LAW OF THE KYRGYZ REPUBLIC

Bishkek, dated 19 July 2017 No.128

On Electronic Signature

Article 1. Scope of the Law

1. This Law shall regulate relations on the use of electronic signatures when making civil transactions, providing public and municipal services, performing public and municipal functions, as well as committing legally significant actions.

2. Laws of the Kyrgyz Republic may establish peculiarities of using electronic signatures in certain types of relations (preparation and holding of elections, performance of civil law transactions, provision of public and municipal services, performance of banking operations, accounting, etc.).

Article 2. Terms Used in this Law

The terms used for the purposes of this Law shall mean the following:

1) **electronic signature** - information in electronic form which is attached to and/or logically linked to other information in electronic form and is used to identify the person on whose behalf the information is signed;

2) **signature verification key certificate** - an electronic document or a hard copy issued by the certification authority and confirming that the signature verification key belongs to the owner of the signature verification key certificate;

3) **qualified signature verification key certificate (hereinafter referred to as a qualified certificate)** - a signature verification key certificate issued by an accredited certification authority or an authorized person of the accredited certification authority or an executive body responsible for the use of electronic signature which performs the functions of the principal (root) certification authority;

4) **owner of the** **signature verification key certificate** - a person to whom a signature verification key certificate has been issued by the certification authority pursuant to the procedure established by this Law;

5) **signature key** - a unique sequence of characters designed to create an electronic signature;

6) **signature verification key** - a unique sequence of characters, unambiguously associated with the signature key and intended for verification of electronic signature authenticity (hereinafter referred to as electronic signature verification);

7) **certification authority** - a legal entity or an individual entrepreneur engaged in activities related to the creation and issuance of signature verification key certificates;

8) **accreditation of a certification authority** - recognition by the executive body responsible for the use of an electronic signature that the certification authority meets the requirements set out in this Law;

9) **electronic signature facilities** - encryption (cryptographic) facilities used to implement at least one of the following functions: creation of an electronic signature, electronic signature verification, creation of signature keys and signature verification keys;

10) **certification authority facilities** - software and/or hardware used to perform the functions of creating, storing and issuing signature verification key certificates, as well as to maintain a register of signature verification key certificates;

11) **electronic interaction participants** - state bodies, local governments, organizations, their unions and associations, as well as citizens exchanging information in electronic form;

12) **corporate information system** - an information system where a specific range of persons is involved in electronic interaction;

13) **public information system** - an information system where the electronic interaction participants are an indefinite range of persons and the use of which cannot be denied to these persons;

14) **information system** **operator** - an individual, legal entity regardless of its legal form and form of ownership, state authority, local government acting directly or through their representatives, carrying out activities related to the operation of the information system, its technical and software support.

Article 3. Legal Regulation of Relations in the Field of Electronic Signature Use

1. Relations in the area of electronic signature use shall be regulated by this Law, other laws of the Kyrgyz Republic in the area of electronic governance.

2. The procedure for using an electronic signature in a corporate information system may be established by the owner of the system or by an agreement of the electronic interaction participants in the system, unless otherwise established by the legislation of the Kyrgyz Republic in the field of electronic governance.

3. Types of electronic signature used by executive authorities and local governments, as well as requirements to ensure the compatibility of such electronic signatures, shall be established by the Government of the Kyrgyz Republic.

Article 4. Principles for Using Electronic Signature

The principles for using electronic signature shall be:

1) the right of electronic interaction participants to use any type of electronic signature at their discretion, if the requirement to use a particular type of electronic signature in accordance with the purposes of its use is not provided for by legislative acts, other normative legal acts (in cases when legislative acts provide for such a possibility) or by agreement of electronic interaction participants;

2) the possibility for electronic interaction participants to use at their discretion any technology and/or hardware that allows to meet the requirements of this Law in respect of the use of particular types of electronic signature;

3) compliance of requirements for the use of a particular type of electronic signature established in legislative and other regulatory acts with the objectives in which this electronic signature is used;

4) inadmissibility of recognition of an electronic signature and/or an electronic document signed by it as invalid only on the grounds that the signature in the electronic document is not a handwritten signature.

Article 5. Types of Electronic Signature

1. The types of electronic signature, relations in the use of which are regulated by this Law, shall be simple electronic signature and enhanced electronic signature. There are an enhanced non-qualified electronic signature (hereinafter referred to as an unqualified electronic signature) and an enhanced qualified electronic signature (hereinafter referred to as a qualified electronic signature).

2. A simple electronic signature is an electronic signature whose signature key matches the electronic signature itself (codes, passwords and other identifiers).

3. An unqualified electronic signature is an electronic signature that corresponds to the following features:

1) an electronic signature is the result of cryptographic transformation of information using the signature key;

2) an electronic signature allows identifying unambiguously a person who has signed the electronic document;

3) an electronic signature allows detecting the fact of making changes to the electronic document after its signing;

4) an electronic signature is created using electronic signature facilities that a person who has signed an electronic document is able to keep under his control.

4. A qualified electronic signature is an electronic signature that corresponds to all features of an unqualified electronic signature and to the following additional features:

1) the electronic signature verification key is specified in a qualified certificate;

2) electronic signature facilities that have received confirmation of compliance with the requirements established in accordance with this Law are used to create and check the electronic signature.

5. When using an unqualified electronic signature, a signature verification key certificate may not be created if the compliance of the electronic signature with the features of an unqualified electronic signature established by this Law can be ensured without using a signature verification key certificate.

Article 6. Conditions for Recognition of Electronic Documents Signed with an Electronic Signature as Equivalent to Hard Copies Signed with a Handwritten Signature

1. Information in electronic form signed with a qualified electronic signature shall be deemed to be an electronic document equivalent to a hard copy signed with a handwritten signature, except for cases when laws or other regulatory acts prohibit compiling such a document in electronic form.

2. Information in electronic form signed with a simple electronic signature or an unqualified electronic signature shall be deemed to be an electronic document equivalent to a hard copy signed with a handwritten signature in cases established by regulatory acts or an agreement of electronic interaction participants, unless laws or other regulatory acts prohibit compiling such a document in electronic form. Normative legal acts and agreements of electronic interaction participants establishing cases when electronic documents signed with an unqualified electronic signature are recognized as equivalent to hard copies signed with a handwritten signature should provide for the procedure of electronic signature verification.

3. If according to the law, other normative legal acts or normal business practice, a hard copy must be stamped, an electronic document signed with an enhanced electronic signature shall be deemed equivalent to a hard copy stamped and signed with a handwritten signature. Normative legal acts or agreement of electronic interaction participants may provide additional requirements for an electronic document with a view of its recognition as equivalent to a stamped hard copy.

4. A package of electronic documents, that is, several electronic documents linked to each other, can be signed with one electronic signature. When signing a package of electronic documents with an electronic signature, each of the documents included in this package is considered to be signed with an electronic signature of the type used to sign the package of electronic documents.

5. If, in accordance with the laws and regulatory legal acts of the Kyrgyz Republic adopted in accordance with these laws, special requirements are imposed for the processing of hard copy with the use of strict reporting forms, an electronic document signed with a qualified electronic signature shall be considered to meet these requirements.

Article 7. Recognition of Foreign Electronic Signatures

1. Electronic signatures created in accordance with the norms of the law of a foreign state shall be recognized in the Kyrgyz Republic as electronic signatures of the type to which they respond in accordance with this Law.

2. An electronic signature and an electronic document signed with it may not be considered null and void simply on the ground that the signature verification key certificate has been issued in accordance with the law of a foreign country.

Article 8. Powers of Executive Authorities in the Field of Electronic Signature Use

1. The executive body authorized in the field of the electronic signatures use (hereinafter referred to as the authorized body) and its powers shall be determined by the Government of the Kyrgyz Republic.

2. The authorized body shall:

1) carry out accreditation of certification authorities, including checks whether accredited certification authorities comply with the requirements for which they have been accredited, and in case of non-compliance issue instructions on elimination of violations;

2) act as the main (root) certification authority for accredited certification authorities.

3. The authorized body is obliged to ensure storage and unhindered round-the-clock access using information and telecommunication networks to the following information:

1) names, addresses of accredited certification authorities;

2) register of qualified certificates issued and cancelled by the authorized body that performs the functions of the main (root) certification authority;

3) list of certification authorities whose accreditation has been revoked;

4) list of accredited authorities whose accreditation has been suspended;

5) list of accredited certification authorities whose activities have been terminated;

6) registers of certificates transferred to the authorized body in accordance with Article 15 of this Law.

4. The Government of the Kyrgyz Republic shall establish:

1) the procedure for transferring registers and other information to the authorized body in the event of termination of the activities of the accredited certification authority;

2) the procedure for creating and maintaining registers of qualified certificates and for providing information from such registers;

3) rules for accreditation of certification authorities, including the procedure for checking whether accredited certification authorities comply with the requirements for which they have been accredited.

See:

[Resolution](toktom://db/159965) No. 742 of the Government of the Kyrgyz Republic dated 31 December 2019 "On Some Issues Related to the Use of Electronic Signature"

5. The executive authority in the field of security shall:

1) set the requirements for a qualified certificate form;

2) set requirements for electronic signature facilities and certification authority facilities;

3) confirm the compliance of electronic signature facilities and certification authority facilities with the requirements set in accordance with this Law, and publish a list of such facilities.

Article 9. Use of Simple Electronic Signature

1. An electronic document shall be considered to be signed with a simple electronic signature if one of the following conditions is met:

1) a simple electronic signature is contained in the electronic document itself;

2) specifying a simple electronic signature key in accordance with the rules established by the operator of the information system with the use of which the electronic document is created and/or sent has been a necessary condition for creation and/or sending of an electronic document using such information system, and the created (sent) electronic document contains information that unambiguously indicates the person on whose behalf an electronic document has been created (sent).

2. Signature verification key, electronic signature facilities and signature verification key certificate shall not be used when using a simple electronic signature.

3. Cases and the procedure for using a simple electronic signature shall be established by normative legal acts and/or agreements of electronic interaction participants providing equivalence of electronic documents signed with a simple electronic signature to hard copies signed with a handwritten signature. Such acts and agreements should provide, inter alia:

1) a mechanism for determining by a simple electronic signature a person on whose behalf an electronic document is signed;

2) obligation to maintain confidentiality of a simple electronic signature key.

4. The rules established for an enhanced electronic signature shall not apply to the creation, issuance and use of a simple electronic signature.

5. It is not allowed to use a simple electronic signature for signing electronic documents containing information constituting a state secret or in an information system containing information constituting a state secret, as well as for creating electronic documents requiring notarization or state registration in accordance with the legislation of the Kyrgyz Republic.

Article 10. Obligations of Electronic Interaction Participants When Using an Enhanced Electronic Signature

When using an enhanced electronic signature, electronic interaction participants are required to:

1) ensure the confidentiality of the signature key, in particular prevent the use of signature keys owned by them without their consent;

2) immediately, but in any case, within no more than one business day from the receipt of information about a violation of the confidentiality of the signature key, notify the certification authority that has issued the signature verification key certificate, and other electronic interaction participants about such violation;

3) if there is reason to believe that the signature key confidentiality is violated, not use this key;

4) use electronic signature facilities that have received confirmation of compliance with the requirements established in accordance with this Law for the exchange of electronic documents signed with a qualified electronic signature.

Article 11. Recognition of Qualified Electronic Signature Authenticity

Unless otherwise determined by the court, a qualified signature shall be deemed authentic, subject to the following conditions:

1) a qualified certificate containing a signature verification key has been created and issued by an accredited certification authority, the accreditation of which is valid (has not been suspended, terminated or canceled) on the day the certificate is issued;

2) a qualified certificate containing a signature verification key is valid (has not expired, has not been canceled) on the day of signing an electronic document (if there is reliable information about the moment of signing an electronic document) or on the day of verification - if the moment of signing is not defined;

3) there is a positive result of verification that the owner of the specified certificate owns the qualified electronic signature with which this electronic document is signed and that there are no changes made to this document after it is signed. In this case, verification is carried out using electronic signature facilities that have received confirmation of compliance with the requirements established in accordance with this Law and using a qualified certificate of the person on whose behalf the document is signed;

4) a qualified electronic signature is used in accordance with the restrictions contained in the qualified certificate of the person on whose behalf this document is signed (if restrictions are established).

Article 12. Electronic Signature Facilities

1. To create and verify electronic signatures, create signature keys and signature verification keys, electronic signature facilities shall be used that:

1) allow to determine whether a signed electronic document has been changed after it has been signed;

2) make it practically impossible to identify the signature key from an electronic signature or from its verification key.

2. When creating an electronic signature, the electronic signature facility must:

1) show the person who signs an electronic document the content of the information he/she signs;

2) create an electronic signature only after the person signing the information confirms the operation to create an electronic signature;

3) clearly and unambiguously indicate that an electronic signature has been created.

3. When verifying an electronic signature, the electronic signature facility must:

1) show the content of an electronic document signed with an electronic signature;

2) show whether changes have been made to an electronic document signed with an electronic signature;

3) identify the person whose signature key has been used to sign electronic documents.

4. Electronic signature facilities designed to create an electronic signature in electronic documents containing information constituting state secrets, or intended for use in the information system containing state secrets, are subject to mandatory certification for compliance with the requirements for protection of information of an appropriate degree of secrecy.

Electronic signature facilities designed to create an electronic signature in electronic documents containing confidential information must not violate the confidentiality of such information.

5. The requirements of parts 2 and 3 of this Article shall not apply to electronic signature facilities used to automatically create or verify electronic signatures in the information system.

Article 13. Certification Authority

1. The certification authority shall:

1) create a signature verification key certificate and issue it to the person who applied for such a certificate (hereinafter - the applicant);

2) set the validity period of signature verification key certificates;

3) revoke the signature verification key certificates issued by it;

4) at the request of the applicant, issue electronic signature facilities containing a signature key and a signature verification key (including those created by a certification authority) or enabling the creation of a signature key and a signature verification key by the applicant;

5) maintain a register of signature verification key certificates issued and revoked by it (hereinafter - the register of certificates), including, but not limited to, the information contained in the signature verification key certificates issued by it, as well as information on the date of expiration (revocation) of the signature verification key certificate and its basis;

6) establish the procedure for maintaining and accessing the register of certificates that are not qualified, and ensure access for persons to the information contained in the register of certificates, including through the Internet;

7) upon request of applicants create signature keys and signature verification keys.

If the certification authority creates signature keys, it shall ensure the confidentiality of such keys;

8) verify the uniqueness of signature verification keys in the register of certificates of this certification authority;

9) perform electronic signature verification based on requests from electronic interaction participants;

10) perform other activities related to the use of electronic signature.

2. The certification authority must:

1) inform applicants in writing about the conditions and procedure for the use of electronic signature and electronic signature facilities, about the risks associated with the use of electronic signature and measures necessary to ensure security of electronic signatures and their verification;

2) ensure that information contained in the register of certificates is up to date and protected from unauthorized access, destruction, modification, blocking or other unlawful acts with respect to such information;

3) provide free of charge to any person upon his or her request in accordance with the established procedure for access to the register of certificates the information contained in the register of certificates of the certification authority, including information on revocation of the signature verification key certificate.

3. The certification authority, in accordance with the legislation of the Kyrgyz Republic, shall be responsible for damage caused to other persons as a result of:

1) non-fulfillment or improper fulfillment of obligations arising from the service agreement by the certification authority;

2) non-fulfillment or improper fulfillment of obligations provided for in clause 9 of part 1, clauses 2 and 3 of part 2 of this Article.

4. The certification authority shall have the right to empower other persons (hereinafter - the authorized persons) to create and issue signature verification key certificates on behalf of the certification authority, signed with an electronic signature based on the signature verification key certificate issued to such an authorized person by the certification authority.

5. The certification authority referred to in part 4 of this Article shall be the main (root) certification authority in relation to authorized persons and shall perform the following functions in relation to them:

1) verify electronic signatures whose signature verification keys are specified in signature verification key certificates issued by authorized persons;

2) ensure electronic interaction between authorized persons as well as electronic interaction of authorized persons with the certification authority.

6. The information entered in the register of certificates is subject to storage during the entire period of activity of the certification authority, if a shorter period is not established by regulatory legal acts. In case of termination of the activities of the certification authority without transfer of its functions to other persons, it must notify in writing not less than one month prior to the date of termination of activity the holders of the signature verification key certificates issued by it, whose validity has not expired. In this case, after the certification authority has completed its activities, the information entered in the register of certificates must be destroyed.

In case of termination of the activities of the certification authority with transfer of its functions to other persons, it must notify in writing not less than one month prior to the date of transfer of its functions the holders of the signature verification key certificates issued by it, whose validity has not expired. In this case, after the certification authority has completed its activities, the information entered in the register of certificates must be transferred to the person that has taken over the functions of the certification authority that has ceased its activities.

7. The procedure for performing the functions of the certification authority, exercising its rights and fulfilling its obligations set out in this Article shall be determined by the certification authority itself, unless otherwise provided for in a regulatory legal act or an agreement between the electronic interaction participants.

8. An agreement on the provision of services by the certification authority that implements its activities in relation to an unlimited number of persons using a public information system shall be a public agreement.

Article 14. Signature Verification Key Certificate

1. The certification authority shall create and issue a signature verification key certificate based on an agreement between the certification authority and the applicant.

2. The signature verification key certificate shall contain the following information:

1) the start and end dates of its validity;

2) name, surname, patronymic (if any) - for individuals (name - for legal entities) or other identifier of the holder of the signature verification key certificate;

3) signature verification key;

4) name of the electronic signature facility used and/or the standards to which the signature key and signature verification key correspond;

5) name of the certification authority that has issued the certificate.

3. In case of issuing a signature verification key certificate to a legal entity, as the holder of the signature verification key certificate, along with an indication of the legal entity, it is necessary to indicate an individual acting on behalf of the legal entity on the basis of constituent documents of the legal entity or power of attorney. It is allowed not to indicate as the holder of the signature verification key certificate an individual acting on behalf of the legal entity in the signature verification key certificates used to automatically create or verify electronic signatures in the information system. The legal entity indicated in this certificate shall be recognized as the holder of such a signature verification key certificate.

4. The certification authority has the right to issue signature verification key certificates both in the form of an electronic document and hard copy. The holder of the signature verification key certificate issued in the form of an electronic document is also entitled to receive a hard copy of the signature verification key certificate attested by the certification authority.

5. The signature verification key certificate shall be valid from the moment of its issuance, unless a different start date for the signature verification key certificate is specified in the signature verification key certificate itself.

Information about the signature verification key certificate must be entered by the certification authority in the register of certificates no later than the start date of the validity of the signature verification key certificate specified in it.

6. Signature key verification certificate shall expire:

1) after the expiration of the term of its validity;

2) at the request of the holder of the signature verification key certificate submitted in the hard copy or electronic form;

3) in the event of termination of the activity of the certification authority without transferring its functions to others;

4) in other cases established by law or agreement between the certification authority and the holder of the signature verification key certificate.

7. Information on the termination of a signature verification key certificate shall be entered by the certification authority into the register of certificates within one business day from the date when the certification authority became aware of circumstances that led to the termination of the signature verification key certificate. A signature verification key certificate will cease to be valid as soon as an entry is made in the register of certificates.

8. The certification authority shall immediately, but not more than within one business day, revoke the signature verification key certificate by making an entry on the revocation in the register of certificates by a court decision that has entered into legal force, in particular if it is established by a court decision that the signature verification key certificate contains invalid data.

9. The use of a revoked signature verification key certificate shall not entail legal consequences, with the exception of those associated with its revocation.

The certification authority shall notify the holder of the signature verification key certificate in writing about the revocation of its signature verification key certificate prior to entering information on the revocation of the signature verification key certificate into the register of certificates.

Article 15. Accredited Certification Authority

1. The certification authority that has received accreditation shall be an accredited certification authority.

2. An accredited certification authority must keep the following information:

1) details of the main document that confirms the identity of the holder of the qualified certificate – an individual;

2) information on the name, number and date of issue of the document confirming the rights to apply for a qualified certificate of a person acting on behalf of the applicant – a legal entity;

3) information on the name, number and date of issue of documents confirming the powers of the qualified certificate holder to act on behalf of third parties, if information on powers of the qualified certificate holder to act on behalf of third parties is included in the qualified certificate.

3. The above information should be kept by an accredited certification authority for the duration of its activity, unless a shorter period of time is stipulated by regulatory legal acts of the Kyrgyz Republic.

The information should be stored in a form that allows verifying its integrity and authenticity.

The certification authority shall provide the qualified certificate holder with access to information relating to the qualified certificate holder stored in the accredited certification authority.

4. In case of termination of the activities of the accredited certification authority, it is obliged to:

1) inform the authorized body about this not later than one month before the date of termination of the activities of the certification authority;

2) transfer the register of certificates to the authorized body in the prescribed manner;

3) transfer to the authorized body in the prescribed manner the information to be stored in an accredited certification authority.

Article 16. Accreditation of the Certification Authority

1. Accreditation of the certification authority shall be carried out by the authorized body in respect of certification authorities that are legal entities.

2. Accreditation of the certification authority shall be carried out on a voluntary basis.

Accreditation of the certification authority shall be carried out for a five-year period, unless a shorter period is specified in the application of the certification authority.

3. Accreditation shall be granted if the certification authority meets the following requirements:

1) the value of the net assets of the certification authority is at least one million KGS;

2) availability of financial security for losses incurred by other persons as a result of their trust in the information specified in the signature verification key certificate issued by such a certification authority, or information contained in the register of certificates of this certification authority, in the amount of not less than one and a half million KGS;

3) availability of electronic signature facilities and certification authority facilities that have received confirmation of compliance with the requirements established by the executive body in the field of security provision;

4) the certification authority has at least 2 employees who are directly engaged in creating and issuing signature verification key certificates who have higher professional education in the field of information technology or information security, or higher or secondary professional education and have undergone retraining or advanced training in the use of electronic signatures.

4. Accreditation of the certification authority shall be carried out upon its application submitted to the authorized body.

Documents confirming the compliance of the certification authority with the requirements established by part 3 of this Article shall be attached to the application.

5. The authorized body on the basis of the submitted documents, within a period not exceeding 30 calendar days, shall make a decision on the accreditation of the certification authority or on refusal of accreditation.

If a decision is made to accredit the certification authority, the authorized body within a period not exceeding 10 days from the date of the decision on accreditation, shall notify the certification authority of the decision and issue a certificate of accreditation in the prescribed form. Simultaneously with the issuance of a certificate of accreditation, the authorized body performing the functions of the main (root) certification authority shall issue to the accredited certification authority a qualified certificate created using the facilities of the specified main (root) certification authority.

If a decision is made to refuse accreditation of the certification authority, the authorized body shall send or hand over to the certification authority a written notification of the decision, indicating the reasons for refusal, within a period not exceeding ten calendar days from the date of the decision to refuse accreditation.

6. The basis for refusal of accreditation shall be the non-compliance of the certification authority with the requirements established by part 3 of this Article, or the presence of false information in the submitted documents.

7. An accredited certification authority must comply during the entire period of its accreditation with the requirements for compliance with which it is accredited. If circumstances arise that make it impossible to comply with them, the certification authority must immediately notify the authorized body in writing.

The accredited certification authority, in the exercise of its functions and fulfillment of obligations assumed, must comply with the requirements established for certification authorities by this Law.

The authorized body throughout the entire period of accreditation shall be obliged to conduct verification of compliance by accredited certification authorities with the requirements established by this Law.

In case of detection of non-compliance by the accredited certification authority with the specified requirements, the authorized body shall be obliged to issue an instruction to the certification authority to eliminate violations with a deadline for their elimination and suspend the validity of the accreditation for the specified period of time with the entry of information about it into a list approved by the authorized body. An accredited certification authority shall notify the authorized body in writing of the elimination of violations that have led to the suspension of its accreditation. The authorized body has the right to check the actual elimination of violations, after which it makes a decision to renew the validity of the accreditation, and in case of their non-elimination within the period specified in the instruction - to revoke the accreditation of the certification authority.

8. State bodies, local governments, state and municipal institutions performing functions of the certification authority shall not be subject to the requirements set forth in clauses 1 and 2 of part 3 of this Article.

9. The main (root) certification authority, whose functions are performed by the authorized body, shall not be subject to accreditation under this Law.

Article 17. Qualified Certificate

1. A qualified certificate shall be created using the facilities of a certification authority that have received confirmation of compliance with the requirements established in accordance with this Law.

2. A qualified certificate shall contain the following information:

1) unique number of a qualified certificate, its start and end dates;

2) surname, name and patronymic (if any), date and place of birth of the qualified certificate holder – an individual or name (firm name), registration number and place of registration and/or actual location of the executive body of the qualified certificate holder – a legal entity;

3) signature verification key;

4) name of the electronic signature facilities and the certification authority facilities used to create the signature key, signature verification key and qualified certificate, as well as details of the document confirming the compliance of the said facilities with the requirements established pursuant to this Law;

5) name and location of the certification authority that has issued a qualified certificate, number of a qualified certificate of the certification authority and details of the certificate of accreditation of this authority;

6) restrictions on the use of a qualified certificate (if any);

7) other information about the applicant (at the request of the applicant).

3. If the applicant has submitted documents to the certification authority confirming its right to act on behalf of third parties, a qualified certificate shall include information confirming such powers of the applicant and the validity period of such powers.

4. A qualified certificate shall be issued in the form, the requirements for which are established by the executive body in the field of security.

5. In case of revocation of a qualified certificate issued to an accredited certification authority which has issued a qualified certificate to the applicant, as well as in case of revocation or expiration of the term of accreditation of the certification authority, a qualified certificate issued by the accredited certification authority to the applicant shall cease to be valid.

6. The holder of a qualified certificate shall:

1) if there are reasons to believe that the confidentiality of the signature key has been violated, not use this key and immediately contact the certification authority that has issued a qualified certificate to terminate this certificate;

2) use a qualified electronic signature in accordance with the restrictions contained in a qualified certificate (if such restrictions are imposed).

Article 18. Issuance of a Qualified Certificate

1. When issuing a qualified certificate, an accredited certification authority shall be obliged to:

1) identify the applicant – an individual who has applied for a qualified certificate;

2) obtain from a person acting on behalf of the applicant - a legal entity, confirmation of the competence to apply for a qualified certificate.

2. When applying to the certification authority, the applicant shall indicate restrictions on the use of a qualified certificate (in cases where restrictions are imposed), and submit to the certification authority the following documents confirming the authenticity of the information provided by the applicant for inclusion in a qualified certificate, or a duly notarized copy thereof:

1) the main document certifying the identity of the applicant – an individual, or constituent documents and certificate on the state registration of the applicant – a legal entity;

2) duly certified translation into the state or official language of documents on state registration of a legal entity in accordance with the legislation of a foreign state (for foreign legal entities);

3) power of attorney or other document confirming the applicant's right to act on behalf of others.

3. When obtaining a qualified certificate, the applicant against receipt must be familiarized by the certification authority with the information contained in a qualified certificate.

4. The certification authority, at the time of issuing a qualified certificate, shall issue to the qualified certificate holder a guide for ensuring the security of the use of a qualified electronic signature and the qualified electronic signature facilities.

Article 19. Final and Transitional Provisions

1. Signature key certificates issued in accordance with the Law of the Kyrgyz Republic "On Electronic Document and Electronic Digital Signature" shall be recognized as signature key verification certificates in accordance with this Law and shall remain valid until the expiration of the time period specified in them according to the rules established by this Law for qualified certificates.

2. An electronic document signed with an electronic digital signature as defined by the Law of the Kyrgyz Republic "On Electronic Document and Electronic Digital Signature" until the effective date of this Law shall be recognized as an electronic document signed with a qualified electronic signature until a court decision establishes otherwise.

Article 20. Entry into Force of this Law

1. This Law shall enter into force fifteen days after the date of its official publication.

Published in the “Erkin Too” newspaper No. 84-84 dated 25 July 2017

2. The Law of the Kyrgyz Republic “On Electronic Document and Electronic Digital Signature” No. 92 dated 17 July 2004 shall be repealed.

3. The Government of the Kyrgyz Republic shall bring its normative legal acts into compliance with this Law.

|  |  |  |
| --- | --- | --- |
| President of the Kyrgyz Republic |  | A.Atambaev |
|  |  |  |
| Adopted by the Jogorku Kenesh of the Kyrgyz Republic |  | [15 June 2017](toktom://db/142905) |