Rulebook on minimum technical standards and accompanying procedures relating to which assurance levels for electronic identification schemes are determined

Rulebook was published in Official Gazette of Montenegro No.
53/2018 and 20/2020

Article 1

This Rulebook shall prescribe minimum technical standards and procedures relating to which the assurance level of electronic identification schemes for electronic identification means is determined.

Article 2

Terms used in this Rulebook shall have the following meanings:

1) public authority means a state authority, state administration authority, local self-government authority or local government authority and a legal person that performs public function;

2) authoritative source means any data source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to prove identity (registers, records, documents, bodies etc.);

3) relying party means a natural, legal person or public authority that rely on electronic identification or electronic trust service;

4) authentication factor means a factor confirmed as being bound to a person, which falls into any of the following categories: possession-based authentication factor (authentication factor where the subject is required to demonstrate possession of it), knowledge-based authentication factor (authentication factor where the subject is required to demonstrate knowledge of it), inherent authentication factor (factor that is based on a physical attribute of a natural person);

5) dynamic authentication means an electronic process using cryptography or other techniques to provide a means of creating on demand an electronic proof that the subject is in control or in possession of the identification data and which changes with each authentication between the subject and the system verifying the subject's identity;

6) authentication means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed.

Article 3

Determining the assurance level of electronic identification means is done by verifying the essential elements in the electronic identification scheme.

The verification referred to in paragraph 1 of this Article shall include procedures and activities during which:

1) enrolment shall be verified for:

- completeness and accuracy of data in the relying party's application for the issuance of electronic identification means and registration of relying parties when issuing electronic identification means,
- reliability and quality of proving and verifying the identity of a natural person as a relying party,
- reliability and quality of proving and verifying the identity of the legal person as a relying party,
- reliability and quality of binding the means of electronic identification of the legal person and the natural person authorised to represent the legal person

2) management of electronic identification means shall be verified for the reliability and quality of:

- characteristics and design of electronic identification means,
- issuance, delivery and activation of electronic identification means,
- suspension, revocation and reactivation of electronic identification means,
- renewal and replacement of electronic identification means

3) authentication shall be verified for the reliability and quality of the authentication mechanism;

4) management and organization shall be verified for reliability and quality of:

- internal acts on the manner and procedures of issuing electronic identification means,
- published notices and user information,
- information security management,
- keeping records of issued means of electronic identification,
- facilities and staff with respect to the electronic identification scheme,
- technical controls carried out by a natural person, legal person, or a public authority issuing electronic identification means,
- compliance and audits of electronic identification schemes.

Article 4

Determination of assurance level based on procedures for submitting application and registration of relying party referred to in Article 3 paragraph 2 item 1 indent 1 of this Rulebook (assurance level low, assurance level substantial and assurance level high) shall include determination that:

1) the applicant is aware of the terms and conditions related to the use of the electronic identification means;

2) the applicant is aware of recommended security precautions related to the electronic identification means;

3) the applicant's relevant identity data required for identity proofing and verification is collected.

Article 5

Determination of assurance level based on identity proofing and verification procedures referred to in Article 3 paragraph 2 item 1 indent 2 of this Rulebook shall include determination:

1) for the assurance level "low" the existence of:

a) assumption that the natural person is in possession of evidence confirming the claimed identity,

b) assumption that the evidence of identity is genuine, i.e. it is based on true representations,

c) an authoritative source knowing that the claimed identity exists and that it may be assumed that the such identity corresponds to the natural person claiming the identity;

2) for the assurance level "substantial", in addition to evidence of existence of the assurance level "low", the existence of one of the following evidence:

a) that during the relying party's registration process it has been verified that a natural person was in possession of evidence of identity recognised by Montenegro, which confirmed that natural person's identity, that the submitted evidence is verified and that steps have been taken to minimise the risk that the person's identity is not the claimed identity (the risk of lost, stolen, suspended, revoked or expired document)

b) that during the relying party's registration process an evidence on natural person's identity, issued in Montenegro, has been presented, that it is assumed that the evidence relates to that person, and that steps have been taken to minimise the risk that the person's identity is not the claimed identity (the risk of lost, stolen, suspended, revoked or expired document),

c) that a natural person, a legal person or a public authority issuing electronic identification means previously used procedures for a purpose other than the issuance of electronic identification means, which guaranteed at least assurance level substantial, which was determined by assurance level determination authority,

d) that electronic identification means issuance is based on a valid notified electronic identification means having at least the assurance level substantial, and taking into account the risks of a change in the identification data;

3) for the assurance level "high", in addition to evidence of existence of assurance level "substantial", the existence of one of the following evidence:

a) that the natural person has been verified to be in possession of photo or biometric identification evidence recognised by Montenegro and the natural person is identified as the claimed identity through comparison of at least one physical characteristic,

b) that a natural person, a legal person or a public authority issuing electronic identification means previously used procedures for a purpose other than the issuance of electronic identification means, which guaranteed at least assurance level "high", which was determined by assurance level determination authority,

c) that electronic identification means are issued on the basis of a valid notified electronic identification means having at least the assurance level high, taking into account the risks of a change in the identification data,

d) that, in the case where the natural person does not present any recognised photo or biometric identification evidence, such photograph or biometric identification data is obtained in the manner of obtaining those data when issuing identification documents, in accordance with the law.

Article 6

Determination of assurance level based on identity proofing and verification procedures referred to in Article 3 paragraph 2 item 1 indent 3 of this Rulebook shall include determination:

1) for the assurance level "low" the existence of:

a) assumption that the legal person identity is demonstrated on the basis of evidence stated in the application or during the relying party's registration (legal person's registered name, legal form etc.)

b) assumption that legal person's identity data stated in the application correspond to an authoritative source,

c) assumption that the natural person is authorised to represent the legal person;

2) for the assurance level "substantial", in addition to evidence of existence of the assurance level "low", the existence of one of the following evidence:

a) that during the relying party's registration process it has been verified that a legal person was in possession of evidence of identity recognised by Montenegro, which confirmed that legal person's identity ((legal person's registered name, legal form etc.), that the submitted evidence is verified and

that steps have been taken to minimise the risk that the legal person's identity is not the claimed identity (the risk of lost, stolen, suspended, revoked or expired document),

b) that a natural person, a legal person or a public authority issuing electronic identification means previously used procedures for a purpose other than the issuance of electronic identification means, which guaranteed at least assurance level substantial, which was determined by assurance level determination authority,

c) that electronic identification means issuance is based on a valid notified electronic identification means having at least the assurance level substantial, and taking into account the risks of a change in the identification data;

3) for the assurance level "high", in addition to evidence of existence of assurance level "substantial", the existence of one of the following evidence:

a) that during the relying party's registration process the legal person has been verified to be in possession of identification evidence recognised by Montenegro, which confirms that legal person's identity (legal person's registered name, legal form etc.) and at least one identifier representing the legal person and which is used in the country of the legal person's registration, as well as that the evidence are checked for accuracy determination,

b) that a natural person, a legal person or a public authority issuing electronic identification means previously used procedures for a purpose other than the issuance of electronic identification means, which guaranteed at least assurance level "high", which was determined by assurance level determination authority,

c) that electronic identification means are issued on the basis of a valid notified electronic identification means having at least the assurance level high, taking into account the risks of a change in the identification data.

Article 7

Determination of assurance level based on binding between the electronic identification means of natural and legal persons referred to in Article 3 paragraph 2 item 1 indent 4 of this Rulebook shall include determination:

1) for the assurance level "low" that:

a) the identity proofing of the natural person acting on behalf of the legal person has been conducted with at least assurance level low,

b) the binding has been established on the basis of procedures recognised in Montenegro,

c) the natural person was authorised for acting on behalf of the legal person;

2) for the assurance level "substantial", in addition to requirements of the assurance level "low" referred to in item 1 sub item c) of this Article , the existence of evidence that:

a) the identity proofing of the natural person acting on behalf of the legal person has been conducted at assurance level substantial or high,

b) the binding has been established on the basis of recognised procedures in Montenegro, which resulted in the registration of the binding in an authoritative source,

c) the binding has been verified on the basis of information from an authoritative source;

3) for the assurance level "high", in addition to requirements of the assurance levels "low" and "substantial" referred to in item 1) sub item c) and item 2) sub item b) of this Article, the existence of evidence that:

a) the identity proofing of the natural person acting on behalf of the legal person has been performed at assurance level high,

b) The binding has been verified on the basis of a unique identifier representing the legal person and on the basis of data on the natural person kept in an authoritative source.

Article 8

Determination of assurance level on the bases of electronic identification means characteristics and design referred to in Article 3 paragraph 2 item 2 indent 1 of this Rulebook shall include determination:

1) for assurance level "low" that:

a) the electronic identification means utilises at least one authentication factor,

b) the electronic identification means is designed so that the issuing natural person, legal person or public authority can determine that means is used only under the control of or by the person to whom it belongs;

2) for assurance level "substantial" that:

a) the electronic identification means utilises at least two authentication factors from different categories,

b) the electronic identification means is designed so that means is used only under the control of or by the person to whom it belongs;

3) for assurance level "high", in addition to requirements for assurance level "substantial" that:

a) the electronic identification means protects against duplication and tampering,

b) the electronic identification means is designed so that it can be reliably protected by the person to whom it belongs against use by other persons.

Article 9

Determination of assurance level based on procedures for issuance, delivery and activation of electronic

identification means referred to in Article 3 paragraph 2 item 2 indent 2 of this Rulebook shall include determination:

1) for assurance level "low" that, after issuance, the electronic identification means is delivered via a mechanism by which it s assumed that ensures delivery to the person to whom the means was issued;

2) for assurance level "substantial" that, after issuance, the electronic identification means is delivered via a mechanism by which it s assumed that ensures personal delivery to the person to whom the means was issued;

3) for assurance level "high" that it will be verified by activation that the electronic identification means was delivered to the person to whom the means was issued.

Article 10

Determination of assurance level on the bases of procedures for suspension, revocation and reactivation of the electronic identification means referred to in Article 3 paragraph 2 item 2 indent 3 of this Rulebook shall include determination for assurance level "low" that:

1) it is possible to suspend and/or revoke an electronic identification means in a timely and effective manner;

2) the existence of measures that prevent unauthorised suspension, revocation and/or reactivation;

3) reactivation shall be possible only if the same assurance requirements as established before the suspension or revocation continue to be met.

Procedures referred to in paragraph 1 of this Article shall apply also to determination of assurance level substantial and high.

Article 11

Determination of assurance level on the bases of procedures for renewal and replacement of the electronic identification means referred to in Article 3 paragraph 2 item 2 indent 4 of this Rulebook shall include determination:

1) for assurance level "low" and "substantial" that renewal or replacement meets the same assurance requirements as initial identity proofing and verification or is based on a valid electronic identification means of the same, or higher, assurance level;

2) for assurance level "high" that renewal or replacement meets the same requirements as for the assurance levels "law" and "substantial", and where renewal or replacement is based on a valid electronic identification means, the identity data is verified with an authoritative source.

Article 12

Determination of assurance level on the bases of authentication referred to in Article 3 paragraph 2 item 3 of this Rulebook shall include determination:

1) for assurance level "low" that:

a) the revealing and forwarding of person identification data is preceded by reliable verification of the electronic identification means and its validity,

b) person's identification data, if stored as part of the authentication mechanism, is adequately protected against loss and against compromise,

c) the authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities of intruding into system (password guessing, eavesdropping, replay or manipulation of communication etc) could subvert the authentication mechanism;

2) for assurance level "substantial" that:

a) the electronic identification means meets requirements for assurance level "low",

b) the revealing and forwarding of person identification data is preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication,

c) the authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities of intruding into system (password guessing, eavesdropping, replay or manipulation of communication etc) could subvert the authentication mechanism;

3) for assurance level "high":

a) that the electronic identification means meets requirements for assurance level "substantial", and

b) that the authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities of intruding into system (password guessing, eavesdropping, replay or manipulation of communication etc) could subvert the authentication mechanism.

Article 13

The assurance level on the bases of internal acts on the manner and procedures of issuing electronic identification means referred to Article 3 paragraph 2 item 4 indent 1 of this Rulebook shall be determined depending on whether those internal acts are publically available and whether they are updated regularly.

Article 14

Determination of assurance level on the bases of published notices and user information referred to in Article 3 paragraph 2 item 4 indent 2 of this Rulebook shall include determination:

1) that there is published service definition that includes all applicable terms, conditions, and fees, including any limitations of its usage, as well as privacy policy;

2) that appropriate policies and procedures are put in place in order to ensure that users of the service are informed in a timely and reliable fashion of any changes to the service definition including change of service terms and conditions, fees, any limitations of its usage as well as privacy policy;

3) that appropriate policies and procedures are put in place providing for full and correct responses to requests for information.

Article 15

Determination of assurance level on the bases of information security management referred to in Article 3 paragraph 2 item 4 indent 3 of this Rulebook shall include determination:

1) for the assurance level "law" that there is an effective information security management system for the management and control of information security risks;

2) for the assurance levels "substantial" and "high":

a) that requirements for the assurance level "law" are met, and

b) that in implementing the information security management system measures and activities are applied in accordance with Article 52 paragraph 2 of the Law on Electronic Identification and Electronic Signature (hereinafter: the Law) or principles for the management and control of information security risks.

Article 16

Determination of assurance level on the bases of record keeping referred to in Article 3 paragraph 2 item 4 indent 4 of this Rulebook shall include determination:

1) that record keeping and maintaining relevant information using an effective record-management system is performed in accordance with the law governing personal data protection;

2) that data in the records is retained in accordance with the Law.

Article 17

Determination of assurance level on the bases of the requirements with respect to facilities and staff referred to in Article 3 paragraph 2 item 4 indent 5 of this Rulebook shall include determination that:

1) facilities used for providing the service are continuously monitored for, and protect against, damage caused by environmental events, unauthorised access and other factors that may impact the security of the electronic identification scheme;

2) facilities used for processing personal, cryptographic or other sensitive information can be accessed only by authorised staff or subcontractors;

3) employees or subcontractors have education qualification level VI, i.e. VII1 in the fields of information and communication technologies, adequate work experience and expertise (training, appropriate certificate or work experience), depending on the job position; and

4) it is ensured that tasks of employees or subcontractors in accordance with job position definitions established by the internal organisation and systematisation act, special act or other document.

Article 18

Determination of assurance level on the bases of technical controls carried out by a natural person, legal person, or a public authority issuing electronic identification means referred to in Article 3 paragraph 2 item 4 indent 6 of this Rulebook shall include determination:

1) for the assurance level "law" that:

a) there are proportionate technical controls to manage the risks posed to the security of the services, protecting the confidentiality, integrity and availability of the information processed,

b) electronic communication channels used to exchange personal or sensitive information are protected against eavesdropping, manipulation and replay,

c) access to sensitive cryptographic material, if used for issuing electronic identification means and authentication, is restricted to the roles and applications strictly requiring access and storage of such material shall be ensured in the format other than plain text,

d) procedures exist to ensure that security is maintained over time and that there is an ability of the system to respond to changes in risk levels, incidents and security breaches,

e) all media containing personal, cryptographic or other sensitive information are stored, transported and disposed of in a safe and secure manner;

2) for assurance levels "substantial" and "high" in addition to requirements for assurance level "low" referred in item 1 of this paragraph, that sensitive cryptographic material, if used for issuing electronic identification means and authentication is protected from tampering.

Article 19

Determination of assurance level on the bases of compliance and audit referred to in Article 3 paragraph 2 item 4 indent 7 of this Rulebook shall include determination:

1) for assurance level "low" that there are periodical internal audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with the Law;

2) for assurance level "substantial" that there are periodical internal or external audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with the Law;

3) for assurance level "high" that there are periodical independent external audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with the Law.

Article 20

Where the electronic identification means meets requirements for higher assurance level, it is implied that the means also meets requirements for lower assurance level.

Article 21

This Rulebook shall enter into force on the eighth day from the day of its publication in the Official Gazette of Montenegro.