Rulebook on measures and activities for protection of certificate for electronic signature and electronic seal

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

Article 1

The electronic trust service provider and public authorities referred to in Article 4 of the Law on Electronic Identification and Electronic Signature shall apply organisational and technical measures for the protection of a certificate for electronic signature and a certificate for electronic seal and data related to signatory and creator of electronic seal, and establish and apply a system of protection of access to records of certificates and revoked and suspended certificates and which shall enable access only to authorised persons and which provides verification of the accuracy of data transfer and timely insight into possible errors of technical means in accordance with standards prescribed by this Rulebook.

Article 2

Terms used in this Rulebook shall have the following meanings:

1) signatory is a natural person signing on its behalf or on behalf of a natural or legal person by using data for electronic signature creation;

2) creator of a electronic seal is a legal person or public authority who uses an electronic seal by using data for electronic signature creation seal;

3) certificate for electronic seal is an electronic attestation that links electronic seal validation data to a legal person or a public authority and confirms the name of that legal person or public authority;

4) certificate for electronic signature is a document in electronic form signed by the electronic trust service provider, which links date for verification of electronic signature to a person and confirms the identity of that person.

Article 3

Measures and activities referred to in Article 1 of this Rulebook are as follows:

1) general measures and activities contained in the standard ETSI EN 319 401, Electronic Signatures and Infrastructures (ESI); General Requirements for Trust Service Providers;

2) measures to protect schemes for services of issuance of certificates for electronic signature, electronic seal and website authentication, contained in the following standards:

- ETSI EN 319 411-1, Electronic Signatures and Infrastructures (ESI); Policy and safety/security requirements for Service Providers issuing certificates: General requirements,
- ETSI EN 319 411-2, Electronic Signatures and Infrastructures (ESI); Policy and safety/security requirements for Service Providers issuing certificates: Requirements for Service Providers issuing qualified EU certificates,
- ETSI EN 319 412-1, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and Common Data Structures,
- ETSI EN 319 412-2, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons,
- ETSI EN 319 412-3, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons,
- ETSI EN 319 412-4, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for Website Certificates,
- ETSI EN 319 412-5, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: Qualified Certificate Statement;

3) measures to protect schemes for electronic time stamp issuance services, contained in the following standards:

- ETSI EN 319 421, Electronic Signatures and Infrastructures (ESI); Policy and safety/security requirements for Service Providers issuing electronic time stamp,
- ETSI EN 319 422, Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles;

4) measures to protect schemes for verification service and electronic signatures and electronic seals preservation service, contained in the following standards:

- ETSI EN 319 122-1, Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures,
- ETSI EN 319 122-2, Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures,
- ETSI TS 119 122-3, Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 3: Incorporation of Evidence Record Syntax in CAdES,

- ETSI EN 319 132-1, Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures,
- ETSI EN 319 132-2, Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; - Part 2: Extended XAdES signatures,
- ETSI EN 319 142-1, Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building Blocks and PAdES baseline signatures,
- ETSI EN 319 142-2, Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles,
- ETSI TS 119 142-3, Electronic Signatures and Infrastructures (ESI); ETSI TS 119 142-3 PAdES digital signatures; Part 3: PAdES Document Time-stamp digital signatures (PAdES-DTS),
- ETSI EN 319 162-1, Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers,
- ETSI EN 319 162-2, Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 2: Additional ASiC containers,
- ETSI EN 319 102-1, Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation,
- ETSI TS 119 172-1, Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents;

5) Cryptographic data protection measures, in accordance with the following standards:

- ETSI TR 119 300, Electronic Signatures and Infrastructures (ESI); Guidance on the use of standards for cryptographic suites,
- ETSI TS 119 312, Electronic Signatures and Infrastructures (ESI); Cryptographic suites.

Article 4

On the day this Rulebook enters into force the Rulebook on measures and procedures of protection of certificates and data related to signatories (Official Gazette of Montenegro number 61/11) and the Rulebook on protection measures of electronic signature and advanced electronic signatures (Official Gazette of Montenegro number 61/11) shall be repealed.

Article 5

This Rulebook shall enter into force on the eighth day from the day of its publication in the Official Gazette of Montenegro.