* 312, 075 227 125

Official Gazette number: 35/2020

Official Gazette publication date: 11.02.2020

Constitutional Court Resolution number (U.no.): /

**MINISTRY OF INFORMATION SOCIETY AND ADMINISTRATION**

Pursuant to Article 40 paragraph (1), Article 44, Article 45 paragraph (3), Article 47 paragraph (3) and Article 48 paragraph (2) of the Law on Electronic Documents, Electronic Identification and Trust Services (\*) (“Official Gazette of Republic of North Macedonia” no. 101/19 and 275/19), the Minister of Information Society and Administration adopted the following

**RULEBOOK ON SETTING THE STANDARDS WHICH SHOULD BE CONTAINED IN THE QUALIFIED CERTIFICATES FOR ELECTRONIC SIGNATURE AND ELECTRONIC SEAL, THE MEETING OF THE TECHNICAL STANDARDS, THE METHOD OF CREATING QUALIFIED ELECTRONIC SIGNATURES OR QUALIFIED ELECTRONIC SEALS, THE STANDARDS WHICH SHOULD BE CONTAINED IN THE CERTIFICATES FOR VALIDATION OF QUALIFIED ELECTRONIC SIGNATURE OR QUALIFIED ELECTRONIC SEAL AND THE STANDARDS WHICH SHOULD BE MET BY THE QUALIFIED TRUST SERVICE FOR STORAGE OF QUALIFIED ELECTRONIC SIGNATURES OR QUALIFIED ELECTRONIC SEALS**

**Article 1**

The Rulebook herein shall prescribe the standards which should be contained in the qualified certificates for electronic signature and electronic seal, the meeting of the technical standards, the method of creating qualified electronic signatures or qualified electronic seals, the standards which should be contained in the certificates for validation of qualified electronic signature or qualified electronic seal and the standards which should be met by the qualified trust service for preservation of qualified electronic signatures or qualified electronic seals.

**Article 2**

The standards which should be contained in the qualified certificates for electronic signature and the qualified certificates for electronic seal shall be as follows:

- ETSI EN 319 412-1 and

- ETSI EN 319 412- 5.

Apart from the standards referred to in paragraph 1 of this Article which should be contained in the qualified certificates for electronic signature, the qualified certificates issued to natural persons should also contain the ETSI EN 319 412-2 standard.

Apart from the standards referred to in paragraph 1 of this Article which should be contained in the qualified certificates for electronic signature or for electronic seal issued to legal entities, the qualified certificates should also contain the ETSI EN 319 412-3 standard.

The qualified certificates for electronic signature shall contain the following:

(a) Indicator in a form suitable for automatic processing, showing that the certificate was issued as qualified certificate for electronic signature;

(b) Sum of data which unequivocally represent the qualified trust service provider who issued the qualified certificate for electronic signature:

- For the legal entity: Name and registration number of the legal entity;

- For natural person: Name of the person;

(c) Clearly specified name or nickname of the signatory, if nickname is being used;

(d) Data for validation of the electronic signature corresponding to the data for creating the electronic signature;

(e) Information on the beginning and the end of the validity period of the qualified certificate;

(f) Identification code of the certificate, unique for the qualified trust service provider;

(g) Advanced electronic signature or advanced electronic seal of the qualified trust service provider who issued the certificate;

(h) Location of the certificate supporting the advanced electronic signature or the advanced electronic seal specified in item (g), without any compensation;

(i) Location of the services where request can be sent for checking the status of qualified certificate validity;

(j) When the data for creating electronic signature are linked with the data for validation of the electronic signature, they are found in the mean for creating qualified electronic signature and specified accordingly in a form suitable for automatic processing.

The qualified certificates for electronic signature shall contain the following:

(a) Indicator in a form suitable for automatic processing, showing that the certificate was issued as qualified certificate for electronic seal;

(b) Sum of data which unequivocally represent the qualified trust service provider who issued the qualified certificate for electronic seals:

-  For the legal entity: Name and registration number of the legal entity;

-  For natural person: Name of the person;

(c) Name of the creator of the electronic seal and personal identification number of the person;

(d) Data for validation of the electronic seal corresponding to the data for creating the electronic seal;

(e) Information on the beginning and the end of the validity period of the qualified certificate;

(f) Identification code of the certificate, unique for the qualified trust service provider;

(g) Advanced electronic signature or advanced electronic seal of the qualified trust service provider who issued the certificate;

(h) Location of the certificate supporting the advanced electronic signature or the advanced electronic seal specified in item (g), without any compensation;

(i) Location of the services where request can be sent for checking the status of qualified certificate validity;

(j) When the data for creating electronic signature are linked with the data for validation of the electronic signature, they are found in the mean for creating qualified electronic signature and specified accordingly in a form suitable for automatic processing.

The qualified certificates for electronic seals issued to the legal entities performing payment operations should meet ETSI TS 119 495 standard.

**Article 3**

The qualified certificates for electronic signature and the qualified certificates for electronic seal should be issued by a qualified trust service provider and meet the technical standards:

-  ETSI EN 319 401;

-  ETSI EN 319 411-1;

-  ETSI EN 319 411-2; and

-  ETSI TR 119 411-4.

**Article 4**

The means for creating qualified electronic signature, via suitable technical and procedural measures, should meet the following standards:

(a) Secure validation of the data for creating electronic signature;

(b) Unique data for creating electronic signature;

(c) Data for creating electronic signature are not available without the electronic signature and it is protected from forgery by using the available technology;

(d) The signatory may safely protect the data for creating electronic signature from other persons.

The means for creating qualified electronic signature are unable to change the data on which the electronic signature should be put and the signatory may see the data prior to the signing.

The creation and management of the data for creating electronic signature on behalf of the signatory should be solely done by the qualified trust service provider who issues the electronic signature.

The qualified trust service providers managing data for creating electronic signature on behalf of the signatory may multiply the data for creating electronic signature solely for the purpose of backup, such as:

(a) The security of the multiple data is on the same level as the security of the original data;

(b) The number of multiplied data does not exceed the minimum necessary for ensuring service continuity.

**Article 5**

The means for creating qualified electronic signature and qualified electronic seal when the data for creating electronic signature or electronic seal are kept in their entirety, but not strictly managed by the user, shall be deemed secure information technology products, if the following standards are met:

a) ISO / IEC 15408 - Information technology – Security techniques - IT security evaluation criteria, Parts 1 through 3, as specified below:

1. ISO / IEC 15408-1: 2009 - Information technology – Security techniques - IT security evaluation criteria, Part 1, ISO, 2009;

2. ISO / IEC 15408-2: 2008 - Information technology – Security techniques - IT security evaluation criteria, Part 2, ISO, 2008;

3. ISO / IEC 15408-3:2008 - Information technology – Security techniques – IT security evaluation criteria, Part 3, ISO, 2008; and

b) ISO / IEC 18045: 2008: Information technology – Security techniques -

IT security evaluation methodology; and

c) EN 419 211 – Protection of profiles for secure creating of mean for electronic signature, Parts 1 through 6 – as specified below:

1. EN 419211-1: 2014 - Protection of profiles for secure creating of mean for electronic signature - Part 1: Review;

2. EN 419211-2: 2013 - Protection of profiles for secure creating of mean for electronic signature - Part 2: Mean with creation token;

3. EN 419211-3: 2013 - Protection of profiles for secure creating of mean for electronic signature - Part 3: Mean with incorporating a token;

4. EN 419211-4: 2013 - Protection of profiles for secure creating of mean for electronic signature - Part 4: Upgrade of the mean with creation token and trust source for certification of the creating application;

5. EN 419211-5: 2013 - Protection of profiles for secure creating of mean for electronic signature - Part 5: Upgrade of the mean with creation token and trust source for certification of the application for creating electronic signature;

6. EN 419211-6: 2014 - Protection of profiles for secure creating of mean for electronic signature - Part 6: Upgrade of the mean with incorporating a token and trust source of the application for creating electronic signature;

In the event when the qualified electronic signature or the qualified electronic seal is created in a manner suitable for remote signing or printing, the systems used for creating thereof should meet the following standards:

-  CEN EN 419 241-1;

-  CEN prEN 419 241-2; and

-  CEN EN 419 221-5.

The qualified trust service provider issuing qualified electronic signature or qualified electronic seal used for signing or remote signing, should meet the following standards:

-  ETSI TS 119 431-1;

-  ETSI TS 119 431-2; and

- ETSI TS 119 432.

In the event when the qualified electronic signature or the qualified electronic seal is created in a manner suitable for mechanical format professing, the following technical standards should be met:

-  ETSI TS 119 172-2 for HML format for signing or printing; and

-  ETSI TS 119 172-3 for ASN.1 format for signing or printing.

**Article 6**

The certificate for validation of qualified electronic signature and for validation of qualified electronic seal should be issued in accordance with ETSI TS 119 102-2 standard.

The qualified trust service provider, for the purpose of validation of qualified electronic signature and for validation of qualified electronic seal, should meet the ETSI TS 119 441 standard and implement the protocol for validation of qualified electronic signature determined with ETSI TS 119 442 standard.

**Article 7**

The qualified trust service – keeping qualified electronic signatures or qualified electronic seals should meet the following standards:

- ETSI TS 119 511; and

- ETSI TS 119 512.

**Article 8**

The creating of the electronic signature and validating thereof should be in accordance with ETSI TR 119 100 standard.

The policies and security requirements which should be met by the applications for creating electronic signature and validating thereof should be in accordance with ETSI TS 119 101 standard.

The cryptographic packages containing electronic signatures should be in accordance with ETSI TS 119 312 standard.

The use of cryptographic packages should be in accordance with the instructions specified with ETSI TR 119 300 standard.

**Article 9**

In the event when advanced electronic signature supported by qualified certificate is required, the advanced electronic signature in XML, CMS or PDF format shall be used:

-   At basic conformity level; or

-   Verified with electronic timestamp; or

-   Electronic signature containing long-term data; or

-   Accompanying electronic signature packages, when such signatures are in accordance with the technical standards determined with Articles 13 and 14 of the Rulebook herein.

**Article 10**

In the event when advanced electronic seal supported by qualified certificate is required, the advanced electronic seal in XML, CMS or PDF format shall be used:

-   At basic conformity level; or

-   Verified with electronic timestamp; or

-   Electronic seal containing long-term data; or

-   Accompanying electronic seal packages, when such seals are in accordance with the technical standards determined with Articles 13 and 14 of the Rulebook herein.

**Article 11**

The following standards should be met for advanced electronic signatures in XML, CMS or PDF format and the accompanying signature packages:

-   ETSI TS 103171 v.2.1.1 standard shall apply to the XadES basic profile;

-   ETSI TS 103173 v.2.2.1 standard shall apply to the CadES basic profile;

-   ETSI TS 103172 v.2.2.2 standard shall apply to the PadES basic profile.

Advanced electronic signatures should be created by using procedures determined with ETSI EN 319 102-1 standard.

The validation of advanced electronic signatures should be in accordance with the procedures determined with ETSI EN 319 102-1 standard.

**Article 12**

The accompanying package of the electronic signature should meet ETSI TS 103174 v.2.2.1 standard.

**Article 13**

The following standards should be met for advanced electronic seals in XML, CMS or PDF format and the accompanying seal packages:

-   ETSI TS 103171 v.2.1.1 standard shall apply to the XadES basic profile;

-   ETSI TS 103173 v.2.2.1 standard shall apply to the CadES basic profile;

-   ETSI TS 103172 v.2.2.2 standard shall apply to the PadES basic profile.

**Article 14**

The accompanying package of the electronic seal should meet ETSI TS 103174 v.2.2.1 standard.

**Article 15**

The Rulebook herein shall enter into force on the next day as of the day of publishing thereof in the “Official Gazette of the Republic of North Macedonia”.

|  |  |
| --- | --- |
|  No. 11/1-964/1       |  Minister of Information |
|   10 February 2020  | Society and Administration |
|     Skopje              |  **Damjan Mancevski** |