EUROPEAN COMMISSION

Brussels, 4.6.2012
COM(2012) 238 final

2012/0146 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

(Text with EEA relevance)

{SWD(2012) 135 final}
{SWD(2012) 136 final}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

This memorandum explains a proposed legal framework designed to enhance trust in electronic transactions in the internal market.

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

The *Digital Agenda for Europe*[1] identifies existing barriers to Europe's digital development and proposes legislation on e-signatures (Key Action 3) and the mutual recognition of e-identification and authentication (Key Action 16), establishing a clear legal framework so as to eliminate fragmentation and the lack of interoperability, enhance digital citizenship and prevent cybercrime. Legislation ensuring the mutual recognition of electronic identification and authentication across the EU and review the Directive on Electronic Signatures is also a key action in the *Single Market Act*[2], for the realisation of the digital single market. The *Roadmap for Stability and Growth*[3] underlines the key role for the development of the digital economy of the future common legal framework for the mutual recognition and acceptance of electronic identification and authentication across borders.

The proposed legal framework, consisting of a '*Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market*', seeks to enable secure and seamless electronic interactions between businesses, citizens and public authorities, thereby increasing the effectiveness of public and private online services, e-business and electronic commerce in the EU.

The existing EU legislation, namely Directive 1999/93/EC on a '*Community framework for electronic signatures*'[4], essentially covers electronic signatures only. There is no comprehensive EU cross-border and cross-sector framework for secure, trustworthy and easy-to-use electronic transactions that encompasses electronic identification, authentication and signatures.

The aim is to enhance existing legislation and to expand it to cover the mutual recognition and acceptance at EU level of notified electronic identification schemes and other essential related electronic trust services.

2. RESULTS OF CONSULTATIONS WITH INTERESTED PARTIES AND IMPACT ASSESSMENTS

This initiative is the result of extensive consultations on a review of the current legal framework on electronic signatures in the course of which the Commission gathered feedback from Member States, the European Parliament and other stakeholders[5]. An online public consultation was complemented by an 'SME Test Panel' to identify the specific views and

1 COM(2010) 245 of 19.5.2010
2 COM(2011) 206 final of 13.4.2011
3 COM(2011) 669, 12.10.2011
4 OJ L 13, 19.1.2000, p. 12
5 For details on the consultations, see http://ec.europa.eu/information_society/policy/esignature/eu_legislation/revision

needs of SMEs; and other targeted consultations with stakeholders[6,7]. The Commission also launched a number of studies in relation to electronic identification, authentication, signature and related trust services (eIAS).

The consultations made clear that a large majority of stakeholders agreed on the need to review the current framework to fill the gaps left by the electronic signature Directive. It was felt that this would better respond to challenges posed by the rapid development of new technologies (particularly online and mobile access) and by increased globalisation, while maintaining the technological neutrality of the legal framework.

In line with its 'Better Regulation' policy, the Commission conducted an impact assessment of policy alternatives. Three sets of policy options were assessed, dealing respectively with (1) the scope of the new framework, (2) the legal instrument and (3) the level of supervision required[8]. The preferred policy option proved to be enhancing legal certainty, boosting coordination of national supervision, ensuring mutual recognition and acceptance of electronic identification schemes and incorporating essential related trust services. The impact assessment concluded that doing this would lead to considerable improvements to legal certainty, security and trust in terms of cross-border electronic transactions, resulting in less fragmentation of the market.

3. LEGAL ELEMENTS OF THE PROPOSAL

3.1 Legal Basis

This proposal is based on Article 114 TFEU, which concerns the adoption of rules to remove existing barriers to the functioning of the internal market. Citizens, businesses and administrations will be able to benefit from the mutual recognition and acceptance of electronic identification, authentication, signatures and other trust services across borders when needed for the access and completion of electronic procedures or transactions.

A Regulation is considered to be the most appropriate legal instrument. The direct applicability of a Regulation pursuant to Article 288 TFEU will reduce legal fragmentation and provide greater legal certainty by introducing a harmonised set of core rules contributing to the functioning of the internal market.

3.2 Subsidiarity and proportionality

In order for EU action to be justified, the subsidiarity principle must be respected:

a) Transnational nature of the problem (necessity test)

6 A stakeholder workshop was organised on 10.3.2011 with representatives from the public and private sectors and academia to discuss what legislative measures were needed to address the challenges ahead. This was an interactive forum to exchange views and to point up the different positions on the questions raised in the public consultation. Several organisations spontaneously sent position papers.

7 In particular, the Polish EU Presidency organised a meeting with Member States on electronic signature in Warsaw on 9.11.2011 and on electronic identification in Poznan on 17.11.2011. On 25.1.2012, the Commission convened a workshop with Member States to discuss remaining issues on electronic identification, authentication and signature.

8 Under the first set, four options were examined: repealing the e-signature Directive; no policy change; enhancing legal certainty, boosting coordination of national supervision and ensuring mutual recognition and acceptance of electronic identification throughout the EU; and fourthly, expansion to incorporate certain related trust services. The second set consisted of assessing the relative merits of the opportunities of regulating via one or two instruments, and via a directive versus a regulation. The third set examined the possibilities offered by implementing national supervision schemes based on common essential supervision requirements versus an EU-based supervision system. Each policy option was assessed, with the help of a group which brought together all interested Directorates General of the Commission, in terms of its effectiveness in achieving the policy objectives, its economic impact on stakeholders (including on the EU Institutions' budget), its social and environmental impact, and its effect on administrative burden.

The transnational nature of eIAS requires EU action. Domestic (i.e. national) action alone would not suffice to meet the objectives, nor achieve the targets set out in the *Europe 2020 Strategy*[9]. Conversely, experience has shown that national measures have *de facto* created barriers to the EU-wide interoperability of electronic signatures, and that they are currently having the same effect on electronic identification, electronic authentication and related trust services. It is therefore necessary for the EU to create an enabling framework to address cross-border interoperability and to improve the coordination of national supervision schemes. However, electronic identification cannot be addressed in the proposed Regulation in the same generic manner as the other trust electronic services because issuing means of identification is a national prerogative. The proposal therefore focuses strictly on cross-border aspects of electronic identification.

The proposed Regulation creates a level playing field for businesses providing trust services where the currently existing differences in national legislation often lead to legal uncertainty and additional burden. Legal certainty is significantly increased through clear acceptance obligations by Member States of qualified trust services which will create additional incentive for businesses to go abroad. For example a company will be able to participate electronically to a public call for tenders launched by the administration of a different Member State without its electronic signature being blocked due to specific national requirements and interoperability problems. Similarly, a company will have the opportunity to sign contracts electronically with a counterpart based in a different Member State without fearing different legal requirements for trust services such as electronic seals, electronic documents or time stamping. Finally, a notice of default will be delivered from one Member State to another with the certainty of its legal validity in both Member States. Finally, online commerce will be more trustworthy when shoppers will have the means to verify that they indeed access the website of the merchant of their choice instead of a possibly fake website.

Mutually recognised electronic identification means and widely accepted electronic signatures will facilitate cross-border provision of numerous services in the internal market and enable businesses to go cross-border without facing obstacles in interactions with public authorities. In practice this will mean significant efficiency improvements both for businesses and citizens when complying with the administrative formalities. For example, giving the opportunity to a student to enrol electronically in a university abroad, to a citizen to submit tax declaration online to another Member State or to a patient to access his or her health data online. If there is no such mutually recognised electronic identification means, a doctor will not be able to access the patient medical data needed to treat him or her and the medical and laboratory tests that the patient has already undertaken will have to be repeated.

b) Added value (effectiveness test)

The objectives outlined above are currently not being achieved by voluntary coordination among Member States, nor is this reasonably likely to happen in the future. This leads to duplication of efforts, setting different standards, transnational characteristics of the spill-overs generated by ICT, and administrative complexity of establishing such coordination by way of bilateral and multilateral agreements.

In addition, the need to overcome such problems, as (a) an absence of legal certainty due to heterogeneous national provisions stemming from divergent interpretations of the electronic signature Directive and (b) a lack of interoperability of the electronic signature systems set up

[9] Communication from the Commission: *Europe 2020. A strategy for smart, sustainable and inclusive growth*, COM(2010) 2020, 3.3.2010.

at national level due to the non-uniformly application of technical standards, requires the kind of coordination across EU Member States which can be done more effectively at the EU level.

3.3 Detailed explanation of the proposal

3.3.1 CHAPTER I – GENERAL PROVISIONS

Article 1 defines the subject matter of the Regulation.

Article 2 defines the material scope of the Regulation.

Article 3 contains definitions of the terms used in the Regulation. While some definitions are taken over from Directive 1999/93/EC, others are clarified, complemented with additional elements, or newly introduced.

Article 4 determines the internal market principles with regard to the territorial application of the Regulation. Explicit mention is made of the imposition of no restrictions on the freedom to provide services and the free circulation of products.

3.3.2 CHAPTER II – ELECTRONIC IDENTIFICATION

Article 5 provides for the mutual recognition and acceptance of electronic identification means falling under a scheme which will be notified to the Commission on the conditions laid down in the Regulation. Most EU Member States have introduced some form of electronic identification system. However, they differ in many aspects. The lack of a common legal basis requiring each Member State to recognise and accept electronic identification means issued in other Member States to access online services, along with the inadequate cross-border interoperability of national electronic identifications, creates barriers which prevent citizens and businesses from benefiting fully from the digital single market. The mutual recognition and acceptance of any electronic identification means falling under a notified scheme under this Regulation removes these legal barriers.

The Regulation does not oblige Member States to introduce or notify electronic identification schemes, but to recognise and accept notified electronic identifications for those online services where electronic identification is required to get access at national level. The potential increase of economies of scale created through the cross-border use of notified electronic identification means and authentication systems may stimulate Member States to notify to their electronic identification schemes.Article 6 sets out the five conditions for the notification of electronic identification schemes:

Member States can notify the electronic identification schemes that they accept under their jurisdiction where electronic identification is required for public services. A further requirement is that the respective electronic identification means must be issued by, on behalf of or at least under the responsibility of the Member State notifying a scheme.

Member States must ensure an unambiguous link between the electronic identification data and the person concerned. This obligation does not mean that a person cannot have multiple electronic identification means, but they must all link to the same person.

The reliability of an electronic identification depends on the availability of means of authentication (i.e. the possibility to check the validity of the electronic identification data). The Regulation obliges the notifying Member States to provide online authentication free of

charge vis-à-vis third parties. The authentication possibility must be available without interruption. No specific technical requirements, such as hardware or software can be imposed on the parties relying on such authentication. This provision does not apply to any requirements vis-à-vis the users (holders) of the electronic identification means that are technically necessary for the use of the electronic identification means, such as card readers.

Member States must accept liability for the unambiguity of the link (i.e. that the identification data attributed to the person are not linked to any other person) and the authentication possibility (i.e. the possibility to check the validity of the electronic identification data). The liability of Member States does not cover other aspects of the identification process or any transaction that requires identification.

Article 7 contains rules on notifying the Commission of electronic identification schemes.

Article 8 aims to ensure the technical interoperability of the notified identification schemes through a coordination approach, including delegated acts.

3.3.3 CHAPTER III – TRUST SERVICES

3.3.3.1 Section 1 – General provisions

Article 9 sets out the principles relating to the liability of both non-qualified and qualified trust service providers. It builds on Article 6 of Directive 1999/93/EC and extends entitlement to compensation of damage caused by any negligent trust service provider for failure to comply with security good practices which result in a security breach which has a significant impact on the service.

Article 10 describes the mechanism for the recognition and acceptance of qualified trust services provided by a provider established in a third country. It builds on Article 7 of Directive 1999/93/EC but retains only the sole practically feasible option which is to allow such recognition under an international agreement between the European Union and third countries or international organisations.

Article 11 sets out the principles of data protection and minimisation. It builds on Article 8 of Directive 1999/93/EC.

Article 12 makes trust services accessible to disabled people.

3.3.3.2 Section 2 – Supervision

Article 13 obliges Member States to establish supervisory bodies, based on Article 3(3) of Directive 1999/93/EC, clarifying and enlarging their remit with regard to both trust service providers and qualified trust service providers.

Article 14 introduces an explicit mechanism of mutual assistance between supervisory bodies in Member States to facilitate the cross-border supervision of trust service providers. It introduces rules on joint operations and supervisory authorities' right to participate in such operations.

Article 15 introduces an obligation for both qualified and non-qualified trust service providers to implement appropriate technical and organisational measures for the security of their activities. Furthermore, the competent supervisory bodies and other relevant authorities must

be informed of any security breaches. If appropriate, they will in turn inform other Member States' supervisory bodies and will, directly or via the trust service provider concerned, inform the public.

Article 16 sets out the conditions for the supervision of qualified trust service providers and qualified trust services provided by them. It obliges qualified trust service providers to be audited on a yearly basis by a recognised independent body to confirm to the supervisory body that they fulfil the obligations laid down in the Regulation. Moreover, Article 16(2) gives the supervisory body the right to carry out on-the-spot audits of the qualified trust service providers at any time. The supervisory body is also empowered to issue binding instructions to qualified trust service providers to remedy, in a proportionate manner, any failure to meet an obligation revealed by a security audit.

Article 17 concerns the activity carried out by the supervisory body at the request of a trust service provider wishing to initiate a qualified trust service.

Article 18 provides for the establishment of trusted lists[10] containing information on qualified trust service providers who are subject to supervision and to the qualified services they offer. This information must be made publicly available through a common template in order to facilitate its automated use and ensure an appropriate level of detail.

Article 19 sets out the requirements the qualified trust service providers must meet in order to be recognised as such. It draws on Annex II of Directive 1999/93/EC.

3.3.3.3 Section 3 – Electronic signature

Article 20 enshrines the rules related to the legal effect of natural persons' electronic signatures. It clarifies and expands Article 5 of Directive 1999/93/EC introducing an explicit obligation to give to qualified electronic signatures the same legal effect as handwritten signatures. Moreover, Member States must ensure the cross-border acceptance of qualified electronic signatures, in the context of the provision of public services, and they must not introduce any additional requirements which might result in barriers to the use of such signatures.

Article 21 sets out the requirements for qualified signature certificates. It clarifies Annex I of Directive 1999/93/EC and removes provisions which did not work in practice (e.g. limitations on transactions value).

Article 22 sets out the requirements for qualified electronic signature creation devices. It clarifies the requirements for secure signature creation devices laid down in Article 3(5) of Directive 1999/93/EC, which now have to be considered as qualified signature creation devices under this Regulation. It also makes it clear that the scope of a signature creation device can be much wider than just something containing signature creation data. The Commission may also establish a list of reference numbers of standards for security requirements on devices.

Article 23, building on Article 3(4) of Directive 1999/93/EC, introduces the concept of certification of qualified electronic signature devices to determine their conformity with the security requirements laid down in Annex II. These devices must be recognised by all

[10] The trusted list as established by the Commission Decision 2009/767/EC as amended by the Commission Decision 2010/425/EU shall be the basis for a new Commission Decision on trusted lists under this Regulation.

Member States as matching the requirements when a certification procedure is conducted by a certification body designated by a Member State. The Commission will publish a positive list of such certified devices according to Article 24. The Commission may also establish a list of reference numbers of standards for the security assessment of information technology products referenced in Article 23(1).

Article 24 concerns publication of a list of qualified electronic signature creation devices by the Commission after notification of conformity by the Member States.

Article 25 builds on the recommendations of Annex IV of Directive 1999/93/EC to lay down binding requirements for the validation of qualified electronic signatures with a view to increasing the legal certainty of such a validation.

Article 26 sets out the conditions for qualified validation services.

Article 27 sets out the condition for the long-term preservation of qualified electronic signatures. This is possible due to the use of procedures and technologies capable of extending the trustworthiness of the qualified electronic signature validation data beyond the time of their technological validity when forgery may become easy to do for cyber criminals.

3.3.3.4 Section 4 – Electronic seals

Article 28 concerns the legal effect of electronic seals of legal persons. A specific legal presumption is bestowed on a qualified electronic seal which guarantees the origin and integrity of electronic documents to which it is linked.

Article 29 sets out the requirements for qualified certificates for electronic seals.

Article 30 sets out the requirements for and certification and publication of list for the qualified electronic seal creation devices.

Article 31 sets out the condition of validation and preservation of qualified electronic seals.

3.3.3.5 Section 5 – Electronic time stamp

Article 32 concerns the legal effect of electronic time stamps. A specific legal presumption is bestowed on qualified electronic time stamps with regard to the certainty of the time.

Article 33 sets out the requirements for qualified electronic time stamps.

3.3.3.6 Section 6 – Electronic documents

Article 34 is related to the legal effects and the conditions of acceptance of electronic documents. There is a specific legal presumption of the authenticity and integrity of any electronic document signed with a qualified electronic signature or bearing a qualified electronic seal. With regard to the acceptance of electronic documents, when an original document or a certified copy is required for the provision of a public service, at least electronic documents issued by the persons who are competent to issue the relevant documents and that are considered to be originals or certified copies in accordance with national law of the Member State of origin, shall be accepted in other Member States without additional requirements.

3.3.3.7 Section 7 – Electronic delivery services

Article 35 concerns the legal effect of data sent or received using an electronic delivery service. A specific legal presumption regarding the integrity of data which are sent or received and the accuracy of the time on which the data are sent or received is guaranteed for qualified electronic delivery services. It also ensures the mutual recognition of qualified electronic delivery services at EU level.

Article 36 sets out the requirements for qualified electronic delivery services.

3.3.3.8 Section 8 – Website authentication

This section is intended to ensure that the authenticity of a website with respect to the owner of the site will be guaranteed.

Article 37 sets out the requirements for qualified certificates for website authentication, which can be used to guarantee the authenticity of a website. A qualified certificate for website authentication will provide a minimal set of trustworthy information on the website and on the legal existence of its owner.

3.3.4 CHAPTER IV – DELEGATED ACTS

Article 38 contains the standard provisions for exercising the delegations in line with Article 290 TFEU (delegated acts). This allows the legislator to delegate to the Commission the power to adopt non-legislative acts of general application to supplement or amend certain non-essential elements of a legislative act.

3.3.5 CHAPTER V – IMPLEMENTING ACTS

Article 39 contains the provision covering the Committee procedure needed to confer implementing powers on the Commission wherever, in accordance with Article 291 TFEU, uniform conditions for implementing legally binding acts of the Union are needed. The examination procedure applies.

3.3.6 CHAPTER VI – FINAL PROVISIONS

Article 40 obliges the Commission to evaluate the Regulation and report on its findings.

Article 41 repeals Directive 1999/93/EC and provides for the smooth transition of the existing electronic signature infrastructure to the new requirements of the Regulation.

Article 42 sets out the date of the entry into force of the Regulation.

4. BUDGETARY IMPLICATIONS

The specific budgetary implications of the proposal relate to the tasks allocated to the European Commission as specified in the legislative financial statements accompanying this proposal.

The proposal has no implications on operational expenditure.

The legislative financial statement accompanying this proposal for a Regulation covers the budgetary impacts for the Regulation itself.

2012/0146 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the European Commission,

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

Having regard to the opinion of the European Economic and Social Committee[11],

After consulting the European Data Protection Supervisor[12],

Acting in accordance with the ordinary legislative procedure,

Whereas:

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

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

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

---

11 OJ C , , p. .

12 OJ C, , p. .

13 OJ L 13, 19.1.2000, p. 12

(4) The Commission's Digital Agenda for Europe[14] identified the fragmentation of the digital market, the lack of interoperability and the rise in cybercrime as major obstacles to the virtuous cycle of the digital economy. In its Citizenship Report 2010 the Commission further highlighted the need to solve the main problems which prevent European citizens from enjoying the benefits of a digital single market and cross-border digital services[15].

(5) The European Council invited the Commission to create a digital single market by 2015[16] to make rapid progress in key areas of the digital economy and to promote a fully integrated digital single market[17] by facilitating the cross-border use of online services, with particular attention to facilitating secure electronic identification and authentication.

(6) The Council invited the Commission to contribute to the digital single market by creating appropriate conditions for the mutual recognition of key enablers across borders, such as electronic identification, electronic documents, electronic signatures and electronic delivery services, and for interoperable eGovernment services across the European Union[18].

(7) The European Parliament stressed the importance of the security of electronic services, especially of electronic signatures, and of the need to create a public key infrastructure at pan-European level, and called on the Commission to set up a European validation authorities gateway to ensure the cross-border interoperability of electronic signatures and to increase the security of transactions carried out using the internet[19].

(8) Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market[20] requests Member States to establish 'points of single contact' (PSC) to ensure that all procedures and formalities relating to access to a service activity and to the exercise thereof can be easily completed, at a distance and by electronic means, through the appropriate point of single contact and with the appropriate authorities. Many online services accessible through PSCs require electronic identification, authentication and signature.

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

---

14 COM(2010) 245 final/2

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

16 4/2/2011: EUCO 2/1/11

17 23/10/2011: EUCO 52/1/11

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

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

20 OJ L 376, 27.12.2006, p. 36

(10) Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare[21] sets up a network of national authorities responsible for eHealth. To enhance safety and the continuity of cross-border healthcare, the network is required to produce guidelines on cross-border access to electronic health data and services, including by supporting '*common identification and authentication measures to facilitate transferability of data in cross-border healthcare*'. Mutual recognition and acceptance of electronic identification and authentication is key to make cross border healthcare for European citizens a reality. When people travel for treatment, their medical data needs to be accessible in the country of treatment. This requires a solid, safe and trusted electronic identification framework.

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

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

(13) Some conditions need to be set in the Regulation with regard to which electronic identification means have to be accepted and how the schemes should be notified. These should help Member States to build the necessary trust in each other's electronic identification schemes and to mutually recognise and accept electronic identification means falling under their notified schemes. The principle of mutual recognition and acceptance should apply if the notifying Member State meets the conditions of notification and the notification was published in the Official Journal of the European Union. However, the access to these online services and their final delivery to the applicant should be closely linked to the right to receive such services under the conditions set by national legislation.

(14) Member States should be able to decide to involve the private sector in the issuance of electronic identification means and to allow the private sector the use of electronic identification means under a notified scheme for identification purposes when needed for online services or electronic transactions. The possibility to use such electronic identification means would enable the private sector to rely on electronic identification and authentication already largely used in many Member States at least for public services and to make it easier for businesses and citizens to access their online services across borders. In order to facilitate the use of such electronic identification means across borders by the private sector, the authentication possibility provided by the

[21] OJ L 88, 4.4.2011, p. 45

Member States should be available to relying parties without discriminating between public or private sector.

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

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

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

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

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

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

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

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

(23) In line with the obligations under the UN Convention on the Rights of Persons with Disabilities that has entered into force in the EU, persons with disabilities should be able to use trust services and end user products used in the provision of those services on equal bases with other consumers.

(24) A trust service provider is a controller of personal data and therefore has to comply with the obligations set out in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the

processing of personal data and on the free movement of such data[22]. In particular the collection of data should be minimised as much as possible taking into account the purpose of the service provided.

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

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

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

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

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

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

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

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

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

(34) To facilitate the supervision of qualified trust services providers, for example when a provider is providing its services in the territory of another Member State and is not

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

subject to supervision there, or when the computers of a provider are located in the territory of another Member State than the one where it is established, a mutual assistance system between supervisory bodies in the Member States should be set up.

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

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

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

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

(39) While a high level of security is needed to ensure mutual recognition of electronic signatures, in specific cases, such as in the context of Commission Decision 2009/767/EC of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the 'points of single contact' under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market[23], electronic signatures with a lower security assurance should also be accepted.

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

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

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

elements should make qualified electronic signature validation easy and convenient for all parties at Union level.

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

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

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

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

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

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

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

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

particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level.

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

(51) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission, in particular for specifying reference numbers of standards which use would give a presumption of compliance with certain requirements laid down in this Regulation or defined in delegated acts. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers[24].

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

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

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

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter

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

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

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

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

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

Article 2

Scope

1. This Regulation applies to electronic identification provided by, on behalf or under the responsibility of Member States and to trust service providers established in the Union.

2. This Regulation does not apply to the provision of electronic trust services based on voluntary agreements under private law.

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

Article 3

Definitions

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

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

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

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

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

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

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

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

(a) it is uniquely linked to the signatory;

(b) it is capable of identifying the signatory;

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

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

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

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

(10) ‘certificate’ means an electronic attestation which links electronic signature or seal validation data of a natural or a legal person respectively to the certificate and confirms those data of that person;

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

(12) ‘trust service’ means any electronic service consisting in the creation, verification, validation, handling and preservation of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic delivery services, website authentication, and electronic certificates, including certificates for electronic signature and for electronic seals;

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

(14) ‘trust service provider’ means a natural or a legal person who provides one or more trust services;

(15) ‘qualified trust service provider’ means a trust service provider who meets the requirements laid down in this Regulation;

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

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

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

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

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

(21) ‘advanced electronic seal’ means an electronic seal which meets the following requirements:

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

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

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

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

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

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

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

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

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

(27) ‘electronic document’ means a document in any electronic format;

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

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

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

(31) ‘validation data’ means data which are used to validate an electronic signature or an electronic seal.

Article 4

Internal market principle

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

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

CHAPTER II

ELECTRONIC IDENTIFICATION

Article 5

Mutual recognition and acceptance

When an electronic identification using an electronic identification means and authentication is required under national legislation or administrative practice to access a service online, any electronic identification means issued in another Member State falling under a scheme included in the list published by the Commission pursuant to the procedure referred to in Article 7 shall be recognised and accepted for the purposes of accessing this service.

Article 6

Conditions of notification of electronic identification schemes

1. Electronic identification schemes shall be eligible for notification pursuant to Article 7 if all the following conditions are met:

(a) the electronic identification means are issued by, on behalf of or under the responsibility of the notifying Member State;

(b) the electronic identification means can be used to access at least public services requiring electronic identification in the notifying Member State;

(c) the notifying Member State ensures that the person identification data are attributed unambiguously to the natural or legal person referred to in Article 3 point1;

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

(e) the notifying Member State takes liability for:

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

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

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

Article 7

Notification

1. Member States which notify an electronic identification scheme shall forward to the Commission the following information and without undue delay, any subsequent changes thereof:

(a) a description of the notified electronic identification scheme;

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

(c) information on by whom the registration of the unambiguous person identifiers is managed;

(d) a description of the authentication possibility;

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

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

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

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

Article 8

Coordination

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

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

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

CHAPTER III

TRUST SERVICES

Section 1

General provisions

Article 9

Liability

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

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

Article 10

Trust services providers from third countries

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

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

Article 11

Data processing and protection

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

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

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

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

Article 12

Accessibility for persons with disabilities

Trust services provided and end user products used in the provision of those services shall be made accessible for persons with disabilities whenever possible.

Section 2

Supervision

Article 13

Supervisory body

1. Member States shall designate an appropriate body established in their territory or, upon mutual agreement, in another Member State under the responsibility of the designating Member State. Supervisory bodies shall be given all supervisory and investigatory powers that are necessary for the exercise of their tasks.

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

(a) monitoring trust service providers established in the territory of the designating Member State to ensure that they fulfil the requirements laid down in Article 15;

(b) undertaking supervision of qualified trust service providers established in the territory of the designating Member State and of the qualified trust services they provide in order to ensure that they and the qualified trust services provided by them meet the applicable requirements laid down in this Regulation;

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

3. Each supervisory body shall submit a yearly report on the last calendar year's supervisory activities to the Commission and Member States by the end of the first quarter of the following year. It shall include at least:

(a) information on its supervisory activities;

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

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

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

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

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

Article 14

Mutual assistance

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

2. A supervisory body to which a request for assistance is addressed may not refuse to comply with it unless:

(a) it is not competent to deal with the request; or

(b) compliance with the request would be incompatible with this Regulation.

3. Where appropriate, supervisory bodies may carry out joint investigations in which staff from other Member States' supervisory bodies is involved.

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

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

Article 15

Security requirements applicable to trust service providers

1. Trust service providers who are established in the territory of the Union shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. Having regard to state of the art, these measures shall ensure that the level of security is appropriate to the degree of risk. In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of adverse effects of any incidents.

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

2. Trust service providers shall, without undue delay and where feasible not later than 24 hours after having become aware of it, notify the competent supervisory body, the competent national body for information security and other relevant third parties such as data protection authorities of any breach of security or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained therein.

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

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

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

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

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

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

Article 16

Supervision of qualified trust service providers

1. Qualified trust service providers shall be audited by a recognised independent body once a year to confirm that they and the qualified trust services provided by them fulfil the requirements set out in this Regulation, and shall submit the resulting security audit report to the supervisory body.

2. Without prejudice to paragraph 1, the supervisory body may at any time audit the qualified trust service providers to confirm that they and the qualified trust services provided by them still meet the conditions set out in this Regulation, either on its own initiative or in response to a request from the Commission. The supervisory body shall inform the data protection authorities of the results of its audits, in case personal data protection rules appear to have been breached.

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

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

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

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

Article 17

Initiation of a qualified trust service

1. Qualified trust service providers shall notify the supervisory body of their intention to start providing a qualified trust service and shall submit to the supervisory body a security audit report carried out by a recognised independent body, as provided for in Article 16(1). Qualified trust service providers may start to provide the qualified trust service after they have submitted the notification and security audit report to the supervisory body.

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

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

The supervisory body shall indicate the qualified status of the qualified service providers and the qualified trust services they provide in the trusted lists after the positive conclusion of the verification, not later than one month after the notification has been done in accordance with paragraph 1.

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

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

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

Article 18

Trusted lists

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

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

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

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

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

6. The Commission may, by means of implementing acts, define the technical specifications and formats for trusted lists applicable for the purposes of paragraphs 1 to 4. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

Article 19

Requirements for qualified trust service providers

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

Such information shall be verified by the qualified service provider or by an authorised third party acting under the responsibility of the qualified service provider:

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

(b) remotely, using electronic identification means under a notified scheme issued in compliance with point (a).

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

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

(b) bear the risk of liability for damages by maintaining sufficient financial resources or by an appropriate liability insurance scheme;

(c) before entering into a contractual relationship, inform any person seeking to use a qualified trust service of the precise terms and conditions regarding the use of that service;

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

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

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

– only authorised persons can make entries and changes,

– information can be checked for authenticity;

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

(g) record for an appropriate period of time 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. Such recording may be done electronically;

(h) have an up-to-date termination plan to ensure continuity of service in accordance with arrangements issued by the supervisory body under point (c) of Article 13(2);

(i) ensure lawful processing of personal data in accordance with Article 11.

3. Qualified trust service providers issuing qualified certificates shall register in their certificate database the revocation of the certificate within ten minutes after such revocation has taken effect.

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

5. The Commission may, by means of implementing acts, establish reference numbers of standards for trustworthy systems and products. Compliance with the requirements laid down in Article 19 shall be presumed where trustworthy systems and products meet those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2). The Commission shall publish those acts in the *Official Journal of the European Union*.

Section 3

Electronic signature

Article 20

Legal effects and acceptance of electronic signatures

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

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

3. Qualified electronic signatures shall be recognised and accepted in all Member States.

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

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

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

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

Article 21

Qualified certificates for electronic signature

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

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

3. If a qualified certificate for electronic signature has been revoked after initial activation, it shall lose its validity, and its status shall not in any circumstances be reverted by renewing its validity.

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

5. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified certificates for electronic signature. Compliance with the requirements

laid down in Annex I shall be presumed where a qualified certificate for electronic signature meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2). The Commission shall publish those acts in the *Official Journal of the European Union*.

Article 22

Requirements for qualified electronic signature creation devices

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

2. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified electronic signature creation devices. Compliance with the requirements laid down in Annex II shall be presumed where a qualified electronic signature creation device meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2). The Commission shall publish those acts in the *Official Journal of the European Union.*

Article 23

Certification of qualified electronic signature creation devices

1. Qualified electronic signature creation devices may be certified by appropriate public or private bodies designated by Member States provided that they have been submitted to a security evaluation process carried out in accordance with one of the standards for the security assessment of information technology products included in a list that shall be established by the Commission by means of implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2). The Commission shall publish those acts in the *Official Journal of the European Union.*

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

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

Article 24

Publication of a list of certified qualified electronic signature creation devices

1. Member States shall notify to the Commission without undue delay, information on qualified electronic signature creation devices which have been certified by the bodies referred to in Article 23. They shall also notify to the Commission, without undue delay, information on electronic signature creation devices that would no longer be certified.

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

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

Article 25

Requirements for the validation of qualified electronic signatures

1. A qualified electronic signature shall be considered as valid provided that it can be established with a high level of certainty, that at the time of signing:

(a) the certificate, that supports the signature, is a qualified electronic signature certificate complying with the provisions laid down in Annex I;

(b) the qualified certificate required is authentic and valid;

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

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

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

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

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

(h) the requirements provided for in Article 3 point7 are met;

(i) the system used for validating the signature provides to the relying party the correct result of the validation process and allows the relying party to detect any security relevant issues.

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

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

Article 26

Qualified validation service for qualified electronic signatures

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

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

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

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

Article 27

Preservation of qualified electronic signatures

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

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

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

Section 4

Electronic seals

Article 28

Legal effects of electronic seal

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

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

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

4. If an electronic seal security assurance level below the qualified electronic seal is required, in particular by a Member State for accessing a service online offered by a public sector body

on the basis of an appropriate assessment of the risks involved in such a service, all electronic seals matching at a minimum the same security assurance level shall be accepted.

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

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

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

Article 29

Requirements for qualified certificates for electronic seal

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

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

3. If a qualified certificate for an electronic seal has been revoked after initial activation, it shall lose its validity, and its status shall not in any circumstances be reverted by renewing its validity.

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

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

Article 30

Qualified electronic seal creation devices

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

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

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

Article 31

Validation and preservation of qualified electronic seals

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

Section 5

Electronic time stamp

Article 32

Legal effect of electronic time stamps

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

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

3. A qualified electronic time stamp shall be recognised and accepted in all Member States.

Article 33

Requirements for qualified electronic time stamps

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

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

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

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

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

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

Section 6

Electronic documents

Article 34

Legal effects and acceptance of the electronic documents

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

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

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

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

Section 7

Qualified electronic delivery service

Article 35

Legal effect of an electronic delivery service

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

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

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

Article 36

Requirements for qualified electronic delivery services

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

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

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

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

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

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

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

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

Section 8

Website authentication

Article 37

Requirements for qualified certificates for website authentication

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

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

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

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

CHAPTER IV

DELEGATED ACTS

Article 38

Exercise of the delegation

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

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

3. The delegation of power referred to in Articles 8(3), 13(5), 15(5), 16(5), 18(5), 20(6), 21(4), 23(3), 25(2), 27(2), 28(6), 29(4), 30(2), 31, 35(3) and 37(3) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

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

5. A delegated act adopted pursuant to Articles 8(3), 13(5), 15(5), 16(5), 18(5), 20(6), 21(4), 23(3), 25(2), 27(2), 28(6), 29(4), 30(2), 31, 35(3) and 37(3) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

CHAPTER V

IMPLEMENTING ACTS

Article 39

Committee procedure

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

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

CHAPTER VI

FINAL PROVISIONS

Article 40

Report

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

Article 41

Repeal

1. Directive 1999/93/EC is repealed.

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

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

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

Article 42

Entry into force

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

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

Done at Brussels,

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

ANNEX 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 registration number as stated in the official records,
- for a natural person: the person's name;

(c) a set of data unambiguously representing the signatory to whom the certificate is issued including at least the name of the signatory or a pseudonym, which shall be identified as such;

(d) electronic signature validation data which correspond to the electronic signature creation data;

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

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

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

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

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

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

ANNEX II

Requirements for qualified signature creation devices

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

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

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

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

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

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

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

4. Qualified trust service providers managing electronic signature creation data on behalf of the signatory may duplicate the electronic signature creation data 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 registration number as stated in the official records,
- for a natural person: person's name;

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

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

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

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

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

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

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

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

ANNEX IV

Requirements for qualified certificates for website authentication

Qualified certificates for website authentication shall contain:

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

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

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

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

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

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

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

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

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

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

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

LEGISLATIVE FINANCIAL STATEMENT

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

This financial statement details the requirements in terms of administrative expenditure in order to implement the proposed Regulation on *electronic identification and trust services for electronic transactions in the internal market*.

Following the legislative procedure and discussion for the adoption by the EP and the Council of the proposed Regulation, twelve FTE will be required by the Commission to devise the related delegated and implementing acts, to ensure the availability of organisational and technical standards, to handle the information notified by Member States, in particular to maintain the information related to trusted lists, to ensure the awareness of stakeholders – in particular citizens and SMEs - of the advantages of using electronic identification, authentication, signature and related trust services (eIAS) and to engage discussions with third countries in view of achieving eIAS interoperability at global level.

1.1. Title of the proposal/initiative

Commission proposal for a Regulation on electronic identification and trust services for electronic transactions in the internal market

1.2. Policy area(s) concerned in the ABM/ABB structure[25]

09 INFORMATION SOCIETY

1.3. Nature of the proposal/initiative

☐ The proposal/initiative relates to **a new action**

☐ The proposal/initiative relates to **a new action following a pilot project/preparatory action**[26]

☐ The proposal/initiative relates to **the extension of an existing action**

☑ The proposal/initiative relates to **an action redirected towards a new action**

1.4. Objectives

1.4.1. The Commission's multiannual strategic objective(s) targeted by the proposal/initiative

The general objectives of the proposal are those of general EU policies in which the proposal situates, such as the EU 2020 Strategy. It aims to ensure that Europe would 'be turned into a smart, sustainable and inclusive economy delivering high levels of employment, productivity and social cohesion.'

25 ABM: Activity-Based Management – ABB: Activity-Based Budgeting.

26 As referred to in Article 49(6)(a) or (b) of the Financial Regulation.

1.4.2. Specific objective(s) and ABM/ABB activity(ies) concerned

To enhance trust in pan-European electronic transactions and to ensure cross-border legal recognition of electronic identification, authentication, signature and related trust services as well as a high level of data protection and user empowerment in the single market (see Digital Agenda for Europe, key actions 3 and 16).

ABM/ABB activity(ies) concerned

09 02 - Regulatory framework for the Digital Agenda for Europe

1.4.3. Expected result(s) and impact

Specify the effects which the proposal/initiative should have on the beneficiaries/groups targeted.

Establish a clear regulatory environment for eIAS services that would boost user convenience, trust and confidence in the digital world.

1.4.4. Indicators of results and impact

Specify the indicators for monitoring implementation of the proposal/initiative.

1. Existence of eIAS suppliers that have activities in multiple EU Member States:

2. Degree to which devices become inter-operational (e.g. smartcard readers) between sectors and countries;

3. Usage of eIAS by all categories of population;

4. Extent to which eIAS are used by end-users for national transactions and international (cross-border) transactions;

5. Degree of harmonization across Members States of eIAS legislation;

6. Electronic identification schemes notified to the Commission;

7. Services accessible with notified electronic identification means in the public sector (e.g. eGovernment, eHealth, eJustice, eProcurement);

8. Services accessible with notified electronic identification means in the private sector (e.g. online banking, eCommerce, eGambling, login to websites, safer internet services).

1.5. Grounds for the proposal/initiative

1.5.1. Requirement(s) to be met in the short or long term

The divergent national implementations of the electronic signature Directive due its to different interpretations by Member States lead to cross-border interoperability problems and thus to a segmented EU landscape and distortions in the internal market. This is accompanied by a lack of trust and confidence in electronic systems which impede European citizens to benefit from the same kind of services in the digital world as in the physical world.

1.5.2. Added value of EU involvement

Action at EU level would produce clear benefits compared with action at the level of Member States. Experience has shown indeed that national measures are not only insufficient to make electronic transactions possible across borders, but they have on the contrary created barriers to the EU-wide interoperability of electronic signatures, and that they are currently having the same effect for electronic identification, authentication and related trust services.

1.5.3. Lessons learned from similar experiences in the past

The proposal builds on the experience with e-signature Directive and the problems encountered due to fragmented transposition and implementation of that Directive, which have blocked it from achieving its objectives.

1.5.4. Coherence and possible synergy with other relevant instruments

The electronic signature Directive is referenced through several other EU initiatives which have been set up to eliminate interoperability challenges and cross border recognition and acceptance issues related to certain types of electronic interactions, e.g., the Services Directive, the Public Procurement Directives, the revised VAT (e-invoicing) Directive or the European Citizen Initiative Regulation. Moreover, the proposed Regulation will provide a legal framework beneficial for the wide take-up of the Large Scale Pilots (LSPs) have been put in place at the EU level to support the development of interoperable and trustworthy means of electronic communication (including SPOCS, supporting the implementation of the Services Directive; STORK, supporting the development and use of interoperable eIDs; PEPPOL, supporting the development and use of interoperable eProcurement solutions; epSOS, supporting the development and use of interoperable eHealth solutions; eCodex, supporting the development and use of interoperable eJustice solutions).

1.6. Duration and financial impact

☐ Proposal/initiative of **limited duration**

– ☐ Proposal/initiative in effect from [DD/MM]YYYY to [DD/MM]YYYY

– ☐ Financial impact from YYYY to YYYY

☑ Proposal/initiative of **unlimited duration**

1.7. Management mode(s) envisaged[27]

☑ **Centralised direct management** by the Commission

☐ **Centralised indirect management** with the delegation of implementation tasks to:

[27] Details of management modes and references to the Financial Regulation may be found on the BudgWeb site: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

– ☐ executive agencies

– ☐ bodies set up by the Communities[28]

– ☐ national public-sector bodies/bodies with public-service mission

– ☐ persons entrusted with the implementation of specific actions pursuant to Title V of the Treaty on European Union and identified in the relevant basic act within the meaning of Article 49 of the Financial Regulation

☐ **Shared management** with the Member States

☐ **Decentralised management** with third countries

☐ **Joint management** with international organisations ***(to be specified)***

If more than one management mode is indicated, please provide details in the "Comments" section.

Comments

[//]

[28] As referred to in Article 185 of the Financial Regulation.

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

Specify frequency and conditions.

The first evaluation will take place 4 years after the entry into force of the Regulation. An explicit clause on report, by which the Commission will report to the European Parliament and the Council on its application, is included in the regulation. Subsequent reports will be submitted every 4 years thereafter. The Commission methodology on evaluation will be applied. These evaluations will be conducted with the help of targeted studies on the implementation of the legal instruments, questionnaires to national authorities, expert discussions, workshops, Eurobarometer surveys, and so forth.

2.2. Management and control system

2.2.1. Risk(s) identified

An Impact Assessment has been carried to accompany the proposal for the Regulation. The new legal instrument will provide for mutual recognition and acceptance of electronic identification across borders, improve the current electronic signature framework, strengthening national supervision of trust service providers and give legal effect and recognition to related trust services. It also introduces the use of delegated and implementing acts as a mechanism to ensure flexibility vis-à-vis technological developments.

2.2.2. Control method(s) envisaged

Existing control methods applied by the Commission will cover the additional appropriations.

2.3. Measures to prevent fraud and irregularities

Specify existing or envisaged prevention and protection measures.

Existing fraud prevention measures applied by the Commission will cover the additional appropriations.

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

- Existing expenditure budget lines

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number [Description……...…….]	Diff./non-diff. (29)	from EFTA[30] countries	from candidate countries[31]	from third countries	within the meaning of Article 18(1)(aa) of the Financial Regulation
5	09. 01 01 01 Expenditure related to staff in active employment in the DG Information Society and Media	Non-diff.	NO	NO	NO	NO
5	09. 01 02 01 External staff	Non-diff.	NO	NO	NO	NO

29 Diff. = Differentiated appropriations / Non-diff. = Non-Differentiated Appropriations

30 EFTA: European Free Trade Association.

31 Candidate countries and, where applicable, potential candidate countries from the Western Balkans.

3.2. Estimated impact on expenditure

3.2.1. Summary of estimated impact on expenditure

Heading of multiannual financial framework:	Number	[Heading 1. **Smart and Inclusive Growth** ……...……]

DG: INFSO			Year **2014**	Year **2015**	Year **2016**	Year **2017**	Year 2018	**Year 2019**	**Year 2020**	**TOTAL**
• Operational appropriations										
Number of budget line- N.A.	Commitments	(1)	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
	Payments	(2)	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
Number of budget line -N.A.	Commitments	(1a)	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
	Payments	(2a)	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
Appropriations of an administrative nature financed from the envelope for specific programmes[32]			0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
Number of budget line		(3)	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
TOTAL appropriations for DG INFSO	Commitments	=1+1a +3	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
	Payments	=2+2a +3	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**

Heading of multiannual financial	**5**	" Administrative expenditure "

[32] Technical and/or administrative assistance and expenditure in support of the implementation of EU programmes and/or actions (former "BA" lines), indirect research, direct research.

framework:		

EUR million (to 3 decimal places)

		Year **2014**	Year **2015**	Year **2016**	Year **2017**	Year **2018**	Year **2019**	Year **2020**	**TOTAL**
		DG: INFSO							
• Human resources		1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**
• Other administrative expenditure									
TOTAL DG INFSO	Appropriations	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

TOTAL appropriations under HEADING 5 of the multiannual financial framework	(Total commitments = Total payments)	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

EUR million (to 3 decimal places)

		Year **2014**	Year **2015**	Year **2016**	Year **2017**	Year **2018**	Year **2019**	Year **2020**	**TOTAL**
TOTAL appropriations under HEADINGS 1 to 5 of the multiannual financial framework	Commitments	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**
	Payments	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

3.2.2. Estimated impact on operational appropriations

– ☑ The proposal/initiative does not require the use of operational appropriations

– ☐ The proposal/initiative requires the use of operational appropriations, as explained below:

3.2.3. Estimated impact on appropriations of an administrative nature

3.2.3.1. Summary

– ☐ The proposal/initiative does not require the use of administrative appropriations

– ☑ The proposal/initiative requires the use of administrative appropriations, as explained below:

EUR million (to 3 decimal places)

	Year **N 2014**	Year **2015**	Year **2016**	Year **2017**	Year **2018**	Year **2019**	Year **2020**	**TOTAL**
HEADING 5 of the multiannual financial framework								
Human resources	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**
Other administrative expenditure								
Subtotal HEADING 5 of the multiannual financial framework	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

Outside HEADING 5[33] of the multiannual financial framework								
Human resources								
Other expenditure of an administrative nature								
Subtotal outside HEADING 5 of the multiannual financial framework								

TOTAL	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

[33] Technical and/or administrative assistance and expenditure in support of the implementation of EU programmes and/or actions (former "BA" lines), indirect research, direct research.

3.2.3.2. Estimated requirements of human resources

– ☐ The proposal/initiative does not require the use of human resources

– ☑ The proposal/initiative requires the use of human resources, as explained below:

Estimate to be expressed in full amounts (or at most to one decimal place)

	Year **2014**	Year **2015**	Year **2016**	Year **2017**	Year **2018**	Year **2019**	Year **2020**
• Establishment plan posts (officials and temporary agents)							
09 01 01 01 (Headquarters and Commission's Representation Offices)	9	9	9	9	9	9	9
XX 01 01 02 (Delegations)							
XX 01 05 01 (Indirect research)							
10 01 05 01 (Direct research)							
• External personnel (in Full Time Equivalent unit: FTE)[34]							
09 01 02 01 (CA, INT, SNE from the "global envelope")	3	3	3	3	3	3	3
XX 01 02 02 (CA, INT, JED, LA and SNE in the delegations)							
XX 01 04 ***yy*** [35] - at Headquarters[36]							
XX 01 04 ***yy*** [35] - in delegations							
XX 01 05 02 (CA, INT, SNE - Indirect research)							
10 01 05 02 (CA, INT, SNE - Direct research)							
Other budget lines (specify)							
TOTAL	**12**	**12**	**12**	**12**	**12**	**12**	**12**

The human resources required will be met by staff from the DG who are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

Description of tasks to be carried out:

Officials and temporary agents	Manage the legislative procedures for the adoption by the EP and the Council of the planned Regulation and related delegated / implementing acts. Priority Areas: 1. Establishment of a new legislative framework on electronic trust services 2. Fostering take-up of electronic trust services by raising SME and citizens awareness on their potential 3. Follow-up of Directive 1999/93/EC including international aspects 4. Leveraging the large scale pilots to accelerate the concrete realisation of the objective of the new legislative framework.
External personnel	Idem as above

34 CA= Contract Agent; INT= agency staff ("*Intérimaire*"); JED= "*Jeune Expert en Délégation*" (Young Experts in Delegations); LA= Local Agent; SNE= Seconded National Expert;

35 Under the ceiling for external personnel from operational appropriations (former "BA" lines).

36 Essentially for Structural Funds, European Agricultural Fund for Rural Development (EAFRD) and European Fisheries Fund (EFF).

3.2.4. Compatibility with the current multiannual financial framework

– ☑ Proposal/initiative is compatible the current multiannual financial framework.

– ☐ Proposal/initiative will entail reprogramming of the relevant heading in the multiannual financial framework.

Explain what reprogramming is required, specifying the budget lines concerned and the corresponding amounts.

– ☐ Proposal/initiative requires application of the flexibility instrument or revision of the multiannual financial framework[37].

Explain what is required, specifying the headings and budget lines concerned and the corresponding amounts.

3.2.5. Third-party contributions

– ☑ The proposal/initiative does not provide for co-financing by third parties

– ☐ The proposal/initiative provides for the co-financing estimated below:

3.3. Estimated impact on revenue

– ☑ Proposal/initiative has no financial impact on revenue.

– ☐ Proposal/initiative has the following financial impact:

- ☐ on own resources
- ☐ on miscellaneous revenue

[37] See points 19 and 24 of the Interinstitutional Agreement.