, the Presidency considers that the distinction should be made between the entry into force of this Regulation and its date of application. In order to define the date of application, the following aspects should be taken into account :

    - adoption of the implementing and the delegated acts without which the Regulation could not be effectively applicable. It is the understanding of the Presidency, those are implementing and delegated acts which the Commission is required to adopt ("The Commission shall adopt …"). A specific deadline for the adoption of each of those acts should be provided for in the Regulation.

    - a lapse of time is necessary between the adoption of all the acts referred to in the previous indent and the actual date of application of the Regulation in order to allow the Member States to prepare for the application of this act.

    - the number of and importance of (new) obligations foreseen for the Member States and for the operators.

Cluster 6: Preamble

19. The Preamble will be aligned with the operative part of the proposal once the latter one is more or less stable. However, the Presidency has introduced several new recitals (13a, 28a to 28c and 48a) that were already suggested during previous discussions.

20. At the WP TELE on 26 September, delegations will be invited to take position on the changes and/or issues listed above. Delegations are kindly requested to submit their written contributions including concrete drafting suggestions to the chair of the WP TELE (and to teleinfso@consilium.europa.eu) prior to the meeting if possible.

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 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 levels 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.

(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.

(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.

(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.

(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.

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

(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, 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.

(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.

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

(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.

(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:

---

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

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter

1. This Regulation 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.

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.**~~

Article 2

Scope

1. This Regulation applies to electronic identification 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.

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

3. This Regulation does not apply to 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.

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**;

(2) 'electronic identification means' means a material 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~~**;

(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 of the electronic identification of a natural or legal person; or of the origin and integrity of an electronic data;

(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;

(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;

(c) it is created using electronic signature creation data that the signatory can, with high level of confidence, 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;

(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;

(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 **~~ofto~~** a natural **~~or a legal~~** person **~~respectively to the certificate~~** and confirms **~~those data~~ the name or the pseudonym** of that person;

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

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

- the creation, verification**~~, and~~** validation**~~, handling and preservation~~** of electronic signatures, electronic seals, 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~~**;

(13) ‘qualified trust service’ means a trust service that meets the **~~applicable~~** requirements provided for in this Regulation;

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

[(14) 'trust service provider' means **qualified and non-qualified trust service providers**;

(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 meets the requirements laid down in this Regulation; *]*[18]

(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;

(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;

(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

(d) it is linked to the data to which it relates 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;

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

---

18 Delegations are invited to provide suggestions for definitions of TSP', 'non-qualified TSP' and 'qualified TSP'.

(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;

(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;

(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**;**

(31a) 'validation' means the process of checking the validation data to confirm that the electronic signature or seal is valid.

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.

2. Products **and trust services** which comply with this Regulation shall be permitted to circulate freely 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[19].

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.]

[19] This provision should 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~~

1. When an electronic identification using an electronic identification means and authentication is required under national legislation or administrative practice to access a service 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 ~~th~~ean electronic identification scheme included in the list published by the Commission pursuant to Article 7;

b. the ~~identity~~ assurance level of that electronic identification means corresponds to one of the ~~identity~~ assurance levels set out in Annex 0.

Such recognition shall take place no later than ~~6~~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 access~~for authentication for online services defined in accordance with Article 8(2b).

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;

(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;

(ba) that scheme and the electronic identification means issued thereunder meet the requirements of one of the ~~identity~~ assurance levels set out in Annex 0;

(c) the notifying Member State ensures that the 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 ~~identity~~ assurance level set out in Annex 0;

(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.** 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~~;

(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).~~

~~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 ~~technological progress~~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 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 ~~identity~~ assurance level and the issuer(s) of electronic identification means under that scheme**;

(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~~**;

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

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

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

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**.

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).

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 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 7b

Liability

1. The notifying Member State shall be liable ~~under national law~~ for ~~any~~ 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 ~~under national law~~ for ~~any~~ 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 ~~under national law~~ for ~~any~~ 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 8

~~Coordination~~ Cooperation 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 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:

(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;

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

(c) 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 ~~identity~~ assurance levels defined in Annex 0;

(b) a mapping of national ~~identity~~ assurance levels of notified electronic identification schemes into the ~~identity~~ assurance levels defined in Annex 0;

(c) reference to minimum technical requirements for interoperability;

(d) rules of procedure[20];

(e) arrangements for dispute resolution.

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 ~~identity~~ assurance levels;

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

(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.~~**

[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

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 ~~identity~~ 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 ~~identity~~ assurance level has shown the appropriatness of such a requirement;

(b) the requirement for a specific ~~identity~~ assurance level shall be proportionate to the objective of public policy, public security or protection of ~~sensitive~~ 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 ~~identity~~ assurance level would expose a fundamental interest of society to threats.

3. ~~Those i~~Implementing acts **referred to in paragraphs 2, 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.~~

CHAPTER III

TRUST SERVICES

Section 1

General provisions

Article 9

Liability[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~~, 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.**

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

~~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. ~~Subject to the following conditions, trust service providers may limit the liability set out in paragraph 1:~~

~~(a) they duly inform their customers in advance about the limitations on the use of the services they provide, and~~

~~(b) those limitations are recognisable to third parties.~~

Where ~~conditions set out in the previous subparagraph are met~~, 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.

Article 10

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

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**.

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

~~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 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**~~.

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.

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:**~~

(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;**~~

22 Explanatory recital could clarify that the feasibility assessment should also include economic considerations made by the TSP.

23 Explanatory recital could clarify that there could be several supervisory bodies in one Member State. Similar approach was taken in recital 11 of the Framework Directive.

(b) ~~**undertaking supervision of qualified**~~ **to monitor non-qualified trust service providers established in the territory of the designating Member State to verify, whenever needed and through ex post supervisory activities, that they and the trust services they provide meet the requirements** ~~**and of the qualified trust services they provide in order to ensure that they and the qualified trust services provided by them qualified trust service providers meet the applicable requirements**~~ **laid down in this Regulation**~~**;**~~

~~**(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.**~~

2a. ~~**In order to ensure that qualified trust service providers established in the territory of the designating Member State and the qualified trust services they provide fulfil the requirements of this Regulation,**~~ **For the purposes of paragraph 2 and subject to the limitations provided therein, the tasks of the supervisory body**~~**ies subject to the conditions laid down in this Regulation**~~**, shall** ~~**perform the following tasks**~~ **include in particular:**

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

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

(c) to ~~**ensure that**~~ **inform other supervisory bodies**~~**,**~~ **and the public** ~~**and the Commissionare informed**~~ **about** ~~**any**~~ **breaches of security or loss of integrity in accordance with Article 15(2);**

(d) to report to the Commission about its 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); ~~**and**~~

(ea) to inform the data protection authorities about the results ~~**thereof**~~ **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 witdraw the qualified status, unless this body is the supervisory body itself;

(h) to adopt provisions on termination plans in cases where the qualified trust service providers cease their activities;

(i) to require that ~~appropriate action be taken by qualified~~ trust service providers remedy any ~~in case of their~~ failure to fulfil the requirements of this Regulation.

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**~~ activities ~~**to the Commission and Member States by the end of the first quarter of the following year. It shall include at least:**~~

~~**(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)~~**;**~~**. The Commission may communicate that summary to the European Network and Information Security Agency (ENISA).**

~~**(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.**~~

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.**~~

~~**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.**~~

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).

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.

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**:

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

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.**

~~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).~~

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.

~~**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]

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, 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.

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)**~~.

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 is in the public interest.

---

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

[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.~~

~~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]

~~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.~~

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).

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**.

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~~**.

~~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]

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

[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** 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]

~~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.~~

~~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).~~

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.~~

~~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.~~

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

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.

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.

~~**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. 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).

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.

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.**~~

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).

Article 19

Requirements for qualified trust service providers

1. When issuing a qualified certificate, a qualified trust service provider shall verify, by appropriate means [and in accordance with national law][29], 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** 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 **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.

[29] Possibly to be deleted as apparently in contradiction with subparagraph 2.

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

(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 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**;

(d) use trustworthy systems and products which are protected against 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:

- they are publicly available for retrieval only where the consent of the person to whom the data ~~**has been issued**~~ **relates** 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[30]**, 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;

[30] 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.

(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~~**;.**~~

(k) 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**[31] ~~**after**~~ **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**.

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.

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*.**~~

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

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.

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

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

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.

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.

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.

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*.~~**

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.

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*.**~~ 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*.**~~ 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*.**~~

~~**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.

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).

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**~~**T**he 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*.**~~

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*.~~**

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*.~~**

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.

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

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.

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.

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*.**~~

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.

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*.**~~

Article 30

Qualified electronic seal creation devices

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

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

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

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.

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.

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*.**

[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.

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.

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.

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).

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.

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.

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.

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.

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.]

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.

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.

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

5. A delegated act adopted pursuant to 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.

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.

2. Where reference is made to this paragraph, Article 5 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.

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 a~~Assurance 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:

(~~c~~d) the quality of the entity issuing electronic identification means;

(~~d~~e) ~~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'[32] ~~identity~~ assurance level shall fulfill all the following requirements:

(a) The identity of the natural or legal person~~s~~ 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.

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

The ~~verification of the identity referred to in the previous subparagraph requires the~~ physical ~~appearance~~presence 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.**

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

(~~e~~d) 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'[33] ~~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 person~~s~~ 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 follows~~delivered 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.**

(~~e~~c) the authentication process offer~~s~~ protection against most ~~type of attacks~~ threats to the use of the electronic identification means.

(~~e~~d) 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~~;

---

[33] 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;

(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;

(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;*

(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;

(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;

(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.]

_____