Pursuant to Article 46, paragraph 5 and Article 47, 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 has passed the following

RULEBOOK

on the mandatory requirements for the qualified devices for electronic signature and/or seal creation and on mandatory requirements for the appointed body

I. INTRODUCTORY PROVISIONS

Article 1

This Rulebook shall lay down:

1) the requirements that the devices for qualified electronic signature and/or seal creation must conform to, including:

(1) the technical solutions and criteria that a qualified electronic signature and/or seal creation device must fulfil,

(2) the technical and technological procedures for electronic signature and/or seal forming that such device applies in creation of the signature and/or seal,

(3) the criteria that must be fulfilled when the device is used through the qualified electronic signature and/or seal creation device management service;

2) the requirements that the appointed body for conformity assessment of the qualified devices for electronic signature and/or seal creation must conform to.

Article 2

The technical solutions and criteria that must be fulfilled by a qualified device for electronic signature and/or seal creation, the technical and technological procedure for electronic signature and/or seal creation that such device applies and the criteria that must be fulfilled when the device is used through the qualified electronic signature and/or seal device management service must be in conformity with the relevant international standards and recommendations and/or other standards, documents and recommendations, which are related to the devices and procedures determined by this Rulebook.

II. TECHNICAL SOLUTIONS AND CRITERIA

Article 3

In addition to the requirements referred to in Article 46 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), the qualified device for electronic signature and/or seal creation must additionally comply with the following criteria:

1) that it is ensured that the qualified electronic signature and/or seal creation device is used solely by the signatory and/or creator of the seal following the completion of a trustworthy authentication procedure;

2) that the device must be such that the signatory and/or creator of the seal can use it in different applications and information and technological environments, while additionally bearing in mind the provision of Article 6 of the Law and the user's need to use the device when using other trust services.

Article 4

The qualified device for electronic signature and/or seal creation must ensure that data for electronic signature and/or seal creation is generated in such a manner that it can exist in such device only.

Article 5

The qualified device for electronic signature and/or seal creation must be in conformity with one of the following requirements:

1) profile protection requirements defined in the SRPS EN 419211-2:2014 standard – Protection profiles for secure signature creation device - Part 2: Device with key generation examined according to the Common Criteria level EAL4+;

2) profile protection requirements defined in the SRPS EN 419211-3:2014 standard – Protection profiles for secure signature creation device - Part 3: Device with key import examined according to the Common Criteria level EAL4+, where the requirement referred to in Article 3 of this Rulebook is fulfilled as well;

The subject matter of the conformity assessment of a qualified device for signature and/or seal creation shall be the device itself that provides data for electronic signature and/or seal forming. The connection between the device and the applications for electronic signature and/or seal forming shall not necessarily be included in the scope of conformity assessment.

III. PROCEDURES FOR ELECTRONIC SIGNATURE AND/OR SEAL CREATION

Article 6

When creating the electronic signature and/or seal, the qualified device for electronic signature and/or seal creation shall use one of the standardized asymmetric cryptographic algorithms, and specifically:

1) *RSA (Rivest Shamir Adleman)* by applying the PKCS#1 standard with minimum length of the RSA modulus n of 2048 bits;

2) *DSA (Digital Signature Algorithm)* with the minimum lengths of the parameters p and q of 2048 and 224 bits respectively;

3) *ECDSA (Elliptic Curve Digital Signature Algorithm)* with the minimum lengths of the parameters p and q of 256 bits.

Article 7

When forming the qualified electronic signature, the hash functions shall additionally apply to obtaining

message prints of the fixed size (160 bits at the minimum). The hash functions referred to in paragraph 1 of this Article shall be realized through application of one of the following standardized hash algorithms:

1) SHA-224, SHA-256, SHA-384, SHA-512;

2) SHA3-256, SHA3-384, SHA3-512.

Article 8

The set of standard algorithms referred to in Articles 5 and 6 of this Rulebook combined with the requirements relating to the parameter selection, as well as the list of standard combinations of applied algorithms in the form of algorithm connections ("signature suites"), must be in compliance with the ETSI TS 119 312 V1.2.1 document "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites" and document ETSI TR 119 300 „Electronic Signatures and Infrastructures (ESI); Guidance on the Use of Standards for Cryptographic Suites".

IV. QUALIFIED DEVICE USED THROUGH THE MANAGEMENT SERVICE

Article 9

The qualified device for electronic signature and/or seal creation that is used through the management service as a qualified trust service in compliance with Article 46, paragraph 3 of the Law (hereinafter: the remote qualified device) must ensure, with a high level of reliability, that the user has exclusive control over data for electronic signature and/or seal creation.

Article 10

When used jointly with the remote qualified device, data for electronic signature and/or seal creation must be initially created in the qualified device for electronic signature and seal creation which complies with the requirements referred to in the Law and this Rulebook.

Article 11

The remote qualified device must ensure that data for electronic signature and/or seal creation can be activated solely by the signatory upon prior completion of a trustworthy authentication procedure.

It shall be necessary that each activation of data for electronic signature and/or seal creation in the remote qualified device is linked to the valid user authorization and the concrete application for electronic signature and/or seal creation.

Article 12

The remote qualified device must ensure that electronic signature and/or seal creation can happen only in the qualified device for electronic signature and/or seal creation.

Article 13

The remote qualified device must be in conformity with the requirements prescribed by the profile defined standard CEN EN 419 241-2 Protection profile for QSCD for server signing examined according

to the Common Criteria level EAL4 increased by AVA_VAN.4 vulnerability analysis or a higher level.

Article 14

The remote qualified device in the procedure of electronic signature and/or seal creation must ensure the same security level that is prescribed for the qualified devices for electronic signature and/or seal creation, in particular when bearing in mind the selection of the standardized cryptographic algorithms, the selection of the hash functions for prints obtaining and the minimum length of the parameters.

V. CONFORMITY ASSESSMENT BODY

Article 15

The appointed body for conformity assessment of the qualified devices for electronic signature and/or seal creation (hereinafter: the appointed body) must be competent, provide the necessary human resources, expert knowledge and equipment, as well as be trained to conduct the conformity assessment procedure for the device to the technical requirements as defined by the Law and this Rulebook.

As proof of compliance with competence and stated requirements, the appointed body shall be obliged to be accredited, in compliance with the law regulating accreditation, in accordance with the standard SRPS ISO/IEC 17065:2016 – Conformity assessment - Requirements for bodies certifying products, processes and services, within the scope of accreditation that provides verification of conformity of the qualified device for electronic signature and/or seal creation, in accordance with the following list of standards:

1) SRPS ISO/IEC 15408-1:2014 – Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model;

2) SRPS ISO/IEC 15408-1:2014 – Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Functional security requirements;

3) SRPS ISO/IEC 15408-1:2014 – Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Requirements for security assurance;

4) ISO/IEC 18045:2008: Information technology – Security techniques – Methodology for IT security evaluation.

Article 16

The appointed body must be comply with the principle of independence and impartiality when assessing conformity.

In the assessment procedure in particular, but in the accreditation acquiring procedure as well, the persons related to the device that is subject to conformity assessment may not participate in the work of the appointed body.

That shall be without prejudice to the potential for exchange of technical information between the appointed body and the manufacturer of the devices.

Article 17

The appointed body shall be obliged to regulate the actions and decision making upon complaints against the operations and decisions passed relating to the conformity assessment tasks.

The appointed body shall be obliged to, without delay and within seven days at the latest, notify the Ministry in charge of information society (hereinafter: the Ministry) of the existence of complaints against the operations of the appointed body and a decision passed, and in relation to the certificates of conformity for the device that were issued by that body for the devices entered in the Register of qualified devices for electronic signature and/or seal creation referred to in Article 47 of the Law.

Article 18

When concluding the conformity assessment of the device, the appointed body may not make use of information classified as business secret.

Article 19

In compliance with the law regulating technical requirements for products and conformity assessment, the appointed body shall be liable for the damage incurred through the use of the device for which the body has issued the certificate of conformity where it turns out that the device does not fulfil the technical requirements defined by the Law and this Rulebook, where the damage is caused intentionally or through negligence of the appointed body.

The appointed body shall be obliged to provide the financial resources for insurance from the risk from liability for the damage arising from the business activity so that:

1) the insured sum for which the insurance per single harmful event must be contracted may not be lower than 20,000 Euros in dinar counter value, where the harmful event shall be understood to comprise of individual damage incurred through a single use of the assessed device;

2) the total insured sum for which the liability insurance of the appointed body must be contracted on the annual level cumulatively, per all the harmful events, must not be lower than 1,000,000 Euros in dinar counter value.

VI. TRANSITIONAL AND FINAL PROVISIONS

Article 20

As of the date of entry into force of this Rulebook, it shall be considered that the device for qualified electronic signature creation that was provided for the user by the certification body referred to in Article 73, paragraph 3 of the Law, and which complies with the requirements referred to in the Rulebook on technical and technological procedures for qualified electronic signature creation and required criteria for the devices for qualified electronic signature creation (Official Gazette of the RS, No. 26/08, 13/10 and 23/15) complies with the requirements referred to in Article 5 of this Rulebook until the expiry of the validity term of the qualification certificate issued according to the asymmetric pair of keys generated in such device, where the qualified certificate is issued prior to the expiry of the time limit referred to in Article 73, paragraph 5 of the Law.

The Ministry shall additionally enter in the Register of qualified devices for electronic signature and

electronic seal creation the devices referred to in paragraph 1 of this Article, with a note on the method of compliance with the requirements referred to in Article 5 of this Rulebook and the time limit until which it shall be considered that the device is conformant with these requirements.

Article 20a

Qualified devices for creating electronic signatures and electronic seal that meet the requirements of FIPS 140-2 (Federal Information Processing Standard) level 2 or higher, and which are entered in the Register of qualified devices for creating electronic signatures and electronic seal, are considered valid until expiration the validity of qualified electronic certificates for the creation of electronic signatures and electronic seals created by such qualified device.

Qualified devices from the Paragraph 1. of this article may be issued to users until 31th December 2020 years.

Article 21

Upon the entry into force of this Rulebook, the Rulebook on technical and technological procedures for qualified electronic signature creation and required criteria for the devices for qualified electronic signature creation (Official Gazette of the RS, No. 26/08, 13/10 and 23/15) shall cease to be in force.

Article 22

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 110-00-18/2018-12

In Belgrade, on April 20, 2018

The Minister,

Rasim Ljajić, PhD., own signature