Pursuant to Article 18, paragraph 2 of the Law on Electronic Document, Electronic Identification and Trust Services in Electronic Business (Official Gazette of the RS, No. 94/17) and Article 42, paragraph 1 of the Law on Government (Official Gazette of the RS, No. 55/05, 71/05 – corrigendum, 101/07, 65/08, 16/11, 68/12 – CC, 72/12, 7/14 – CC, 44/14 and 30/18 – other law),

The Government has passed

REGULATION

On more detailed regulation of the mandatory requirements for electronic identification schemes for specific assurance levels

Subject Matter of the Regulation

Article 1

This Regulation shall regulate in more detail the requirements that the electronic identification schemes for specific assurance levels must comply with.

All the terms used in this Regulation of the masculine gender shall include the same terms of the feminine gender.

Electronic Identification

Article 2

Electronic identification means the procedure of using personal identification data in electronic form that is uniquely determining a legal person, a natural person or a natural person in the capacity of a registered entity.

Where a registered electronic identification scheme complies with the requirements for a higher assurance level of an electronic identification scheme, it shall be considered that in such a case it also complies with the requirements for lower assurance levels.

Application for Issuing of Means of Electronic Identification

Article 3

Application for issuing of electronic identification means shall be submitted to the provider of electronic identification service.

When submitting the application for issuing of electronic identification means, the electronic identification service provider shall be obliged to acquaint the applicant with:

1) the method of use of the electronic identification means;

2) regulations and rules pertaining to the use of electronic identification service;

3) information on the assurance level of the electronic identification scheme for which the application is submitted;

4) risks from possible misuse and/or misrepresentation;

5) measures that the applicant should take in order to securely use the electronic identification means.

The electronic identification provider shall be obliged to acquire user's consent for personal data processing within provision of electronic identification service and to act in all respects in compliance with the law regulating protection of personal data.

Identity verification for issuing of electronic identification means of the basic assurance level

Article 4

Identity verification for issuing of electronic identification means of the basic assurance level shall be performed based on one of the following methods:

1) identity card or another public document bearing a photograph;

2) a public document serving as means of remote identification;

3) a means of identification that has been issued within a registered scheme of the same or a higher assurance level.

In the case where an application for issuing of an electronic identification means of the basic assurance level is submitted by a legal person, identity verification of the authorized representative of the legal person shall be performed by providing proof of authorisation.

The proof referred to in paragraph 1, item 1) and paragraph 2 of this Article shall be delivered by the applicant electronically to the service provider.

Issuing of electronic identification means of the basic assurance level can be performed by the physical presence of the applicant, where provided so in the internal acts of the provider of the electronic identification service.

Identity verification for issuing of electronic identification means of the medium assurance level

Article 5

Identity verification for issuing of electronic identification means of the medium assurance level shall be performed based on one of the following methods:

1) identity card or travel document with physical presence of the applicant;

2) a public document serving as a means of remote identification;

3) a means of identification that has been issued within the registered scheme of the same or a higher assurance level.

In the case where an application for issuing of an electronic identification means of the medium assurance level is submitted by a legal person, identity verification of the authorized representative of the legal person shall be performed, by means of *mutatis mutandis* application of paragraph 1 of this Article, with providing proof of authorisation.

Where the identity verification of the applicant is performed on the basis of the document referred to in paragraph 1, item 1) of this Article, the provider of electronic identification may perform a document validity check and verification of accuracy of information from the document with the authority in charge of document issuing in compliance with the law regulating records and processing of data in the field of interior affairs.

The authority in charge of issuing of the documents referred to in paragraph 1, item 1) of this Article shall provide validity check of the document and verification of accuracy of information from the document for the needs of the electronic identification provider through an electronic service, by applying adequate information security measures.

Identity verification for issuing of electronic identification means of high assurance level

Article 6

Identity verification for issuing of electronic identification means of the high assurance level shall be performed based on one of the following methods:

1) identity card or travel document with physical presence of the applicant;

2) a public document serving as a means of remote identification, in compliance with the law;

3) a means of identification that has been issued within the registered scheme of the high assurance level.

In the case where an application for issuing of an electronic identification means of the high assurance level is submitted by a legal person, identity verification of the authorized representative of the legal person shall be performed, by means of *mutatis mutandis* application of paragraph 1 of this Article, with providing proof of authorisation.

Where the identity verification of the applicant is performed on the basis of the document referred to in paragraph 1, item 1) of this Article, the provider of electronic identification may perform a document validity check and verification of accuracy of information from the document with the authority in charge of document issuing in compliance with the law regulating records and processing of data in the field of interior

affairs.

The authority in charge of issuing of the documents referred to in paragraph 1, item 1) of this Article shall provide validity check of the document and verification of accuracy of information from the document for the needs of the electronic identification provider through an electronic service, by applying adequate information security measures.

Identity verification for a foreign national

Article 7

Identity verification for a foreign national shall be performed based on the foreign travel document, travel document for foreigners or identity card for foreigners which are issued by the competent authorities of the Republic of Serbia.

The electronic identification provider may perform a validity check of the travel document for foreigners or identity card for foreigners and verification of the accuracy of information from these documents with the authority competent for document issuing, in compliance with the law regulating records and processing of data in the field of interior affairs.

The authority in charge of issuing of the document referred to in paragraph 2 of this paragraph shall provide validity check of these documents and verification of accuracy of information from the documents for the needs of the electronic identification provider through the electronic service, by applying adequate information security measures.

Issuing and activation of electronic identification means

Article 8

In the procedure of issuing, the electronic identification means shall be delivered in the manner that will ensure delivery to the person to which it is intended only, i.e. to the user of the means.

Following the delivery, the electronic identification means of the medium and high assurance level shall be activated by using the activation code delivered to the applicant.

Suspension, revocation and reactivation of electronic identification means

Article 9

The electronic identification means can be suspended and/or revoked.

Provider of electronic identification service shall be obliged to take measures in order to prevent unauthorized suspension, revocation or reactivation.

The electronic identification means can be issued anew where requirements for reliable issuing are complied with.

In the case of renewal or replacement of the electronic identification means, it shall be necessary to perform identity proofing and verification anew, in the manner envisaged in Articles 4 through 7 of this Regulation.

Authentication mechanism for electronic identification scheme of the basic assurance level

Article 10

Provider of electronic identification service of the basic assurance level shall be obliged to:

1) issue the electronic identification means which comprises at least one element of authentication;

2) take measures that ensure that the electronic identification means can be used by user of the means only;

3) ensure reliable check of the electronic identification means and their validity on the occasion of disclosing of personal identification data of the user of the means;

4) ensure protective controls for the check of electronic identification means on the occasion of authentication process, with the aim of preventing jeopardizing of the authentication mechanism, such as disclosing of the authentication factors, unauthorized access, unauthorized interception and other methods of jeopardizing thereof.

Authentication mechanism for electronic identification scheme of the medium assurance level

Article 11

Provider of electronic identification service of the medium assurance level shall be obliged to:

1) issue the electronic identification means that includes at least two elements of authentication of different categories (something that the person know, something that the person possesses, something that the person is);

2) the means referred to in item 1 of this paragraph is designed in such a manner as to ensure the possibility of use of the electronic identification means to the user of means only, i.e. that it can be assumed that the electronic identification means is used only under control of the user of the means;

3) ensure reliable check of the electronic identification means and their validity on the occasion of disclosing of the personal identification data through dynamic authentication;

4) provide protective controls for the check of electronic identification means on the

occasion of authentication process, with the aim of preventing jeopardising of the authentication mechanism, such as the disclosing of authentication factors, unauthorized access, unauthorized interception and other methods of jeopardizing.

Dynamic authentication is an electronic process in which cryptography or other techniques are used in order to create a piece of electronic proof that the user controls or possesses identification data, which is changed with each authentication.

Authentication mechanism for electronic identification scheme of the high assurance level

Article 12

Provider of electronic identification service of the high assurance level shall be obliged to:

1) take measures that ensure that the electronic identification means can be used by the user of the means only, i.e. that it can be assumed that the electronic identification means is used only under control of the user of the means;

2) ensure reliable check of the electronic identification means and their validity through dynamic authentication referred to in Article 11, paragraph 2 of this Regulation prior to disclosing of personal identification data of the user of the means;

3) provide protective controls for the check of electronic identification means during the authentication process, with the aim of preventing jeopardising of the authentication mechanism, such as the disclosing of authentication factors, unauthorized access, unauthorized interception and other methods of jeopardizing;

4) provide a high level of protection of electronic identification means from copying, unauthorized alterations and abuse by other persons;

5) issue a qualified means for electronic signature i.e. seal creation which shall at the same time be the means of identification;

6) perform authentication of the users on the basis of qualified electronic signature i.e. qualified electronic seal of the user that shall thus be identified, based on the user certificates that they have issued themselves.

Technical, organisational and security requirements for electronic identification service providers

Article 13

A provider of electronic identification service shall be a legal or a natural person in the capacity of a registered entity that is providing the services of electronic identification.

The electronic identification service providers shall be obliged to:

1) adopt and apply the General Conditions for service provision, the Service Provision Policy and the Practical Rules for the Provision of Services, in compliance with regulations, as well as with the domestic and international standards in the field of electronic identification;

2) acquaint the user of the means with the conditions regarding the use of the service, including any limitations on its use, as well as with any service fees;

3) adopt the privacy protection policy, in compliance with the regulations of the Republic of Serbia;

4) establish adequate policies and procedures that ensure timely and reliable information to the user of the means on the amendments to the conditions of use of the service, i.e. privacy protection policy for a specific service;

5) keep information on issuing of electronic identification means, including information relating to users' identity verification, for a minimum period of ten years following the issue thereof;

6) maintain the records and keep information on significant events relating to the operational work of the provider and the security presumptions of the registered scheme of electronic identification;

7) maintain the records on the use of electronic identification means and keep data from the records where that is necessary for the needs of the audit, investigation in cases of information security breaches and for the needs of data retention, in compliance with the law;

8) provide a source of accurate time that shall be synchronized with the source of reference time determined by the Ministry in charge of information society and reliably integrate information on accurate time in the records referred to in items 5), 6) and 7) of this Article;

9) ensure that their employees and subcontractors are trained and qualified for the tasks pertaining to the electronic identification service;

10) ensure an adequate number of employees and subcontractors for appropriate carrying out of the service;

11) ensure direct supervision and protection of the facilities used for the provision of service, from damage caused by atmospheric conditions, unauthorized access and other causes that may impact the security of the service;

12) ensure that in the facilities that are used for the provision of service access to the areas in which the personal, cryptographic or other confidential data is located or processed can be provided to the authorized employed persons or subcontractors only;

13) obliged to have an termination plan in case of termination of electronic identification service provision, whereby notification of the users on termination of services provision and adequate preservation of data are ensured;

14) ensure that, with the aim of bringing the service in line with the relevant policy, periodic audits are carried out which shall cover all parts pertaining to the delivery of services, and specifically:

(1) periodical internal audits in cases where the electronic identification service of the basic assurance level is provided;

(2) periodical independent internal or external audits in cases where the electronic identification service of the medium assurance level is provided;

(3) periodical independent external audits in cases where the electronic identification service of the high assurance level is provided.

Technical and security characteristics of the electronic identification means

Article 14

The electronic identification service provider shall be obliged to establish an efficient information security management system with the aim of managing the risks pertaining to information security.

The provider of electronic identification services of medium and high assurance levels shall be obliged to establish the system referred to in paragraph 1 of this Article in compliance with the standards and principles for the management of risks pertaining to information security.

The electronic identification service provider shall be obliged to:

1) establish adequate technical controls for risk management for the security of services whereby confidentiality, integrity and accessibility of information processed is protected;

2) ensure that the electronic communication channels used for exchange of personal or confidential information are protected from unauthorized access, unauthorized interception, unauthorized use and other methods of jeopardizing thereof;

3) restrict access to the cryptographic material, where it is used for issuing of electronic identification means and authentication, to duly authorized persons and applications for which such access is explicitly required, as well as to ensure that such material is never continuously preserved in the format of an ordinary non-encrypted text;

4) ensure continuous security of information, as well as ensure that the system is resistant to changes in the risk levels, incidents and security breaches;

5) ensure that the media containing personal, cryptographic or other confidential information are stored, transported and destroyed in a secure manner.

In addition to the requirements referred to in paragraph 3 of this Article, the providers of electronic identification services of medium and high assurance levels shall be obliged to protect the confidential cryptographic material, where it is used for issuing of electronic identification means and authentication, from unauthorized alterations.

Interoperability of electronic identification schemes

Article 15

With the aim of ensuring interoperability of electronic identification schemes, providers of electronic identification service must comply with the technical and organisational requirements referred to in Articles 13 and 14 of this Regulation.

Providers of electronic identification service shall be obliged to: enable identity verification to the relying parties through the "OAuth" protocol in compliance with the RFC 6749 standard "The OAuth 2.0 Authorization Framework" or through the SAML protocol in compliance with the "OASIS Security Assertion Markup Language (SAML) v2.0" standard, which shall not exclude the possibility to offer additional identity verification methods.

Final provision

Article 16

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

05 number 110-3780/2018-1

In Belgrade, on August 2, 2018

The Government

The Prime Minister,

Ana Brnabic, own signature