Rulebook on manner of assessing compliance of qualified devices for creating electronic signatures and electronic seals and on content of list of certified qualified devices for creating electronic signatures and electronic seals

The Rulebook is published in the Official Gazette of Montenegro No. 53/2018 and 20/2020.

Article 1

This Rulebook shall regulate the manner of assessing compliance of qualified devices for creating electronic signatures and electronic seals with requirements referred to in Article 19 of the Law on Electronic identification and Electronic Signature (hereinafter: the Law) and on content of list of certified qualified devices for creating electronic signatures and electronic seals.

Article 2

The compliance of qualified devices for creating electronic signatures and electronic seals with requirements referred to in Article 19 of the Law shall be assessed based on documentation on compliance with standards set forth in the Annex of this Rulebook (Annex 1).

Article 3

The documentation referred to in Article 2 of this Rulebook shall be submitted to the state administration authority responsible for electronic administration and electronic business by a legal or natural person entered in the register of qualified electronic trust service providers in accordance with the Law (hereinafter: electronic trust service provider) i.e. public authority referred to in Article 4, paragraph 4 of the Law, along with the request for compliance assessment referred to in Article 1 of this Rulebook.

The request referred to in paragraph 1 of this Article shall contain the following information:

1) registered name, i.e. name and surname of the electronic trust service provider, i.e. public authority referred to in Article 4, paragraph 4 of the Law;
2) data on the qualified device for creating an electronic signature, i.e. electronic seal (manufacturer, model and version);
3) the beginning of validity of the qualified device for creating an electronic signature, i.e. an electronic seal;
4) validity period of the qualified device for making the electronic signature, i.e. electronic seal;
5) indication of the qualified device for which the request is submitted (QSCD, SSCD);
6) data on the documentation referred to in Article 2 of this Rulebook.

Article 4

The list of certified qualified devices for creating an electronic signature, i.e. electronic seal shall contain:

1) registered name, i.e. name and surname of the electronic trust service provider, i.e. public authority referred to in Article 4, paragraph 4 of the Law;
2) data on the qualified device for creating an electronic signature, i.e. electronic seal (manufacturer, model and version);
3) certification date of the qualified device for creating an electronic signature, i.e. electronic seal;
4) the date of placing the device for creating a qualified electronic signature, i.e. a qualified electronic seal on the list;
5) the validity period of the qualified device for creating the electronic signature, i.e. the electronic seal;
6) indication of the qualified device for which the application is submitted (QSCD, SSCD);
7) data on the documentation referred to in Article 2 of this Rulebook

Article 5

This Rulebook shall enter into force on the eight day of its publishing in the Official Gazette of Montenegro.

ANNEX 1

1. ISO / IEC 15408 - Information technology - Security techniques – Evaluation criteria for information technology security, Parts 1 to 3 as follows bellow:

- ISO/IEC 15408 – 1:2009 - Information technology - Security techniques – Evaluation criteria for information technology security, - Part 1 ISO 2009,
- ISO/IEC 15408 - 2:2008 - Information technology - Security techniques – Evaluation criteria for information technology security, - Part 2 ISO 2008,
- ISO/IEC 15408 - 3:2008 - Information technology - Security techniques – Evaluation criteria for information technology security, - Part 3 ISO 2008;

2. ISO/IEC 18045:2008: Information technology — Security techniques — Methodology for IT security evaluation; and

3. ETSI EN 419 211 - Protection Profiles for Secure Signature Creation Devices, Parts 1 to 6 - namely:

- EN 419211 - 1:2014 - Protection Profiles for Secure Signature Creation Devices - Part 1: Overview,
- EN 419211 - 21:2014 - Protection Profiles for Secure Signature Creation Devices - Part 2 Device with key generation,
- EN 419211 - 31:2014 - Protection Profiles for Secure Signature Creation Devices - Part 3 Device with key import,
- EN 419211 - 41:2014 - Protection Profiles for Secure Signature Creation Devices - Part 4 Extension for device with key generation and trusted communication with certificate generation application,
- EN 419211 - 51:2014 - Protection Profiles for Secure Signature Creation Devices - Part 5 Extension for device with key generation and trusted communication with signature creation application and
- EN 419211 - 61:2014 - Protection Profiles for Secure Signature Creation Devices - Part 6 Extension for device with key import and trusted communication with certificate signature creation application.