* 3212 312, 075 227 125

Official Gazette number: 53/2020

Official Gazette publication date: 28.02.2020

Constitutional Court Resolution number (U.no.): /

**MINISTRY OF INFORMATION SOCIETY AND ADMINISTRATION**

Pursuant to Article 18 paragraph (3) of the Law on Electronic Documents, Electronic Identification and Trust Services (\*) (“Official Gazette of Republic of North Macedonia” no. 101/19 and 275/19), the Minister of Information Society and Administration adopted the following

**RULEBOOK ON THE PROCEDURES AND STANDARDS FOR MEETING THE TECHNICAL, PHYSICAL AND ORGANIZATIONAL SECURITY MEASURES FOR ELECTRONIC IDENTIFICATION SCHEMES**

**Article 1**

The Rulebook herein shall prescribe the procedures and standards for meeting the technical, physical and organizational security measures for electronic identification schemes.

**Article 2**

The level of security of the means for electronic identification issued within the registered scheme for electronic identification shall be provided through:

a) Procedures for management of the means for electronic identification;

b) Procedures for authentication of the means for electronic identification;

c) Procedures and standards for meeting the technical, physical and organizational security measures for electronic identification schemes.

The means for electronic identification issued within the registered electronic identification scheme provisioning high security level shall be deemed that they also ensure the lower security level as well.

**Article 3**

Particular terms used in this Rulebook shall have the following meaning:

-     “Trust source” shall refer to the source of necessary data which can be trusted that it provides accurate data or evidence which can be used for proving the identity of the person using the mean for electronic identification;

-     “Authentication factor” shall refer to a particular factor specified in electronic form deemed essential in the authentication process, and for which it is validated for being connected to the person referring to such factor. The authentication factor may be one of the following categories:

(a) “Owned authentication factor” shall refer to the authentication factor for which it is required from the subject of electronic identification to prove that they own the factor as part of the mean for electronic identification;

(b) “Known authentication factor” shall refer to the authentication factor for which it is required from the subject of electronic identification to prove that they know particular data related to the mean for electronic identification;

(c) “Characteristic authentication factor” shall refer to the authentication factor based on the physical attributes of the person being subject of electronic identification, which factor should be provided by the subject of electronic identification;

-      “Dynamic identification” shall refer to the electronic process using cryptographic or other techniques for provisioning means for electronic identification in the form of electronic validation or proof that the subject of electronic identification owns or has the identification data, whereby it is changed in the system validating the identity of the subject of electronic identification and is different for every particular authentication of the subject;

-     “Network and information system security management” shall refer to the capability of the network and information systems to a particular trust level to contradict any action compromising the availability, authenticity, integrity or trustity of the preserved or transferred or processed data or related services being offered or made available through such networks and information systems;

-     “Node” shall refer to the connection point which is part of the interoperability architecture for electronic identification and is included in the cross border authentication of persons with the option to recognize and process or transfer them to another nodes by using the national infrastructure for electronic identification to the interface of the national infrastructure for electronic identification of another country;

-     “Node operator” shall refer to the legal entity responsible for node maintenance and for proper and secure performance of its functions as a connection point.

**Article 4**

The procedures and standards referring to the technical measures for security of the electronic identification scheme shall also apply to the means for electronic identification issued within the electronic identification scheme.

The electronic identification schemes may be of low, significant and high level with regards to the procedures used for:

- Sign in and sign up of the subject of electronic identification;

- Check of the identity and verification of natural persons; or

- Check of identity and verification of legal entities.

Depending on the level of the electronic identification scheme, the means for electronic identification issued within that scheme are on the same level of electronic identification.

The nodes should be different between the bodies of the public and private sector through the technical means being used.

**Article 5**

The security level of the electronic identification scheme in the sign in and sign up phase may be:

-     Low security level;

-     Significant security level; and

-     High security level.

When using the electronic identification schemes for low, significant and high security level in the sign in and sign up phase the following should be done:

-     The subject of electronic identification to be aware of the conditions related to the use of the means for electronic identification;

-     The subject of electronic identification to be aware of the recommendations for the security measures related to the mean for electronic identification; and

-     All relevant data on the identity of the subject of electronic identification to be provided, which are necessary for proving the connection between the mean for electronic identification and the subject of electronic identification and verification of their identity.

**Article 6**

The security level of the electronic identification scheme in the early phase of the identity check and verification of natural persons can be:

-     Low security level;

-     Significant security level; and

-     High security level.

**Article 7**

When using the electronic identification scheme at a low security level in the phase of identity check and verification of natural person:

-      It should be deemed that the natural person owns the proof needed for issuance of the mean for electronic identification;

-     It should be deemed that the natural person who owns the proof required for issuing the mean for electronic identification in original or according to the data obtained from reliable source show that the proof is valid;

-     According to the data obtained from reliable source it can be confirmed that the natural person exists and that the natural person is linked to the identity it shows.

**Article 8**

When using the electronic identification scheme at a significant security level, apart from the standards referring to the electronic identification scheme at low security level in the phase of identity and verification check of natural persons, the following should be done:

-     To be confirmed with certainty that the natural person possesses the proof required for issuance of electronic identification in original form to be confirmed by a reliable source that the natural person exists and the taken measures for identity check lead to the same natural person, considering the risk of lost, stolen, suspended, confiscated or expired proof at the disposal of the reliable source; or

-     The natural person to present a proof of their personal identification for the purpose of issuance of mean for electronic identification and taken measures for reducing the risk that the proof for personal identification is lost, stolen, suspended, confiscated or expired; or

-     The procedure for identity check of the natural person requesting mean for electronic identification to be already conducted by registered or certified trust service provider for the issuance of advanced electronic signature and such procedure to have the equivalent validity according to the reports of the compliance assessment body; or

-     The natural person being checked to possess already issued valid mean i.e. advanced electronic signature issued by registered or certified trust service provider.

**Article 9**

When using the electronic identification scheme at a high security level, apart from the standards referring to the electronic identification scheme at significant security level in the phase of identity and verification check of natural persons, the following should be done:

-     The identity check of the natural person should be done by using biometric data or physical features which uniquely link the person with the personal identification document with a certificate from reliable source; or

-     Already done identity check of the natural person for the purpose of issuing other equivalent mean i.e. qualified electronic signature by another qualified trust service provider and taken measures for confirmation of the validity of the previous check; or

-     The natural person being checked to possess already issued equivalent valid mean i.e. qualified electronic signature issued by registered or certified qualified trust service provider.

**Article 10**

When using the electronic identification scheme at a low security level in the phase of identity check and verification of natural person:

-     Relevant data should be enclosed on the identity of the legal entity to the request for issuing mean for electronic identification, confirming the entry of the legal entity in the relevant register for entry of legal entities;

-     In order to assume that the proof confirming the entry of the legal entity in the relevant register for entry of legal entities is original or according to the data obtained from a reliable source to show that the proof is valid.

**Article 11**

When using the electronic identification scheme at a significant security level, apart from the procedures referring to the electronic identification scheme at low security level in the phase of identity and verification check of legal entities, the following should be done:

-     To establish with certainty that the legal entity possesses the proof for entry of the legal entity in the relevant register for entry of legal entities containing data on the name and the form of the legal entity, as well as data on the registration in original, and according to the reliable source to be confirmed that the legal entity exists and the taken measures for identity check refer to the same legal entity, considering the risk of lost, stolen, suspended, confiscated or expired proof at the disposal of the reliable source; or

-     The procedure for identity check of the legal entity requesting the issuance of mean for electronic identification to be already conducted by registered or certified trust service provider for the issuance of other mean i.e. advanced electronic seal and such procedure to have the equivalent validity according to the reports of the compliance assessment body; or

-     The legal entity already has other valid mean i.e. advanced electronic seal issued by registered or certified trust service provider.

**Article 12**

When using the electronic identification scheme at a high security level, apart from the standards referring to the electronic identification scheme at significant security level in the phase of identity and verification check of legal entities, the following should be done:

-     The legal entity to possess the original proof confirming the entry of the legal entity in the relevant register for entry of legal entities containing data on the name and the form of the legal entity, and according to the reliable source to be confirmed that the legal entity exists in the legal operations; or

-     The procedure for identity check of the legal entity requesting the issuance of mean for electronic identification to be already conducted by qualified trust service provider for the issuance of other mean i.e. qualified electronic seal and such procedure to have the equivalent validity according to the reports of the compliance assessment body; for which the appropriate measures were taken in order to establish whether the results from the other procedure are still valid; and

-     The legal entity to have other valid mean i.e. qualified electronic seal issued by registered or certified qualified trust service provider for which the appropriate measures were taken in order to establish whether the qualified electronic seal is still valid.

**Article 13**

The mean for electronic identification of the natural person which is the authorized person of the legal entity shall be linked with the mean for electronic identification of the legal entity if:

-     The link between the two means can be terminated via activation, suspension, renewal or confiscation of one mean for electronic identification, irrespective of the other mean for electronic identification, in accordance with the regulations from the area of the activity performed by the legal entity, as well as the regulations referring to the natural person as authorized person of the legal entity;

-     The natural person who is the authorized person of the legal entity whose mean for electronic identification is linked to the mean for electronic identification of the legal entity may delegate the performance of particular tasks of another natural person on behalf of the legal entity, whereby the responsibility shall be borne by the authorized person of the legal entity.

The security levels of the mean for electronic identification linked to the natural person who is the authorized person of the legal entity can be:

-     Low security level;

-     Significant security level; and

-     High security level.

**Article 14**

The mean for electronic identification of the natural person which is the authorized person of the legal entity shall be linked with the mean for electronic identification of the legal entity at low security level if:

-     The check and verification of the identity of the natural person which is the authorized person of the legal entity was done at low security level;

-     The connection of the natural person with the legal entity is in accordance with the regulations referring to the authorizations of the natural persons as authorized persons of the legal entities; and

-     The natural person met the conditions stipulated by law referring to the natural persons as authorized persons of the legal entities.

**Article 15**

The mean for electronic identification of the natural person which is the authorized person of the legal entity shall be linked with the mean for electronic identification of the legal entity at significant security level if:

-     The natural person met the conditions stipulated by law referring to the natural persons as authorized persons of the legal entities;

-     The check and verification of the identity of the natural person which is the authorized person of the legal entity was done at significant or high security level;

-     The natural person was recorded as authorized person of the legal entity based on relevant proof i.e. based on the entry of the legal entity in the relevant register for entry of legal entities; and

-     The connection of the natural person with the legal entity is verified with information obtained from competent body.

**Article 16**

The mean for electronic identification of the natural person which is the authorized person of the legal entity shall be linked with the mean for electronic identification of the legal entity at high security level if:

-     The natural person met the conditions stipulated by law referring to the natural persons as authorized persons of the legal entities;

-     The natural person was recorded as authorized person of the legal entity based on relevant proof i.e. based on the entry of the legal entity in the relevant register for entry of legal entities;

-     The check and verification of the identity of the natural person which is the authorized person of the legal entity was done at low security level; and

-     The connection was confirmed by the legal entity with qualified electronic seal or with mean for electronic communication from high security level.

**Article 17**

The standards for meeting the technical security measures of the electronic identification schemes at low security level, referring to the features and the design of the means for electronic identification at high level shall be as follows:

-     The mean for electronic identification shall use at least one authentication factor.

-     The mean for electronic identification shall be designed in a manner in which the issuer of the mean is deemed to have taken reasonable measures to check whether the mean is used only under control or in possession of the person to which such mean was issued.

The standards for meeting the technical security measures of the electronic identification schemes at significant security level, referring to the features and the design of the means for electronic identification at significant level shall be as follows:

-     The mean for electronic identification shall use at least two authentication factors from different categories; and.

-     The mean for electronic identification shall be designed in a manner where it can be assumed that the mean is used only under control or in possession of the person to which such mean was issued.

The standards for meeting the technical security measures of the electronic identification schemes at high security level, referring to the features and the design of the means for electronic identification at high level shall be as follows:

-     The mean for electronic identification shall use at least two authentication factors from different categories;

-     The mean for electronic identification shall be designed in a manner where it can be assumed that the mean is used only under control or in possession of the person to which such mean was issued;

-     The mean for electronic identification shall be protected from multiplying and intrusion, as well as from attack with high potential for disrupting its security; and

-     The mean for electronic identification shall be designed in a manner where it can be fully protected by the person it belongs to from the use of other parties.

The procedures for issuance, delivery and activation of the means for electronic identification at low level shall include issuance of the mean for electronic identification and delivery thereof through mechanism with which it can be assumed that the subject requesting such mean for electronic identification shall obtain the mean.

The procedures for issuance, delivery and activation of the means for electronic identification at significant level shall include issuance of the mean for electronic identification and delivery thereof through mechanism with which it can be assumed that the subject requesting such mean for electronic identification shall possess the mean.

The procedures for issuance, delivery and activation of the means for electronic identification at high level in the process for activation of the mean for electronic identification shall confirm that such mean shall be given into possession of the person - owner of the mean for electronic identification.

The procedures for suspension, revocation and reactivation of the means for electronic identification at low, significant and high level should confirm that:

-     There is a possibility for timely and efficient suspension or revocation of the mean for electronic identification;

-     There are established measures taken over in order to prevent unauthorized suspension, revocation and reactivation of the mean for electronic identification; and

-     Reactivation can be made only if the conditions which were valid prior to the suspension or revocation were met.

The procedures for renewal and replacement of the means for electronic identification at low and significant security level, considering the risks of change in the data on the person’s identity, should confirm that:

-     The same standards applicable for the first identity and verification check of the person were met; or

-     The procedure for renewal and replacement was conducted by using valid mean for electronic identification at the same or higher security level.

When the renewal or replacement of the means for electronic identification at high security level is conducted by using valid mean for electronic identification, the procedures for renewal and replacement of the means should, apart from the standard referred to in paragraphs 1, 2 and 3 of this Article, to also confirm the identity data from reliable source.

**Article 18**

The authentication of the means for electronic identification at low level should:

1. Ensure verification of the means for electronic identification and confirmation of the validity thereof prior publishing the data on identification of the person;

2. Keep the data on identification of the persons as part of the authentication mechanism, thus ensuring that the information are protected from loss or compromising thereof, including their processing outside the network systems.

3. Be conducted in a manner including security controls for verification of the means for electronic identification, as well as measures for protection from potential attack, interception, reoccurrence or manipulation in the course of electronic communication from the threats for possible attack on the authentication mechanisms.

Authentication of the means for electronic identification at significant security level, apart from the standards referred to in paragraph 1 of this Article, should:

1. Ensure verification of the means for electronic identification via dynamic authentication prior publishing the data on identification of the person;

2. Be conducted in a manner including conducting of security controls for verification of the means for electronic identification, as well as measures for protection from potential attack, interception, reoccurrence or manipulation in the course of electronic communication from the threats for possible attack on the authentication mechanisms.

The authentication of the means for electronic identification at high security level, apart from the criteria referred to in paragraph 2 of this Article, should contain in the authentication mechanism security controls for verification of the means for electronic identification, as well as measures for protection and prevention from potential attack, interception, reoccurrence or manipulation in the course of electronic communication from the threats for possible attack on the authentication mechanisms.

**Article 19**

The issuer of electronic identification schemes should use equipment, procedures and measures for administration and management of the security of the used infrastructure meeting the standards for information security management i.e. the standards from ISO 27000 series.

The system and the technical equipment used for issuance of electronic identification schemes, as well as for other services offered by the issuer of electronic identification schemes should be designed and used solely for such purpose.

The physical access to the capacities, information and systems of the issuer of the electronic identification schemes shall be allowed only to the authorized persons of the legal entity.

If other persons needs access to the capacities, information and systems of the issuer of the electronic identification schemes, it should be accompanied and monitored by the authorized person.

The issuer of electronic identification schemes should provide the following:

1. 24-hour physical and electronic monitoring for the purpose of preventing unauthorized access to the premises used for the functions of electronic identification scheme management;

2. Ensure the equipment, information, media and program used by the issuer of the electronic identification schemes not to be taken out of the premises without previous authorization; and

3. Keep records of every access to the premises and perform periodical control thereof.

The physical security of the premises of the issuer of electronic identification schemes should have a clear description including the following:

-   Established security zones and their security features;

-   The connections with the protected means; and

-   Full and updated list of persons employed at the issuer of electronic identification schemes with granted right to access to the determined zones, available for an insight.

The technical equipment used by the issuer of electronic identification schemes should be protected from unauthorized access.

The capacities of the issuer of the electronic identification schemes shall be protected from the risks in the surrounding by applying measures and controls reducing the risk of potential threats, including theft, fire, explosions, smoke, water, dust, vibrations, chemical effects, obstacles in the electricity supply and electromagnetic radiation.

The issuer of electronic identification schemes should ensure safe system management.

The persons employed at the issuer of electronic identification schemes should maintain and improve the service trustity.

The systems in possession of the issuer of electronic identification schemes should have access control and should be used only by authorized persons.

The systems should identify every user and successfully confirm the credibility thereof before allowing any action on behalf of that user or the role thereof.

In the event when the system user, who previously signed out, reappears the system should confirm its credibility.

If the number of unsuccessful attempts to confirm the credibility is the same with the maximum number of allowed attempts, the system should deny any further attempts for confirming the credibility, unless the person has administrator role.

The provisions referred to in paragraphs 1 through 14 of this Article referring to system security shall also apply to the operating system or to the level of particular system elements.

**Article 20**

The issuers of electronic identification schemes should meet the following standards:

-     Set internal rules for the information types that may be required, the procedure for proving the identity of entities requesting issuance or using mean for electronic identification and information whether such data can be kept and the period of keeping thereof;

-     Publish the basic features for the scheme, including all applicable conditions, limitation of use and compensations for provisioning thereof, including privacy policy;

-     Establish efficient system for records management for the purpose of keeping records and relevant information, considering the applicable standards and good practices with regards to the data protection and keeping thereof;

-     Establish procedures providing training, qualifications, experience and skills necessary for performance of the tasks performed by the persons hired by the issuers of electronic identification schemes and their subcontractors;

-     Provide persons – employees/hired persons for the purpose of performing their activity and for provisioning of the service according to the established procedures for provisioning thereof; and

-     Take measures for protection of the means and facilities it uses from damage caused by ecologic events, unauthorized access and other factors which may affect the security of the service.

The issuers of electronic identification schemes, which also provide other type of trust services stipulated by law, should have internal organization which should be fully operational in all departments referring to the provisioning of trust services.

The means and facilities used by the issuer of electronic identification schemes should guarantee that the means on which personal, cryptographic or other sensitive data and information are being kept or processes are protected from unauthorized access.

**Article 21**

The issuer of electronic identification scheme at low security level should:

-     Take measures to ensure conducting proportional technical controls of risk management which may affect the security of the provisioned services, protection of the trustity, integrity and availability of the processed information;

-     Protect electronic communication channels used in the course of exchange of personal or sensitive information for the purpose of their protection from interception, manipulation and reproduction;

-     Clearly limit the access to sensitive cryptographic material if used for issuance of means for electronic identification and authentication and protect thereof from unauthorized access and take measures in order to ensure that such material is not preserved in the form of ordinary text;

-     Implement procedures ensuring maintenance of the security for a long period of time and possibility to respond to the changes in the level of risk, incident and disruptions of the security of information systems and means it uses; and

-     For all media containing personal, cryptographic or other sensitive information to ensure keeping, transport and removal in a safe and secure manner.

The issuer of electronic identification scheme at significant and high security level, apart from the measures referred to in paragraph 1 of this Article, should take measures for protection of the sensitive cryptographic material, if being used for issuance of means for electronic identification and authentication, from potential disruptions.

**Article 22**

The issuer of electronic identification scheme at low security level should ensure conducting of periodical internal controls including control of all parts relevant for the provisioning of trust services, for the purpose of obtaining assessment of compliance with the relevant standards.

The issuer of electronic identification scheme at significant security level should ensure conducting of periodical internal and external controls including control of all parts relevant for the provisioning of trust services, for the purpose of obtaining assessment of compliance with the relevant standards.

The issuer of electronic identification scheme at high security level should ensure conducting of periodical external controls including control of all parts relevant for the provisioning of trust services, for the purpose of obtaining assessment of compliance with the relevant standards.

External control shall be conducted every three years for assessment of the compliance of the electronic identification schemes with the relevant standards, which are issued for realization of the competences of the state administration bodies.

**Article 23**

The protection of the privacy and trustity of the exchanged data and keeping the data integrity between the nodes shall be provided by using the best available technical solutions and practices for protection.

The nodes shall not contain personal data, apart from the purpose referred to in Article 26 paragraph 3 of the Rulebook herein.

**Article 24**

The communication between the nodes should ensure data integrity and authenticity for the purpose of ensuring that all requests and answers are authentic and unchanged.

The nodes shall use technical and technological solutions which were successfully implemented for operational use.

**Article 25**

The nodes should use syntax formats of usual messages based on standards used more than once for communication and for which it is confirmed that they function in operational environment.

The syntax should allow:

(a) Proper processing of the minimum set of data for identification of persons which uniquely represent particular natural person or legal entity;

(b) Proper processing of the level of security of the means for electronic identification;

(c) Difference between the bodies of the public and private sector;

(d) Flexibility for meeting the needs for additional attributes related to the identification.

**Article 26**

The node operator shall communicate metadata for node management of standardized mechanical processing method, which is safe and trust.

The security relevant parameters shall be automatically taken over.

The node operator shall keep data which, in the event of incident, ensure reconstruction of the sequence of exchange of messages for determining the place and nature of the incident.

The data shall be kept for a period of 5 years and shall consist of the following elements:

(a) Node identification;

(b) Message identification;

(c) Date and time of message.

**Article 27**

The node operators ensuring authentication should prove that, with regards to the nodes participating in the interoperability frame, the authentication method meets the ISO/IEC 27001 standard, via certification or with equivalent assessment method.

The node operators should ensure critical security updates without any unnecessary delay.

**Article 28**

The minimum data set for personal identification, which uniquely represent particular natural person, should contain the following:

1.  Mandatory attributes, cumulatively:

(a) Current surname(s);

(b) Current name(s);

(c) Date of birth;

(d) Unique identifier created by the sender in line with the technical specifications for the purposes of cross border identification which shall not change with time.

2.  One or multiple of the following additional attributes:

(a) Name(s) and surname(s) at birth;

(b) Place of birth;

(c) Current address;

(d) Sex.

The minimum data set for personal identification, which uniquely represent particular legal entity, should contain combination of attributes, as follows:

1.  Mandatory attributes, cumulatively:

(a) Current name of the legal entity;

(b) Unique identifier created by the sender in line with the technical specifications for the purposes of cross border identification which shall not change with time.

2.  One or multiple of the following additional attributes:

(a) Current address;

(b)Unique tax number;

(c) Unique identification number of the entity.

The data shall be transferred based on original signs and if appropriate shall be translated with Latin letters.

**Article 29**

The Rulebook herein shall enter into force on the next day as of the day of publishing thereof in the “Official Gazette of the Republic of North Macedonia”.

|  |  |
| --- | --- |
| No. 08/1-1205/2 | Minister of Information |
| 26 February 2020 | Society and Administration |
| Skopje | **Damjan Mancevski** |