Appendix
to Resolution of the Board of Directors
No. 0320/5 dated 20.03.2025.

"Approved by"
the Minutes of the Management Board
Bank CenterCredit JSC
No. 0217/6 dated 17.02.2025

POLICY FOR THE APPLICATION OF REGISTRATION CERTIFICATES OF THE CERTIFICATION AUTHORITY OF BANK CENTERCREDIT JSC

Revision 2.2

Almaty, 2025

Content

Section 1. Introduction

Chapter 1.1. General

1. This Policy for Application of Registration Certificates of the Certification Authority of Bank CenterCredit JSC (hereinafter – the Registration Certificates Policy) has been developed in accordance with the requirements of legal acts of the Republic of Kazakhstan on issues of electronic document and electronic digital signature in order to ensure the functioning of the Certification Authority of Bank CenterCredit JSC (hereinafter – the Certification Authority).

2. The Registration Certificates Policy was developed taking into account international industry recommendations RFC 3647 “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”.

3. The Certification Authority of JSC Bank CenterCredit was created to provide services for issuing registration certificates to individuals – clients of JSC Bank CenterCredit, including individual entrepreneurs operating in the form of personal entrepreneurship, based on the current legislation of the Republic of Kazakhstan:

1) RoK Law "On Informatization";

2) RoK Law “On Electronic Document and Electronic Digital Signature”;

3) RoK Law “On personal data and their protection”;

4) legal act on creation, use and storage of private keys of an electronic digital signature in Certification Authority[1] (hereinafter – Cloud EDS Rules);

5) legal act on the authentication of an electronic digital signature[2] (hereinafter – the EDS Verification Rules);

6) legal act on the issue, storage, revocation of registration certificates and confirmation of the ownership and validity of the public key of an electronic digital signature by Certification Authority[3] (hereinafter – the Rules for the issuance and revocation of registration certificates);

7) ST RK 1073-2007. Cryptographic information protection tools. General Technical Requirements (hereinafter – the Standard).

4. The Registration Certificates Policy defines type of registration certificates issued by the Certification Authority, basic principles and general requirements for their applicability in interested information systems, united by standard information security requirements, which guarantees a certain level of trust in the information systems using these registration certificates.

5. The Registration Certificates Policy does not define the detailed order and procedures for functioning of the Certification Authority, ensuring the security of the public key infrastructure, which, in accordance with the requirements of legal acts of the Republic of Kazakhstan and international industry recommendations RFC 3647, are included in a separate internal regulatory document of Bank CenterCredit JSC (hereinafter referred to as the Regulations for the Activities of the Certification Authority).

6. From the moment the member of the information system using the services of the Certification Authority files (signs) the electronic application for the issuance of the registration certificate, the member becomes obliged to comply with requirements of the Registration Certificates Policy applicable to it, which is referred to in the application (electronic application) and the Registration Certificates Policy.

7. All registration certificates issued by the Certification Authority for clients of JSC Bank CenterCredit have a single profile and a common identifying feature – the value “c0” in the “keyUsage” extension.

As of the date of approval of the Registration Certificate Policy, the following apply:

[1]Rules for creation, use and storage of private keys of an electronic digital signature in a certification authority, as amended by the order of the Minister of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan dated March 17, 2023 No. 95/NK;

[2]Rules for verifying authenticity of an electronic digital signature, as amended by the order of the Minister of Information and Communications of the Republic of Kazakhstan dated December 30, 2016 No. 316;

[3]Rules for issuing, storing, revoking registration certificates and confirming the ownership and validity of the public key of an electronic digital signature by a certification authority, with the exception of the root certification authority of the Republic of Kazakhstan, the certification authority of state bodies, the national certification authority of the Republic of Kazakhstan and a trusted third party of the Republic of Kazakhstan, as amended by the order of the Acting Minister of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan dated March 30, 2023 No. 115/NK.

Chapter 1.2. Document name and attributes

8. Full document name – Policy for Application of Registration Certificates of the Certification Authority of JSC Bank CenterCredit.
9. The object identifier is 1.2.398.3.24.1.1.1.
10. Document version – 2.2.
11. The server address for publishing the document – https://www.bcc.kz/product/pki/?tab=DPP

Chapter 1.3. Participants of the public key infrastructure

1.3.1. Certification Authority

12. Certification Authority – in the context of the Registration Certificate Policy, this term refers to a hardware and software complex for issuing, servicing and revoking registration certificates, accredited in accordance with the legislation and operating in accordance with the approved Regulations of the Certification Authority.
13. The Certification Authority performs following functions of the public key infrastructure:
1) processing of applications for issuance and revoking of registration certificates;
2) publication of the list of revoked registration certificates;
3) online processing of requests to registration certificate status verification protocol service;
4) processing requests to the timestamp protocol service.
14. Certification Authority labeling in registration certificates:
C = KZ
O = Bank CenterCredit JSC
CN=Certification Authority

1.3.2. Registration Authority

15. Registration Authority – in the context of the Registration Certificates Policy, this term refers to the information system of Bank CenterCredit JSC responsible for identifying and/or authenticating applicants, generating, checking and accepting documents for issuing and/or revoking registration certificates and providing applicants with completed registration certificates.

1.3.3. Registration certificate holder

16. Concept of “registration certificate holder” is defined by the Law of the Republic of Kazakhstan “On Electronic Document and Electronic Digital Signature” as “an individual or legal entity in whose name the registration certificate has been issued, rightfully owning a private key corresponding to the public key specified in the registration certificate”.
17. Without limiting the generality of the definition established by the above Law, in the context of the Registration Certificates Policy, the term “holder of a registration certificate” means any individual using the information systems of Bank CenterCredit JSC, as well as any employee of the Certification Authority who owns a technological registration certificate if the registration certificate was issued for them by the Certification Authority.

1.3.4. Trusting party

18. Trusting Party – in the context of the Registration Certificates Policy, this term refers to the registration certificate holder or any other individual using registration certificates issued by the Certification Authority and/or electronic documents with electronic digital signatures in the information systems of Bank CenterCredit JSC, the authenticity of which is verified using these registration certificates.

Chapter 1.4. Assignment of Registration Certificates

19. Purpose of issuing registration certificates by the Certification Authority is to meet the needs of information systems owned by JSC Bank CenterCredit.

20. At the same time, the Certification Authority prohibits the use of registration certificates issued by it in information systems related to the management of high-risk sources (nuclear, air navigation equipment, weapons control systems, etc.), as well as in other information systems in any cases where an error in making a decision on trust based on the registration certificate may result in injury or death of personnel, or damage to the environment.

21. The purpose of the registration certificate issued by the Certification Authority is to confirm the compliance of the electronic digital signature with the requirements established by law, which determines the purpose of using pair of keys of the electronic digital signature, the open one of which is contained in the registration certificate.

22. The scope of permissible use of the registration certificate issued by the Certification Authority may be additionally limited by its "certificatePolicies" extension, which is intended to reflect the object identifiers of the registration certificate application policy.

23. The presence of policy object identifiers in the "cerificatePolicies" extension provides information systems that use registration certificates with the ability to provide additional protection in the form of system control over sets of required and prohibited policy object identifiers with restrictions on the use of inappropriate registration certificates.

24. It is not permitted to use registration certificates issued by the Certification Authority in ways that contradict the legislation of the Republic of Kazakhstan, the Registration Certificate Policy, and the Regulations for the Activities of the Certification Authority.

25. Registration certificates issued by the Certification Authority to their owners are used to work with the software of trusting parties and are not used as technological registration certificates of the information system of the Certification Authority. In turn, technological registration certificates of the information system of the Certification Authority are not used for any purposes other than their direct functional purpose.

Chapter 1.5. Document Management

26. The Registration Certificate Policy is updated by the Directorate of Cryptographic Information Protection (Certification Authority), located at the following address: A05G1D2, Almaty Panfilov Street, 98, Block B.

27. The contact person for document updating issues is the Head of the Directorate of Cryptographic Information Protection (Certification Authority), A05G1D2, Almaty, Panfilov st., 98, Block B, +7 (727) 2-598-583 (ext. 12921), alexey.korobetskikh@bcc.kz.

28. Amendments and additions to the Registration Certificate Policy are prepared by the Certification Authority either in the form of a new version of the document, or in the form of a list of changes and additions to its current version.

29. Prior to approval, amendments and additions to the Registration Certificate Policy shall be coordinated with interested subdivisions and officials of Bank CenterCredit JSC in accordance with internal procedures, with the exception of minor ones (changes in the addresses and links, contact information, correcting typos, etc.).

30. All amendments to the Registration Certificate Policy are published on the Bank CenterCredit JSC official information resource on the Internet at https://www.bcc.kz/product/pki/?tab=DPP.

31. The publication of a new approved edition of the Registration Certificate Policy in the section “Current editions” is an official notice of its entry into force for all holders of registration certificates issued by the Certification Authority and all trusting parties.

32. From the date of official notification of the entry into force of the new version of the Registration Certificate Policy, unless otherwise provided by the transitional provisions of the approving decision, the amendments and additions become mandatory for use by all owners of registration certificates issued by the Certification Authority and all trusting parties.

Chapter 1.6. Terms, Definitions and Abbreviations

33. Terms "Certification Authority", "accreditation of the Certification Authority", "registration certificate", "holder of registration certificate", "electronic document", "electronic document flow",

"electronic digital signature", "public key of electronic digital signature", "private key of electronic digital signature" are applied in the Registration Certificate Policy in accordance with the values established by the Law of the Republic of Kazakhstan "On electronic document and electronic digital signature".

34. The meaning and use of the terms "Certification Authority", "Registration Authority", "trusting party", as well as the peculiarities of the use of the term “holder of registration certificate" in the document are given in Chapter 1.3. of the Regulations for of the Certification Authority.

35. Other special terms used in the Registration Certificate Policy are used in the following meaning:

Term	Definition
Hardware Security Module	Hardware Security Module designed to encrypt information and manage public and private keys of an electronic digital signature
Authentication	Process or security service implementing this process, which is designed to verify that a person (object) is who it claims to be (what it is named by)
Bank	Bank CenterCredit JSC
Biometric authentication	A set of measures identifying a person based on physiological and immutable biological characteristics
Activation data	Any data, except for whole cryptographic keys, which are necessary to perform cryptographic transformations and require protection: personal identification numbers (PIN), passphrases, components of a shared cryptographic key, biometric parameters, etc.
Applicant	An individual who has submitted documents for issuance or revocation of a registration certificate
Identification	Process (or the result of a process) that establishes identity of an individual or legal entity (showing that this person is an unambiguously defined real person), and consists of two stages: • establishing correspondence between the name presented by a person and the person’s real identity and • establishing that the person requesting access to something on a specific behalf is in fact the person they claim to be (authentication)
Information system	Organizationally ordered set of information and communication technologies, service personnel, and technical documentation that implement specific technological actions through information interaction and are designed to solve specific functional problems
Public key infrastructure	A set of forces and means (technical, material, human, etc.), distributed services and components, collectively used to solve cryptographic problems (authentication, encryption, integrity and evidence control) based on public key cryptosystems, capable of independently providing public key management, through which these tasks are solved
Compromise of electronic digital signature keys	Loss by the registration certificate holder of confidence that specific electronic digital signature keys ensure the security of the information protected with their help
Multifactor authentication	Authentication verification method user using a combination of various parameters, including the generation and entry of passwords or authentication features (digital certificates, tokens, smart cards, one-time password generators and biometric identification tools)
Cloud EDS	Certification authority service that allows creation, use, storage and deletion of private keys of an electronic digital signature in the HSM of the certification authority, where the owner can access the private key remotely using at least two authentication factors, one of which is a biometric
Facility	Algorithm, an information system, and other elements used by individuals and legal entities for electronic document management
Object identifier	Unique set of numbers that is associated with an object and uniquely identifies it in the global address space of objects

Term	Definition
Revoked registration certificate	Registration certificate that has been cancelled in accordance with the procedure established by the Rules for the Issue and Revocation of Registration Certificates
Registration Certificate Application Policy	Internal document approved by the certification authority that defines regulations and mechanisms of the Certification Authority in terms of managing registration certificates
BCC Applications	Mobile applications/digital platforms of the Bank providing remote banking services for individuals. At the time of approval of the current version of the Registration Certificates Policy, BCC applications include the bcc.kz and BCC Business mobile applications.
Timestamp protocol	A cryptographic protocol that allows creating proof of the fact of the existence of an electronic document at a certain point in time
Certification Authority activity regulations	Document that defines the procedure for organizing main activities of the Certification Authority, carried out in accordance with the policy for application of registration certificates, including the implementation of the main processes of the Certification Authority
List Revoked registration certificate	Part of the register of registration certificates containing information about registration certificates that have been terminated, their serial numbers, date and reason for revocation (cancellation)
Participants of the public key infrastructure	Set of individuals and legal entities that perform any of the roles in the same public key infrastructure: the role of the registration certificate holder or trusting party – as well as the Certification Authority and Registration Authority(s)

36. The following abbreviations are used in the text of the Registration Certificate Policy:

Abbreviation	Definition
DN	Distinguished Name
HSM	Hardware Security Module
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
TSP	Time Stamp Protocol
PKI	Public key infrastructure
IS	Information system
LRRC	List Revoked registration certificate
CA	Certification Authority of Bank CenterCredit JSC
EDS	Electronic digital signature

Section 2. Responsibility for Storage and Publication of Data

Chapter 2.1. Storage

37. The CA provides following documents for downloading and review:

1) Registration Certificate Policy https://www.bcc.kz/product/pki/?tab=DPP;
2) Certification Authority activity regulations https://www.bcc.kz/product/pki/?tab=DPP;
3) LRRC https://uc.bcc.kz/cgi/crl;
4) CA's Registration Certificates https://www.bcc.kz/product/pki/?tab=KRSSOS.

38. Through the BCC application, application users, as well as Registration Authority employees can apply requests for the following CA services:

1) OCSP https://bcc-app.bank.corp.centercredit.kz:62301/
2) TSP https://bcc-app.bank.corp.centercredit.kz:62302/

3) Certification Authority https://bcc-app.bank.corp.centercredit.kz:62305/
4) Registration Authority https://bcc-app.bank.corp.centercredit.kz:62310/

Chapter 2.2. Publishing Registration Certificate Information to the Repository

39. For each IOC participant, the registration certificates issued in his name, as well as the SORS, are published in the repository.

Chapter 2.3. Frequency of updating data in the repository

40. Issued registration certificates and SORS are entered into the repository and published no later than the date of their commencement.

41. SORS is published as soon as revoked registration certificates appear. In this case, the period of updating the LRRC does not exceed seven (7) calendar days,

42. Information on the status of the registration certificate is published in accordance with the Registration Certificate Policy.

Chapter 2.4. Access control to the repository

43. Access to the repository is provided via LDAP in accordance with RFC 2251 (Lightweight Directory Access Protocol (v3)). The CA provides protection against unauthorized access to the repository.

44. Information published on the CA page of the Bank's official information resource on the Internet is provided to IS participants in free access mode, with "read-only" rights.

Section 3. Identification and authentication

Chapter 3.1. Requirements for names

45. The CA issues registration certificates that comply with the X.509 ITU-T version 3 recommendations and RFC 3280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile". The registration certificate contains a DN in the "Subject" field in the format recommended by the X.520 ITU-T standard. The DN of the registration certificate contains personal data that allows identifying its owner. The DN determines the registration certificate holder and corresponding private key, and also allows you to determine the scope of the registration certificate.

46. More detailed information is provided in the Regulations of the Certification Authority.

Chapter 3.2. Initial identity verification

3.2.1. Identification and authentication when issuing a registration certificate for serviced individuals

47. When submitting an electronic application for issuance of a registration certificate, the serviced individual undergoes a multi-factor authentication procedure, including biometric authentication, in accordance with the Rules of the cloud digital signature.

3.2.2. Identification and authentication when issuing a technological registration certificate (for service users of the CA)

48. Prior to registration of the Application for issuance of the registration certificate, the applicant is identified and authenticated according to the documents certifying his identity, containing his individual identification number, as well as giving him the right to represent the Bank in matters of working with the CA in accordance with the Rules for issuing and revoking registration certificates.

Chapter 3.3. Identification and authentication in requests for changing keys of electronic digital signature

49. Identification and authentication procedures in the processing of digital application and change of the EDS keys are completely similar to identification and authentication procedures in the processing of the application for the issue of the registration certificate set out in Chapter 3.2.

Chapter 3.4. Identification and authentication in revocation of a registration certificate

3.4.1. Identification and authentication when revocation a registration certificate for serviced individuals

50. Digital applications for revocation of registration certificates for served individuals are submitted through a remote channel (BCC application). In the process of revocation of a registration certificate, the applicant must:

1) undergo the biometric authentication procedure;

2) enter the password for private key of the digital signature corresponding to the registration certificate and indicate the reason for the revocation.

3.4.2. Identification and authentication when revocation a technological registration certificate (for service users of the CA)

51. Prior to registration of the Application for revocation of the registration certificate, the applicant shall be identified and authenticated according to the documents certifying his identity, containing his individual identification number, as well as giving him the right to represent the Bank in matters of working with the CA, in accordance with the Rules for issuing and revoking registration certificates.

Section 4. Operational requirements for the life cycle of a registration certificate

Chapter 4.1.

Chapter 4.1. Applications for issuing a registration certificate

52. Each electronic application (statement) for issuance of a registration certificate contains a link to the Policy of Registration Certificates and the Regulations of the Certification Authority and is an obligation of the applicant to comply with the principles and fulfill the requirements of the Policy of Registration Certificates and the Regulations of the Certification Authority in the part concerning the owner of the registration certificate and the trusting party.

53. Obligations of the owner of the registration certificate and the trusting party required by the CA are set out in Section 9.6 of the Registration Certificate Policy.

54. When applicants apply for issuance of a registration certificate through BCC applications in accordance with Section 4.1 of the Regulations on the Activities of the Certification Authority, registration certificates are issued by the CA without preparation and submission of applications in the form of documents on paper, as well as accompanying documents specified in the Rules for the Issuance and Revocation of Registration Certificates.

55. An application for issuance of a registration certificate may be submitted by individuals who have an individual identification number in the national register of the Republic of Kazakhstan.

56. More detailed information is provided in the Regulations of the Certification Authority.

Chapter 4.2. Processing of Applications for Registration Certificate

57. Before saving an electronic application (registration of the application) for issuance of a registration certificate, the applicant is identified and authenticated, as set out in Section 3.2.

58. If the applicant, when submitting an electronic application (statement) for issue of a registration certificate, does not successfully pass the identification and authentication procedure, i.e. does not provide documentary evidence of the reliability of the information specified in the application for the issue of a registration certificate, such an electronic application is not saved and is rejected (such an application is not registered).

59. More detailed information is set out in the Regulations of the Certification Authority.

Chapter 4.3. Issuance of Registration Certificates

60. When issuing a registration certificate, the CA relies on the results of the remote initial verification of identity and information from the application, which were successfully carried out and verified by the Registration Authority during the identification and authentication procedures, in accordance with Section 3.2 of the Regulations of the Certification Authority.

61. Any registration certificate issued by the CA is automatically published in the repository.

62. More detailed information is provided in the Regulations of the Certification Authority.

Chapter 4.4. Acceptance of Registration Certificates

63. More detailed information is provided in the Regulations of the Certification Authority.

Chapter 4.5. Use of registration certificates and key pairs

64. Registration certificates issued by the CA are applicable for verifying the digital signature.

65. Private keys corresponding to the registration certificates of owners issued by the CA are intended for generating the digital signature.

66. The CA protects the private keys of the digital signatures of the owners of registration certificates stored in the HSM from unauthorized access and use in the manner prescribed by the Cloud Digital Signature Rules.

67. The private key of the digital signature and the registration certificate are used by the owner of the registration certificate and trusting parties only in accordance with the legislation of the Republic of Kazakhstan, contractual obligations (if any), the Registration Certificate Policy and the Regulations of the Certification Authority.

68. To verify and make a decision on trust based on the registration certificate issued by the CA, it is necessary to use the Rules for Verifying the Digital Signature.

69. The trusting parties shall use registration certificates strictly in accordance with the information and Regulations of the Certification Authority specified therein. Obtaining additional information and guarantees, in addition to the information specified in the registration certificate, is carried out by trusting parties.

70. The CA shall not be liable to persons using registration certificates who have not undertaken to comply with the requirements of the Registration Certificate Policy and the Regulations of the Certification Authority in the part concerning the obligations of the trusting party, in the form of a written commitment, electronic document or other form of consent recorded in the Bank's IS.

71. If the trusting party, when taking any action based on trust in the registration certificate issued by the CA, has not fulfilled the conditions of Sections 4.5 of the Registration Certificate Policy and the Regulations of the Certification Authority, the CA shall not be liable to the trusting party for the consequences of such an act.

72. More detailed information is provided in the Regulations of the Certification Authority.

Chapter 4.6. Updating Validity Periods of Registration Certificates

73. The CA does not provide services for renewing the validity period of registration certificates.

74. More detailed information is provided in the Regulations of the Certification Authority.

Chapter 4.7. Changing Electronic Digital Signature Key Change in Registration Certificate

75. Key change – procedure for issuing a registration certificate with a new EDS public key and new validity periods without changing other data specified in the current registration certificate. This procedure involves the production of a new private key of the digital signature and a corresponding new registration certificate.

76. More detailed information is provided in the Regulations of the Certification Authority.

Chapter 4.8. Amendment of data specified in the registration certificate

77. The CA does not provide services for changing the information specified in registration certificates.

78. More detailed information is provided in the Regulations of the Certification Authority.

Chapter 4.9. Revocation and Suspension of Registration Certificate

79. Registration certificates issued by the CA may only be revoked by the CA itself.

80. The procedures for identifying and authenticating the applicant when forming an application for revocation of a registration certificate are carried out in accordance with the requirements of Section 3.4 of the Regulations of the Certification Authority.

81. Applications and electronic applications for revocation of a registration certificate are processed within one business day.

82. Any participant of the Bank's IOC uses the OCSP or SORS service to check the status of registration certificates. Information about the OCSP and SORS service addresses is specified in each issued registration certificate.

83. SORS are unified in the sense that they contain revocable registration certificates of all PKI participants: CA, Registration Authorities and holders of registration certificates.

84. LRRC is certified by the EDS Certification Authority. Access to SORS is provided around the clock and continuously, except for the time of scheduled maintenance.

85. The CA does not provide services for temporary suspension of registration certificates.

86. More detailed information is provided in the Regulations of the Certification Authority.

Section 5. Physical, Operational and Management Control

Chapter 5.1. Physical control

87. More detailed information is provided in the Regulations of the Certification Authority.

Chapter 5.2. Operational control

88. The CA ensures information security measures in accordance with:

1) the legislation of the Republic of Kazakhstan;

2) internal regulatory documents of the Bank;

3) job descriptions of the Bank's employees.

89. More detailed information is provided in the Regulations of the Certification Authority.

Chapter 5.3. Personnel Control

90. More detailed information is provided in the Regulations of the Certification Authority.

Chapter 5.4. Procedures for Control Logging and Information Security Incident Management

91. The CA ensures logging of the following events:

1) request for issue of a registration certificate;

2) request for revocation of a registration certificate;

3) generation of a private key of the digital signature of a cloud digital signature;

4) use of a private key of the digital signature of a cloud digital signature;

5) deletion (erasure) of a private key of the digital signature of a cloud digital signature.

92. Private keys of digital signatures and their activation data are not subject to recording in control protocols.

93. More detailed information is provided in the Regulations of the Certification Authority.

Chapter 5.5. Archive maintenance

94. More detailed information is provided in the Regulations of the Certification Authority.

Chapter 5.6. Certification Authority Electronic Digital Signature Key Change

95. The CA changes its key pairs and registration certificates due to their expiration or in the event of their compromise.

96. More detailed information is provided in the Regulations of the Certification Authority.

Chapter 5.7. Restoring operation in the event of compromise or failures

97. More detailed information is provided in the Regulations of the Certification Authority.

Chapter 5.8. Termination of Certification Authority Work

98. More detailed information is provided in the Regulations of the Certification Authority.

Section 6. Technical Safety Control

Chapter 6.1. Manufacturing and Installation of Electronic Digital Signature Key Pairs

99. The CA issues all keys of the EDS that comply with the requirements of the algorithm of GOST 34.310–2004.

100. Any applicant who submits an electronic application to the CA for issue of a registration certificate acknowledges that he thereby gives his consent to the creation, storage and use of his private keys of the EDS on the CA side. The electronic application form contains a note about the specified consent.

101. More detailed information is provided in the Regulations of the Certification Authority.

Chapter 6.2. Electronic Digital Signature Private Key Protection and Hardware Cryptographic Module Engineering Controls

102. Private keys of the Certification Authority are created in HSMs certified for compliance with the Standard at a level not lower than the second.

103. The private keys of users of the Bank's IS - owners of registration certificates are created in HSMs certified for compliance with the Standard at a level not lower than the third.

104. More detailed information is provided in the Regulations of the Certification Authority.

Chapter 6.3. Other features of Electronic Digital Signature Key Management

105. More detailed information is provided in the Regulations of the Certification Authority.

Chapter 6.4. Activation data

106. More detailed information is provided in the Regulations of the Certification Authority.

Chapter 6.5. Security Control of Computing Resources

107. More detailed information is provided in the Regulations of the Certification Authority.

Section 7. Profiles of Registration Certificates, Lists of Revoked Registration Certificates and Online Registration Certificate Status Verification Protocol Service

Chapter 7.1. Profiles of Registration Certificates

108. Certification Authority issues registration certificates that comply with ITU-T X.509 version 3 recommendations.

109. The Certification Authority uses the OID of the Republic of Kazakhstan to identify cryptographic algorithms https://root.gov.kz/oid/.

110. More detailed information is provided in the Regulations of the Certification Authority.

Chapter 7.2. Profiles of Revoked Registration Certificates List

111. More detailed information is provided in the Regulations of the Certification Authority.

Chapter 7.3. Online Registration Certificate Status Verification Protocol Service Profile

112.More detailed information is provided in the Regulations of the Certification Authority.

Section 8. Inspection of Activities

113.Compliance of internal regulatory documents, main equipment and data processing centers of the CA is subject to regular inspections by the authorized body in the field of information security during the accreditation process.

Section 9. Billing And Liability Issues

Chapter 9.1. Tariffs

114.CC services are not charged and not paid.

Chapter 9.2. Responsibility

115.Responsibility of PKI participants serviced by the CA is established by the legislation of the Republic of Kazakhstan[4].

Chapter 9.3. Confidentiality

116.Registration certificates issued by the CA and information on their status are not and are not considered confidential information.

Chapter 9.4. Protection of Personal Data of PKI Participants

117.Any owner of a registration certificate, submitting an electronic application (statement) for issue of a registration certificate to the CA, acknowledges that he gives his consent to the placement of information about himself contained in the application (statement) in the public domain. An electronic application (statement) for issue of a registration certificate confirms the consent of the applicant to collection and processing of his personal data in accordance with the legislation of the Republic of Kazakhstan on personal data and their protection[5].

Chapter 9.5. Intellectual Property Right

118.CA shall not prohibit the holders of registration certificates and trusting parties from copying and distributing registration certificates issued by the CA on a non-exclusive free basis, subject to the conditions of completeness and integrity of the data.

119.Registration certificate holders retain all their rights to names and trademarks specified in the registration certificates.

Chapter 9.6. Warranties and Representations

120.Each registration certificate holder shall ensure:

1) use only that private key of the digital signature for which there is a corresponding registration certificate issued by the CA, accepted by the holder and valid at the time of use (not expired or revoked);

2) protection of the activation data of their private keys of the digital signature from access by any other persons;

3) reliability of the information about themselves provided for the issuance of registration certificates to the Registration Authority and other interested IS of the Bank;

---

[4]The Code of the Republic of Kazakhstan on Administrative Offenses, Article 640.

[5] Law of the Republic of Kazakhstan “On personal data and their protection”, Article 8.

4) verification of reliability of the information about themselves contained in the registration certificate issued to them before accepting it;

5) non-use of their private key of the digital signature for purpose of signing any registration certificates, SORS, any other format of public key certificates of the digital signature or information about its status.

121.Each trusting party shall ensure that when using registration certificates issued by the CA, only informed decisions are made based on a sufficient amount of objective information about the registration certificate and its owner, in accordance with the provisions of Section 4.5 of the Regulations on the Activities of the Certification Authority.

Chapter 9.7. Disclaimer of Warranties

122.The CA shall not provide additional warranties to the owners of registration certificates and trusting parties arising from agreements on the provision of banking services, including warranties of merchantability and conformity, except for those warranties established by the legislation of the Republic of Kazakhstan on electronic documents and electronic digital signatures and declared in the Policy on Registration Certificates.

Chapter 9.8. Limitations of Liability.

123.The liability of the CA, Registration Authorities, owners of registration certificates and trusting parties is limited by the legislation of the Republic of Kazakhstan[6].

Chapter 9.9. Compensation

124.To the extent that it does not contradict the current legislation of the Republic of Kazakhstan, the owners of registration certificates shall bear the costs associated with compensation for:

1) providing erroneous, misleading or knowingly false information in an electronic application (statement) for the issue or revocation of a registration certificate;

2) unintentional or intentional concealment of material facts subject to reflection in an electronic application (statement) for the issue or revocation of a registration certificate;

3) failure to take measures to protect the activation data of one's own private key of an electronic digital signature, which contributes to its compromise or unauthorized use;

4) using names in one's DN that violate the intellectual property rights of third parties.

125.To the extent that it does not contradict the current legislation of the Republic of Kazakhstan, the trusting parties shall bear the costs associated with compensation for:

1) unreasonable trust in a registration certificate, caused by a breach of obligations of the trusting party;

2) failure to take measures to verify the registration certificate in order to determine its validity period and status (revoked/not revoked).

Chapter 9.10. Entering Into Force and Termination

126.Registration Certificate Policy and all amendments and additions thereto shall enter into force no earlier than the day of publication on the Bank's official Internet resource.

127.Registration Certificate Policy, including published amendments and additions thereto, shall remain in effect until the moment of publication of its new version on the Bank's official Internet resource.

128.In the event of cancellation of the Registration Certificate Policy, IS participants who use registration certificates issued by the CA shall remain bound by the requirements of its latest effective version until the expiration of the validity period of the registration certificates.

129.The owner of the registration certificates has the opportunity to initiate early termination of their service at the CA:

---

[6]The Code of the Republic of Kazakhstan on Administrative Offenses, Article 640.

1) by terminating (all) current agreement(s) providing for service;
2) revoking all valid registration certificates before their expiration.

130. After 1 year from the date of expiration of all registration certificates of a specific owner, his/her service in the CA is automatically terminated.

Chapter 9.11. Notifications and communication with participants

131. Participants of the IOC: CA, Registration Authorities, owners of registration certificates and trusting parties - use any appropriate channels for communication with each other that correspond to the subject of interaction, degree of importance and urgency of communication, unless otherwise determined by agreement between the parties.

Section 9.12. Amendments

132. Minor changes to the Registration Certificate Policy (changes in addresses and links, contact information, correction of typos, etc.) are made without prior notification to participants in the public key infrastructure. Decisions on the level of significance of amendments (significant or insignificant) are made by the CA independently.

133. The CA preliminarily publishes significant changes and additions to the Registration Certificate Policy, in draft form, on the Bank's official information resource on the Internet at https://www.bcc.kz/product/pki/?tab=DPP, as a rule, at least 14 calendar days before they come into force, unless otherwise provided by the published changes in the legislation of the Republic of Kazakhstan.

Chapter 9.13. Dispute Resolution

134. Disputes on the merits of the Registration Certificate Policy between IOC participants: between registration certificate holders and trusting parties, as well as between the registration certificate holder or trusting party, on the one hand, and the CA or Registration Authority, on the other hand, are resolved out of court.

135. If the dispute is not resolved out of court, it shall be resolved in court.

Chapter 9.14. Jurisdiction.

136. The legislation of the Republic of Kazakhstan shall apply to the resolution of disputes, the subject of which is disagreement on the essence of the Registration Certificate Policy.

Section 10. Other Issues

Chapter 10.1. Terms of application

137. If some provisions of the Registration Certificate Policy are recognized as inapplicable by a court or authorized state body, the rest of them shall remain in force.

Chapter 10.2. Individual Aspects of Property Rights

138. Any registration certificate issued by the CA and the EDS public key contained therein shall be the property of the Bank. In this case, the applicant who has accepted the registration certificate issued in his name in the manner set out in Section 4.4 of the Regulations on the Activities of the Certification Authority is automatically granted the right to own this registration certificate and the public key of the digital signature.

139. The trusting parties are automatically granted the right to use any registration certificate and the public key of the EDS contained in it from the moment of their publication in the CA.

140. A private EDS key that complies with the registration certificate issued by the CA is the property of the owner of this registration certificate.

Chapter 10.3. Final Provisions

141.Requirements of the Registration Certificate Policy are mandatory for all IOC participants in the part that concerns them.

142.The Bank units interacting with the CA shall be responsible for:

1) compliance with the requirements set out in the Registration Certificate Policy;

2) completeness and timeliness of functions performed within the framework of their powers.

143.All issues not regulated by the Registration Certificate Policy shall be resolved in accordance with the procedure determined by the current legislation of the Republic of Kazakhstan, other regulatory documents and decisions of the Bank's authorized bodies.

144.The Registration Certificate Policy is subject to revision as necessary. The department responsible for reviewing and updating the Registration Certificates Policy is the Bank’s Cryptographic Information Protection Directorate.

Cryptographic Information Protection Directorate