EUROPEAN UNION

THE EUROPEAN PARLIAMENT **THE COUNCIL**

Brussels, 16 July 2014
(OR. en)

2012/0146 (COD) **PE-CONS 60/14**

TELECOM 68
MI 235
DATAPROTECT 38
EJUSTICE 26
CODEC 652

LEGISLATIVE ACTS AND OTHER INSTRUMENTS

Subject:	REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

REGULATION (EU) No …/2014
OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of …

on electronic identification and trust services
for electronic transactions in the internal market
and repealing Directive 1999/93/EC

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[1],

Acting in accordance with the ordinary legislative procedure[2],

[1] OJ C 351, 15.11.2012, p. 73.
[2] Position of the European Parliament of 3 April 2014 (not yet published in the Official Journal) and decision of the Council of …

Whereas:

(1) Building trust in the online environment is key to economic and social development. Lack of trust, in particular because of a perceived lack of legal certainty, makes consumers, businesses and public authorities 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 providing a common foundation for secure electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union.

(3) Directive 1999/93/EC of the European Parliament and of the Council[1], dealt with 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 that Directive.

(4) The Commission communication of 26 August 2010 entitled "A Digital Agenda for Europe " 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 EU Citizenship Report 2010, entitled "Dismantling the obstacles to EU citizens' rights", the Commission further highlighted the need to solve the main problems that prevent Union citizens from enjoying the benefits of a digital single market and cross-border digital services.

[1] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ L 13, 19.1.2000, p. 12).

(5) In its conclusions of 4 February 2011 and of 23 October 2011, the European Council invited the Commission to create a digital single market by 2015, to make rapid progress in key areas of the digital economy and to promote a fully integrated digital single market by facilitating the cross-border use of online services, with particular attention to facilitating secure electronic identification and authentication.

(6) In its conclusions of 27 May 2011, 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.

(7) The European Parliament, in its resolution of 21 September 2010 on completing the internal market for e-commerce[1], 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.

(8) Directive 2006/123/EC of the European Parliament and of the Council[2] requires Member States to establish 'points of single contact' (PSCs) 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 PSC with the appropriate authorities. Many online services accessible through PSCs require electronic identification, authentication and signature.

---

[1] OJ C 50 E, 21.2.2012, p. 1.

[2] Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market (OJ L 376, 27.12.2006, p. 36).

(9) In most cases, citizens cannot use their electronic identification to authenticate themselves in another Member State because the national electronic identification schemes in their country are not recognised in other Member States. That electronic barrier excludes service providers from enjoying the full benefits of the internal market. Mutually recognised electronic identification means will facilitate cross-border provision of numerous services in the internal market and enable businesses to operate on a cross-border basis without facing many obstacles in interactions with public authorities.

(10) Directive 2011/24/EU of the European Parliament and of the Council[1] set up a network of national authorities responsible for eHealth. To enhance the 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 of electronic identification and authentication is key to making 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. That requires a solid, safe and trusted electronic identification framework.

[1] 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 (OJ L 88, 4.4.2011, p. 45).

(11) This Regulation should be applied in full compliance with the principles relating to the protection of personal data provided for in Directive 95/46/EC of the European Parliament and of the Council[1]. In this respect, having regard to the principle of mutual recognition established by this Regulation, authentication for an online service should concern processing of only those identification data that are adequate, relevant and not excessive to grant access to that service online. Furthermore, requirements under Directive 95/46/EC concerning confidentiality and security of processing should be respected by trust service providers and supervisory bodies.

(12) 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 authenticate, for at least public services. This Regulation does not aim to intervene with regard to electronic identity management systems and related infrastructures established in Member States. The aim of this Regulation is to ensure that for access to cross-border online services offered by Member States, secure electronic identification and authentication is possible.

(13) Member States should remain free to use or to introduce means for the purposes of electronic identification for accessing online services. They should also be able to decide whether to involve the private sector in the provision of those means. Member States should not be obliged to notify their electronic identification schemes to the Commission. The choice to notify the Commission of 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 Member States.

[1] 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 (OJ L 281, 23.11.1995, p. 31).

(14) Some conditions need to be set out in this Regulation with regard to which electronic identification means have to be recognised and how the electronic identification schemes should be notified. Those conditions should help Member States to build the necessary trust in each other's electronic identification schemes and to mutually recognise electronic identification means falling under their notified schemes. The principle of mutual recognition should apply if the notifying Member State's electronic identification scheme meets the conditions of notification and the notification was published in the *Official Journal of the European Union*. However, the principle of mutual recognition should only relate to authentication for an online service. The access to those online services and their final delivery to the applicant should be closely linked to the right to receive such services under the conditions set out in national legislation.

(15) The obligation to recognise electronic identification means should relate only to those means the identity assurance level of which corresponds to the level equal to or higher than the level required for the online service in question. In addition, that obligation should only apply when the public sector body in question uses the assurance level "substantial" or "high" in relation to accessing that service online. Member States should remain free, in accordance with Union law, to recognise electronic identification means having lower identity assurance levels.

(16) Assurance levels should characterise the degree of confidence in electronic identification means in establishing the identity of a person, thus providing assurance that the person claiming a particular identity is in fact the person to which that identity was assigned. The assurance level depends on the degree of confidence that electronic identification means provides in claimed or asserted identity of a person taking into account processes (for example, identity proofing and verification, and authentication), management activities (for example, the entity issuing electronic identification means and the procedure to issue such means) and technical controls implemented. Various technical definitions and descriptions of assurance levels exist as the result of Union funded Large Scale Pilots, standardisation and international activities. In particular, the Large Scale Pilot STORK and ISO 29115 refer, inter alia, to levels 2, 3 and 4, which should be taken into utmost account in establishing minimum technical requirements, standards and procedures for the assurances levels low, substantial and high within the meaning of this Regulation, while ensuring consistent application of this Regulation in particular with regard to assurance level high related to identity proofing for issuing qualified certificates. The requirements established should be technology-neutral. It should be possible to achieve the necessary security requirements through different technologies.

(17) Member States should encourage the private sector to voluntarily use 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 any Member State should be available to private sector relying parties established outside of the territory of that Member State under the same conditions as applied to private sector relying parties established within that Member State. Consequently, with regard to private sector relying parties, the notifying Member State may define terms of access to the authentication means. Such terms of access may inform whether the authentication means related to the notified scheme is presently available to private sector relying parties.

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

(19) The security of electronic identification schemes is key to trustworthy cross-border mutual recognition of electronic identification means. In this context, Member States should cooperate with regard to the security and interoperability of the electronic identification schemes at Union level. Whenever electronic identification schemes require specific hardware or software to be used by relying parties at the national level, cross-border interoperability calls for those Member States not to impose such requirements and related costs on relying parties established outside of their territory. In that case appropriate solutions should be discussed and developed within the scope of the interoperability framework. Nevertheless technical requirements stemming from the inherent specifications of national electronic identification means and likely to affect the holders of such electronic means (e.g. smartcards), are unavoidable.

(20) Cooperation by Member States should facilitate the technical interoperability of the notified electronic identification schemes with a view to fostering 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.

(21) This Regulation should also establish a general legal framework for the use of trust services. However, it should not create a general obligation to use them or to install an access point for all existing trust services. In particular, it should not cover the provision of services used exclusively within closed systems between a defined set of participants, which have no effect on third parties. For example, systems set up in businesses or public administrations to manage internal procedures making use of trust services should not be subject to the requirements of this Regulation. Only trust services provided to the public having effects on third parties should meet the requirements laid down in the Regulation. Neither should this Regulation cover aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form laid down by national or Union law. In addition, it should not affect national form requirements pertaining to public registers, in particular commercial and land registers.

(22) In order to contribute to their general cross-border use, it should be possible to use trust services as evidence in legal proceedings in all Member States. It is for the national law to define the legal effect of trust services, except if otherwise provided in this Regulation.

(23) To the extent that this Regulation creates an obligation to recognise a trust service, such a trust service may only be rejected if the addressee of the obligation is unable to read or verify it due to technical reasons lying outside the immediate control of the addressee. However, that obligation should not in itself require a public body to obtain the hardware and software necessary for the technical readability of all existing trust services.

(24) Member States may maintain or introduce national provisions, in conformity with Union law, relating to trust services as far as those services are not fully harmonised by this Regulation. However, trust services that comply with this Regulation should circulate freely in the internal market.

(25) 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.

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

(27) 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.

(28) To enhance in particular the trust of small and medium-sized enterprises (SMEs) and consumers 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 that ensure high-level security of whatever qualified trust services and products are used or provided.

(29) In line with the obligations under the United Nations Convention on the Rights of Persons with Disabilities, approved by Council Decision 2010/48/EC[1], in particular Article 9 of the Convention, persons with disabilities should be able to use trust services and end user products used in the provision of those services on an equal basis with other consumers. Therefore, where feasible, trust services provided and end user products used in the provision of those services should be made accessible for persons with disabilities. The feasibility assessment should include, inter alia, technical and economic considerations.

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

(31) Supervisory bodies should cooperate with data protection authorities, for example, by informing them about the results of audits of qualified trust service providers, where personal data protection rules appear to have been breached. The provision of information should in particular cover security incidents and personal data breaches.

(32) 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.

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

[1] Council Decision 2010/48/EC of 26 November 2009 concerning the conclusion, by the European Community, of the United Nations Convention on the Rights of Persons with Disabilities (OJ L 23, 27.1.2010, p. 35).

(34) 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 those requirements across the Union, Member States should adopt comparable procedures and should exchange information on their supervision activities and best practices in the field.

(35) All trust service providers should be subject to the requirements of this Regulation, in particular those 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.

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

(37) This Regulation should provide 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. In order to facilitate the assessment of financial risk that trust service providers might have to bear or that they should cover by insurance policies, this Regulation allows trust service providers to set limitations, under certain conditions, on the use of the services they provide and not to be liable for damages arising from the use of services exceeding such limitations. Customers should be duly informed about the limitations in advance. Those limitations should be recognisable by a third party, for example by including information about the limitations in the terms and conditions of the service provided or through other recognisable means. For the purposes of giving effect to those principles, this Regulation should be applied in accordance with national rules on liability. Therefore, this Regulation does not affect those national rules on, for example, definition of damages, intention, negligence, or relevant applicable procedural rules.

(38) 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.

(39) 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 Union Agency for Network and Information Security (ENISA).

(40) 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 practice between supervisory bodies and would ensure the verification of the consistent and efficient implementation of the essential supervision requirements in all Member States.

(41) To ensure sustainability and durability of qualified trust services and to boost users' confidence in the continuity of qualified trust services, supervisory bodies should verify the existence and the correct application of provisions on termination plans in cases where qualified trust service providers cease their activities.

(42) To facilitate the supervision of qualified trust service 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 a Member State other than the one where it is established, a mutual assistance system between supervisory bodies in the Member States should be established.

(43) In order to ensure the compliance of qualified trust service providers and the services they provide with the requirements set out in this Regulation, a conformity assessment should be carried out by a conformity assessment body and the resulting conformity assessment reports should be submitted by the qualified trust service providers to the supervisory body. Whenever the supervisory body requires a qualified trust service provider to submit an ad hoc conformity assessment report, the supervisory body should respect, in particular, the principles of good administration, including the obligation to give reasons for its decisions, as well as the principle of proportionality. Therefore, the supervisory body should duly justify its decision to require an ad hoc conformity assessment.

(44) This Regulation aims to ensure a coherent framework with a view to providing a high level of security and legal certainty of trust services. In this regard, when addressing the conformity assessment of products and services, the Commission should, where appropriate, seek synergies with existing relevant European and international schemes such as the Regulation (EC) No 765/2008 of the European Parliament and of the Council[1] which sets out the requirements for accreditation of conformity assessment bodies and market surveillance of products.

(45) 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 a view to facilitating the due diligence leading to the provisioning of qualified trust services.

[1] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

(46) Trusted lists are essential elements in the building of trust among market operators as they indicate the qualified status of the service provider at the time of supervision.

(47) Confidence in and convenience of online services are essential for users to fully benefit and consciously rely on electronic services. To this end, an EU trust mark should be created to identify the qualified trust services provided by qualified trust service providers. Such an EU trust mark for qualified trust services would clearly differentiate qualified trust services from other trust services thus contributing to transparency in the market. The use of an EU trust mark by qualified trust service providers should be voluntary and should not lead to any requirement other than those provided for in this Regulation.

(48) 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[1], electronic signatures with a lower security assurance should also be accepted.

(49) This Regulation should establish the principle that an electronic signature should not be denied legal effect on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic signature. However, it is for national law to define the legal effect of electronic signatures, except for the requirements provided for in this Regulation according to which a qualified electronic signature should have the equivalent legal effect of a handwritten signature.

[1] 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 (OJ L 274, 20.10.2009, p. 36).

(50) 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.

(51) It should be possible for the signatory to entrust qualified electronic signature creation devices to the care of a third party, 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 electronic signature requirements are met by the use of the device.

(52) The creation of remote electronic signatures, where the electronic signature creation environment is managed by a trust service provider on behalf of the signatory, is set to increase in the light of its multiple economic benefits. However, in order to ensure that such electronic signatures receive the same legal recognition as electronic signatures created in an entirely user-managed environment, remote electronic signature service providers should apply specific management and administrative security procedures and use trustworthy systems and products, including secure electronic communication channels, in order to guarantee that the electronic signature creation environment is reliable and is used under the sole control of the signatory. Where a qualified electronic signature has been created using a remote electronic signature creation device, the requirements applicable to qualified trust service providers set out in this Regulation should apply.

(53) The suspension of qualified certificates is an established operational practice of trust service providers in a number of Member States, which is different from revocation and entails the temporary loss of validity of a certificate. Legal certainty calls for the suspension status of a certificate to always be clearly indicated. To that end, trust service providers should have the responsibility to clearly indicate the status of the certificate and, if suspended, the precise period of time during which the certificate has been suspended. This Regulation should not impose the use of suspension on trust service providers or Member States, but should provide for transparency rules when and where such a practice is available.

(54) Cross-border interoperability and recognition of qualified certificates is a precondition for cross-border recognition of qualified electronic signatures. Therefore, qualified certificates should not be subject to any mandatory requirements exceeding the requirements laid down in this Regulation. However, at national level, the inclusion of specific attributes, such as unique identifiers, in qualified certificates should be allowed, provided that such specific attributes do not hamper cross-border interoperability and recognition of qualified certificates and electronic signatures.

(55) IT security certification based on international standards such as ISO 15408 and related evaluation methods and mutual recognition arrangements is an important tool for verifying the security of qualified electronic signature creation devices and should be promoted. However, innovative solutions and services such as mobile signing and cloud signing rely on technical and organisational solutions for qualified electronic signature creation devices for which security standards may not yet be available or for which the first IT security certification is on-going. The level of security of such qualified electronic signature creation devices could be evaluated by using alternative processes only where such security standards are not available or where the first IT security certification is ongoing. Those processes should be comparable to the standards for IT security certification insofar as their security levels are equivalent. Those processes could be facilitated by a peer review.

(56) This Regulation should lay down requirements for qualified electronic signature creation devices to ensure the functionality of advanced electronic signatures. This Regulation should not cover the entire system environment in which such devices operate. Therefore, the scope of the certification of qualified signature creation devices should be limited to the hardware and system software used to manage and protect the signature creation data created, stored or processed in the signature creation device. As detailed in relevant standards, the scope of the certification obligation should exclude signature creation applications.

(57) To ensure legal certainty as regards the validity of the signature, it is essential to specify the components of a qualified electronic signature, which should be assessed by the relying party carrying out the validation. Moreover, specifying the requirements for qualified trust service providers that can provide a qualified validation service to relying parties unwilling or unable to carry out the validation of qualified electronic signatures themselves, should stimulate the private and public sector to invest in such services. Both elements should make qualified electronic signature validation easy and convenient for all parties at Union level.

(58) 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.

(59) 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.

(60) Trust service providers issuing qualified certificates for electronic seals should implement the necessary measures in order to be able to establish the identity of the natural person representing the legal person to whom the qualified certificate for the electronic seal is provided, when such identification is necessary at national level in the context of judicial or administrative proceedings.

(61) This Regulation should ensure the long-term preservation of information, in order to ensure the legal validity of electronic signatures and electronic seals over extended periods of time and guarantee that they can be validated irrespective of future technological changes.

(62) In order to ensure the security of qualified electronic time stamps, this Regulation should require the use of an advanced electronic seal or an advanced electronic signature or of other equivalent methods. It is foreseeable that innovation may lead to new technologies that may ensure an equivalent level of security for time stamps. Whenever a method other than an advanced electronic seal or an advanced electronic signature is used, it should be up to the qualified trust service provider to demonstrate, in the conformity assessment report, that such a method ensures an equivalent level of security and complies with the obligations set out in this Regulation.

(63) Electronic documents are important for further development of cross-border electronic transactions in the internal market. This Regulation should establish the principle that an electronic document should not be denied legal effect on the grounds that it is in an electronic form in order to ensure that an electronic transaction will not be rejected only on the grounds that a document is in electronic form.

(64) When addressing formats of advanced electronic signatures and seals, the Commission should build on existing practices, standards and legislation, in particular Commission Decision 2011/130/EU[1].

(65) 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, such as software code or servers.

[1] Commission Decision 2011/130/EU of 25 February 2011 establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market (OJ L 53, 26.2.2011, p. 66).

(66) It is essential to provide for a legal framework to facilitate cross-border recognition between existing national legal systems related to electronic registered delivery services. That framework could also open new market opportunities for Union trust service providers to offer new pan-European electronic registered delivery services.

(67) Website authentication services provide a means by which a visitor to a website can be assured that there is a genuine and legitimate entity standing behind the website. Those services contribute to the building of trust and confidence in conducting business online, as users will have confidence in a website that has been authenticated. The provision and the use of website authentication services are entirely voluntary. However, in order for website authentication to become a means to boosting trust, providing a better experience for the user and furthering growth in the internal market, this Regulation should lay down minimal security and liability obligations for the providers and their services. To that end, the results of existing industry led initiatives, for example the Certification Authorities / Browsers Forum - CA/B Forum, have been taken into account. In addition, this Regulation should not impede the use of other means or methods to authenticate a website not falling under this Regulation nor should it prevent third country providers of website authentication services from providing their services to customers in the Union. However, a third country provider should only have its website authentication services recognised as qualified in accordance with this Regulation, if an international agreement between the Union and the country of establishment of the provider has been concluded.

(68) The concept of 'legal persons', according to the provisions of the Treaty on the Functioning of the European Union (TFEU) 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 TFEU, means all entities constituted under, or governed by, the law of a Member State, irrespective of their legal form.

(69) The Union institutions, bodies, offices and agencies are encouraged to recognise electronic identification and trust services covered by this Regulation for the purpose of administrative cooperation capitalising, in particular, on existing good practices and the results of on-going projects in the areas covered by this Regulation.

(70) 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 TFEU should be delegated to the Commission in respect of criteria to be met by the bodies responsible for the certification of qualified electronic signature creation devices. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. 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.

(71) 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 the use of which would raise a presumption of compliance with certain requirements laid down in this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[1].

(72) When adopting delegated or implementing acts, the Commission should take due account of the standards and technical specifications drawn up by European and international standardisation organisations and bodies, in particular the European Committee for Standardisation (CEN), the European Telecommunications Standards Institute (ETSI), the International Organisation for Standardisation (ISO) and the International Telecommunication Union (ITU), with a view to ensuring a high level of security and interoperability of electronic identification and trust services.

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

(74) To ensure legal certainty for market operators already using qualified certificates issued to natural persons in compliance with Directive 1999/93/EC, it is necessary to provide for a sufficient period of time for transitional purposes. Similarly, transitional measures should be established for secure signature creation devices, the conformity of which has been determined in accordance with Directive 1999/93/EC, as well as for certification service providers issuing qualified certificates before 1 July 2016. Finally, it is also necessary to provide the Commission with the means to adopt the implementing acts and delegated acts before that date.

---

[1] 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 (OJ L 55, 28.2.2011, p. 13).

(75) The application dates set out in this Regulation do not affect existing obligations that Member States already have under Union law, in particular under Directive 2006/123/EC.

(76) Since the objectives of this Regulation cannot be sufficiently achieved by the Member States but can rather, 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 those objectives.

(77) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 of the European Parliament and of the Council[1] and delivered an opinion on 27 September 2012[2],

HAVE ADOPTED THIS REGULATION:

---

[1] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

[2] OJ C 28, 30.1.2013, p. 6.

CHAPTER I
GENERAL PROVISIONS

Article 1

Subject matter

With a view to ensuring the proper functioning of the internal market while aiming at an adequate level of security of electronic identification means and trust services this Regulation:

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

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

(c) establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication.

Article 2

Scope

1. This Regulation applies to electronic identification schemes that have been notified by a Member State, and to trust service providers that are established in the Union.

2. This Regulation does not apply to the provision of trust services that are used exclusively within closed systems resulting from national law or from agreements between a defined set of participants.

3. This Regulation does not affect national or Union law related to the conclusion and validity of contracts or other legal or procedural obligations relating to form.

Article 3

Definitions

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

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

(2) 'electronic identification means' means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service;

(3) 'person identification data' means a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established;

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

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

(6) 'relying party' means a natural or legal person that relies upon an electronic identification or a trust service;

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

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

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

[1] Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (OJ L 94, 28.3.2014, p. 65).

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

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

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

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

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

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

(16) 'trust service' means an electronic service normally provided for remuneration which consists of:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(39) 'qualified certificate for website authentication' means a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV;

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

(41) 'validation' means the process of verifying and confirming that an electronic signature or a seal 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 State for reasons that fall within the fields covered by this Regulation.

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

Article 5

Data processing and protection

1. Processing of personal data shall be carried out in accordance with Directive 95/46/EC.

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

CHAPTER II
ELECTRONIC IDENTIFICATION

Article 6

Mutual recognition

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

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

   (b) the assurance level of the electronic identification means corresponds to an assurance level equal to or higher than the assurance level required by the relevant public sector body to access that service online in the first Member State, provided that the assurance level of that electronic identification means corresponds to the assurance level substantial or high;

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

Such recognition shall take place no later than 12 months after the Commission publishes the list referred to in point (a) of the first subparagraph.

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

Article 7

Eligibility for notification of electronic identification schemes

An electronic identification scheme shall be eligible for notification pursuant to Article 9(1) provided that all of the following conditions are met:

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

(i) by the notifying Member State;

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

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

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

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

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

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

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

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

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

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

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

Article 8

Assurance levels of electronic identification schemes

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

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

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

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

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

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

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

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

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

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

(d) the entity issuing the electronic identification means;

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

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

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

* OJ: Please insert the date: 12 months after the entry into force of this Regulation.

Article 9

Notification

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

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

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

(i) the party issuing the electronic identification means, and

(ii) the party operating the authentication procedure;

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

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

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

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

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

2. One year from the date of application of the implementing acts referred to in Articles 8(3) and 12(8), the Commission shall publish in the *Official Journal of the European Union* a 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 expiry of the period referred to in paragraph 2, it shall publish in the *Official Journal of the European Union* the amendments to the list referred to in paragraph 2 within two months from the date of receipt of that notification.

4. A Member State may submit to the Commission a request to remove an electronic identification scheme notified by that Member State from the list referred to in paragraph 2. The Commission shall publish in the *Official Journal of the European Union* the corresponding amendments to the list within one month from the date of receipt of the Member State's request.

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

Article 10

Security breach

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

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

3. If the breach or compromise referred to in paragraph 1 is not remedied within three months of the suspension or revocation, the notifying Member State shall notify other Member States and the Commission of the withdrawal of the electronic identification scheme.

   The Commission shall publish in the *Official Journal of the European Union* the corresponding amendments to the list referred to in Article 9(2) without undue delay.

Article 11

Liability

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

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

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

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

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

Article 12

Cooperation and interoperability

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

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

3. The interoperability framework shall meet the following criteria:

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

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

   (c) it facilitates the implementation of the principle of privacy by design; and

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

4. The interoperability framework shall consist of:

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

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

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

(d) a reference to a minimum set of person identification data uniquely representing a natural or legal person, which is available from electronic identification schemes;

(e) rules of procedure;

(f) arrangements for dispute resolution; and

(g) common operational security standards.

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

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

(b) the security of the electronic identification schemes.

6. The cooperation between Member States shall consist of:

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

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

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

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

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

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

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

---

* OJ: Please insert the date: 6 months after the entry into force of this Regulation.

** OJ: Please insert the date: 1 year after the entry into force of this Regulation.

CHAPTER III
TRUST SERVICES

SECTION 1
GENERAL PROVISIONS

Article 13
Liability and burden of proof

1. Without prejudice to paragraph 2, trust service providers shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under this Regulation.

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

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

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

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

Article 14

International aspects

1. Trust services provided by trust service providers established in a third country shall be recognised as legally equivalent to qualified trust services provided by qualified trust service providers established in the Union where the trust services originating from the third country are recognised under an agreement concluded between the Union and the third country in question or an international organisation in accordance with Article 218 TFEU.

2. Agreements referred to in paragraph 1 shall ensure, in particular, that:

   (a) the requirements applicable to qualified trust service providers established in the Union and the qualified trust services they provide are met by the trust service providers in the third country or international organisations with which the agreement is concluded, and by the trust services they provide;

(b) the qualified trust services provided by qualified trust service providers established in the Union are recognised as legally equivalent to trust services provided by trust service providers in the third country or international organisation with which the agreement is concluded.

Article 15

Accessibility for persons with disabilities

Where feasible, trust services provided and end user products used in the provision of those services shall be made accessible for persons with disabilities.

Article 16

Penalties

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

SECTION 2

SUPERVISION

Article 17

Supervisory body

1. Member States shall designate a supervisory body established in their territory or, upon mutual agreement with another Member State, a supervisory body established in that other Member State. That body shall be responsible for supervisory tasks in the designating Member State.

   Supervisory bodies shall be given the necessary powers and adequate resources for the exercise of their tasks.

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

3. The role of the supervisory body shall be the following:

   (a) 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 those qualified trust service providers and the qualified trust services that they provide meet the requirements laid down in this Regulation;

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

4. For the purposes of paragraph 3 and subject to the limitations provided therein, the tasks of the supervisory body shall include in particular:

(a) to cooperate with other supervisory bodies and provide them with assistance in accordance with Article 18;

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

(c) to inform other supervisory bodies and the public about breaches of security or loss of integrity in accordance with Article 19(2);

(d) to report to the Commission about its main activities in accordance with paragraph 6 of this Article;

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

(f) to cooperate with the data protection authorities, in particular, by informing them without undue delay, about the results of audits of qualified trust service providers, where personal data protection rules appear to have been breached;

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

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

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

(j) to require that trust service providers remedy any failure to fulfil the requirements laid down in this Regulation.

5. Member States may require the supervisory body to establish, maintain and update a trust infrastructure in accordance with the conditions under national law.

6. By 31 March each year, each supervisory body shall submit to the Commission a report on its previous calendar year's main activities together with a summary of breach notifications received from trust service providers in accordance with Article 19(2).

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

8. The Commission may, by means of implementing acts, define the formats and procedures for the report referred to in paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 18

Mutual assistance

1. Supervisory bodies shall cooperate with a view to exchanging good practice.

   A supervisory body shall, upon receipt of a justified request from another supervisory body, provide that body with assistance so that the activities of supervisory bodies can be carried out in a consistent manner. Mutual assistance may cover, in particular, information requests and supervisory measures, such as requests to carry out inspections related to the conformity assessment reports as referred to in Articles 20 and 21.

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

   (a) the supervisory body is not competent to provide the requested assistance;

   (b) the requested assistance is not proportionate to supervisory activities of the supervisory body carried out in accordance with Article 17;

   (c) providing the requested assistance would be incompatible with this Regulation.

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

Article 19

Security requirements applicable to trust service providers

1. Qualified and non-qualified trust service providers shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. Having regard to the latest technological developments, those measures shall ensure that the level of security is 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 such incidents.

2. Qualified and non-qualified trust service providers shall, without undue delay but in any event within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein.

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

Where appropriate, in particular if a breach of security or loss of integrity concerns two or more Member States, the notified supervisory body shall inform the supervisory bodies in other Member States concerned and ENISA.

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

3. The supervisory body shall provide ENISA once a year with a summary of notifications of breach of security and loss of integrity received from trust service providers.

4. The Commission may, by means of implementing acts,:

(a) further specify the measures referred to in paragraph 1, and

(b) define the formats and procedures, including deadlines, applicable for the purpose of paragraph 2.

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

SECTION 3

QUALIFIED TRUST SERVICES

Article 20

Supervision of qualified trust service providers

1. Qualified trust service providers shall be audited at their own expense at least every 24 months by a conformity assessment body. The purpose of the audit shall be to confirm that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in this Regulation. The qualified trust service providers shall submit the resulting conformity assessment report to the supervisory body within the period of 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, at the expense of those trust service providers, to confirm that they and the qualified trust services provided by them fulfil the requirements laid down in this Regulation. Where personal data protection rules appear to have been breached, the supervisory body shall inform the data protection authorities of the results of its audits.

3. Where the supervisory body requires the qualified trust service provider to remedy any failure to fulfil requirements under this Regulation and where that provider does not act accordingly, and if applicable within a time limit set by the supervisory body, the supervisory body, taking into account, in particular, the extent, duration and consequences of that failure, may withdraw the qualified status of that provider or of the affected service it provides and inform the body referred to in Article 22(3) for the purposes of updating the trusted lists referred to in Article 22(1). The supervisory body shall inform the qualified trust service provider of the withdrawal of its qualified status or of the qualified status of the service concerned.

4. The Commission may, by means of implementing acts, establish reference number of the following standards:

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

(b) auditing rules under which conformity assessment bodies will carry out their conformity assessment of the qualified trust service providers as referred to in paragraph 1.

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

Article 21

Initiation of a qualified trust service

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

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

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

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

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

4. The Commission may, by means of implementing acts, define the formats and procedures for the purpose of paragraphs 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 22

Trusted lists

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

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

3. Member States shall notify to the Commission, without undue delay, information on the body responsible for establishing, maintaining and publishing national trusted lists, and details of where such lists are published, the certificates used to sign or seal the trusted lists and any changes thereto.

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

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

Article 23

EU trustmark for qualified trust services

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

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

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

---

* OJ: Please insert the date: 12 months after the entry into force of this Regulation.

Article 24

Requirements for qualified trust service providers

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

   The information referred to in the first subparagraph shall be verified by the qualified trust service provider either directly or by relying on a third party in accordance with national law:

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

   (b) remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorised representative of the legal person was ensured and which meets the requirements set out in Article 8 with regard to the assurance levels 'substantial' or 'high', or

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

   (d) by using other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body.

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

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

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

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

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

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

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

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

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

(iii) the data can be checked for authenticity;

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

(h) record and keep accessible for an appropriate period of time, 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;

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

(j) ensure lawful processing of personal data in accordance with Directive 95/46/EC;

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

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

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

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 points (e) and (f) of paragraph 2 of this Article. Compliance with the requirements laid down in this Article shall be presumed where trustworthy systems and products meet those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

SECTION 4

ELECTRONIC SIGNATURES

Article 25

Legal effects of electronic signatures

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

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

3. A qualified electronic signature based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic signature in all other Member States.

Article 26

Requirements for advanced electronic signatures

An advanced electronic signature shall meet the following requirements:

(a) it is uniquely linked to the signatory;

(b) it is capable of identifying the signatory;

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

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

Article 27

Electronic signatures in public services

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

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

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

4. The Commission may, by means of implementing acts, establish reference numbers of standards for advanced electronic signatures. Compliance with the requirements for advanced electronic signatures referred to in paragraphs 1 and 2 of this Article and in Article 26 shall be presumed when an advanced electronic signature meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

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

---

* OJ: Please insert the date: 12 months after the entry into force of this Regulation.

Article 28

Qualified certificates for electronic signatures

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

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

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

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

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

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

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

6. 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 48(2).

Article 29

Requirements for qualified electronic signature creation devices

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

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

Article 30

Certification of qualified electronic signature creation devices

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

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

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

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

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

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

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

Article 31

Publication of a list of certified qualified electronic signature creation devices

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

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

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

Article 32

Requirements for the validation of qualified electronic signatures

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

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

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

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

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

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

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

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

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

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

3. 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 48(2).

Article 33

Qualified validation service for qualified electronic signatures

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

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

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

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

Article 34

Qualified preservation service for qualified electronic signatures

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

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

SECTION 5

ELECTRONIC SEALS

Article 35

Legal effects of electronic seals

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

2. A qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked.

3. A qualified electronic seal based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic seal in all other Member States.

Article 36

Requirements for advanced electronic seals

An advanced electronic seal shall meet the following requirements:

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

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

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

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

Article 37

Electronic seals in public services

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

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

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

4. The Commission may, by means of implementing acts, establish reference numbers of standards for advanced electronic seals. Compliance with the requirements for advanced electronic seals referred to in paragraphs 1 and 2 of this Article and Article 36shall be presumed when an advanced electronic seal meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

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

---

* OJ: Please insert the date: 12 months after the entry into force of this Regulation.

Article 38

Qualified certificates for electronic seals

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

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

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

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

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

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

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

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

Article 39

Qualified electronic seal creation devices

1. Article 29 shall apply mutatis mutandis to requirements for qualified electronic seal creation devices.

2. Article 30 shall apply mutatis mutandis to the certification of qualified electronic seal creation devices.

3. Article 31 shall apply mutatis mutandis to the publication of a list of certified qualified electronic seal creation devices.

Article 40

Validation and preservation of qualified electronic seals

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

SECTION 6

ELECTRONIC TIME STAMPS

Article 41

Legal effect of electronic time stamps

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

2. A qualified electronic time stamp shall enjoy the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound.

3. A qualified electronic time stamp issued in one Member State shall be recognised as a qualified electronic time stamp in all Member States.

Article 42

Requirements for qualified electronic time stamps

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

   (a) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably;

   (b) it is based on an accurate time source linked to Coordinated Universal Time; and

(c) it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method.

2. The Commission may, by means of implementing acts, establish reference numbers of standards for the binding of date and time to data and for accurate time sources. Compliance with the requirements laid down in paragraph 1 shall be presumed where the binding of date and time to data and the accurate time source meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

SECTION 7

ELECTRONIC REGISTERED DELIVERY SERVICES

Article 43

Legal effect of an electronic registered delivery service

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

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

Article 44

Requirements for qualified electronic registered delivery services

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

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

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

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

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

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

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

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

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 48(2).

SECTION 8

WEBSITE AUTHENTICATION

Article 45

Requirements for qualified certificates for website authentication

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

2. 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 48(2).

CHAPTER IV
ELECTRONIC DOCUMENTS

Article 46

Legal effects of electronic documents

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

CHAPTER V
DELEGATIONS OF POWER AND IMPLEMENTING PROVISIONS

Article 47

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Article 30(4) shall be conferred on the Commission for an indeterminate period of time from …*.

* OJ: Please insert date: the date of entry into force of this Regulation.

3. The delegation of power referred to in Article 30(4) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

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

5. A delegated act adopted pursuant to Article 30(4) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Article 48

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

CHAPTER VI
FINAL PROVISIONS

Article 49

Review

The Commission shall review the application of this Regulation and shall report to the European Parliament and to the Council no later than 1 July 2020. The Commission shall evaluate in particular whether it is appropriate to modify the scope of this Regulation or its specific provisions, including Article 6, point (f) of Article 7 and Articles 34, 43, 44 and 45, taking into account the experience gained in the application of this Regulation, as well as technological, market and legal developments.

The report referred to in the first paragraph shall be accompanied, where appropriate, by legislative proposals.

In addition, the Commission shall submit a report to the European Parliament and the Council every four years after the report referred to in the first paragraph on the progress towards achieving the objectives of this Regulation.

Article 50

Repeal

1. Directive 1999/93/EC is repealed with effect from 1 July 2016.

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

Article 51

Transitional measures

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

2. Qualified certificates issued to natural persons under Directive 1999/93/EC shall be considered as qualified certificates for electronic signatures under this Regulation until they expire.

3. A certification-service-provider issuing qualified certificates under Directive 1999/93/EC shall submit a conformity assessment report to the supervisory body as soon as possible but not later than 1 July 2017. Until the submission of such a conformity assessment report and the completion of its assessment by the supervisory body, that certification-service-provider shall be considered as qualified trust service provider under this Regulation.

4. If a certification-service-provider issuing qualified certificates under Directive 1999/93/EC does not submit a conformity assessment report to the supervisory body within the time limit referred to in paragraph 3, that certification-service-provider shall not be considered as qualified trust service provider under this Regulation from 2 July 2017.

Article 52

Entry into force

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

2. This Regulation shall apply from 1 July 2016, except for the following:

   (a) Articles 8(3), 9(5), 12(2) to (9), 17(8), 19(4), 20(4), 21(4), 22(5), 23(3), 24(5), 27(4) and (5), 28(6), 29(2), 30(3) and (4), 31(3), 32(3), 33(2), 34(2), 37(4) and (5), 38(6), 42(2), 44(2), 45(2), and Articles 47 and 48 shall apply from …*;

   (b) Article 7, Article 8(1) and (2), Articles 9, 10, 11 and Article 12(1) shall apply from the date of application of the implementing acts referred to in Articles 8(3) and 12(8);

   (c) Article 6 shall apply from three years as from the date of application of the implementing acts referred to in Articles 8(3) and 12(8).

---

* OJ: Please insert the date of entry into force of this Regulation.

3. Where the notified electronic identification scheme is included in the list published by the Commission pursuant to Article 9 before the date referred to in point (c) of paragraph 2 of this Article, the recognition of the electronic identification means under that scheme pursuant to Article 6 shall take place no later than 12 months after the publication of that scheme but not before the date referred to in point (c) of paragraph 2 of this Article.

4. Notwithstanding point (c) of paragraph 2 of this Article, a Member State may decide that electronic identification means under electronic identification scheme notified pursuant to Article 9(1) by another Member State are recognised in the first Member State as from the date of application of the implementing acts referred to in Articles 8(3) and 12(8). Member States concerned shall inform the Commission. The Commission shall make this information public.

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

Done at …,

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

ANNEX I

REQUIREMENTS
FOR QUALIFIED CERTIFICATES FOR ELECTRONIC SIGNATURES

Qualified certificates for electronic signatures shall contain:

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

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

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

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

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

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

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

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

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

(i) the location of the 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 is located in a qualified electronic signature creation device, an appropriate indication of this, at least in a form suitable for automated processing.

ANNEX II

REQUIREMENTS
FOR QUALIFIED ELECTRONIC SIGNATURE CREATION DEVICES

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

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

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

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

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

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

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

4. Without prejudice to point (d) of point 1, 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: the person's name;

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

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

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

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

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

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

(i) the location of the services that can be used to enquire as to the validity status of the qualified certificate;

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

ANNEX IV

REQUIREMENTS
FOR QUALIFIED CERTIFICATES FOR WEBSITE AUTHENTICATION

Qualified certificates for website authentication shall contain:

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

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

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

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

(c) for natural persons: at least the name of the person to whom the certificate has been issued, or a pseudonym. If a pseudonym is used, it shall be clearly indicated;

for legal persons: at least the name of the legal person to whom the certificate is issued and, where applicable, registration number as stated in the official records;

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

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

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

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

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

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

(j) the location of the certificate validity status services that can be used to enquire as to the validity status of the qualified certificate.