Pursuant to Article 48, paragraph 4 ad Article 49, paragraph 2 of the Law on Electronic Document, Electronic Identification and Trust Services in Electronic Business (Official Gazette of the RS, No. 94/17),

The Minister of Trade, Tourism and Telecommunications is hereby passing the following

RULEBOOK

on validation of qualified electronic signatures and qualified electronic seals

"Official Gazette of the RS", No. 43 of June 19, 2019

Scope of the Rulebook

Article 1

This Rulebook shall prescribe requirements for qualified electronic signature and qualified electronic seal validation procedure and requirements for qualified validation service provision for the qualified electronic signature and qualified electronic seal in more detail.

Meanings of individual terms

Article 2

Individual terms within the meaning of this Rulebook shall have the following meanings:

1) *a qualified validation service* shall be the common name for the qualified validation service for qualified electronic signatures and for the qualified validation service for qualified electronic seals;

2) *a validation application* shall be a software product within which validation of electronic signature and/or seal is technically implemented;

3) *a driving application* shall be a software product that uses a validation application to perform validation of a qualified electronic signature and/or seal;

4) *validation status* shall be the end result of validation that is produced by the validation application and returned to the driving application;

5) *a validation report* shall be a report on validation that the validation application delivers to the driving application and through it to the relying party in order to enable inspection of the reasons for the resulting relevant validation status.

Validation application and driving application

Article 3

The system referred to in Article 48, paragraph 2 of the Law on Electronic Document, Electronic Identification and Trust Services in Electronic Business (hereinafter: the Law) that is used for validation of a qualified electronic signature and/or seal shall include a validation application, within which validation is technically implemented, and a driving application through which the relying party initiates validation and obtains the validation status and the validation report.

The technical implementation of validation referred to in paragraph 1 of this Article must be in conformity with the requirements referred to in the Law.

The validation application and the driving application must be in compliance with the requirements from the ETSI EN 319 102-1 standard "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation" that pertains to signature validation and to the requirements from the ETSI TS 119 172-4 standard "Electronic Signatures and Infrastructures (ESI); Signature policies; Part 4: Signature validation policy for European qualified electronic signatures/seals using trusted lists" which apply mutatis mutandis to the Trusted Lists of qualified trust services.

Validation status

Article 4

The validation status can have one of the following three values: "passed", "indeterminate" and "failed".

The "passed" validation status means that all the cryptographic checks of the signature and/or seal succeeded, as well as all other checks are in compliance with the validation rules referred to in Article 3, paragraph 2 of this Rulebook have been passed.

The "indeterminate" validation status means that not all the requirements for the "passed" validation status have been fulfilled, where there is a possibility that conditions will be met for the "passed" validation status based on additional facts that were considered to be unknown during the course of the validation procedure.

The "failed" validation status means that neither the requirements for the "passed" validation status, nor the requirements for the "indeterminate" validation status have been fulfilled.

The validation application can enable that additional requirements are stated through the driving application whereby facts of relevance for validation are specified in cases where without such facts the validation status would be "indeterminate".

Where the standards referred to in this Rulebook are applied, requirements pertaining to the statuses marked in the standards with "TOTAL-PASSED", "INDETERMINATE" and "TOTAL-FAILED", in that order shall apply to the validation statuses "passed",

“indeterminate” and “failed”.

Application of ETSI TS 119 441 standard

Article 5

The qualified validation service shall be carried out in compliance with the requirements from the ETSI TS 119 441 standard “Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services” (hereinafter: ETSI TS 119 441) that pertain to the qualified validation service, including the requirements from other standards which are directly and indirectly referred to in that standard, relevant international standards and recommendations and/or other standards, documents and recommendations relating to provision of qualified validation service determined by this Rulebook.

Qualified validation service policy and qualified validation service practice statement

Article 6

The policy of the qualified validation service (hereinafter: the validation service policy) shall define requirements that the qualified validation service should fulfil, while the practice statement for provision of qualified validation service (hereinafter: the validation service practice statement) shall define operational procedures aimed at fulfilling these requirements, i.e. the manner in which the qualified validation service provider fulfils the technical, organisational and procedural business requirements specified in the validation policy.

The validation service policy shall be defined independently from the specific operating environment of the qualified validation service provider, while the validation service practice statement shall provide a detailed description of the organisational structure, operating procedures, as well as the physical and computer environment of the qualified validation service provider.

Requirements to be fulfilled by the validation service policy and the validation service practice statement

Article 7

The validation service policy and the validation service practice statement must be in conformity with the provisions of the Law, provisions of the regulations passed on the basis of the Law, as well as with the requirements from the standards prescribed to be applied by these regulations.

The validation service policy should comply with the requirements from the ETSI TS 119 441 standard, including the requirements from other standards referred to directly and indirectly in that standard, which are relating to the signature validation service policy.

The validation service practice statement should comply with the requirements from the ETSI TS 119 441 standard, including the requirements from other standards referred to directly and indirectly in that standard, which are relating to the signature validation service practice statement.

Supported electronic signature and/or seal formats

Article 8

The qualified validation service shall mandatorily support the electronic signature and/or seal formats that are in conformity with the requirements referred to in Article 4, paragraph 2 of the Rulebook on the requirements for procedures and technological solutions used during reliable electronic document preservation (Official Gazette of the RS, No. 94/18).

Technical communication protocol

Article 9

The qualified validation service should enable the use of the service through the validation protocol in conformity with the ETSI TS 119 442 standard “Electronic Signatures and Infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital signature validation services”.

User interface

Article 10

In addition to the use of the service in the manner referred to in Article 9 of this Rulebook, the qualified validation service can include the user interface through which the service can be used and in such a case the user interface, in addition to displaying the validation status, should:

1) present the result of the cryptographic check of the signature and/or of the seal (hereinafter: verification) in the manner that is understandable to the user;

2) enable, at the request of the user, summary display of the validation results in the form understandable to the user;

3) enable displaying of the validation report;

4) in the case of an electronic signature validation, enable displaying of the identity of the signatory, including:

(1) the name and surname or pseudonym of the signatory, where in case where the pseudonym is stated, a clear indication must be provided that it is a pseudonym,

(2) UCIN i.e. the records number for a foreigner, where it is included in the certificate,

(3) the numbers of travel documents, where they are included in the certificate,

(4) other attributes of the field “Subject” from the certificate that are not included among information from subitems (1) through (3) of this item, if any,

(5) the signed attributes, if any,

(6) the name of the qualified electronic certificate issue service provider that has issued the certificate;

5) in the case of electronic seal validation, enable displaying the identity of the creator of the seal, including:

(1) the name and/or the full business name of the creator of the seal,

(2) the registration number of the creator of the seal, where it is included in the certificate,

(3) the tax identification number of the creator of the seal, where it is included in the certificate,

(4) other attributes of the field “Subject” from the certificate that are not covered by data referred to in subitems (1) through (3) of this item, if any,

(5) signed attributes, if any,

(6) the name of the qualified electronic certificate issue service provider that has issued the certificate;

6) display a note that the verification has been performed in compliance with the verification rules of the qualified electronic signature and/or seal in accordance with the regulations of the Republic of Serbia;

7) display a note on additional requirements specifying the facts of relevance for validation referred to in Article 4, paragraph 5 of this Rulebook, where such additional requirements exist;

8) be in conformity with the provisions of the ETSI TS 119 101 standard “Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation” relating to the user interface.

Article 11

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

Number 110-00-39/2019-12

In Belgrade, on June 1, 2019

The Minister,

Rasim Ljajić, PhD., own signature