

Pursuant to Article 38, paragraph 4 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 the form and publication method of the Trusted List**

#### Article 1

This Rulebook shall prescribe the form and publication method for the Trusted List.

#### Article 2

The Trusted List shall provide reliable information to the relying parties on the status of qualified trust service providers and their qualified services according to information entered in the Register of Qualified Trust Service Providers (hereinafter: the Register) referred to in Article 35 of the Law on Electronic Document, Electronic Identification and Trust Services in Electronic Business (hereinafter: the Law).

The Trusted List shall comprise information on relevant past events relating to the status of present and former service providers and their services over time, including information on the start of service provision, loss of integrity of the trust service, temporary ban, cessation of service provision, deletion from the Register and other events recorded in the course of Register maintenance tasks, inspections or events reported by the service providers, which are impacting acceptability of the qualified trust service and the procedure for determining its status at a certain point of time.

#### Article 3

The relying party shall use the Trusted List in the procedure of determining the qualified status of the service provider, provided qualified trust service and qualified status of other elements resulting from the service provided, such as determining the qualified status of the certificate issued for electronic signature, seal or website authentication, in relation to the present or a specific moment of time in the past following the provision of the service.

#### Article 4

The Ministry in charge of electronic business shall act as the Trusted List Scheme Operator (TLSO) in accordance to the ETSI TS 119 612 standard “Electronic Signatures and Infrastructures (ESI); Trusted Lists” and Article 38, paragraph 5 of the Law, and in relation to Article 22, paragraph 3 of the eIDAS Regulation (hereinafter: the Operator).

#### Article 5

The Operator shall establish and publish the Trusted List in compliance with ETSI TS 119 612 standard in a form suitable for automatic processing as an electronic document in XML format signed by the advanced electronic seal.

The Operator shall establish and publish an accompanying document that shall include

SHA-256 imprint of the signed List referred to in paragraph 1 of this Article.

The documents referred to in paragraphs 1 and 2 of this Article shall be published on the dedicated Trusted List website.

In addition to the last published issue, the Operator may also made available the archive of the previous issues of the documents referred to in paragraphs 1 and 2 of this Article.

#### Article 6

The Operator shall be obliged to ensure a high level of accessibility and up-to-dateness of the published Trusted List as well as the compatibility of the published List with the current technical standards.

#### Article 7

The website of the Trusted List must be registered in the gov.rs domain, on an unchangeable address, in order to ensure long-term accessibility of the website.

The updated version of the document referred to in Article 5, paragraph 1 of this Rulebook may be downloaded through the website of the Trusted List in compliance with the ETSI TS 119 612 standard, section “6.1 TL publication”. The web address of the document in XML format shall mandatorily end in “.xml”. The accompanying document referred to in Article 5, paragraph 2 of this Rulebook shall be published on the web address the ending extension “.xml” of which is replaced by the extension “.sha2”.

The website shall mandatorily deliver the document with HTTP heading “Content-Type: application/vnd.etsi.tsl+xml”.

#### Article 8

The Trusted List may additionally be presented in the form suitable for presentation to the relying party providing that it has been specifically noted in the document in such form that information comprised in the document corresponds to the information in document referred to in Article 5 of this Rulebook, as well as that in addition to that only the document in the form referred to in Article 5 of this Rulebook shall be the reference source of information on the qualified status of the service provider and their services.

#### Article 9

The Trusted List shall comprise the following field values in accordance with the ETSI TS 119 612 standard:

1) Field “TSLType” section 5.3.3 shall be set to

“<http://uri.etsi.org/TrstSvc/TrustedList/TSLType/RSlist>”.

- 2) Field “StatusDeterminationApproach” section 5.3.8 shall be set to “<http://uri.etsi.org/TrstSvc/TrustedList/StatusDetn/RSdetermination>”.
- 3) Field “SchemeTerritory” section 5.3.10 shall be set to “RS”.

#### Article 10

According to the ETSI TS 119 612 standard, data shall be entered in the Trusted List in English language with the encoding tag “en” in UTF-8 encoding.

The fields that are supporting entries in multiple languages shall be entered at least in Serbian and English language. The language tag shall be set according to the IETF RFC 5646 document. Data in Serbian language shall be entered in Cyrillic script with “sr-cyrl” tag in UTF-8 encoding.

Links to other webpages shall be marked by means of adequate tags according to the language and script of the target page.

Identification and address information of the qualified trust service providers shall be transferred directly from the relevant Register in the original language and script with the relevant tag (“sr-cyrl”, “sr-latn” or other).

Where the identification and address information are not entered in at least one language in Latin script (according to the ISO 10646 definition), in compliance with ETSI TS 119 612 standard Annex E, in addition to the original entry in multilingual field an entry made in transliteration in Latin script in at least one language shall be added in Latin script with an adequate tag (“sr-latn”, “en” or other).

#### Article 11

The TSL name field according to ETSI TS 119 612 standard section 5.3.6 shall have a multilingual value:

- 1) For the language tag “sr-cyrl”, value “RS: Javna lista kvalifikovanih usluga poverenja prema Zakonu o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju” (RS: Trusted List in accordance to Law on Electronic Document, Electronic Identification and Trust Services in electronic business);
- 2) For the language tag “en”, value “RS: Public qualified service status list in accordance to Law on Electronic Document, Electronic Identification and Trust Services in electronic business”.

#### Article 12

The Operator shall be obliged to provide a page with additional information on the Trusted List, in Serbian and in English language, which shall provide to the relying party an overview of the legislative framework for the qualified trust services, and in particular:

- 1) identification and contact information of the Ministry as:
  - (1) the Operator of the Trusted List in compliance with this Rulebook;

(2) the body conducting inspection of the application of the Law, i.e. of the qualified trust service providers;

2) the criteria for acquiring the qualified status of a trust service provider in compliance with Article 35 of the Law and obligations that the trust service providers and qualified trust service providers must fulfil in order to retain the status of a qualified trust service provider and qualified trust service;

3) conditions on which temporary bans or revocation of the qualified status of the trust service provider and qualified trust service can be imposed.

The Trusted List shall include links to the webpages in Serbian and in English languages referred to in paragraph 1 of this Article according to ETSI TS 119 612 standards in the field “SchemeInformationURI” (section 5.3.7), field “SchemeTypeCommunityRules” (section 5.3.8) and field “PolicyOrLegalNotice” (section 5.3.11).

#### Article 13

The Operator shall provide information support in the form of an application, applicative solution and/or an information system for establishing, signing and publication of the Trusted List.

#### Article 14

In establishing, signing and publication of the Trusted List, the Operator should provide the following:

1) the XML document and the imprint referred to Article 5 of this Rulebook should be made and updated by using the tool referred to in Article 13 of this Rulebook;

2) the devices used for signing i.e. sealing the Trusted List should guarantee reliability and integrity when managing such devices, i.e. during the procedure of creation, advertising, preservation, activation of the devices and deactivation of such devices;

3) application of the measures with a view to preventing unauthorized use of the devices for signing and/or sealing, as well as unauthorized publication on the website on which the Trusted List is published;

4) a timely response in case of an incident, including compromising of the devices for signing and/or sealing of the Trusted List, compromising or unavailability of the website on which the Trusted List is published or unavailability of the technical solution used to produce the documents referred to in Article 13 of this Rulebook;

5) up-to-date, accurate, complete and authentic information in the published Trusted List.

#### Article 15

The Operator shall ensure that at any given moment there are at least two independent sets of signature creation data which can be used to sign the Trusted List with a different end date.

Data on the certificate supporting the signature on the Trusted List, including the SHA-256

imprint, shall be published in the Official Gazette of the Republic of Serbia.

All available certificates for signing the following issue of the published List shall be integrated in the published List in the field “PointersToOtherTSL” under the path “OtherTSLPointer / ServiceDigitalIdentities / ServiceDigitalIdentity / DigitalId” including the certificate associated with verification data for signature or seal that will be used for signing the current issue of the List.

#### Article 16

The Operator shall ensure integrity and authenticity of the XML document referred to in Article 5 of this Rulebook by means of the advanced electronic seal in XAdES-BES format in accordance with the ETSI TS 101 903 standard “XML Advanced Electronic Signatures (XAdES)” by means of a procedure defined in the internal rules referred to Article 14 of this Rulebook.

The seal creation device must comply with the conditions referred to in Article 46 of the Law.

The Operator may use the device and the electronic certificate associated with seal verification data issued within the internal PKI infrastructure of the Operator, a self-signed certificate or a certificate issued by a qualified trust service provider whose service is included in the established list, in the manner provided for in the internal rules referred to in Article 13 of this Rulebook.

Where the Operator uses the certificate issued by a qualified trust service provider, the qualified status of the trust service provider and of the certificate issued is not relevant for determining validity of the signature on the Trusted List.

The electronic seal of the XML document referred to in paragraph 1 of this Article may include only one certificate associated with the seal verification data.

#### Article 17

The electronic certificate referred to in Article 15 of this Rulebook shall mandatorily have the following values:

- 1) In the field “Subject”, value “Country code” shall be “RS”, and “Organization” shall match the identification of the Operator;
- 2) The field “KeyUsage” shall have the value “nonrepudiation” (contentCommitment);
- 3) The field “ExtendedKeyUsage” shall have the value “id-tsl-kp-tslSigning” (0.4.0.2231.3.0);
- 4) The field “BasicConstraints” shall have the value “CA=false”;
- 5) The field “SubjectKeyIdentifier” must be present in compliance with the note in ETSI TS 101 903 section 5.7.1.

The electronic certificate referred to in Article 15 of this Rulebook shall always be issued in relation to new data for verification and creation of electronic signature and/or seal. The permitted term for use of the key shall correspond to the validity of the electronic certificate.

## Article 18

The Operator shall establish and publish the Trusted List at least once every six months and on occasion of each change of status of the qualified trust service providers and qualified trust services.

The Operator shall provide procedure for notifications provision among the Operator and the qualified trust service providers, as well as inspections for electronic identification and trust services in electronic business so that on occasion of each modification of data published in the Trusted List, the new issue of the List is published within 24 hours from the modification at the latest.

By way of exception from paragraph 2 of this Article, the Operator shall ensure that on occasion of each change in the qualified status of the provider or trust service a new issue of the list is published within four hours from the corresponding change at the latest.

## Article 19

The Trusted List shall permanently retain all the records on the status of the qualified trust service providers and qualified trust services that are entered from the beginning of the Trusted List maintenance.

Upon termination of a qualified trust service, the status of the service shall be changed to “ceased”.

In case of deletion of a qualified trust service from the Register, the status of the service shall be changed to “withdrawal”.

## Article 20

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 110-00-66/2018-12

In Belgrade, on January 14, 2019

The Minister,

**Rasim Ljajić**, PhD., own signature