Pursuant to Article 62, paragraph 3 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 requirements for procedures and technological solutions used during trustworthy electronic preservation of documents

Introductory Provision

Article 1

This Rulebook shall laid down the requirements for procedures and technological solutions used during trustworthy electronic preservation of documents comprising in their original form a qualified electronic signature and/or seal and of the documents the fidelity of which to the original document and accuracy of the additionally included data are verified by means of a qualified electronic signature and/or seal in compliance with Article 61, paragraph 1, item 4) of the Law on Electronic Document, Electronic Identification and Trust Services in Electronic Business (hereinafter: the Law).

Internal Rules

Article 2

Trustworthy preservation of documents shall be carried out in compliance with the internal rules for trustworthy electronic preservation of documents (hereinafter: the internal rules), based on which actions shall be taken during trustworthy electronic preservation and whereby conformity of the trustworthy electronic preservation with the requirements from the law is provided for.

Objectives of Trustworthy Document Preservation

Article 3

In order to provide for the possibility of verifying the validity of the qualified electronic signature and/or seal during the entire period of preservation, the trustworthy electronic preservation of documents shall imply provision of:

1) proof that the document existed at a precisely determined moment, based on the qualified time-stamp;
2) maintenance of the validity status of the qualified electronic signature or seal in relation to the moment of time referred to in item 1) of this Article;
3) availability of the originally preserved electronic document and any additional data verifying compliance with the conditions referred to in items 1) and 2) of this Article;
4) maintenance of trust in integrity and authenticity of all pieces of data referred to in item 3) of this Article under the presumption that during the preservation period doubt can arise regarding the previously used cryptographic algorithms, algorithms, hash functions and procedures or that the user's certificates or the certificates of the trust service provider can be revoked.

Application of standards

Article 3a.

The service of qualified electronic preservation of documents is performed in accordance with the requirements of the following standards:

1) ETSI TS 119 511 „Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers Providing Long-Term Preservation of Digital Signatures or General Data Using Digital Signature Techniques ";

2) ETSI TS 119 512 „Electronic Signatures and Infrastructures (ESI); Protocols for Trust Service Providers Providing Long-Term Data Preservation Services ".

The service of qualified electronic preservation of the document is performed in accordance with the requirements from other standards which are directly and indirectly referred to from the standards from paragraph 1 of this article.

Qualified Electronic Signature and/or Seal on Trustworthy Electronically Preserved Documents

Article 4

A document that is being trustworthy electronically preserved must mandatorily have an associated qualified electronic signature and/or seal, irrespective of whether it is a document that in its original form includes a qualified electronic signature and/or seal or a document whose fidelity to the original document and accuracy of additionally included data has been verified by means of the qualified electronic signature and/or seal referred to in Article 61, paragraph 1, item 4) of the Law.

The format of the qualified electronic signature and/or seal referred to in paragraph 1 of this Article must comply with one of the following requirements:

1) PDF in compliance with ISO 32000 "Document management Portable document format" and PAdES format of electronic signature and/or seal in compliance with ETSI EN 319 142 "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures";
2) ASiC-S container that includes the document and the electronic signature and/or seal of such document in the XAdES or CAdES format in compliance with ETSI EN 319 162 "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC)";
3) XAdES format of the electronic signature and/or seal that includes the signed and/or sealed document in compliance with ETSI EN 319 132 "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures";
4) CAdES format of the electronic signature and/or seal that includes the signed and/or sealed document in compliance with ETSI EN 319 122 "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures".

The levels of XAdES, CAdES and PAdES formats of the electronic signature and/or seal referred to in paragraph 1 of this Article must be XAdES-B-LTA or XAdES-E-A, CAdES-B-LTA or CAdES-E-A and PAdES-B-LTA or PAdES-E-LTV in the stated order.

Upgrading of Qualified Electronic Signatures and/or Seals

Article 5

When commencing trustworthy electronic preservation, upgrading procedure of the qualified electronic signature and/or seal into XAdES, CAdES or PAdES format shall be carried out on the document to be preserved, which shall include:

1) where the qualified electronic signature and/or seal is on the basic XAdES, CAdES and/or PAdES level, a qualified time-stamp shall be added to the qualified electronic signature and/or seal;
2) validation of the qualified electronic signature and/or seal shall be performed and during that data for validity check shall be acquired, such as certificates and revocation statuses;
3) in accordance with the format, the missing data for validity check shall be added to the qualified electronic signature and/or seal, hash shall be calculated for the originally signed and/or sealed document together with the signature and/or seal itself, a qualified time-stamp shall be created based on such hash and such time-stamp shall also be added in the qualified electronic signature and/or seal.

Qualified Electronic Signature and/or Seal on Document Received for Trustworthy Electronic Preservation

Article 6

The document that is received for trustworthy electronic preservation must comply with the requirements referred to in Article 4, paragraphs 1 and 2 of this Rulebook, as well as with the condition that it shall be possible to ensure the levels referred to in Article 4, paragraph 3 of this Rulebook following the upgrading of the qualified electronic signature and/or seal in compliance with Article 5 of this Rulebook.

Renewed Upgrading of Qualified Electronic Signature and/or Seal

Article 7

Renewed upgrading of a qualified electronic signature and/or seal on an electronic document that is preserved shall be mandatorily carried out prior to:

1) the expiry of the certificate of the last time-stamp in the qualified electronic signature and/or seal;
2) due to the technical or formal reasons, the cryptographic algorithm or hashing algorithm that is used in the last time-stamp in the qualified electronic signature and/or seal can become the basis for contesting the validity of the qualified electronic signature and/or seal.

Renewed upgrading of a qualified electronic signature and/or seal shall be performed by following the procedure referred to in Article 5 of this Rulebook.

Information System for Trustworthy Electronic Preservation

Article 8

Trustworthy electronic preservation of documents shall be performed within the information system specifically intended for such purpose (hereinafter: the information system) which shall be operated by and taken care of by the preservation handler.

The information systems, together with the relevant measures determined in the internal rules, must ensure that the renewed upgrading of the qualified electronic signature and/or seal is

carried out in a timely manner, in order to provide for the possibility of evidencing the validity of the qualified electronic signature and/or seal during the entire preservation period.

The information system must ensure a high level of protection against any losses of data that is preserved, compromising integrity of such data and unauthorized access to such data.

The preservation handler shall manage the information system in accordance with the ISO/IEC 27001 standard "Information security management" in such a manner that the incidents leading to the loss of data preserved, compromising of the integrity of such data, unauthorized access to such data or the loss of possibility to prove validity of the qualified electronic signature and/or seal during the entire preservation period are considered to be the incidents involving high risk.

The protection measures required by the standard referred to in paragraph 4 of this Article shall be documented in the internal rules.

Article 9

With the aim of ensuring the flows of accessing, exchange and processing of data, in compliance with the ratified international agreements, the Ministry of Interior may, in addition to applying this Rulebook, apply other requirements relating to trustworthy electronic preservation of documents, which shall be applied due to the specificities of information systems and technical and technological procedures in the Ministry of Interior.

Entry into Force

Article 10

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 110-00-53/2018-12
In Belgrade, on November 21, 2018
The Minister,
Rasim Ljajić, PhD, own signature