On approval of the Rules for creation, use, and storage of electronic digital signature private keys in the certification center

Unofficial translation

Order of the Minister of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan dated October 27, 2020 № 405/НҚ. Registered with the Ministry of Justice of the Republic of Kazakhstan on October 30, 2020 № 21549.

Unofficial translation

In accordance with subparagraph 13-3) of paragraph 1 of Article 5 of the Law of the Republic of Kazakhstan dated January 7, 2003 "On Electronic Document and Electronic Digital Signature" **I HEREBY ORDER:**

1. To approve the attached Rules for the creation, use, and storage of private keys of electronic digital signature in the certification center.

2. The Committee for Public Services of the Ministry of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan, in accordance with the established legislative procedure, shall ensure:

1) state registration of this Order with the Ministry of Justice of the Republic of Kazakhstan;

2) posting this Order on the Internet resource of the Ministry of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan after its official publication ;

3) within ten working days after the state registration of this Order with the Ministry of Justice of the Republic of Kazakhstan, submission to the Legal Department of the Ministry of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan the information on the implementation of the measures provided for in subparagraphs 1) and 2) of this paragraph.

3. Control over the implementation of this Order shall be entrusted to the supervising Vice-Minister of Digital Development, Innovation, and Aerospace Industry of the Republic of Kazakhstan.

4. This Order shall come into effect upon the expiration of ten calendar days after the day of its first official publication.

Minister of Digital Development
Innovation and Aerospace
Industry of the Republic of Kazakhstan *B. Mussin*

"AGREED"
Ministry of Trade and Integration of the
Republic of Kazakhstan

"AGREED"
National Security Committee of the
Republic of Kazakhstan

Approved
by Order of the Minister of Digital
Development, Innovation and
Aerospace Industry of the
Republic of Kazakhstan
dated October 27, 2020
№ 405/НҚ

Rules for creation, use, and storage of private keys of electronic digital signature in the certification center Chapter 1. General Provisions

1. These Rules for the creation, use and storage of private keys of an electronic digital signature in a certification centre (hereinafter referred to as the Rules) have been developed in accordance with the Law of the Republic of Kazakhstan "On Electronic Documents and Electronic Digital Signatures" (hereinafter referred to as the Law) and shall determine the procedure for creation, use, and storing private keys of electronic digital signatures in cloud services.

Footnote. Paragraph 1 – as amended by the order of the Minister of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan dated 17.03.2023 № 95/ НҚ (shall come into effect ten calendar days after the day of its first official publication).

2. The following concepts shall be applied in these Rules:

1) biometric authentication – a set of measures that identify a person based on physiological and immutable biological characteristics;

2) blockchain - information and communication technology that ensures the immutability of information in a distributed data platform based on a chain of interconnected data blocks, specified integrity confirmation algorithms and encryption tools;

3) multi-factor authentication – a method of verifying user authenticity using a combination of various parameters, including generating and entering passwords or authentication features (digital certificates, tokens, smart cards, one-time password generators and biometric identification tools);

4) certification centre (hereinafter referred to as CA) - a legal entity that certifies the correspondence of the public key of an electronic digital signature to the private key of an electronic digital signature, as well as confirming the authenticity of the registration certificate;

5) owner of the registration certificate (hereinafter referred to as the Owner) - an individual or legal entity in whose name the registration certificate was issued, who legally owns the private key corresponding to the public key specified in the registration certificate;

6) electronic digital signature (hereinafter referred to as EDS) – a set of electronic digital symbols created through an electronic digital signature and confirming the authenticity of the electronic document, its ownership and immutability of content;

7) EDS public key - a sequence of electronic digital symbols, accessible to any person and intended to confirm the authenticity of an electronic digital signature in an electronic document;

8) EDS private key - a sequence of electronic digital symbols intended to create an electronic digital signature using electronic digital signature tools;

9) electronic digital signature tools - a set of software and hardware used to create and verify the authenticity of an electronic digital signature;

10) cloud digital signature – a service of a certification centre that allows the creation, use , storing and deletion of private keys of an electronic digital signature in the HSM of a certification centre, where access to the private key is carried out by the owner remotely through at least two authentication factors, one of which is biometric;

11) hash – the transformation of an array of input data of arbitrary length into a bit side of a fixed length;

12) hardware cryptographic module (Hardware Security Module) (hereinafter referred to as HSM) - a hardware cryptographic module designed to encrypt information and manage public and private digital signature keys.

Footnote. Paragraph 2 – as amended by the order of the Minister of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan dated 17.03.2023 № 95/ НҚ (shall come into effect ten calendar days after the day of its first official publication).

Chapter 2. The procedure for creation private EDS keys in the certification center

3. Private EDS keys shall be created by the CC:

1) on the carrier of the owner's key information, which shall be transferred to the owner;

2) in the cloud EDS.

4. Private EDS keys of cloud EDS shall be generated strictly within HSM. The private key shall not be retrieved in clear text from the HSM.

Therewith the HSM shall:

1) correspond to at least the third level of security in accordance with the requirements established by ST RK 1073-2007 “Means of cryptographic information protection. General technical requirements";

2) be designed with physical perimeter security (anti-tamper security), using sensors to detect tampering and then remove key information required by the HSM.

3) comply with the standards of protection efficiency and methods for assessing the security of information and technical means in accordance with the requirements of the current legislation of the Republic of Kazakhstan.

5. Archiving of key information from HSM shall be possible only in encrypted form and only with the division of the encryption key according to the M out of N scheme (at least 3 out of 5). Encryption keys according to the M of N scheme shall be stored on secured tokens. For state CCs, N of tokens shall be permanently stored in the authorized body in the field of informatization, in the national security bodies, and at the CC. Protected tokens shall be used only when restoring an archive to a backup HSM.

6. Before the creation of a private EDS key and issuing an EDS registration certificate, the owner shall grant consent to the collection and processing of personal data.

The owner shall be authenticated:

1) remotely, using multi-factor authentication, one of the methods shall be biometric authentication;

2) at the registration center of the CC using biometric authentication, if necessary, having passed the procedure for collecting biometric data, the CC shall provide storage of biometric data.

The owner shall grant consent to store the private EDS key in the CC cloud EDS.

7. After creation, the private EDS key shall be saved in HSM in encrypted form using the GOST 28147-89 standard. In the function of the secret values, the password shall be used, set by the owner, which shall not be stored in the CC. The CC, to verify the password from the owner's private key, shall store the password hash in the HSM.

Chapter 3. The procedure for using private EDS keys stored in the certification center

8. When using private EDS keys stored in the CC, the owner shall undergo multi-factor authentication, one of the methods shall be biometric authentication.

9. Signing of electronic documents shall be carried out in the HSM memory by transferring the signed file or its hash to the HSM.

10. When the owner is authenticated in the CC, the password shall be transferred from the owner (browser, mobile application) to the HSM in encrypted form, while the password is encrypted on the owner's side, in a personal computer or smartphone.

11. Password recovery from the private EDS key in the cloud EDS shall not be performed .

12. The CC shall provide the owner of the cloud EDS private key with access to information on all signed electronic documents through the CC's account. The storage period for information on all signed electronic documents shall be at least one year after the expiration of the owner's registration certificate.

13. In case of revealing the fact of compromise of the private keys of the electronic signature of the owners of registration certificates, the CC shall immediately publish information on this fact and the measures taken to minimize the damage caused on its Internet resource.

14. CA shall provide logging of the following events:

1) generating a private EDS key for a cloud EDS;

2) use of the private EDS key of the cloud EDS;

3) deletion (erasure) of the private EDS key of the cloud EDS.

The storage period for the work protocols shall be one year from the date of the expiration of the registration certificate.

When logging actions, the following information shall be recorded:

1) owner ID;

2) date, time;

3) event.

15. Event logs shall be converted daily into a hash and the hash data shall be stored in the blockchain event chain. The blockchain used for this shall be available on the Internet.

Chapter 4. The procedure for storing private EDS keys in the certification center

16. The CC shall ensure the protection of the EDS private keys in the CC.

17. The storage period for private EDS keys in the cloud EDS shall be described in the Rules for the application of CA registration certificates approved by the CC in accordance with subparagraph 2-1) of paragraph 1 of Article 21 of the Law.

18. According to paragraph 92 of the Uniform requirements in the field of information and communication technologies and information security, approved by the Government of the Republic of Kazakhstan dated December 20, 2016 № 832 (hereinafter referred to as ET), the cloud EDS software and hardware shall be located on the territory of the Republic of Kazakhstan.

19. Protection of private keys shall be provided by a complex of organizational, software, and technical measures in accordance with the requirements described in ET.

20. The CA shall ensure that it is not possible to sign electronic documents using private EDS keys of a cloud EDS without multi-factor authentication.

Footnote. Paragraph 20 – as amended by the order of the Minister of Digital Development , Innovation and Aerospace Industry of the Republic of Kazakhstan dated 17.03.2023 № 95/ НҚ (shall come into effect ten calendar days after the day of its first official publication).

21. Fulfillment of the requirements of these Rules shall be a prerequisite for the accreditation of the CC in accordance with the Rules for the accreditation of certification centers approved by Order of the Minister of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan dated June 1, 2020 № 224/NҚ (registered in the State Registration Register of Regulatory Legal Acts under № 20815).