for general use

THE RULES OF
THE CERTIFICATION CENTER OPERATIONS

THE RULES

The Rules of the Certification Center Operations (hereinafter referred to as the Rules) were developed in accordance with the Resolution of the Management Board of the National Bank of the Republic of Kazakhstan (hereinafter referred to as the NBRK) dated 27 March 2018 No. 48 "On approval of the Requirements for ensuring information security of banks, branches of non-resident banks of the Republic of Kazakhstan and organizations conducting certain types of banking operations, Rules and deadlines for providing data about information security incidents, including data about violations, failures in information systems, by decree of the Government of the Republic of Kazakhstan dated 20 December 2016 No. 832 "On approval of uniform requirements in the field of information and communication technologies and security information security", Law of the Republic of Kazakhstan dated 7 January 2003 No. 370-II "On Electronic Documents and Electronic Digital Signatures" (hereinafter referred to as the Law), RFC 3647 Recommendations (Certificate Policy and Certification Practices Framework), RFC 2251 (Lightweight Directory Access Protocol), RFC 2560 (Online Certificate Status Protocol - OCSP), RFC 3161 (Time-Stamp Protocol - TSP), RFC 5280 (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile), by order of the Minister of Culture and Information of the Republic of Kazakhstan dated 17 June 2025 No. 279- НҚ "On approval of the List of standard documents generated in the activities of state and non-state organizations, indicating storage periods" (hereinafter referred to as the List), by order of the Minister of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan dated 1 June 2020 No. 224/НҚ "On approval of the Rules for the issuance and revocation of accreditation certificates of certification centers", by order of the Minister of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan dated 27 October 2020 No. 405/НК "On approval of the Rules for the creation, use and storage of closed keys of electronic digital signature in the Certification Center", by order of the Minister of Investment and Development of the Republic of Kazakhstan dated 23 December 2015 No. 1231 "On approval of the Rules for the issuance, storage, revocation of registration certificates and confirmation of ownership and validity of the public key of electronic digital signature by the Certification Center, with the exception of the root Certification Center of the Republic of Kazakhstan, the Certification Center of government bodies, the National Certification Center of the Republic of Kazakhstan and the trusted third party of the Republic of Kazakhstan," as well as the internal normative documents (hereinafter referred to as INDs) of Eurasian Bank JSC (hereinafter referred to as the Bank), including the Internal Normative Regulation Policy.

Section 1. GENERAL PROVISIONS

1. The Rules describe the procedure for providing the services of the Certification Center owned by the Bank (hereinafter referred to as the CC) and the rules for its use by the participants of the CC. The description of the process is provided in Appendix No. 5 (SIPOC). The business owner of the process is the IT Block.

2. The Rules are an agreement that imposes obligations on all parties involved, as well as a means of officially notifying and informing all parties in the relationship arising in the process of providing and using the services of the CC. Any participant of the CC accepts the Rules from the moment the use of the CC begins.

3. The Rules define the requirements, mechanisms and conditions for the provision and use of the CC services, including the rights, duties and responsibilities of the CC participants, work protocols, accepted data formats, basic organizational and technical measures, including, but not limited to, operations such as the issuance, use and revocation of registration certificates (hereinafter referred to as RC) of public keys.

4. The Rules use the basic concepts provided for by the legislation of the Republic of Kazakhstan, the electronic reference book, as well as the following terms:

1) the closed key of an electronic digital signature (hereinafter referred to as the EDS closed key) is a sequence of electronic digital symbols designed to create an electronic digital signature using electronic digital signature tools;

2) request – an appeal to the information system of the Certification Center in order to obtain the appropriate service and/or information;

3) the applicant is an individual or a legal entity that has submitted documents for the issue or revocation of a RC;

4) key compromise - loss of trust in the fact that the keys used by the owner ensure the security of information;

5)   the open key of an electronic digital signature (hereinafter referred to as the EDS open key) is 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;

6)   IT Security Subdivision (hereinafter referred to as ITSS) is a subdivision responsible for ensuring the information security of the CC;

7)   The Policy of Application of Registration Certificates (hereinafter referred to as the Policy) is an internal document defining the rules and mechanisms of work of the Certification Center in terms of managing the RC. The policy is posted on the Internet resource https://eubank.kz/policy-of-application-of-registration-certificates /;

8)   registration of a CC participant – entering registration information about the owner of the RC into the storage of the CC;

9)   registration certificate is an electronic document issued by the CC to confirm the compliance of an electronic digital signature with the requirements established by the Law;

10) cryptographic information security tool (hereinafter referred to as CIST) is a tool that implements algorithms for cryptographic transformations, generation, formation, distribution or management of encryption keys;

11) the list of revoked RCs (hereinafter referred to as LRRCs) is a part of the register of registration certificates containing information about registration certificates that have been terminated, their serial numbers, date and reason for revocation;

12) the status of a RC is a composite concept that reflects the result of checking the validity of a RC. For example, overdue – not overdue, revoked – not revoked;

13) RC storage – directory of all RCs and LRRCs;

14) hash is transformation of an input data array of arbitrary length into a bit string of fixed length;

15) electronic document – a document in which information is presented in electronic and digital form and certified by means of an electronic digital signature;

16) an electronic digital signature (hereinafter referred to as an EDS) is a set of electronic digital symbols created by means of an electronic digital signature and confirming the authenticity of an electronic document, its belonging and the immutability of the content;

17) LDAP (Lightweight Directory Access Protocol) is an application–level protocol for accessing the directory service developed on the recommendations of the International Telecommunication Union – Telecommunication sector (hereinafter – ITU-T) X.500;

18) the software administrator (hereinafter referred to as the software) of the control center is an employee responsible for maintaining the operability of the technical and software components of the CC;

19) the authorized person of the Certification Center is a ITSS employee responsible for issuing RC keys and managing them;

20) biometric authentication is a set of measures that identify a person based on physiological and unchangeable biological characteristics;

21) multi–factor authentication is a method of verifying user authentication 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);

22) hardware cryptographic module (Hardware Security Module) (hereinafter referred to as HSM) is a hardware cryptographic module designed to encrypt information and manage open and closed keys of the EDS;

23) certification center – a legal entity certifying the compliance of the open key of an electronic digital signature with the closed key of an electronic digital signature, as well as confirming the authenticity of the registration certificate;

24) blockchain is an 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.

25) cloud EDS is a CC service that allows creating, usage, storage and deleting of private keys of an electronic digital signature in the HSM of the certification center, where access to the closed key is performed by the owner remotely through at least two authentication factors, one of which is biometric;

26) key information carrier is a specialized carrier in which cryptographic information protection devices are used to protect stored closed keys of an electronic digital signature, which has a certificate of compliance with the requirements of the National Standard of the Republic of Kazakhstan 1073-2007

"Cryptographic information protection devices. General technical requirements" (not lower than the second level).

Section 2. SPECIAL PROVISIONS
Chapter 1. Participants of the CC

5. The Participants of the CC are:
1) The Certification Center is an automated set of configurable services for issuing and managing RC keys, operating in accordance with approved security policies;
2) Registration Center is a component of the CC designed to perform identification, authentication and verification of the applicant's authorities;
3) Storage of RCs and lists of revoked RCs is a directory used by the Certification Center to gain access to the RCs, the RCs verification service, storage of archival information and other functions;
4) The owner of the RC is a natural or legal person in whose name the Certification Center issued the RC, legally owning a closed key corresponding to the open key specified in the RC;
5) A RC user is a natural or legal person who legally owns the closed key of an EDS and has the right to use it on an electronic document;
6) The trusting party is information systems that use the information about the RC received from the Certification Center to verify that the electronic digital signature belongs to the owner of the RC;
7) The timestamp server is a service for setting a timestamp on an electronic document. The service operates on the basis of - Time-Stamp Protocol (TSP);
8) The RC status verification server is a RC status determination service. The service operates on the basis of the Online Certificate Status Protocol (OCSP).

Chapter 2. Organizational, technical and administrative security measures

6. To ensure the security of the CC, organizational, technical and administrative measures are applied to ensure the correct functioning of technical means of processing and transmitting information, as well as the establishment of appropriate rules for service personnel allowed to work with confidential information.
7. Protection of information from unauthorized access is performed at all technological stages of information processing and in all modes of operation, including during repair and routine maintenance.
8. Protection of information from unauthorized access provides for monitoring the effectiveness of means of protection against unauthorized access. ITSS checks for compliance with information security requirements in accordance with the Instructions for conducting checks of information systems for compliance with information security requirements.
9. Control and management of access to the premises of the CC is performed according to the Rules on Critical Zones.
10. The Certification Center that processes the requests of the CC participants is located in a room specialized for hosting servers and equipment, control and access to which is performed according to the Rules on Critical Zones. Access to the data processing center is provided to persons whose list is approved by the head of the information technology subdivision in coordination with the information security subdivision. The Bank maintains a log of the access control and management system to the data processing center, which is stored for at least 1 (one) year.
11. The security rooms of the Certification Center's information technologies are located in a non-residential premises, equipped with uninterruptible power supplies, ventilation, air conditioning, as well as fire extinguishing and humidity control facilities in accordance with the "Rules on Critical Zones", ensuring compliance with the established parameters of temperature and humidity conditions, ventilation and air purification in accordance with the norms established by the legislation of the Republic of Kazakhstan.
12. The equipment of the server room must be connected to the main electrode of the grounding system of the building with a conduit of at least 1.5 cm in size, the ceiling height of the server room must be at least 2.44 meters. Responsible employees keep a laced log of the work performed in the server room.

13. The process of hiring employees, including background checks and training of new employees, is performed in accordance with the <u>Rules of recruitment, admission and adaptation of personnel</u>.

14. In the case of transferring the facilities of the CC to new equipment or software, the staff of the Certification Center takes a training course on working with new facilities.

15. In exceptional cases, when the services of independent contractors are required to perform work on setting up or maintaining the equipment and information system of the CC, the contractor's specialists perform work only under the supervision and with the permission of the CC employees within the framework of the Rules for the delimitation of access rights to electronic information resources

16. The activities of the employees of the CC are regulated by the internal normative documents of the Bank, including:
1) "<u>Information security policy of the Certification Center</u>";
2) "<u>Regulations on the Certification Center</u>";
3) "<u>Policy of application of registration certificates of the Certification Center</u>";
4) "<u>Instructions on maintenance, administration, issue of registration certificates in emergency-crisis situations</u>";
5) "<u>Instructions for installing and configuring the Certification center software</u>";
6) "<u>Instructions on backup of information resources of the Certification Center</u>";
7) "<u>Instructions for securing the functions and powers of the administrator of the server of the Certification Center</u>";
8) "<u>Rules for the organization of the authentication procedure</u>";
9) "<u>Rules of differentiation of access rights to electronic information resources</u>";
10) "<u>Rules for ensuring the confidentiality of information</u>";
11) "<u>Rules for the safe use of information resources</u>";
12) "<u>Instructions for conducting checks of information systems for compliance with information security requirements</u>";
13) "<u>Instructions for managing vulnerabilities of information systems</u>";
14) "<u>Instructions for managing information security incidents</u>";
15) "<u>Instructions for managing access on firewalls</u>";
16) "<u>Rules for the organization of anti-virus protection of information systems</u>";
17) "<u>Standard of Bank information systems</u>";
18) "<u>Instructions for managing service requests and IT incidents</u>";
19) "<u>Regulations for the acceptance of systems/functionality into commercial operation/decommissioning</u>".

17. The access of the employees of the CC to the documents and documentation that make up the documentary fund of the CC is organized in accordance with the functional responsibilities.

18. The software and hardware complex of the CC, in addition to those established by the <u>Standard of the Bank's Information Systems</u>", registers the following types of audit events:
- system-wide software system events;
- acceptance of a request to issue a RC;
- RC release;
- placing the request for a RC;
- acceptance of a request for a RC;
- rejection of a request for a RC;
- release/reissue of the list of revoked RCs;
- failure to perform an internal operation of the software component.
− formation of the closed key of the RC in the cloud component of the CC;
− using the closed key of the RC cloud EDS;
− deleting (erasing) the closed key of the RC of the cloud EDS.

18-1. The storage period of the work protocols is at least one year from the date of expiration of the RCs. When logging actions, the following information is recorded:
− owner ID;
− date, time;
− event.

18-2. The event logs are converted into a hash daily, and the hash data is stored in the blockchain event chain. The blockchain used for this is available on the Internet.

19. Audit events are automatically recorded in logs by means of application and system-wide software.

20. Audit logs are constantly automatically analyzed using the log monitoring and analysis system in order to detect vulnerabilities and violations in the operation of the software and hardware of the Certification Center. The logs are stored and protected in accordance with the Bank's Information Systems Standard.

21. In the process of analyzing audit logs, all significant work violations are investigated, and adequate response measures are taken, according to the "Instructions for Managing Service Requests and IT Incidents" and "Instructions for Managing Information Security Incidents".

22. The CC maintains an electronic archive:
- audit logs in accordance with paragraph 20 of the Rules;
- applications for the issuance and withdrawal of RCs;
- copies of identity documents and data from them;
- RC of users of the CC whose validity period has expired;
- revoked RC of users of the CC;
- lists of revokedRCs of CC;
- protocols of operation of the CC software;
- other documents, the storage of which is performed according to the List.

23. The CC ensures the maintenance of the archive and the storage of archival documents in accordance with the legislation of the Republic of Kazakhstan, while ensuring the permanent storage of the archive:
- RCs keys of electronic digital signatures;
- documents on the creation and cancellation of an electronic digital signature (applications, RCs, notifications and other documents);
- logs (lists, registers) of accounting for issued registration certificates confirming compliance with an electronic digital signature.

24. Only authorized employees of the Certification Center have access to the archive, according to the "Instructions for securing the functions and powers of the administrator of the server of the Certification Center".

25. The allocation for destruction and destruction of documents that are not subject to archival storage in accordance with the List is performed by employees of the CC, according to the Rules for ensuring confidentiality of information.

26. 10 working days before the expiration of the closed key of the authorized person of the Certification Center, the administrator of the CC software generates a new closed key and the RC of the authorized person of the Certification Center and publishes it in the appropriate section of the RC repository, similar to the primary generation, according to the Instructions for installing and configuring the software of the certification center.

27. Upon expiration of the Certificate Center's closed key, the key information carriers with the closed key and its copies are destroyed by the act of the responsible employees of the ITSS under the supervision of the head of the ITSS, in the ways described in the Rules for ensuring confidentiality of information.

28. Excluded.

29. To prevent loss, the data of the Certification Center (the repository of issued RCs, the keys of the Certification Center) are archived and placed in specially designated storage for these purposes. Archiving of the storage of issued RCs and LRRCs is performed automatically at least once a day. Backup is performed at least once a month, duplication of keys between the main and backup HSM occurs once a day.

30. In case of equipment damage, software and/or hardware failures, an incident is registered and actions are taken to solve it and minimize the consequences, as well as data on preventing it in the future are recorded, according to the "Instructions for maintenance, administration, issuance of registration certificates in emergency-crisis situations".

31. In case of technical failures in the operation of the CC Internet resource, the RC revocation is suspended until the operation of the CC Internet resource is restored.

32. The closed keys of the RC of the cloud component of the CC are generated strictly inside the HSM. The closed key is not extracted from the HSM in the clear. At the same time HSM:

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

2) designed with physical perimeter protection (protection against opening of the case), using sensors to determine the fact of opening of the case and the subsequent removal of key information necessary for the HSM.

3) complies with the standards of protection effectiveness 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.

33. Excluded.

34. Excluded.

35. Excluded.

36. EDS keys are generated and used by cryptographic transformation according to the GOST 34.310-2004 algorithm:
- closed key – 256 bits;
- the open key is 512 bits.

37. The purposes of using the key (the order of filling in the key usage field of RC x.509v3) are filled in according to the Policy.

38. All actions with key information carriers must be performedstrictly in accordance with the instructions for their operation provided by the supplier of key information carriers and the safety requirements described in the documents specified in paragraph 16 of the Rules.

39. The term of storage of revoked registration certificates in the register of registration certificates is at least 5 (five) years from the date of revocation. After the expiration of the storage period, the revoked RCs are electronically transferred to archival storage in accordance with the List.

40. Excluded.

41. Documents (applications for the production of EDS, registration certificate, applications and notifications of revocation of registration certificate, acts of destruction of the closed key of EDS and other documents) on the creation and revocation of EDS are stored permanently according to the List.

42. Backup of the closed key of the Certification Center is performed by the responsible employees of the CC after its generation in accordance with the operational documentation of the cryptographic information protection tool provided by the supplier of the cryptographic information protection tool, according to the scheme n of m, which implies the division of the secret into N parts, of which only M parts of the secret are sufficient for decryption. Each part of the secret is owned by a separate p——erson. A backup copy of the Certificate Center's closed key is stored separately from the cryptographic module in an encrypted archive on a storage medium stored in a closed physical storage.

43. The recording of the closed key on the key information carrier and the destruction of the expired closed keys is performedin accordance with the operational documentation. Archived storage of closed keys that are not issued by the cloud is not allowed.

44. Excluded.

45. The provision of the open key of the Certification Center is implemented by publishing its RC in the repository and on the Internet resource http://crt.eubank.kz/EubankCA.crt.

46. The security of the RC of the Certification Center is implemented by providing information about the serial number of the RC and its hash value, with the provision of the possibility for trusting parties to check it on the Internet resource https://eubank.kz/data-of-the-registration-certificate-of-the-certification-center/".

47. In the event of a change of the Certification Center's signature keys and the release of a new Certification Center RC, its distribution can be performed using the cross-certification mechanism.

48. Excluded.

49. Computers working in the CC meet the following requirements:
- RC signing computers are isolated for unauthorized access;
- operating systems are maintained at a high level of protection, with regular use of all operating system vendor-recommended and appropriate protection packages, including antiviruses;
- monitoring is performedto detect unauthorized program changes;
- the number of running system services is minimized.

50. Computers of RC users and trusted parties must meet the following requirements:
- use of licensed software;

- operating systems are maintained at a high level of protection, with regular use of all operating system vendor-recommended and appropriate protection packages, including antiviruses and firewalls.;
- in cases of computer sharing by several users, access differentiation is applied based on the use of different accounts with complex passwords;
- there are no cryptographic information protection tools on the computer other than those defined in the Rules.

51. The security of the Certification Center is provided by firewalls and other information security software and hardware.

Chapter 3. Initial registration procedure

52. The initial registration of an applicant is a process as a result of which an individual or a legal entity for the first time reports itself to the CC, before the RC for this individual or legal entity is issued. The end result of this process (if it is successful) is the issuance of a RC for the applicant's open key and the issuance of a RC to him and/or placing it in the RC storage.

53. Individuals and legal entities, residents of the Republic of Kazakhstan have the right to submit an application for the issuance of a RC.

54. A person wishing to undergo the registration procedure must confirm their full and unconditional adherence to the Rules and Policies, as well as consent to:

- videotaping/photographing yourself and your documents, as well as the use of these images in order to obtain services within the Rules;
- collection, processing of personal and biometric data in order to obtain the issuance and revocation of the registration certificate of the CC.

54-1. The owner can get a RC:

1) remotely, in this case, the RC is stored in the CC. The owner agrees to store the closed key of the EDS in the cloud component of the CC;

2) on purpose in the registration center of the CC, in this case, the RC is stored by the owner in the form of an electronic document by recording registration certificates on a data carrier.

54-2. In case of biometric authentication, the CC ensures the storage of the owner's biometric data in accordance with Стандарту проведения биометрической идентификации.

55. To obtain a RC remotely via the Internet resources of the CC, an individual authenticates using multi-factor authentication, in which one of the methods is biometric authentication, photographs the identity document of an individual, and signs an OTP application for the issuance of registration certificates from an individual in the form according to Appendix No. 1 to these Rules, as well as an application for the collection and processing of personal data. The password specified by the owner, which is not stored in the CC, is used as secret value. To verify the password from the owner's closed key, the CC stores the password hash in the HSM. When the password is transmitted from the owner (browser, mobile application) to the HSM, it is encrypted, while the password is encrypted on the owner's side, in a personal computer or smartphone. Password recovery from the closed key of the EDS in the cloud component of the EDS is not carried out.

56. When physically applying to the Registration Center to obtain registration certificates, a legal entity (or its representative by proxy) purposely provides the following documents to the registration center:

1) application for the issuance of registration certificates from a legal entity in the form according to Appendix No. 2 to these Rules;

2) the identity document of the representative of the legal entity, for identification;

3) a certificate or certificate of state registration (re–registration) of the applicant's legal entity as a legal entity (or a notarized copy in case of failure to submit the originals) - for the legal entity;

4) a power of attorney for a representative of a legal entity, indicating the authority to submit documents for the issuance of registration certificates of the certification center and sign the relevant documents for the execution of the order determined by the power of attorney.

57. Excluded.

58. The CC processes applications for the issuance of applicants' RCs within 1 (one) working day from the date of submission of the application.

59. The CC reserves the right to verify the information specified in the application for the issuance of the RCs, as well as to require the applicant to submit additional documents confirming the information specified in the application.

60. Registration of a RC may be refused if:
- the applicant has not provided (or not fully provided) the necessary information;
- the applicant provided false information;
- the court's decision has entered into legal force;
- the person has not reached the age of sixteen.

61. In case of refusal to register a RC, the applicant is notified using one of the available communication channels (e-mail, phone call, sms, Internet resource, push notification) no later than 1 (one) business day from the date of submission of the application. If the applicant eliminates the reasons for the refusal to provide the service, the applicant submits a repeated application to receive the service for issuing and revoking the RCs in accordance with the procedure established in the Rules.

62. Excluded.

63. Excluded.

64. Excluded.

65. Excluded.

66. The following actions of the owner of the RC mean the recognition of the RC:
- obtaining a registration certificate;
- the owner has no motivated objections (claims) about the contents of the RC.

Chapter 4. Procedure for revocation of registration certificates

67. Replacement of keys before the expiration of the RC can be performed when submitting a request to revoke the RC, with further passage of the initial registration procedure described in Chapter 3.

68. An application for the withdrawal of a RC can be submitted by its owner or his representative by proxy.

69. RCs are revoked on the basis of the provision of the following documents in the Bank branch by the owner of the registration certificate – an individual (or his representative by proxy):

1) application for revocation of the registration certificate from an individual in the form according to Appendix No. 3 to these Rules;

2) the identity document of an individual, for identification;

3) a power of attorney for a representative of an individual, notarized with an indication of the authority to submit documents for revocation of registration certificates of the certification center and sign the relevant documents for the execution of the order determined by the power of attorney – when representing the interests of an individual by a third party.

69-1. After collecting the necessary documents, an employee of the Bank's branch sends a request via Naumen to the Registration Center for the withdrawal of the RC.

70. RCs are revoked on the basis of the provision of the following documents in the Bank branch by the owner of the registration certificate – a legal entity (or its representative by proxy):

1) application for revocation of the registration certificate from a legal entity in the form according to Appendix No. 4 to these Rules;

2) the identity document of the representative of the legal entity, for identification;

3) a power of attorney for a representative of a legal entity, indicating the authority to submit documents for revocation of registration certificates of the certification center and sign the relevant documents for the execution of the order determined by the power of attorney.

70-1. After collecting the necessary documents, an employee of the Bank's branch sends a request via Naumen to the Registration Center for the withdrawal of the RC.

71. The CC revokes the RC within 1 (one) business day from the moment the CC accepts the application received from the owner of the RC (or his representative by proxy) to revoke the RC.

72. In case of revocation of registration certificates, the certification center notifies the owner of the registration certificate by immediately entering relevant information into the register of registration certificates indicating the date and time of revocation of registration certificates, which is an official notification of the participants of the CC about the revocation of the RCs.

73. The certification center publishes on the Internet resource http://crl.eubank.kz/GOST.crl information about the revoked registration certificates, their serial numbers, date and reason for revocation in the LRRCs.

74. The LRRCs is updated as requests are received to change the status of the Registration Certificate. Revoked expired RCs are removed from the LRRCs.

75. The owner of the Registration Certificate independently verifies the fact of revocation of the Registration certificate. Verification of the fact of the revocation can be performed using the LRRCs.

76. The application for revocation of the RC should be submitted within the shortest possible time after such a need arises (for example, in case of compromise of the closed key). In case of detection of the fact of compromising the closed keys of the electronic signature of the owners of registration certificates, the CC immediately publishes on its Internet resource information about this fact and the measures taken to minimize the damage caused.

77. The CC may revoke the RC and publish it in the LRRCs in the following cases:

1. at the request of the owner of the registration certificate or his representative;

2. when establishing the fact of submitting false information or an incomplete package of documents upon receipt of the registration certificate;

3. death of the owner of the registration certificate;

4. changes in the surname, first name or patronymic (if it is indicated in the identity document) of the owner of the registration certificate;

5. change of name, reorganization, liquidation of the legal entity – the owner of the registration certificate, change of the head of the legal entity;

6. provided for by the agreement between the certification center and the owner of the registration certificate;

7. by a court decision that has entered into legal force.

77-1. The certification center revokes the registration certificate without a statement from the applicant upon receipt of reliable information about the occurrence of one of the cases specified in sub-paragraphs 2, 3, 4, 5, 6, 7 of paragraph 77 of these Rules.

78. When violations are detected in the functioning of the control center, an action plan is developed to eliminate the identified violations in accordance with the "Instructions for Managing Information Security Incidents". If the detected violations led to the issuance of RCs that violate the security of the CC, these RCs will be immediately withdrawn. In case of detection of violations in functioning, the Management Center will inform about the actions that need to be taken to restore proper functioning. If the Certification Center functioned with violations during the RC manufacturing process, the RCs issued at that time should be withdrawn.

Chapter 5. Operational requirements for the life cycle of a RC

79. The beginning of the validity period of the Certification Center's RC is calculated from the date and time of its generation. The validity period of the root RC of the CC is 20 (twenty) years.

80. The validity period of the user RC is from 3 months to 3 years. The beginning of the validity period of the closed key of the owner of the RC is calculated from the date and time of the beginning of the validity of the corresponding RC of the owner of the RC.

80-1. The CC provides the owner of the closed key of the cloud component of the EDS with access to information about all signed electronic documents through the personal account of the CC. The storage period of information on all signed electronic documents is at least one year after the expiration of the owner's registration certificate. Electronic documents are signed in the HSM memory by transferring the signed file or its hash to the HSM.

81.   The closed key of the Certification Center is used to generate EDS, RCs, open keys of users and lists of revoked RCs.

82. The closed keys of the users of the CC are used to generate EDS of electronic documents.

83. The closed key is used to form an electronic digital signature.

84. The RC is used to confirm the authenticity of an electronic digital signature. Verification is performed by providing information on the status of the issued RCs and RCs of authorized persons of the Certification Center to the participants of the CC, according to Chapter 6. Each RC issued by the CC contains a link to the lists of revoked RCs.

85. After the start of using the RC, it is considered to be the recognized owner of the RC.

86. The RC user must use the RC strictly in accordance with the information specified in it and the Rules. Obtaining additional information and guarantees, in addition to the information specified in the RCs, is performed by the participants of the CC independently.

87. The owner of the RC must independently verify the status of the RC.

88. In case of compromise of the keys of authorized persons of the Certification Center, the CC immediately notifies the participants of the CC by any of the available methods.

89. RC owners can be participants in a single trust space with RC owners issued by other Certification Centers in cases where a corresponding agreement has been concluded between the Certification Centers and the necessary organizational and technical measures have been taken.

90. Excluded.

91. The list of revoked RCs is provided to RC owners in electronic form in the format defined by RFC 5280 (Certificate and Certificate Revocation List (CRL) Profile). The list is certified by the EDS of the Certification Center.

92. A CC participant may terminate the use of CC services by revoking his RC or refusing to change key pairs after their expiration date.

93. The procedure for verifying the EDS of an electronic document includes verifying the validity of the use of the RCs at the time of signing, verifying the authenticity of the EDS and verifying the compliance of the use of the EDS with the information in the RCs.

Chapter 6. The procedure for confirming the ownership and validity of the open key of the digital signature of the CC

94. Confirmation of the ownership and validity of the open key of the EDS of the CC is performed by the participant of the CC or the information system of the CC when exchanging electronic documents between the participants of the CC.

95. Upon receipt of an electronic document containing the RC of the signing party, the participant of the CC checks it for confirmation of the ownership and validity of the open key of the EDS by:
1) verification of registration certificates of the signing party;
2) verification of EDS in an electronic document.

96. Verification of the registration certificates of the signatory party is performed through the following checks using the CC CIST:
1) verification of the constrCCtion of the correct chain from the verified registration certificates to the trusted root registration certificate of the CC, taking into account the intermediate registration certificates of the CC;
2) checking the validity of registration certificates. Verification of the validity period from the verified registration certificates to the trusted root registration certificate of the CC, taking into account the intermediate registration certificates of the CC;
3) verification of registration certificates for revocation. Verification of registration certificates for the withdrawal of the signing party is performedby one of the methods:
- based on the CC LRRCs. This verification method confirms whether the tested RCs have been withdrawn at the time of the beginning of the validity period of the CC LRRCs;
- online verification of registration certificates for revocation based on the OCSP protocol. This verification method confirms whether the RC being checked has been revoked at the time of sending the request (current time);
4) checking the key usage area. The verification consists in determining the presence of the required values of the field of registration certificates "key usage" (KeyUsage). If the "key usage" field contains the values "Digital signature" and "Non-Repudiation", then these RCs are used for EDS;
5) checking the policy number of registration certificates and the permitted ways of using them. If the policy of the verified registration certificates provides for the restriction of their use (only in one system), then the RC data and the corresponding closed key are not used in other systems;
6) checking the timestamp. The proof of signing the document at the specified time is the timestamp received in the CC and containing the time of signing the document. This check is performed for electronic documents of long-term storage and is formed at the time of signing the document;
7) excluded;
8) verification of the confirmation of the ownership and validity of the EDS open key in an electronic document is performed using the CC CIST by using the open key contained in the registration certificate of the signing party. The technical implementation of the EDS verification is assigned to the owner of the information system;

9) if the EDS or registration certificate does not meet the requirements of at least one of the criteria of the above checks, with the exception of checking the timestamp, then the EDS or registration certificate is considered invalid;

10) the technical implementation of the verification of the ownership and validity of the open key of the EDS and the registration certificate is assigned to the information system by using high-level development functions using the CC CIST.

Chapter 7. Confidentiality

97. The participants of the CC recognize that information, access to which is restricted in accordance with the legislation of the Republic of Kazakhstan and which is a commercial, official, banking, personal and other legally protected secret, is considered confidential information.

98. The participants of the CC acknowledge that the contents of the RC, information about their withdrawal or other information about the status of the RC, the public part of the repository and the information contained therein are not considered confidential information. Information not listed in paragraph 102 of the Rules is not considered confidential, unless otherwise provided by the current legislation of the Republic of Kazakhstan.

99. CC participants are required to keep confidential information considered confidential.

100.   The CC ensures the protection of information about the owners of the RC and discloses them only in cases provided for by the legislation of the Republic of Kazakhstan.

101.   CC in its activities is guided by the current legislation of the Republic of Kazakhstan on the protection of personal data. In particular, the CC does not disclose information identifying applicants for the issuance of RCs, with the exception of the information listed in paragraph 103 of the Rules.

102. The information considered confidential is indicated in the Register of Confidential Data.

103. Information that is not considered confidential:
- lists of revoked RCs;
- the status of the RCs of the participant of the CC;
- the open key of the RC of the CC participant.

104.   Statistics regarding the issuance and withdrawal of a RC do not contain any personal information and are not considered confidential.

Chapter 8. Responsibilities

105. The participant of the CC undertakes:
1)   excluded;
2)   not to disclose confidential information to third parties and use it only for the purposes for which it was transferred (received);
3)   observe and take measures established by the CC to protect confidential information transmitted (received) on tangible media:
- the storage and use of confidential information must be performedby the participant of the Control center in places that ensure the physical safety of confidential information and access authorization;
- passwords must be set on devices that are the material carrier of key information in order to ensure the safety of this information and exclude access to confidential information of all persons except the person authorized to have access to the carrier;
- extraction of confidential information outside the places of its storage/use is not allowed;
- while working (performing actions, operations) with confidential information, the possibility of familiarization with it by persons not authorized for such familiarization (access) should be excluded;
- copying or other reproduction of confidential information and/or its material carriers is allowed only with the written consent of the CC. At the same time, unsuccessful or unnecessary copies and other results of reproduction of confidential information (its material carriers) are subject to mandatory destruction with the help of special mechanical devices or manually. With respect to copies and other results of reproduction of confidential information band/or its material carriers, the participant of the CC is obliged to adhere to the same protection measures as with respect to the originals;
- when providing confidential information in cases established by law to a public authority, other state bodies, local self-government bodies, simultaneously with such provision, notify the CC in writing about this.

106. In case of disclosure by the Owner of the RC, the User of the RC of confidential information, both through the fault of the latter, and without it, the CC is not responsible for the negative consequences caused by the disclosure of confidential information.

107. The Certification Center is responsible for the manufacture of RCs and their subsequent management in accordance with these Rules, in particular, it:

- processes requests for the issuance of RCs and issues new RCs, in accordance with the requested scope of application;
- confirms requests for the issuance of RCs from the participants of the CC requesting RCs according to the procedures described in the Rules;
- issues a RC based on requests from authenticated applicants;
- sends a notification about the status of issued RCs at the request of applicants;
- publishes information about issued RCs in the RC repository;
- publishes the root RC of the Certification Center to the RC repository;
- processes RC revocation requests;
- Confirms requests for the withdrawal of RCs from applicants according to the procedures described in this document;
- releases the LRRCs;
- publishes information about revoked RCs;
- stores the closed keys of the owner of the registration certificate on the side of the CC in the HSM.

108. The Registration Center is responsible for conducting identification and authentication procedures, in particular, they:

- check the information provided by the applicant when registering with the CC for completeness, reliability and accuracy;
- they transmit requests for the release of the RC via a secure channel to the Certification Center;
- provide consultation of applicants on the subject of passing identification and authentication procedures in the CC.

109. By submitting a request for the issuance of a RC, the applicants agree:

- accept the terms and follow the procedures described in the Rules;
- provide reliable and accurate information when registering with the CC;
- if you change the credentials provided in the documents during registration, immediately send an application for the withdrawal of the RC;
- use the CC services in accordance with the Rules;
- to use for the formation of EDS only the valid closed key of the EDS corresponding to the open key of the EDS specified in the RC of the participant of the CC;
- apply secret keys and their corresponding RC in accordance with the scope and policies specified in the RC;
- ensure the safety of the carrier of key information and prevent the unlawful dissemination of information about your closed key;
- not use secret keys and their corresponding RCs after their expiration date;
- not use secret keys and their corresponding RCs in case of their revocation;
- immediately send a request to the Control Center to revoke the RC if the secret key is lost or there is reason to believe that information about the secret key has become available to third parties.

110. When using a RC issued by the CC, the trusting parties agree:

- accept the terms and follow the procedures described in the Rules;
- check expiration dates, EDS and RCs policies;
- not use secret keys and their corresponding RCs after their expiration date;
- check the status of the RCs using the lists of revoked RCs;
- not use secret keys and their corresponding RCs in case of their revocation;
- use the RC in accordance with the Rules, Policies and current legislation.

111. The RC cannot be used before the expiration date or after the expiration date, in case of incorrect EDS and/or after suspension/revocation.

Chapter 9. Responsibility

112. CC employees are responsible for their actions in accordance with the legislation of the Republic of Kazakhstan.

113. The CC is not responsible for the consequences resulting from the violation by users and/or relying parties of the provisions of the Rules and/or current legislation.

114. The CC guarantees the processing of requests for the issuance of a RC according to the procedures described in the Rules.

115. The CC guarantees the processing of revocation requests according to the procedures described in the Rules.

116. The CC guarantees that there are no intentional distortions of the data of the participants of the CC in the RC.

117. Claims against the CC are limited to indicating that its actions do not comply with the Rules.

118. The CC is not obliged to reimburse the costs associated with:

- submission of erroneous, misleading or knowingly false information by the participants of the CC during registration (in the application for the release of the RC);

- failure by the participants of the CC to take measures to protect their own closed key, which led to its compromise, loss, disclosure, modification or unauthorized use;

- failure by the participants of the CC to take measures to verify the RC in order to determine its status (revoked/valid), scope (policy) and expiration dates;

- the use by the participants of the CC as part of their distinctive names that violate the intellectual property rights of third parties.

Section 3. FINAL PROVISIONS

119. Excluded.

120. The official notification of the participants of the CC on the approval of changes to the Rules is the publication on the Internet resource https://eubank.kz/rules-of-operation-of-the-certification-center /.

121. CC reserves the right to make changes and additions to the Rules without prior notice, including, but not limited to correcting typos, changing link addresses and contact information.

122. The Rules must be brought into compliance in connection with emerging internal and external changes and must necessarily be changed, clarified and improved to maintain the effectiveness of information security management of the CC.

123. All changes made to the Rules come into force and become binding on all participants of the CC immediately after their publication on the Internet resource https://eubank.kz/rules-of-operation-of-the-certification-center /.

124. In case of disagreement with the amendments (additions) the Owner of the RC is obliged to revoke the RC in accordance with the procedure provided for in Chapter 5 of the Rules.

125. If a part of the provisions of the Rules is declared unenforceable by a court or an authorized state body, the rest of it remains in force.

126. From the moment of termination of the Rules, the participants of the CC remain bound by its terms for all RC until the expiration of their validity period.

127. The applicable law for the resolution of disputes, the subject of which are disagreements on the substance of the Rules, is the legislation of the Republic of Kazakhstan.

128. Issues not regulated by the Rules are resolved in accordance with the legislation of the Republic of Kazakhstan and the INDs.

_____

Director of IT Security Service
Rustamov E. A.

LIST OF APPENDICES

№	Appendix Number	Name of the Appendix
1.	Appendix No. 1	Application form for the issuance of registration certificates from an individual
2.	Appendix No. 2	Application form for the issuance of registration certificates from a legal entity
3.	Appendix No. 3	Application for revocation of registration certificates from an individual
4.	Appendix No. 4	Application for revocation of registration certificates from a legal entity
5.	Appendix No. 5	SIPOC

LIST OF CHANGES AND ADDITIONS

No. p / p	Protocol number	Date of the protocol	Effective date	Initiator of changes
1.	149-08	26.10.2020	16.11.2020	IT Security Service
2.	165-13	23.11.2020	22.01.2021	IT Security Service
3.	155-05	04.09.2023	12.09.2023	IT Security Service
4.	152-03	02.09.2025	16.09.2025	IT Security Service