Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

CHAPTER III

TRUST SERVICES

SECTION 1

General provisions

Article 13

Liability and burden of proof

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

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

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

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

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

Article 14

International aspects

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

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

a the requirements applicable to qualified trust service providers established in the Union and the qualified trust services they provide are met by the trust service providers in

the third country or international organisations with which the agreement is concluded, and by the trust services they provide;

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

Article 15

Accessibility for persons with disabilities

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

Article 16

Penalties

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

SECTION 2

Supervision

Article 17

Supervisory body

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7 The Commission shall make the annual report referred to in paragraph 6 available to Member States.

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

Article 18

Mutual assistance

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

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

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

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

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

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

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

Article 19

Security requirements applicable to trust service providers

1 Qualified and non-qualified trust service providers shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk. In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of the adverse effects of any such incidents.

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

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

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

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

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

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

a further specify the measures referred to in paragraph 1; and

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

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

SECTION 3

Qualified trust services

Article 20

Supervision of qualified trust service providers

1 Qualified trust service providers shall be audited at their own expense at least every 24 months by a conformity assessment body. The purpose of the audit shall be to confirm that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in this Regulation. The qualified trust service providers shall submit the resulting conformity assessment report to the supervisory body within the period of three working days after receiving it.

2 Without prejudice to paragraph 1, the supervisory body may at any time audit or request a conformity assessment body to perform a conformity assessment of the qualified trust service providers, at the expense of those trust service providers, to confirm that they and the qualified trust services provided by them fulfil the requirements laid down in this Regulation. Where personal data protection rules appear to have been breached, the supervisory body shall inform the data protection authorities of the results of its audits.

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

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

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

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

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

Article 21

Initiation of a qualified trust service

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

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

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

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

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

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

Article 22

Trusted lists

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

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

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

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

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

Article 23

EU trust mark for qualified trust services

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

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

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

Article 24

Requirements for qualified trust service providers

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

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

a by the physical presence of the natural person or of an authorised representative of the legal person; or

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

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

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

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

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

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

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

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

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

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

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

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

(iii) the data can be checked for authenticity;

g take appropriate measures against forgery and theft of data;

h record and keep accessible for an appropriate period of time, including after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service provider, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. Such recording may be done electronically;

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

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

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

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

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

5 The Commission may, by means of implementing acts, establish reference numbers of standards for trustworthy systems and products, which comply with the requirements under points (e) and (f) of paragraph 2 of this Article. Compliance with the requirements laid down in this Article shall be presumed where trustworthy systems and products meet those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

SECTION 4

Electronic signatures

Article 25

Legal effects of electronic signatures

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

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

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

Article 26

Requirements for advanced electronic signatures

An advanced electronic signature shall meet the following requirements:

(a) it is uniquely linked to the signatory;

(b) it is capable of identifying the signatory;

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

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

Article 27

Electronic signatures in public services

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

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

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

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

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

Article 28

Qualified certificates for electronic signatures

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

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

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

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

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

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

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

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

Article 29

Requirements for qualified electronic signature creation devices

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

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

Article 30

Certification of qualified electronic signature creation devices

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

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

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

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

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

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

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

Article 31

Publication of a list of certified qualified electronic signature creation devices

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

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

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

Article 32

Requirements for the validation of qualified electronic signatures

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

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

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

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

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

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

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

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

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

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

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

Article 33

Qualified validation service for qualified electronic signatures

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

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

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

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

Article 34

Qualified preservation service for qualified electronic signatures

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

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

SECTION 5

Electronic seals

Article 35

Legal effects of electronic seals

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

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

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

Article 36

Requirements for advanced electronic seals

An advanced electronic seal shall meet the following requirements:

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

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

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

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

Article 37

Electronic seals in public services

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

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

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

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

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

Article 38

Qualified certificates for electronic seals

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

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

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

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

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

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

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

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

Article 39

Qualified electronic seal creation devices

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

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

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

Article 40

Validation and preservation of qualified electronic seals

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

SECTION 6

Electronic time stamps

Article 41

Legal effect of electronic time stamps

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

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

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

Article 42

Requirements for qualified electronic time stamps

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

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

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

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

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

SECTION 7

Electronic registered delivery services

Article 43

Legal effect of an electronic registered delivery service

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

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

Article 44

Requirements for qualified electronic registered delivery services

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

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

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

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

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

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

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

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

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

SECTION 8

Website authentication

Article 45

Requirements for qualified certificates for website authentication

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

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