Commission Implementing Decision (EU) 2016/650

of 25 April 2016

laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 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 COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to 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, and in particular Articles 30(3) and 39(2) thereof,

Whereas:

(1) Annex II to Regulation (EU) No 910/2014 sets out the requirements for qualified electronic signature creation devices and qualified electronic seal creation devices.

(2) The task of drawing up the technical specifications needed for the production and placing on the market of products, taking into account the current stage of technology, is carried out by organisations competent in the standardisation area.

(3) ISO/IEC (International Organisation for Standardization/International Electrotechnical Commission) establishes the general concepts and principles of IT security and specifies the general model of assessment to be used as the basis for evaluation of security properties of IT products.

(4) The European Committee for Standardisation (CEN) has developed, under the standardisation mandate M/460 given by the Commission, standards for qualified electronic signature and seals creation devices, where the electronic signature creation data or electronic seal creation data is held in an entirely but not necessarily exclusively user-managed environment. These standards are considered suitable for the assessment of conformity of such devices with the relevant requirements set out in Annex II to Regulation (EU) No 910/2014.

(5) Annex II to Regulation (EU) No 910/2014 sets that only a qualified trust service provider can manage electronic signature creation data on behalf of a signatory. Security requirements and their respective certification specifications are different when the signatory physically possesses a product and when a qualified trust service provider operates on behalf of the signatory. To address both situations as well as to favour the development over time of products and assessment standards suitable to particular needs, the Annex to this Decision should list standards covering both situations.

(6) At the time this Commission Decision has been adopted, several trust service providers already offer solutions managing electronic signature creation data on behalf of their customers. Certifications of products are currently limited to the hardware security modules certified against different standards but are not yet certified specifically against the requirements for qualified signature and seal creation devices. Nevertheless, published standards, such as EN 419 211 (applicable to electronic signature created in an entirely but not necessarily exclusively user-managed environment) do not yet exist for an equally important market of certified remote products. Since standards that might be appropriate for such purposes are currently under development, when such standards are available and assessed as compliant with the requirements set out in Annex II to Regulation (EU) No 910/2014, the Commission will complement this Decision. Until the moment where the list of such standards is established, an alternative process can be used for the assessment of the conformity of such products under the conditions provided for under point (b) of Article 30(3) of Regulation (EU) No 910/2014.

(7) The Annex lists EN 419 211 which consists of different parts (1 to 6) covering different situations. EN 419 211 Part 5 and 419 211 Part 6 give extensions related to the qualified signature creation device environment, such as communication with trusted signature creation applications. Product manufacturers are free to apply such extensions. According to recital 56 of Regulation (EU) No 910/2014, the scope of certification under Articles 30 and 39 of that Regulation is limited to protecting the signature creation data and signature creation applications are excluded from the scope of the certification.

(8) To ensure that the electronic signatures or seals generated by a qualified signature or seal creation device are reliably protected against forgery, as required by Annex II to Regulation (EU) No 910/2014, suitable cryptographic algorithms, key lengths and hash functions are the prerequisite for the security of the certified product. Since this matter has not been harmonised at European level, Member States should cooperate to agree on cryptographic algorithms, key lengths and hash functions to be used in the field of electronic signatures and seals.

(9) The adoption of the present Decision renders Commission Decision 2003/511/EC obsolete. It should therefore be repealed.

(10) The measures provided for in this Decision are in accordance with the opinion of the Committee referred to in Article 48 of Regulation (EU) No 910/2014,

HAS ADOPTED THIS DECISION:

Article 1

1. The standards for the security assessment of information technology products that apply to the certification of qualified electronic signature creation devices or qualified electronic seal creation devices according to point (a) of Article 30(3) or 39(2) of Regulation (EU) No 910/2014, where the electronic signature creation data or electronic seal creation data is held in an entirely but not necessarily exclusively user-managed environment are listed in the Annex to this Decision.

2. Where a qualified trust service provider manages the electronic signature creation data or electronic seal creation data on behalf of a signatory or of a creator of a seal, the certification of such products shall be based on a process that, pursuant to Article 30(3)(b), uses security levels comparable to those required by Article 30(3)(a).

Article 2

Decision 2003/511/EC is hereby repealed.

Article 3

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

Done at Brussels, 25 April 2016.

ANNEX

LIST OF STANDARDS REFERRED TO IN ARTICLE 1(1)

- ISO/IEC 15408 — Information technology — Security techniques — Evaluation criteria for IT security, Parts 1 to 3 as listed below:

    - ISO/IEC 15408-1:2009 — Information technology — Security techniques — Evaluation criteria for IT security — Part 1. ISO, 2009.

    - ISO/IEC 15408-2:2008 — Information technology — Security techniques — Evaluation criteria for IT security — Part 2. ISO, 2008.

    - ISO/IEC 15408-3:2008 — Information technology — Security techniques — Evaluation criteria for IT security — Part 3. ISO, 2008,

  and

- ISO/IEC 18045:2008: Information technology — Security techniques — Methodology for IT security evaluation,

  and

- EN 419 211 — Protection profiles for secure signature creation device, Parts 1 to 6 — as appropriate — as listed below:

    - EN 419211-1:2014 — Protection profiles for secure signature creation device — Part 1: Overview

    - EN 419211-2:2013 — Protection profiles for secure signature creation device — Part 2: Device with key generation

    - EN 419211-3:2013 — Protection profiles for secure signature creation device — Part 3: Device with key import

    - EN 419211-4:2013 — Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application

    - EN 419211-5:2013 — Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted channel to signature creation application

    - EN 419211-6:2014 — Protection profiles for secure signature creation device — Part 6: Extension for device with key import and trusted channel to signature creation application