Pursuant to Article 43, paragraph 3 of the Law on Electronic Document, Electronic Identification and Trust Services in Electronic Business (Official Gazette of the RS, number 94/17),

The Minister of Trade, Tourism and Telecommunications has passed the following

RULEBOOK

on the mandatory requirements for qualified electronic certificates

I. INTRODUCTORY PROVISIONS

Article 1

This Rulebook shall lay down the requirements that the qualified electronic certificates for electronic signature, electronic seal and website authentication must conform to.

Article 2

The qualified electronic certificates for electronic signature, electronic seal and website authentication must conform to the relevant international standards and recommendations, i.e. to other standards, documents and recommendations, which are related to the format and contents of electronic certificates.

The provider of the qualified electronic certificate issuance service (hereinafter: the certificate issuer) shall issue the qualified electronic certificates in compliance with the recommendation ITU X.509 and documents ETSI EN 319 412-1 “Electronic Signatures and Infrastructures (ESI) – Certificate Profiles – Part 1: Overview and common data structures” and IETF RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”.

Article 3

The qualified electronic certificate shall mandatorily contain one or multiple statements that the certificate is used as a qualified electronic certificate (field ”qcStatements”) in accordance with document ETSI EN 319 412-5 “Electronic Signatures and Infrastructures (ESI) – Certificate Profiles – Part 5: QCStatements” based on the document IETF RFC 3739 “Internet X.509 Public Key Infrastructure: Qualified Certificates Profile”, in compliance with the certificate issuance policy applied by the certificate issuer and the requirements laid down by this Rulebook for individual certificate types.

Article 4

The certificate issuer shall issue the qualified electronic certificates in compliance with the certificate issuance policy which is applicable to certificate issuing, by creating an advanced electronic signature or an advanced electronic seal on the basis of their own asymmetric private key.

The selection of algorithm of the advanced electronic signature should be made in compliance with the document ETSI TS 119 312 “Electronic Signatures and Infrastructures (ESI) – Cryptographic Suites”.

The qualified electronic certificate shall mandatorily contain the indication of the provider’s policy that has been applied to certificate issuance.

Article 5

The qualified electronic certificate shall mandatorily contain the exact time of certificate issuance.

II. QUALIFIED ELECTRONIC CERTIFICATES FOR ELECTRONIC SIGNATURE

Article 6

The qualified electronic certificate for electronic signature shall mandatorily have the contents in compliance with Article 43 of the Law on Electronic Document, Electronic Identification and Trust Services in Electronic Business (Official Gazette of the RS, No. 94/17 – hereinafter: the Law) in the part thereof pertaining to the certificate for electronic signature and the signatory.

The certificate issuer shall issue the qualified electronic certificates for electronic signature in compliance with the document ETSI EN 319 412-2 "Electronic Signatures and Infrastructures (ESI) – Certificate Profiles – Part 2: Certificate profile for certificates issued to natural persons".

Article 7

The field "Subject" of the qualified electronic certificate for electronic signature shall include a set of attributes that is uniquely identifying the signatory, and at the minimum:

1) The attribute "countryName" that contains a two letter code for the country in accordance with the EN ISO 3166-1:2013 standard "Codes for the representation of names of countries and their subdivisions – Part 1: Country codes", with the meaning that is defined in the policy of the service provider of certificate issuance;

2) Both the attributes "givenName" and "surname" that shall contain the full given name and surname of the signatory in the state order, where the certificate does not include the pseudonym, i.e. only the "pseudonym" attribute, which shall include the pseudonym, where the pseudonym is used in the certificate;

3) The attribute "commonName" which begins with the values of the attributes "givenName" and "surname" separated by a space where the certificate does not include a pseudonym, i.e. with the value of the attribute "pseudonym" where the pseudonym is used in the certificate;

4) One or multiple attributes "serialNumber" which contain identification of the signatory in accordance with the format from the ETSI EN 319 412-1 document "Electronic Signatures and Infrastructures (ESI) – Certificate Profiles – Part 1: Overview and common data structures", section 5.1.3.

The attribute "commonName" must not end in 13 or more successive numeric characters and must not end in a hyphen followed by two letter characters and a series of numeric characters.

The attributes "givenName", "surname", "pseudonym" and "commonName" shall mandatorily be presented in UTF8String encoding is such a manner that all the letters are faithfully presented by adequate characters.

The attribute "serialNumber" shall be presented in PrintableString encoding in accordance with ASN.1 specification in compliance with the IETF RFC 5280 document.

The attribute “serialNumber” referred to in this Article as defined in accordance with the ITU-T X.520 document shall present a part of the unique name of the signatory in the field “Subject” and shall be different from the field “serialNumber” of the certificate. The field “serialNumber” of the certificate shall mandatorily contain the serial number of the qualified electronic certificate, which is unique within the issuer of the qualified electronic certificate in compliance with Article 43 of the Law, presented as a positive whole number presented in accordance with the IETF RFC 5280 document.

Article 8

Where the signatory has requested in the application for certificate issuance that the certificate contains UCIN and where the certificate contains UCIN, the certificate issuer shall enter UCIN in one of the attributes “serialNumber” only from the field “Subject” in the manner specified in the ETSI EN 319 412-1 document, section 5.1.3, for the reference type “PNO” and specifically in the format: three letter PNO code (according to the ASCII encoding sequence 80, 78, 79), followed by the two letter country code RS (according to the ASCII encoding sequence 82, 83), hyphen (45 according to the ASCII encoding) and at the end the UCIN of the signatory.

Article 9

Where the qualified electronic certificate for electronic signature contains one or multiple numbers of the travel document of the signatory, each number of the travel document shall be entered in one of the attributes “serialNumber” from the field “Subject” in the manner specified in the ETSI EN 319 412-1 document, section 5.1.3 for the reference of “PAS” type and specifically in the format: three letter PAS code (according to the ASCII encoding sequence 80, 65, 83), two letter country code of the issuer of the travel document in accordance with the EN ISO 3166-1:2013 standard presented by the ASCII characters, hyphen (45 according to the ASCII encoding) and at the end the number of the travel document of the signatory.

Where multiple attributes with the travel document number appear in the qualified electronic certificate for electronic signature, the country code of the issuer of the travel document must be unique in each one of them.

Where the qualified electronic certificate for electronic signature contains the number of the travel document, the certificate issuer shall be obliged to ensure by means of the certificate issuance policy that the certificate is not be valid after the expiry date of either one of the travel documents the numbers of which are contained in the certificate.

Article 10

The qualified electronic certificates for electronic signature that include the UCIN or the number of the travel document of the signatory must not be made publicly accessible by the certificate issuer, except where the consent from the signatory has been provided for that.

Article 11

In the field “Subject”, the qualified electronic certificates for electronic signature may also contain additional “serialNumber” attributes in accordance with one of the schemes from the ETSI EN 319 412-1 standard, section 5.1.3 including the locally defined schemes.

The use of the local schemes “CA:” (according to the ASCII encoding sequence 67, 65, 58) and “SN:”

(according to the ASCII encoding sequence 83, 78, 58) with two letter country code RS shall be reserved for the needs of the certificate issuer in the manner and where provided for in the policy of the certificate issuer.

Article 12

In the field "qcStatements", the qualified electronic certificate for electronic signature shall mandatorily contain the predefined "qcStatement-2" statement according to the IETF RFC 3739 document that shall include the semantic identifier "id-etsi-qcs-semanticsId-Natural" which is determined in the ETSI EN 319 412-1 standard, section 5.1.2.

Where in the qualified electronic certificate for electronic signature one or more "serialNumber" attributes appear according to a scheme reserved for the needs of the issuer, the "qcStatement-2" statement shall mandatorily contain the list "nameRegistrationAuthorities" and in that list the reference to the policy of the issuer or to another document that defines the semantics of the local scheme, in compliance with the ETSI EN 319 412-1 standard, section 5.1.3.

Article 13

The field "Subject" of a qualified electronic certificate for electronic signature may include other attributes as well which are, for example, relating the signatory with the legal person or another organisation, all in compliance with this Rulebook and the policy of the issuer.

In the field "Subject", attributes "countryName" and "commonName" shall appear once only.

Article 14

The field "Key Usage" of a qualified electronic certificate for electronic signature must include the "Non-Repudiation" i.e. "contentCommitment" bit.

Article 15

In the field "Certificate Policies", the qualified electronic certificate for electronic signature shall mandatorily include at least the QCP-n-qscd policy identifier in compliance with the ETSI EN 319 411-2 document "Electronic Signatures and Infrastructures (ESI) – Policy and security requirements for Trust Service Providers issuing certificates – Part 2: Requirements for trust service providers issuing EU qualified certificates", section 4.2.5.

Article 16

In the field "qcStatements", the qualified electronic certificate for electronic signature shall mandatorily include the QcCompliance, QcSSCD statements and the QcType statement with "id- etsi-qcs-esign" identifier, in accordance with the ETSI EN 319 412-5 document.

III. QUALIFIED ELECTRONIC CERTIFICATES FOR ELECTRONIC SEAL

Article 17

The qualified electronic certificates for electronic seal shall mandatorily have the contents in compliance with Article 43 of the Law in the part thereof pertaining to the certificate for electronic

seal and for the creator of the seal.

Where the creator of the seal is a legal person or a natural person in the capacity of a registered entity, the certificate issuer shall issue the qualified electronic certificates for electronic seal in compliance with the ETSI EN 319 412-3 document "Electronic Signatures and Infrastructures (ESI) – Certificate Profiles – Part 3: Certificate profile for certificates issued to legal persons".

Where the creator of the seal is a natural person, the name from the Article 43, paragraph 1, item 3, subitem 2 of the Law shall include the capacity in which the person presents themselves, which shall be evidenced by means of the public document issued on the basis of the law.

Provisions of this Rulebook pertaining to the natural person in the capacity of a registered entity shall apply *mutatis mutandis* in the case referred to in paragraph 3 of this Article.

Article 18

The field "Subject" of the qualified electronic certificate for electronic seal shall contain the set of attributes that are uniquely identifying the creator of the seal, and at the minimum:

1) The attribute "countryName" that contains the two letter code of the country in accordance with the EN ISO 3166-1:2013 standard in which the creator of the seal is registered;

2) The attribute "organizationName" that contains the name and/or the full business name of the creator of the seal;

3) The attribute "commonName" that begins with the value of the attribute "organizationName".

The qualified electronic certificate for electronic seal must not contain the attributes "givenName" and "surname" in the field "Subject".

Article 19

The field "Subject" of the qualified electronic certificates for electronic seal may include one or multiple attributes "organizationIdentifier" which shall include identification of the creator of the seal according to the format from the ETSI EN 319 412-1 document "Electronic Signatures and Infrastructures (ESI) – Certificate Profiles – Part 1: Overview and common data structures", section 5.1.4.

Where the creator of the seal has the registration number that was allocated to the creator of the seal by the Statistical Office of the Republic of Serbia (registration number), the field "Subject" shall mandatorily contain the "organizationIdentifier" attribute according to the ETSI EN 319 412-1 document, section 5.1.4 for the reference of the local scheme "MB:" and specifically in the format: MB code: (according to the ASCII encoding sequence 77, 66, 58), followed by the two letter country code RS (according to the ASCII encoding sequence 82, 83), hyphen (45 according to the ASCII encoding) and the registration number at the end.

Where the creator of the seal has the tax identification number (TIN) that was allocated to the creator of the seal by the competent tax authority, the field "Subject" shall mandatorily contain "organizationIdentifier" attribute according to the ETSI EN 319 412-1 document, section 5.1.4 for the reference of the "VAT" type and specifically in the format: three letter VAT code (according to ASCII

encoding sequence 86, 65, 84), followed by the two letter country code RS (according to ASCII encoding sequence 82, 83), hyphen (45 according to ASCII encoding) and the TIN at the end.

Article 20

In the field “qcStatements”, the qualified electronic certificates for electronic seal shall mandatorily contain the predefined statement “qcStatement-2” in accordance with the IETF RFC 3739 document which shall include the semantic identifier “id-etsi-qcs-semanticsId-Legal” as determined in the ETSI EN 319 412-1 standard, section 5.1.2.

Where the qualified electronic certificates for electronic seal contain the registration number, the “qcStatement-2” statement shall mandatorily contain the “nameRegistrationAuthorities” list and in that list the reference to the issuer’s policy or to another document referring to this Rulebook and to the semantics of the local scheme “MB:”, in compliance with the ETSI EN 319 412- 1 standard, section 5.1.4.

Article 21

Attributes “commonName” and “organizationName” shall mandatorily be presented in the UTF8String encoding so that all the letters are faithfully represented by adequate characters.

Article 22

The field “Subject” of the qualified electronic certificates for electronic seal may additionally contain other attributes, all in compliance with this Rulebook and the policy of the issuer.

In the field “Subject”, attributes “countryName” and “commonName” shall appear once only.

Article 23

The field “Key Usage” of the qualified electronic certificates for electronic seal must include “Non-Repudiation” i.e. “contentCommitment” bit.

Article 24

In the field “Certificate Policies”, the qualified electronic certificates for electronic seal shall mandatorily contain at least the policy identifier QCP-l-qscd in compliance with the ETSI EN 319 411-2 document “Electronic Signatures and Infrastructures (ESI) – Policy and security requirements for Trust Service Providers issuing certificates – Part 2: Requirements for trust service providers issuing EU qualified certificates”, section 4.2.5.

Article 25

In the field “qcStatements”, the qualified electronic certificates for electronic seal shall mandatorily contain the QcCompliance, QcSSCD statements and the QcType statement with “id- etsi-qcs-seal” identifier, all in accordance with the ETSI EN 319 412-5 document.

IV. QUALIFIED ELECTRONIC CERTIFICATES FOR WEBSITE AUTHENTICATION

Article 26

The qualified electronic certificate for website authentication shall mandatorily have the contents in compliance with Article 59 of the Law.

The certificate issuer shall issue the qualified electronic certificate for website authentication in compliance with the ETSI EN 319 412-4 document "Electronic Signatures and Infrastructures (ESI) – Certificate Profiles – Part 4: Certificate profile for web site certificates".

Article 27

The contents of the qualified electronic certificate for website authentication that the certificate issuer issues to legal persons, natural persons or to the natural persons as registered entities must be in compliance with the document CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates".

The contents of the qualified electronic certificate for website authentication with extended validation that the certificate issuer issues to the legal persons or to the natural persons as registered entities must be in compliance with the document CA/Browser Forum: "Guidelines for The Issuance and Management of Extended Validation Certificates".

Article 28

In the field "Certificate Policies", the qualified electronic certificate for website authentication shall mandatorily contain at least the QCP-w policy identifier in compliance with the ETSI EN 319 411-2 document "Electronic Signatures and Infrastructures (ESI) – Policy and security requirements for Trust Service Providers issuing certificates – Part 2: Requirements for trust service providers issuing EU qualified certificates", section 4.2.5.

Article 29

In the field "qcStatements", the qualified electronic certificate for website authentication shall mandatorily contain the QcCompliance and QcType statements with identifier "id-etsi-qcs- web", all in accordance with the ETSI EN 319 412-5 document.

V. TRANSITIONAL AND FINAL PROVISIONS

Article 30

As of the date of entry into force of this Rulebook, it shall be considered that the qualified electronic certificates for electronic signatures issued prior to the expiry of the time limit referred to in Article 73, paragraph 5 of the Law and in compliance with the Rulebook on more detailed requirements for qualified electronic certificate issuance (Official Gazette of the RS, No. 26/08) conform to the requirements from this Rulebook prescribed for the qualified electronic certificates for electronic signature until the expiry of the time limit specified in the certificate issued.

Article 31

On the date of entry into force of this Rulebook, the Rulebook on more detailed requirements for qualified electronic certificate issuance (Official Gazette of the RS, No. 26/08) shall cease to be in force.

Article 32

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 110-00-17/2018-12

In Belgrade, on April 20, 2018

The Minister,

Rasim Ljajić, PhD., own signature