Appendix
the Minutes of the Management Board No.0217/3
Dated 17.02.2025

Approved by the Management Board Decision
No. 1003/2 dated 03.10.2024
as amended
Approved by the Management Board
No. 0217/3 dated 17.02.2025

CERTIFICATION AUTHORITY ACTIVITY REGULATIONS JSC BANK CENTERCREDIT

Revision 2.2

Almaty, 2025

Content

Section 1. Introduction

Chapter 1.1. General

1. This Regulations for the Activities of the Certification Authority of Bank CenterCredit JSC (hereinafter – the Regulations) 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), and determines the procedure for its functioning.

2. The regulations were 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 Authorities[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 Authorities[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 Regulations define measures implemented by the Certification Authority when providing a set of services, which is defined by the Policy of Application of Registration Certificates of the Certification Authority of Bank CenterCredit JSC (hereinafter – the Policy of Registration Certificates) and includes, but is not limited to, the issue, management and revocation of registration certificates.

5. 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.

6. The Regulation, unlike the Registration Certificate Policy, defines the order and procedures in accordance with which:

1) the functions (services) of the Certification Authority are performed;

2) security and management of the core of the public key infrastructure are ensured.

On the date of approval of the Regulation, the following shall 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.

7. From the moment the member of the information system using the services of the Certification Authority files the application for the issuance of 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 Regulations.

8. The Regulation also defines verification procedures related to the issuance and subsequent servicing of those types of registration certificates issued by the Certification Authority, in accordance with the Registration Certificates Policy.

Chapter 1.2. Document name and attributes

9. Full name of documents Regulations for Activities of the Certification Authority of Bank CenterCredit JSC.

10. The object identifier is 1.2.398.3.24.1.2.1.

11. Document version – 2.2.

12. 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

13. Certification Authority – in the context of the Regulation, this term refers to a software and hardware complex for issuing, servicing and revoking registration certificates, accredited in accordance with the law and acting in accordance with the approved Regulations.

14. 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.

15. Certification Authority labeling in registration certificates:

C = KZ

O = Bank CenterCredit JSC

CN=Certification Authority

1.3.2. Registration Authority

16. Registration Authority – in the context of the Regulation, 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

17. 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”.

18. Without limiting the generality of the definition established by the above Law, in the context of the Regulaiton, 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

19. Trusting Party – in the context of the Regulation, 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

20. 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.

21. In accordance with section 1.4 of the Certificate of Registration Policy, the certificate of registration issued by the Certification Authority contains object policy identifiers in the "certificatePolicies" extension, which determine the additional scope of their application.

22. Complete list of object policy identifiers specified by the Certification Authority in the issued client registration certificates is provided on the Bank CenterCredit JSC official online information resource at https://www.bcc.kz/product/pki/?tab=OIPS.

Chapter 1.5. Document Management

23. Regulation is updated by the Directorate of Cryptographic Information Protection (Certification Authority), located at the following address: A05G1D2, Almaty Panfilov Street, 98, Block B.

24. 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.

25. Amendments and additions to the Regulation 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.

26. Prior to approval, amendments and additions to the Regulaiton 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.).

27. Amendments to the Regulations shall be approved by a protocol decision of the Management Board of Bank CenterCredit JSC, with the exception of minor ones (changes in addresses and links, contact information, correction of typos, etc.).

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

29. The publication of a new approved edition of the Regulations 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.

30. From the date of official notification of the entry into force of the new version of the Regulaiton, 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.

31. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

32. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

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
Blockchain	Information and communication technology that ensures invariability of information in a distributed data platform based on a chain of interconnected data blocks, specified integrity algorithms and encryption tools
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

Term	Definition
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)
Key Information Medium	Key a specialized medium in which a cryptographic information protection tool with a certificate of compliance with the standard requirements is used to protect stored private keys of an electronic digital signature.
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
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 apps	Mobile applications/digital platforms of the Bank providing remote banking services for individuals. At the time of approval of the current version of the Regulation, 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)
Funds Cryptographic Information Protection	A tool that implements cryptographic transformation algorithms, generation, creating, distribution or key management
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)
Hash	Convert an array of arbitrary-length input data to a fixed-length bit string

36. Following abbreviations are used in the Regulation:

Abbreviation	Definition
DN	Distinguished Name

Abbreviation	Definition
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
KIM	Key Information Medium
CPIM	Cryptographic protection of information means
LRRC	List Revoked registration certificate
CA	Certification Authority of Bank CenterCredit JSC
RA	Registration Authority
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) https://www.bcc.kz/product/pki/?tab=DPP Regulations;
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 RA employees can apply requests for the following CA services:

1) OCSP https://bcc-app.bank.corp.centercredit.kz:62301/
2) TSPhttps://bcc-app.bank.corp.centercredit.kz:62302/
3) Certification Authority https://bcc-app.bank.corp.centercredit.kz:62305/
4) RA 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 7 calendar days,

42. Information on the status of the registration certificate is published in accordance with the Regulaiton.

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. Each registration certificate holder has a unique DN.

47. Uniqueness of identification is achieved by using individual identification numbers (IIN) from a single republican register, based on the identification and authentication methods used.

48. Anonymity and aliases are not allowed when generating a DN.

Chapter 3.2. Initial identity verification

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

49. When submitting an 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)

50. 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

51. Identification and authentication procedures in the processing of 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 of the Regulation.

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

52. 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)

53. 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

54. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

55. Applications for issuance of registration certificates are submitted by individuals served, including individual entrepreneurs operating as personal entrepreneurs, through a remote channel (BCC applications). The application is created in electronic form, its form is given in Appendix 1 to the Regulations.

56. Submission of applications for issuing a technological registration certificate for service users of the CA is carried out by personal appearance at the CA, filling out an application for issuing a registration certificate in the form of the Rules for Issuing and Revoking Registration Certificates and certifying it with the personal signature of the applicant.

57. In the context of the Regulation, an application for the issuance of a registration certificate means either an electronic application in the form of Annex 1 to the Regulation, or an application in the form of a paper document in the form of the Rules for the issuance and revocation of registration certificates.

58. In the process of appliying for registration certificate, the applicant shall:

1) give consent (to properly assure approved form of the Bank) to the collection and processing of personal data;

2) familiarize with the Registration Certificate Policy and Regulations;

3) familiarize with the text of the application for issuance of a registration certificate.

Chapter 4.2. Processing of Applications for Registration Certificate

59. In the process of processing applications for the issuance of a registration certificate, individuals served are subject to multi-factor authentication, in accordance with the Cloud EDS Rules, including biometric authentication, via a remote channel (VSS applications).

Service users of the CAare identified and authenticated upon personal appearance at the CA, in accordance with the Rules for Issuing and Revoking Registration Certificates.

60. Refusal to issue a registration certificate in cases where:

1) applicant is not provided (or not fully provided) necessary information;

2) applicant provided false information;

3) applicant has not reached the age of sixteen;

4) there is a court decision that has entered into legal force.

Chapter 4.3. Issuance of Registration Certificates

61. Requests for issue of registration certificates are signed by the EDS of the CA employees who have the right to form them.

62. Requests for issuance of registration certificates for serviced persons are accepted only from the Bank's IS. Requests to the Certification Authority from the EDS cloud subsystem are signed only by the service key of the CA manager.

63. When processing a request for issuing a registration certificate, the CA checks the fact of possession of a private EDS key corresponding to the public EDS key to which the registration certificate is requested. Method of proving possession of private EDS key is an electronic document in the format PKCS # 10.

64. Official notification of the registration certificate holder is its publication in the CA repository and availability of the registration certificate for its owner in in the BCC appendix.

Chapter 4.4. Acceptance of Registration Certificates

6.4.1. 4.4.1. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

65. Fulfillment of all the following conditions means acceptance of the issued registration certificate by its owner:

1) consent to comply with conditions of the Registration Certificate Policy and the Regulations expressed in the application for issuance of the registration certificate;

2) receiving of the registration certificate;

3) owner has no objections (claims) to the registration certificate content;

4) using the private key of the EDS complying with the registration certificate.

6.4.2. 4.4.2. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

66. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

Chapter 4.5. Use of registration certificates and key pairs

4.5.1. Use of electronic digital signature private key and registration certificate by their owner

67. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

67-1. The private key of digital signature is used by the owner only after he has, in accordance with Chapter 4.1 of the Registration Certificate Policy, reviewed the text of the application for the issue of a registration certificate and given an obligation (in the form of an electronic document, a handwritten written obligation, or another form of consent recorded in the Bank's IS) to fulfill the obligations of the owner of registration certificates and the trusting party, the CA has issued a registration certificate of the corresponding public key, and the owner has accepted this registration certificate.

68. The first use of the EDS private key by the registration certificate holder, subject to the remaining conditions of paragraph 4.4.1 of the Regulation, means acceptance of the registration certificate by its owner.

69. Owners of technological registration certificates (service users) of the CA shall take measures to protect their private keys of the digital signature and their activation data from unauthorized access and use in the manner established by the current legislation of the Republic of Kazakhstan, and cease using them after the expiration or revocation of the relevant registration certificate.

70. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

4.5.2. Use of registration certificate and public key of electronic digital signature by trusting party

71. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

72. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

73. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

73-1. Before taking any action based on trust in an electronic document, for verification of which it is necessary to use a registration certificate issued by a CA, the trusting party, in accordance with the Rules for Verification of the EDS, using the means of the relevant IS, verifies each EDS contained in it, including the associated registration certificates, receipts (service responses), timestamps, OCSP or LRRC, and, based on the verification results, independently makes a decision on the authenticity of the electronic document.

73-2. To verify the EDS, the IS:

1) determines and verifies the chain of registration certificates, which allows identifying the entity that generated the EDS. During verification of the chain of registration certificates, the algorithm described in the recommendations of RFC 3280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” is used;

2) during verification of each registration certificate of the chain, additionally checks the content of the extensions “extendedKeyUsage” and/or “keyUsage” for compliance with the purpose of use;

3) independently checks whether the entity that generated digital signature has the authority sufficient to sign the electronic document. The CA IS does not provide services for monitoring the authority of the owners of registration certificates, in addition to the information specified directly in the registration certificate.

73-3. If any step of the verification gives a negative result or cannot be performed, the digital signature is considered invalid and the electronic document is rejected.

73-4. If electronic document contains a timestamp receipt generated by the CA, then in order to perform an action that requires trust in the timestamp, it is also necessary to check this timestamp receipt as an electronic document with a digital signature in the manner established by the Rules for Verifying Digital Signatures.

73-5. If any of the registration certificates in the chain has the “revoked” status at the time of the digital signature verification, the trusting party shall decide at its own risk whether it is justified to rely on the electronic document generated by the owner of the registration certificate prior to the revocation of this registration certificate in the chain. In such cases, the CA shall not be liable to the trusting parties, since filing an application for revocation of the registration certificate is the responsibility of the specific owner of the registration certificate.

73-6. If circumstances indicate the need for additional guarantees from the authors of the electronic document, the trusting party shall obtain such additional guarantees from the owners of the registration certificates independently, without contacting the CA, and before performing actions that require trust in the registration certificate.

Chapter 4.6. Updating Validity Periods of Registration Certificates

74. Renewal of the registration certificate – procedure for issuing registration certificate with new validity periods without changing other data specified in the current registration certificate.

75. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

76. Upon expiration of the registration certificate, if its owner is interested, the CA issues a registration certificate with a new public key of the digital signature at the owner's request.

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

77. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

78. The change of the keys of the digital signature and the registration certificate is initiated by their owner independently.

79. Procedures for submitting an application and issuing a registration certificate when changing the EDS keys are completely similar to procedures for submitting an application for issuing a registration certificate and processing it.

Chapter 4.8. Amendment of data specified in the registration certificate

80. Amendment of data specified in the registration certificate – procedure for issuing registration certificate with new data about its owner without changing the public EDS key and validity periods specified in the current registration certificate.

81. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

82. In case of loss of relevance of the information specified in the current registration certificate, the owner shall revoke the registration certificate in accordance with Chapter 4.9 of the Regulation and apply for the issuance of a new registration certificate in accordance with Chapter 4.1 of the Regulation.

83. Procedure for submitting an application and issuing a registration certificate when changing information specified in it is completely similar to procedures for submitting an application for issuing a registration certificate and processing it.

Chapter 4.9. Revocation and Suspension of Registration Certificate

4.9.1. Grounds for Revocation of Registration Certificate

84. CA may revoke the registration certificate and publish it to the LRRC in the following cases:

1) as required by registration certificate holder;

2) when establishing the fact of providing inaccurate information upon receipt of a registration certificate;

3) upon death of registration certificate holder;

4) changes in the surname, first name or patronymic of the registration certificate holder;

5) provided for by the agreement between the CA and the registration certificate holder;

6) by a court decision that has entered into legal force.

4.9.2. Persons Eligible to Apply for Revocation of Registration Certificate

85. Application for revocation of the registration certificate can be submitted by an individual – its owner or employee of the CA, and for technological registration certificates - by CA employee.

4.9.3. Procedures for Registration Certificate Revocation Applications

86. Applications for revocation of registration certificates for served individuals are submitted through a remote channel (BCC application). The application is created in electronic form, its form is given in Appendix 2 to the Regulations. In this case, corresponding requests to the Certification Authority are generated and processed automatically, provided that the applicant successfully passes identification and authentication procedures.

87. Procedures for identification and authentication of the applicant when forming an application for revocation of registration certificate submitted by the serviced person or employee of

the RA are carried out in accordance with the requirements of paragraph 3.4.1 of the Regulation, using biometric authentication and identification.

88. Submission of applications for revoking technological registration certificate for service users of the CA is carried out by personal appearance at the CA, filling out an application for issuing a registration certificate in the form of the Rules for Issuing and Revoking Registration Certificates and certifying it with the personal signature of the applicant. Applications for revocation of registration certificates are processed by employees of the CA, in accordance with the Rules for the issuance and revocation of registration certificates.

89. Procedure for identification and authentication of the applicant when processing an application for revocation of a technological registration certificate issued by a CA employee is carried out in accordance with the requirements of paragraph 3.4.2 of the Regulations.

90. In the context of the Regulation, an application for revoking registration certificate means either an electronic application in the form of Annex 2 to the Regulation, or an application in the form of a paper document in the form of the Rules for the issuance and revocation of registration certificates.

4.9.4. Deadline for Application for Registration Certificate Revoking

91. Persons entitled to apply for the revocation of registration certificates shall do so immediately as soon as possible as they become aware of occurrence of the grounds listed in paragraph 4.9.1 of the Regulation.

4.9.5. Registration Certificate Revocation Application Processing Time

92. Revocation of applications filed with respect to registration certificates of the persons served is carried out immediately.

93. Revocation of registration certificates for applications issued by the CA employee shall be carried out within no more than one working day.

4.9.6. Requirements on the need to verify the fact of revocation of registration certificate by the trusting party

94. Any Bank PKI participant shall check the status of registration certificates. You can use the LRRC or OCSP service to check. Electronic document verification service is available in the BCC application and is designed to obtain a list of electronic documents that the registration certificate holder has signed.

4.9.7. Frequency of Issuance of List of Revoked Registration Certificates

95. The LRRC is updated when the status of any registration certificate issued by the CA changes. When a new LRRC is issued, revoked expired registration certificates are removed from it.

96. The LRRC is provided in electronic form in a format defined by RFC 3280. Access to LRRC is provided via HTTP.

4.9.8. Maximum Interval Between Releases of List of Revoked Registration Certificate

97. The LRRC is updated no later than 7 calendar days from the date of signing of the previous LRRC.

4.9.9. Online Verification of Registration Certificate Status

98. Information on the status of registration certificate can be obtained using the OCSP service.

99. The OCSP service meets requirements described in RFC 2560. Receipts with the OCSP service result are certified by the OCSP service EDS.

4.9.10. Online Verification of Registration Certificate Status

100. The OCSP service is used when checking electronic documents in the BCC applications.

4.9.11. Other Available Recall Notification Forms

101. The CA does not provide other forms of notification of the revocation of registration certificates.

4.9.12. Special requirements in case of compromise of the private key of an electronic digital signature

102. In the event of a reasonable suspicion of a compromise of the EDS private key, the owner of the relevant registration certificate performs its revocation in accordance with section 4.9 of the Regulation and, if necessary, submits an application for issuance of a new registration certificate.

4.9.13. Conditions for suspension and termination of the registration certificate

103. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

104. Any registration certificate issued by the CA shall become invalid upon expiration of the term specified therein.

105. The Owner shall be entitled to revoke the registration certificate before expiry date in accordance with Chapter 4.9 of the Regulation.

106. The revoked registration certificates are stored in the CA for entire period of operation of the CA, but for at least five years.

107. In case of termination of the CA activity, revoked registration certificates shall be further stored in the Bank in accordance with the legislation of the Republic of Kazakhstan[4] or transferred, in agreement with their owner, to another Certification Authority.

Section 5. Physical, Operational and Management Control

Chapter 5.1. Physical control

108. CA IS, which processes requests of the PKI participants, is located in specialized data centers.

109. Physical access to primary and backup data processing centers is organized and controlled by the same security measures. The server rooms are equipped with the following systems:

1) access control and management;
2) security alarm;
3) video surveillance;
4) guaranteed power supply;
5) electrical grounding;

[4] Law of the Republic of Kazakhstan“On Electronic Document and Electronic Digital Signature”, Article 22, Clause 1.

6) providing a microclimate;
7) fire alarm;
8) gas automatic fire extinguishing.

110. The CA maintains the archive in accordance with the current internal document of the Bank regulating the backup and recovery of information.

111. Disposal of CA confidential data media is carried out in accordance with the current internal document of the Bank regulating destruction of information on technical media.

Chapter 5.2. Operational control

112. For operational control purposes, the powers of CA employees and PKI participants are divided into 3 following categories (roles):

1) CA administrator;
2) CA auditor;
3) CA user.

Chapter 5.3. Personnel Control

5.3.1. Personnel Qualification Requirements

113. Before being appointed to positions in the CA, applicants submit documents determined by the Labor Code of the Republic of Kazakhstan and undergo screening in accordance with the Bank’s internal recruitment document.

5.3.2. Employee Inspection Procedure

114. Employees are checked in accordance with the internal instructions of the Bank's Security Assurance Center.

5.3.3. Personnel Training Requirements

115. Recruitment of CA employees is carried out by specialists of specialized (technical, mathematical, IT) education.

5.3.4. Personnel Development Requirements

116. CA specialists and managers are trained or certified at least once every three years.

5.3.5. Frequency and Sequence of Employee Activity Change

117. Undefined.

5.3.6. Liability for Violations

118. The CA and RA personnel shall be responsible for their actions in accordance with the internal regulatory documents of the Bank and the current legislation of the Republic of Kazakhstan.

5.3.7. Requirements for Independent Contractors

119. In exceptional cases, when the work requires services of independent contractors, the contractors specialists perform the work only under the supervision and with the permission of the CA employees.

5.3.8. Documentation Provided to Personnel

120.Activities of CA employees are regulated by job descriptions and internal regulatory documents of the Bank.

121.Access of CA employees to documentary fund is organized in accordance with job descriptions and functional responsibilities.

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

5.4.1. Types of Events to be Audited

122.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.

123.Shelf life of the work protocols is one year from the date of expiration of the registration certificate.

124.When logging actions, the following information is recorded:

1) date, time;
2) registration certificate holder’s DN;
3) event type

5.4.2. Audit Log Analysis Rate

125.Audit logs are analyzed daily by CA employees in order to detect errors and malfunctions in the software and hardware of the Certification Authority, analyze system performance, as well as as incidents from ISusing CA are recorded.

5.4.3. Audit Log Retention Period

126.The shelf life of the audit log archive is determined in accordance with the requirements of the Cloud EDS Rules.

5.4.4. Audit Log Protection

127.The event protocols are converted to a hash daily, and the hash data is stored in the blockchain event chain. Blockchain system monitoring is available on the Internet at the link: http://91.147.113.4:4000/

5.4.5. Backup Audit Logs

128.Audit logs are backed up daily, with the ability to restore from a backup and verify integrity.

5.4.6. Data Collection Conditions for Auditing

129. Audit events are automatically logged by application and system-wide software.

5.4.7. Notification of the event subject entered in the audit log

130. If you write an event to the audit log, you do not need to notify the subject of the event.

5.4.8. Non-conformance analysis and information security incident management

131. Information security incident management process is carried out in accordance with the Bank's internal regulations on information security incident management.

Chapter 5.5. Archive maintenance

5.5.1. Types of logged events

132. The CA maintains the archive:
1) audit logs in accordance with Chapter 5.4 of the Regulations;
2) registration certificates of CA users, which have expired;
3) revoked registration certificates of CA users;
4) LRRC;
Deleted by the Minutes of the Management Board dated __.02.2025 № ____.

5.5.2. Archive Retention Period

133. The CA maintains the archive throughout its life.

5.5.3. Archive protection

134. CA ensures storage of archival documents in accordance with the legislation of the Republic of Kazakhstan.

5.5.4. Archiving Conditions

135. CA shall maintain the archive in accordance with the legislation of the Republic of Kazakhstan.

5.5.5. Requirements for setting the time for creating archive records

136. Undefined.

5.5.6. Archive Collection System

137. Archived copies of CA data are written to dedicated disk or tape storage systems managed by the responsible IT division of the Bank.

5.5.7. Procedure for obtaining and checking information stored in the archive

138. Only CA administrators have access to the CA archive.

Chapter 5.6. Certification Authority **Electronic** Digital Signature Key Change

139. In advance of the expiration of the EDS private key of the Certification Authority, the CC administrator generates a new EDS private key and the Certification Authority registration certificate and publishes registration certificate to the corresponding storage section.

140. At the end of the validity of the EDS private key of the Certification Authority, its backups are destroyed according to the certificate.

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

5.7.1. Actions to Prevent Compromise and Failures

141. To prevent loss, the Certification Authoritydata (storage, Certification Authoritykeys) are archived and placed in storage facilities specially designated for these purposes.

5.7.2. Hardware, Software and/or Hardware Failures

142. In case of damage to equipment, software and/or hardware failures, information about the incident is received by the management of the Certification Authority, which investigates the incident and takes the necessary measures to eliminate consequences and prevent the recurrence of such incidents.

143. Restoration works are carried out in accordance with the internal recovery plan of the CA.

5.7.3. Compromise of the private key of the electronic digital signature of the information system participant

144. If there is reason to believe that the password to the private EDS key has become available to third parties, it is required to immediately send a request to the CA for revocation of the registration certificate.

5.7.4. Recovery of operability after an accident

145. Cases of damage to computer, software resources and/or data of the CA IS are processed in accordance with the internal regulatory document of the Bank establishing the procedure for actions of employees of the CA abnormal and crisis situations.

6.4.3. 5.7.5. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

146. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

147. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

148. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

5.7.6. Electronic Digital Signature Verification Procedure

149. Procedure for verifying the EDS of an electronic document includes checking validity of the registration certificate at the time of signing and checking compliance with the information in the registration certificate, using the EDS Verification Rules.

Chapter 5.8. Termination of Certification Authority Work

150. If a decision is made to terminate the work of the CA notification of the registration certificates holders, transfer and archival storage of records of the CA are arranged in accordance with Art. 22 of the Law of the Republic of Kazakhstan “On Electronic Document and Electronic Digital Signature”.

Section 6. Technical Safety Control

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

6.1.1. Electronic Digital Signature Key Fabrication and Applied Algorithms

151. The Certification Authority EDS private keys are created by the Bank's CA administrator.

152. Keys of the Certification Authority's digital signature are generated on electronic KIMs in HSM, certified at least to the second security level according to the Standard, and cannot be extracted from it in an unprotected form.

153. The private EDS keys of registration certificate holders stored in the cloud EDS are created strictly inside the HSM. The private key of the EDS of the cloud EDS is not extracted from the HSM in clear text.

154. Cloud EDS HSM requirements:

1) not lower than the third safety level in accordance with the requirements of the Standard;

2) designed with physical perimeter protection (protection against opening of the housing), using sensors to determine the fact of opening of the housing and then delete the key information necessary for HSM;

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

155. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

6.1.2. Transfer of electronic digital signature private key to registration certificate holder

156. Use of private EDS keys created inside the HSM of the cloud EDS by owners of the corresponding registration certificates is carried out only within the same HSM. Physical transfer of copies of the specified private EDS keys to their owners is not provided.

157. Private EDS keys corresponding to the process registration certificates of the CA shall be issued to the CA employees who own them, as a rule, only at the KIM. In exceptional cases, when there is no technical possibility to use such a technological private key directly with the KIM, it is allowed to save it after generation on an unprotected storage medium, but with the obligatory use of activation data in the form of a password.

6.1.3. Transfer of electronic digital signature public keys to trusted parties

158. The CA shall publish registration certificates and LRRC in accordance with the procedure described in the Regulation.

159. When issuing his registration certificate, the IS participant has the opportunity to familiarize with the Registration Certificate Policy and the Regulations. Having read these documents and sending an application for issuing a registration certificate, the user confirms his full and unconditional consent to the terms of use of the CA services.

6.1.4. Delivery of CA public key to trusted parties

160. Provision of the public key of the Certification Authority is implemented by publishing its registration certificate on the Bank's official information resource on the Internet at https://www.bcc.kz/product/pki/docs/CA_GOST.cer?v=2.0.0.

6.1.5. Compromise of electronic digital signature keys

161. When using the EDS scheme according to the algorithm GOST 34.310-2004, length of the private key is 256 bits, the public key is 512 bits.

6.1.6. Generate and verify quality of the parameters of the electronic digital signature public key

162. Parameters of generation and quality check of EDS key parameters are determined automatically by CPIM certified in accordance with the Standard.

6.1.7. Compromise of electronic digital signature keys

163. Values in the Key Usage extension of registration certificates of serviced owners:
1) signature;
2) non-refractory.

6.1.8. Key Media Requirements

164. CA supports the use of electronic KIMs and has the technical capability to work with the following KIMs:
1) CERTEX HSM;
2) CERTEX HSM ES;
3) SafeNet 5100;
4) SafeNet 5110;
5) KAZTOKEN;
6) KAZTOKEN smart card.

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

165. Backup of the user's EDS private key is not provided.

166. Certification Authority EDS private key is backed up in accordance with the HSM operational documentation according to the scheme m of n. Backup copy of the Certification Authority private key is stored separately from the HSM in an encrypted archive.

167. Expired closed keys shall be destroyed in accordance with CPIM operational documentation. Archive storage of EDS private keys is not allowed.

168. After creation, the EDS private key of the cloud EDS is stored in HSM in encrypted form using the GOST 28147-89 standard. As secret values, a password is used, which is not stored in the CA.

169.The cloud EDS EDS private key is recorded in HSM by HSM standard means in accordance with HSM operational documentation.

170.The private EDS keys of the cloud EDS are stored only in encrypted form and do not leave the HSM except in an encrypted archive.

Chapter 6.3. Other features of Electronic Digital Signature Key Management

6.3.1. Archiving of Public Electronic Digital Signature Keys

171.All certificates of registration shall be archived in accordance with the backup procedure established in the CA.

6.3.2. Validity period of registration certificates and electronic digital signature keys

172.Beginning of the validity period of the Certification Authority registration certificate is calculated from the date and time of its release. The validity period of the root registration certificate of the CA is 20 years.

173.The validity period of the registration certificate of individuals served by the CA is one calendar year. Start of the validity period of the EDS private key of the registration certificate holder is calculated from the date and time of the beginning of the validity of the relevant registration certificate.

6.3.3. Restrictions on Use of Electronic Digital Signature Keys

174.The Certification Authority EDS private key is used to form the EDS in the registration certificates of the EDS public keys of their owners, as well as in the EDS.

175.Private EDS keys of individuals served by the CA are used to form the EDS and sign electronic documents in the Bank's IS.

176.If the Certification Authority EDS keys are changed and a new registration certificate of the Certification Authority is issued, it can be implemented using the cross-certification mechanism.

Chapter 6.4. Activation data

6.4.4. Generating and Setting Activation Data

177.To use the private key of the digital signature, the owner of the registration certificate must create and use activation data in the form of a password. The password must contain:

1) Latin letters, uppercase and lowercase;
2) at least one digit;
3) at least one special character;
4) at least 8 characters.

6.4.5. Activation Data Protection

178.It is forbidden to record password of access to private EDS key. The password must be known only to the holder of the relevant registration certificate. Automatic password saving is not allowed in the security features used.

Chapter 6.5. Security Control of Computing Resources

179.Requirements for PKI servers:

1) provision of fault tolerance and safety measures;

2) annual safety scan;

3) resource monitoring.

180. Computers of CA administrators shall meet the following requirements:

1) use of licensed software;

2) operating systems are supported at a high level of protection, with the regular use of all recommended and appropriate protection packages, including antiviruses and firewalls;

3) computer cannot be shared by multiple users;

4) there are no CPIMs on the computer other than those specified in the Regulations.

181. Interaction diagram of CA modules is given in Appendix 3 to the Regulations.

182. Security of Certification Authority hardware is provided by antivirus and firewalls.

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

183. Certification Authority 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".

184. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

185. EDS schemes describing the cryptographic algorithms are given in Appendix 4 to the Regulations.

186. The registration certificates of their owners from among the users of the Bank's IS include the OID of the policy:

for the user of the IS "BCC Business" - 1.2.398.3.24.3.1.2;

for the user of the IS "BCC KZ" - 1.2.398.3.24.3.2.2.

187. CA registration certificate Structure

Name	Content
Version	V3
Serial number	5cd5f1cb8b17936fbe05c2b9ab59174331c8557a
Signature algorithm	GOST 34.310
Supplier	CN=Certification Authority O = Bank CenterCredit JSC C = KZ
Subject	CN=Certification Authority O = Bank CenterCredit JSC C = KZ
Valid from	16 October 2023, 9:47:55
Valid through	16 October 2043, 9:47:55
Public Key algorithm	GOST 34.310 (512 Bits)
Public key	04 40 ec 88 2d cf d7 e1 b5 c7 70 5c 66 15 35 a7 dc 78 c7 bf dd cb 09 7c 8b 6c 95 e3 29 f9 ed b1 93 80 b1 65 9e 3d d1 0c 06 13 7c c9 0c 0c ad 9e ff 4f d3 ff 97 30 c6 1f 2a 19 01 e1 56 6c 0d e8 30 81
Key ID	5cd5f1cb8b17936fbe05c2b9ab59174331c8557a
Certificate Policy	1.2.398.3.24.1.1.1
Key usage	Signing certificates Autonomous signing a revocation list (CRL) Signing a revocation list (CRL)
Signature	EDS

188. Structure of technological registration certificates of Bank employees

Name	Content
Version	V3
Serial number	
Signature algorithm	GOST 34.310
Supplier	CN=Certification Authority O = Bank CenterCredit JSC C = KZ
Subject	[UID = IIN1111111111111] CN=BIN123456789012 or CN=*CN name* [OU=Certification Authority] O = Bank CenterCredit JSC C = KZ
Valid from	
Valid through	
Public Key algorithm	GOST 34.310 (512 Bits)
Public key	
Key ID	
CA key ID	5cd5f1cb8b17936fbe05c2b9ab59174331c8557a
Certificate Policy	1.2.398.3.24.1.1.1
Key usage	Digital signature Non-refractory
Signature	EDS

189. Structure of registration certificate of an individual served by the CA in the IS "BCC.KZ"

Name	Content
Version	V3
Serial number	
Signature algorithm	GOST 34.310
Supplier	C = KZ O = Bank CenterCredit JSC CN=Certification Authority
Subject	UID = IIN1111111111111 OU = BCC.KZ O = Bank CenterCredit JSC C = KZ
Valid from	
Valid through	
Public Key algorithm	GOST 34.310-2004 (512 Bits)
Public key	
Key ID	
CA key ID	5cd5f1cb8b17936fbe05c2b9ab59174331c8557a
Certificate Policy	1.2.398.3.24.1.1.1 1.2.398.3.24.3.2.2
Key usage	Digital signature Non-refractory
Signature	EDS

189-1. The structure of the registration certificate of an individual from among individual entrepreneurs, carrying out their activities in the form of personal entrepreneurship, serviced by the CA in the IS "BCC Business”

Name	Content
Version	V3
Serial number	
Signature algorithm	GOST 34.310
Supplier	C = KZ O = Bank CenterCredit JSC CN=Certification Authority
Subject	UID = IIN1111111111111 CN = IIN1111111111111 OU = BCC Business O = Bank CenterCredit JSC C = KZ
Valid from	
Valid through	
Public Key algorithm	GOST 34.310-2004 (512 Bits)
Public key	
Key ID	
CA key ID	5cd5f1cb8b17936fbe05c2b9ab59174331c8557a
Certificate Policy	1.2.398.3.24.1.1.1 1.2.398.3.24.3.1.2
Key usage	Digital signature Non-refractory
Signature	EDS

Chapter 7.2. Profiles of Revoked Registration Certificates List

Name	Content
Version	V2
Publisher	CN=Certification Authority O = Bank CenterCredit JSC C = KZ
Valid from	
Next update	
Signature algorithm	GOST 34.310
CA key ID	5cd5f1cb8b17936fbe05c2b9ab59174331c8557a
Revocation list	Serial number Date of revocation Revocation List Reason Code

Chapter 7.3. Online Registration Certificate Status Verification Protocol Service Profile

190.OCSP can be used by the trusting parties to determine the status of a specific registration certificate at the current time.

191.The CA generates OCSP bills in version 1 electronic form in accordance with RFC 2560 "Online Certificate Status Protocol - OCSP."

Section 8. Inspection of Activities

192.CA accreditation is carried out for three years[5] in accordance with the legislation of the Republic of Kazakhstan[6].

193.In addition, the activities of the Information Security Center, which includes the CC, are subject to an internal audit on a planned basis in accordance with the internal document of the Bank.

Section 9. Billing And Liability Issues

Chapter 9.1. Tariffs

193-1. The CA provides following services to the IS it services:

1) issuance of registration certificates upon applications from individuals;

2) revocation of registration certificates;

3) placement of registration certificates and LRRC in storage, as well as publication of the Registration Certificate Policy, these Regulations and other relevant client-oriented information on services on the Bank's information resource on the Internet;

4) provision of information on the status of registration certificates online in OCSP format;

5) linking data to real time online in TSP format;

6) creation and secure storage of private keys of the digital signature, generation of the digital signature upon request of the owners of registration certificates.

194.CC services are not charged and not paid.

Chapter 9.2. Responsibility

195.Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

196.The responsibility of the CA and RA personnel established by the legislation of the Republic of Kazakhstan is applied in accordance with employment contracts and job descriptions.

Chapter 9.3. Confidentiality

196-1. With the exception of information available in the CA storage, other information on the activities of the CA is classified as confidential in accordance with the Bank's internal document on classification of certain information as a banking/commercial secret.[7] The same document regulates the responsibility and procedure for handling this information.

Chapter 9.4. Protection of Personal Data of PKI Participants

196-2. CA shall ensure protection of personal data of PKI participants in accordance with the legislation of the Republic of Kazakhstan on personal data and their protection.

196-3. Application for a registration certificate submitted by the applicant gives the CA permission to publish the applicant's registration certificates and information about their status in the repository.

Chapter 9.5. Intellectual Property Right

196-4. In its activities, the CA uses software, copyright and exclusive property rights not belonging to the Bank. Procedure for using software is determined by the terms of the licenses acquired by the Bank.

---

[5]Law of the Republic of Kazakhstan “On electronic document and electronic digital signature”, article 20-2.

[6]On the date of approval of the Regulations, the Rules for issuing and revoking a certificate of accreditation of Certification Authorities are in force as amended by order of the Minister of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan dated September 30, 2022 No. 363/NK.

[7]As of the date of approval of the Regulation, the List of information constituting a banking/commercial secret is in effect, approved by Resolution of the Board of Directors dated August 20, 2020 No. 3-0820-01.

Chapter 9.6. Warranties and Representations

196-5. CA provides:

1) compliance of the data contained in the registration certificates issued by CA with the information provided by RA as part of the request for the issuance of the registration certificate, and the absence of accidental or intentional misrepresentations of this information in these registration certificates due to intent or as a result of erroneous actions of the Certification Authority personnel;

2) compliance of the services provided (issue, revocation of registration certificates, issue of LRRC, online services OCSP and TSP, creation and secure storage of private EDS keys, formation of EDS at the request of the registration certificates holder) with the requirements of the current legislation of the Republic of Kazakhstan on electronic document and electronic digital signature, Registration Certificates Policy and Regulations;

3) publication of the requirements of the Registration Certificates Policy and Regulations on the Bank’s official information resource on the Internet.

196-6. RA provides:

1) compliance of the data sent to the CA for issuance of the registration certificate with the information from those documents provided by the applicant during the identification and authentication procedures, and absence of intentional or accidental distortions made by intent or committed as a result of erroneous actions of the RA IS staff in these requests;

2) compliance of procedures performed by the RA personnel (procedures for identification and authentication of applicants, formation, verification and acceptance of applications for issuance and/or revocation of registration certificates, issuance of registration certificates to their owners) with the requirements of: the current legislation of the Republic of Kazakhstan on issues of electronic documents and electronic digital signatures, the Registration Certificate Policy and the Regulations.

196-7. The CA and RA in their activities comply with the terms of guarantees and assurances of the owner of registration certificates and the trusting party, set out in Chapter 9.6 of the Registration Certificate Policy.

Chapter 9.7. Disclaimer of Warranties

196-8. More information is set out in the Registration Certificate Application Policy.

Chapter 9.8. Limitations of Liability.

196-9. Participants in the public key infrastructure are not responsible for indirect, special, or consequential damage and lost profits.

Chapter 9.9. Compensation

196-10. Expenses related to compensation for:

1) confirmation of erroneous, misleading or knowingly false information in applications for release or revocation of the registration certificate;

2) inadvertent or intentional concealment of material facts to be reflected in the Application for release or withdrawal of the registration certificate, –

in the part that does not contradict the current legislation of the Republic of Kazakhstan, refer to the account of the RA.

Chapter 9.10. Entering Into Force and Termination

196-11. Regulation and all amendments and additions thereto shall enter into force no earlier than the day of publication on the Bank's official Internet resource.

196-12. Regulation , 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.

196-13. In the event of cancellation of the Regulations, IS participants that use registration certificates issued by the CA remain bound by the requirements of the Registration Certificates Policy until the expiration of the registration certificate period.

Chapter 9.11. Notifications and communication with participants

196-14. More information is set out in the Registration Certificate Application Policy.

Chapter 9.12. Amendments

196-15. Minor changes to the Regulation (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.

196-16. The CA preliminarily publishes significant changes and additions to the Regulation, 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

196-17. Disputes on the merits of the Regulation 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.

196-18. If the dispute is not resolved out of court, it shall be resolved in court.

Chapter 9.14. Jurisdiction.

196-19. 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 Regulation.

Section 10. Other Issues

Chapter 10.1. Terms of application

197. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

198. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

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

200. In case of force majeur the PKI participants: CA, RA and holders of registration certificates and trusting parties are guided by the relevant provisions of the agreements in force between them (if any).

Chapter 10.2. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

201. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

202. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

Chapter 10.3. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

203. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

204. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

Chapter 10.4. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

205. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.
206. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.
207. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

Chapter 10.5. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

208. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.
209. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

Chapter 10.6. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

210. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.
211. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.
212. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.
213. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

Chapter 10.7. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

214. Deleted by the Minutes of the Management Board dated 17.02.2025 № 0217/3.

Chapter 10.8. Final Provisions

215. Requirements of Regulations are mandatory for all employees of the Bank units involved in the processes described in the Regulations.

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

1) compliance with the requirements described in the Regulations;

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

217. All issues not regulated by the Regulations 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.

218. The Regulations shall be revised as necessary. The Bank's Coordination and Methodology Directorate shall be responsible for revising and updating the Policy..

Cryptographic Information Protection Directorate

Annex 1

to Regulations for Activities of the Certification Authority of Bank CenterCredit JSC

Form

Annex 1
Rules for issuing, storing, revoking
registration certificates[8]

APPLICATION
for Registration Certificate from Individual

Individual Identification Number*: _____

Surname*: _____
First name*:
_____
Patronymic _____
Area Name: _____
City _____
Email: _____
Phone: _____

Validity periods in registration certificates: _1 year_____
Information on the scope and limitations of the electronic digital signature
_____
Data on the electronic digital signature means used to create the corresponding private key of the electronic digital signature, designation of the standard of the electronic digital signature algorithm and the length of the public key: CERTEX HSM ES III, GOST 34.310-2004, 512 binary digits
_____

I hereby certify that:

1. I have familiarized myself with the Application Policy for Registration Certificates and the Regulations for the Activities of the Certification Authority (https://www.bcc.kz/product/pki/?tab=DPP). I undertake to comply with the requirements of these documents, including guarantees and assurances of the owner of registration certificates and trusting party.
2. I agree to collection, storage and processing of my personal data. I have signed a consent document.
3. I agree fpr storage of my EDS private key in the cloud EDS of the Certification Authority.
4. I agree to sign the application for issuance of a registration certificate by entering a one-time OTP code/password.

[8]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.

* Required fields.

Date "___" _____ 20____
Applicant's certification mark _____

Annex 2

to Regulations for Activities of the Certification Authority of Bank CenterCredit JSC

Form

Annex 8
Rules for issuing, storing, revoking
registration certificates[9]

APPLICATION
for Withdrawal of Registration Certificate from Individual

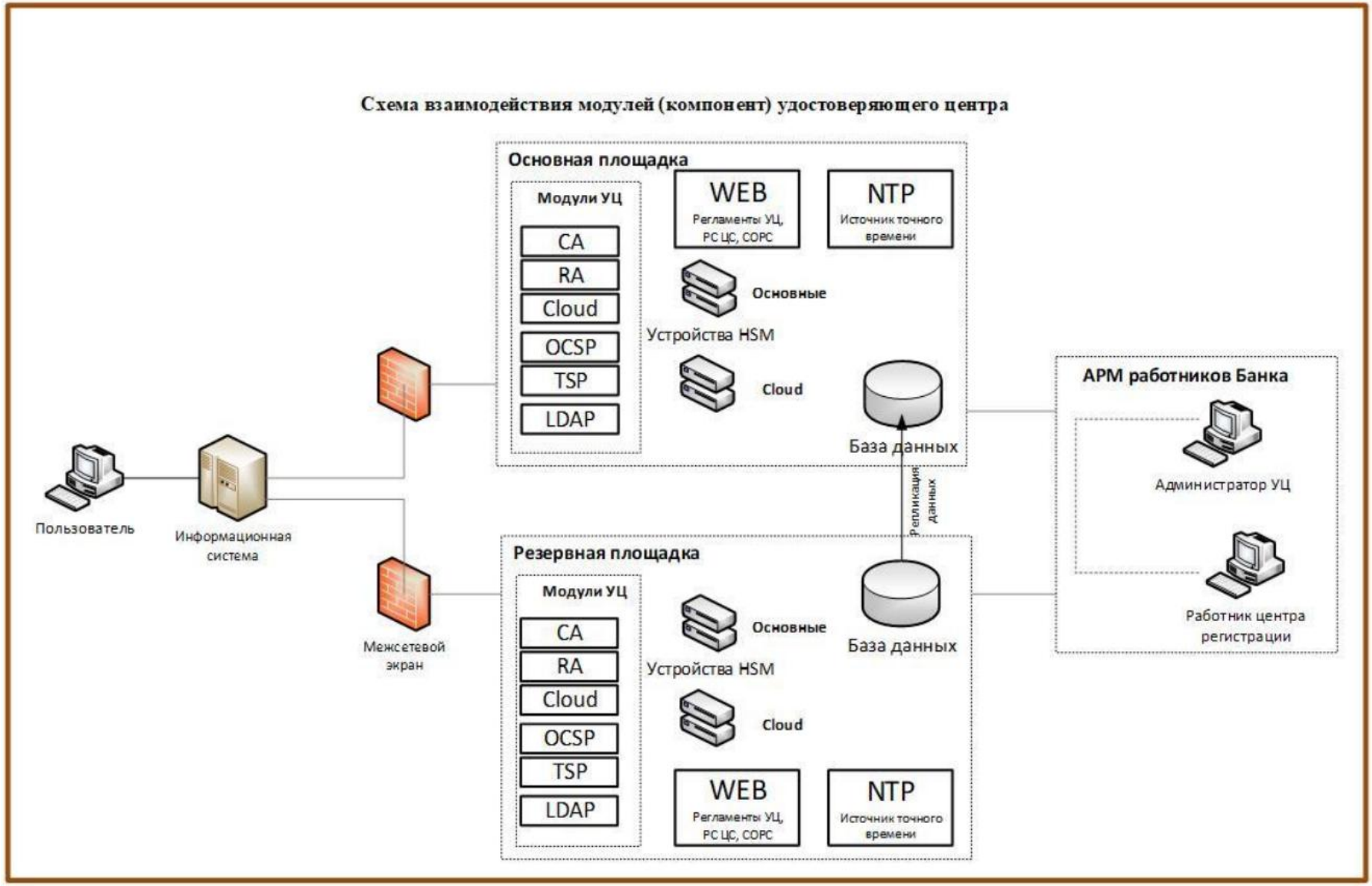
Individual Identification Number*: _____
Surname*: _____
First name*: _____
Patronymic _____
Area Name: _____
City _____
Email: _____
Phone: _____

Identification data on registration certificates:
Serial Number:
_____
_____
_____
_____
_____
_____

Date "___" _____ 20____
Applicant's certification mark _____

[9]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.
* Required fields.

Annex 3
to Regulations for Activities of the Certification Authority of Bank CenterCredit JSC



EXPLANATORY NOTE
to Interaction Diagram of Modules (Components) of the Certification Authority

Interaction of components (primary and backup authority)

Interaction of the modules of the information system of the Certification Authority (hereinafter – CA) with the CA repository for publication and search of registration certificates, lists of revoked registration certificates is carried out using the LDAP protocol.

All CA modules use a single time received from the source of exact time via the NTP protocol.

Security of interaction of CA modules is ensured by the use of the certified cryptographic information protection tool "TUMAR-CSP", corresponding to the second level of security according to ST RK 1073-2007.

HSM secure hardware cryptographic modules corresponding to security level 2 according to ST RK 1073-2007 are used for storage and security of CA private keys.

HSM secure hardware cryptographic modules corresponding to security level 3 according to ST RK 1073-2007 are used to create, store and secure private keys of registration certificate holders.

The system uses firewalls that monitor and filter all incoming network traffic.

Interaction between the working and backup servers of the data processing centers

Data storage and management is provided by the MySQL and/or PostgreSQL DBMS. Data is replicated in real time between the primary and backup data centers by DBMS to improve system resiliency. Protection of replicated data is provided by encryption using the TLS protocol.

Interaction of users with the CA

CA users do not interact directly with the CA services.

Interaction is carried out through targeted (serviced) information systems of the Bank, which have the ability to interact with cloud CA EDS using HTTP(S) protocols.

Interaction of CA employees with CA modules

Interaction of CA employees with CA modules is carried out by means of specialized software using the LDAP and HTTP(S) protocols.

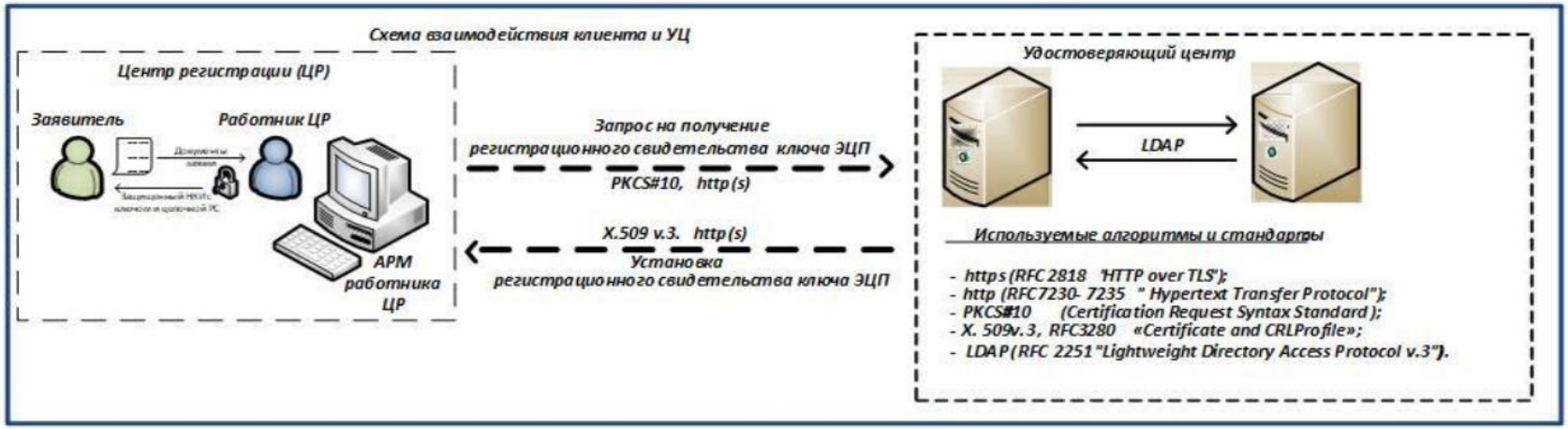
Access from the employee’s workplace to CA modules is possible only if there is a valid registration certificate with certain properties.

In addition, security is ensured by limiting network access to only a certain set of IP addresses.

Annex 4

to Regulations for Activities of the Certification Authority of Bank CenterCredit JSC

Схемы электронной цифровой подписи
с данными о применяемых алгоритмах криптографических преобразований
и другими исходными данными (основными требованиями)
по реализации процесса формирования электронной цифровой подписи
и требованиями к отдельным паратметрам и удостоверяющему центру



Схемы электронной цифровой подписи ... (продолжение)

Особенности процессов при хранении и использовании закрытых ключей владельцев регистрационных свидетельств на стороне Удостоверяющего центра