REPUBLICAN STATE ENTERPRISE ON THE RIGHT OF ECONOMIC USE «STATE TECHNICAL SERVICE» MINISTRY OF INFORMATION AND COMMUNICATION OF THE REPUBLIC OF KAZAKHSTAN

«APPROVED»
by Director
of RSE «State Technical service»
Ministry of information and communication
of the Republic of Kazakhstan

Mr. E.K. Esmambetov _____
2016. «_9_» _September_

REGULATIONS ON USE OF REGISTRATION CERTIFICATES ISSUED BY THE ROOT CERTIFICATION AUTHORITY OF THE REPUBLIC OF KAZAKHSTAN (CERTIFICATE PRACTICE STATEMENT)

Version 2.0

Astana, 2016

VERSION CONTROLS

NO.	Status	Date	Author	Revision description
2.0				
1.0				

Table of Contents

1. INTRODUCTION

The Root Certification Authority of the Republic of Kazakhstan (hereinafter referred to as the "RCA RK") was created in order to confirm the compliance and validity of electronic digital signature public keys (hereinafter referred to as the "EDS") of certification authorities (hereinafter referred to as the "CA"). For this purposes the RCA RK provides issuance (resubordination) of registration certificates provided by accredited CA in accordance with the Decree issued by Government of the Republic of Kazakhstan dated November 19, 2010 No. 1222 concerning approval of the Regulations for certification authority accreditation".

The RCA RK operates in accordance with the following regulatory legal acts of the Republic of Kazakhstan, internal and public documents:

1) Law of the Republic of Kazakhstan dated January 7, 2003 No. 370-II concerning e-document and electronic digital signature;

2) Law of the Republic of Kazakhstan dated November 24, 2015 concerning informatization;

3) Order issued by Minister of Investments and Development of the Republic of Kazakhstan dated December 9, 2015 No. 1184 concerning approval of the Standard provisions for certification authorities;

4) Order issued by Acting Minister of Investments and Development of the Republic of Kazakhstan dated June 26, 2015 No. 727 concerning approval of the Regulations of issuance, storage, revocation of registration certificates and confirmation of the compliance and validity of electronic digital signature public key by Root Certification Authority of the Republic of Kazakhstan, Certification Authority of State Bodies and National Certification Authority of the Republic of Kazakhstan;

5) Decree issued by Government of the Republic of Kazakhstan dated November 19, 2010 No. 1222 concerning approval of the Regulations for certification authority accreditation;

6) ST RK 1073-2007. Cryptographic information protection facilities. General requirements;

7) Policy of use of registration certificates issued by the RCA RK.

The RCA RK issues registration certificates only for subordinated CA of the RCA RK provided that they have been accredited by the competent authority. The RCA RK does not issue registration certificates to ultimate users, but only certifies subordinated CA.

1.1. DEFINITIONS AND ABBREVIATIONS

The following definitions are used herein:

No.	Term	Definition
1.	Assets	The RSE STS resources aimed at ensuring the continuity of the RCA RK work
2.	Inner control environment	Accumulation of process controls of the RCA RK
3.	The RCA RK records of services	The RCA RK IS record file containing events in chronological order
4.	EDS private key	Sequence of electronic digital symbols known to a registration certificate holder and intended to create an electronic digital signature with the use of EDS facilities
5.	Applicant	An individual or legal entity (branch/representative office) submitting documents for issuance or revocation (annulment) of a registration certificate before the registration certificate has been registered or declared invalid (annulled)
6.	Internet resource of the RCA RK	The Internet resource of the RCA RK www.root.gov.kz
7.	Key pair	A set, which consists of two keys: private (secret) key and public key
8.	EDS public key	Sequence of electronic digital symbols, which is available to anyone and designed for confirmation of compliance to EDS in e-document
9.	Registration certificate	Document on paper or an e-document, issued by certification authority for confirmation of compliance to EDS requirements, specified by regulatory legal acts of the Republic of Kazakhstan

The following abbreviations are used herein:

No.	Abbreviation	Definition
1.	TSP	(Time Stamp Protocol) Cryptographic protocol, which allows to create evidence of fact of e-document existence for the time being
2.	WebTrust	International standard "Trust Service Principles and Criteria for Certification Authorities Version 2.0"
3.	PKI	(Public Key Infrastructure)

		Complex of informational systems, organizational and technical arrangements, aimed to control of registration certificates in accordance with the legislation of the Republic of Kazakhstan concerning e-document and electronic digital signature
4.	RCA RK	(Root Certification Authority of the Republic of Kazakhstan) Certification Authority confirming the compliance and validity of electronic digital signature public keys of certification authorities
5.	MIC RK	(Ministry of Information and Communication of the Republic of Kazakhstan)
6.	NCA RK	(National Certification Authority of the Republic of Kazakhstan) A Certification authority, which services subscribers of "electronic government", state and non-state informational systems
7.	RSE STS	(Republican State Enterprise on the Right of Economic Use "State Engineering Service" of the Ministry of Information and Communication Lines of the Republic of Kazakhstan)
8.	RCRL	(Registration Certificate Revocation List) A list of all the RCA RK subscriber's registration certificates, revoked by the time the RCRL has been issued
9.	CASB	(A Certification Authority of State Bodies of the Republic of Kazakhstan) A certification authority, which services state bodies, state body officers in informational systems of the state bodies of the Republic of Kazakhstan
10.	EDS	(Electronic digital signature) A set of electronic digital symbols, produced by means of electronic digital signature and confirming authenticity of e-document, its accessory and invariability of content

1.2. OVERVIEW

These Regulations on use of registration certificates issued by the RCA RK (hereinafter referred to as the "Regulations") regulate the RCA RK activity and specify the Policy of use of registration certificates issued by the RCA RK (hereinafter referred to as the "Policy") for subordinated CA. These Regulations establish the norms implemented by the RCA RK in providing services, defined in the Policy.

These Regulations have been drafted in accordance with the following international standards:

- principles and criteria of the WebTrust international standard for certification authorities, version 2.0 (Trust Services Principle and Criteria for Certification Authorities, version 2.0);
- recommendations to the guidance for development of policies of use of registration certificates and instructions for use of the public key infrastructure registration certificates in accordance with the standard X.509 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" (hereinafter referred to as the "RFC 3647").

In accordance with the above mentioned standards, these Regulations consist of 9 sections, which describe the service provision practice in relation to issuance (resubordination) and revocation of registration certificates issued by subordinated CA, as well as safety controls used to protect the RCA RK PKI. In order to maintain compliance of the Regulations structure with the principles and criteria of the WebTrust international standard and the RFC 3647 section recommendations, the RCA RK PKI not applicable to the practices contain a "not applicable" or "not specified" mark.

These Regulations describe the RCA RK activities, applicable to the RCA RK registration certificates and the subordinated CA registration certificates in accordance with the requirements set out in the Policy of use of the RCA RK registration certificates. The RCA RK practices comply with the requirements contained in the following standards, which are relevant at the time of publication of the Regulations:

- principles and criteria of the WebTrust international standard for certification authorities, version 2.0 (Trust Services Principle and Criteria for Certification Authorities, version 2.0);
- baseline requirements for the issuance and management of public registration certificates, version 1.1.9 (Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 1.1.9).

1.3. NAME AND IDENTIFICATION OF THE DOCUMENT

Name of the document: Regulations on the Use of Registration Certificates Issued by Root Certification Authority of the Republic of Kazakhstan.

Document version: 3.0

Put into effect by RSE STS Director's Order No.___ as of _____ 2016.

Current version of these Regulations has been published on the RCA RK Internet resource.

1.4. THE RCA RK PKI MEMBERS

1.4.1. RCA RK

RCA RK is a certification authority, that issues (resubordinates) registration certificates to accredited CA for the use in accordance with the provisions of Clause 1.5 hereof.

The RCA RK carries out activities, which are directly related to a CA RK, namely:

- receiving and processing of queries for the issuance (resubordination) and revocation of registration certificates issued by accredited CA;
- issuance (resubordination) and revocation of registration certificates issued by accredited and subordinated CA;
- publication and support for the subordinate registration certificate revocation lists issued by subordinated CA (hereinafter referred to as the "RCRL");
- support for the registration certificate register;
- storage of registration certificates.

1.4.2. Accredited CA

CA, officially recognized by competent authority in the field of informatization as a CA competent to provide services in accordance with the legislation of the Republic of Kazakhstan.

1.4.3. Subordinated CA

Accredited CA are considered subordinated CA.

1.4.4. Subordinated CA subscribers

A subordinated CA subscriber means a registration certificate holder, individual or legal entity, in whose name a subordinated CA issued a registration certificate of subscriber, lawfully in possession of a privacy key, corresponding to the public key, indicated in the subscriber's registration certificate.

1.4.5. Relying parties

A relying party is an entity acting based on the subscriber's registration certificate issued by subordinated CA. A relying party may be a subordinated CA subscriber or a subordinated CA.

1.4.6. CA RK

For the purposes of creation of an integrated area of trust framework between members of information exchange in the Republic of Kazakhstan the CA PK system infrastructure has been triggered. Among the CA RK members are as follows:

RCA RK;

subordinated CA, including:

- NCA RK;
- SB CA RK;

holders of registration certificates isued by subordinated CA.

A CA RK supports hierarchical architecture of trust, the main provisions of which are as follows:

- at the top of the hierarchy of CA RK there is RCA RK, which produces the RCA RK self-signed root registration certificates;
- the RCA RK registers (resubordinates) root registration certificates for accredited CA;
- subordinated CA issue registration certificates for their subscribers;
- CA RK members have an EDS public key of the RCA RK and corresponding registration certificates.

When receiving an e-document, containing a registration certificate of a signatory, CA RK members confirm the compliance and validity of an EDS public key via verification:

- of an EDS in the e-document — the verification is performed using the CA CIPF via the use of a public key, which is contained in a registration certificate of a signatory;
- of registration certificate authenticity — the registration certificate authenticity shall be confirmed by EDS private key of the next registration certificate in a set chain of registration certificates;
- of setting of a correct chain from a registration certificate under verification to the RCA RK registration certificate, including intermediate registration certificates issued by subordinated CA;
- of a registration certificate prepared for a revocation (annulment) procedure (RCRL);
- of a registration certificate prepared for a revocation (annulment) procedure online;
- of a number of registration certificate policy and methods of its use permitted;
- of a time stamp;
- of a field of key use.

1.4.7. Other members

Not applicable.

1.5. USE OF A REGISTRATION CERTIFICATE ISSUED BY SUBORDINATED CA

1.5.1. Use of registration certificates issued by subordinated CA

Registration certificates issued by subordinated CA shall be applicable for the following purposes:
issuance and revocation of registration certificates for subordinated CA applicants;
confirmation of the compliance and validity of an EDS public key via verification.

1.5.2. Requirements for use of registration certificates issued by subordinated CA

The use of registration certificates issued by subordinated CA shall not contradict with the current legislation of the Republic of Kazakhstan, as well as with the requirements hereof.

Registration certificates issued by subordinated CA can not be used:

- upon expiry of a validity period of a registration certificate issued by the RCA RK and subordinated CA;
- in the event of revocation of a registration certificate issued by the RCA RK and subordinated CA;
- in the event of compromise suspicion referred to a privacy key, authenticated by subordinated CA registration certificate;
- in the event of discovered compromise referred to a privacy key, authenticated by subordinated CA registration certificate;
- in the events contradicting with Clause 1.5.1 hereof.

1.6. REGULATION MANAGEMENT

1.6.1. Organization, managing the document

RSE STS

1.6.2. Contact person

Senior Specialist of the cross-border cooperation and interdepartmental interaction division of the Public key infrastructure service, Infrastructure solution department, RSE STS - Kenzhebulatov Baurzhan Sairanbekovich, tel. 55-99-99 (Ext. 398), mobile 8(707)-722-11-33, email – b_kenzhebulatov@sts.kz

1.6.3. Person assessing the CA compliance with the Regulations

The RSE STS Director is Yesmambetov Yerlan Kozhabergenovich, tel. 55-99-22, email – info@sts.kz

The RSE STS Director is responsible for the confirmation of compliance of this Regulations with Policy of use of the RCA RK registration certificates (certificate policy).

The RSE STS Director is responsible for defining the general requirements for the public key infrastructure, to these Regulations.

1.6.4. Qualification procedure for rules and regulations

Development, support and updating hereof shall be carried out by RSE STS. Reference details:

- registered office: 1/1, Zhirentaeva str., Astana, Republic of Kazakhstan, 010000;
- physical address: 16, Kuishi Dina str., Astana, Republic of Kazakhstan, 010000;
- Director of the Infrastructure solution department, RSE STS, info@pki.gov.kz, tel. 55 99 99 (399)

Alterations and amendments to these Regulations shall be made after verification of their compliance with the Policy of use of the RCA RK registration certificates. Proposals for alterations and amendments to Regulations shall be made by the RCA RK executive officers and approved through the order issued by the RSE STS Director.

The approved altered or amended Regulations shall be published on the RCA RK Internet resource in a separate document, containing the full text hereof, or notice of the alterations made and the alterations themselves indicating the successive rising version number hereof. All the versions of the Regulations which have become ineffective shall also be published on the RCA RK Internet resource. All the versions of the Regulations which have become ineffective shall contain a mark indicating the date of the Regulations approval and a link to the current version hereof.

2. RESPONSIBILITY IN RESPECT OF THE PUBLICATION AND STORAGE

2.1. STORAGE AND AVAILABILITY OF PUBLIC INFORMATION

The RCA RK provides public availability 24 hours a day, 7 days a week of the following materials on the official RCA RK Internet resource:

- the RCA RK root registration certificate according to the RSA procedure available at http://root.gov.kz/cert/root_rsa.cer;
- the RCA RK root registration certificate according to the State Standard procedure available at http://root.gov.kz/cert/root_gost.cer;
- object identifiers of the Republic of Kazakhstan;
- RCRL (see Clause 2.2.1. ниже);
- Policy of use of the RCA RK registration certificates;
- these Regulations.

The RCRL shelf life in the register of registration certificates shall be not less than five years, with revoked registration certificates included in the RCRL until the expiry of a validity period of a registration certificate.

Upon the expiry of the RCRL shelf life in the register of registration certificates, old RCRL are directed for archival storage in accordance with the current legislation of the Republic of Kazakhstan.

2.2. PUBLICATION OF THE REGISTRATION CERTIFICATE INFORMATION

2.2.1. RCRL issued by subordinated CA

The RCA RK RCRL is available in electronic form and format, defined in the RFC 5280 recommendations (Certificate and Certificate Revocation List (CRL) Profile) and these Regulations. The RCA RK publishes the following types of RCRL:

- RCRL for registration certificates according to the RSA procedure, available at: http://crl.root.gov.kz/rsa.crl;
- RCRL for registration certificates according to the State Standard procedure, available at: http://crl.root.gov.kz/gost.crl.

2.3. PERIOD FOR THE INFORMATION PUBLICATION

A RCRL is issued and published not less than once in 35 days. The RCRL validity period is not more than 35 days.

2.4. ACCESS CONTROL TO THE PUBLIC INFORMATION

The RCA RK has implemented information and physical security measures in order to prevent unauthorized introduction, alteration or deletion of the information contained in the RCA RK RCRL and informational systems.

The RCA RK publishes registration certificates issued by it. In the event of revocation of a registration certificate issued by subordinated CA, the RCA RK deletes this registration certificate from the current storage.

At any time, current versions of the following documents are available on the official RCA RK Internet resource:

- Policy;
- Regulations;
- RCRL;
- Regulatory legal acts in the sphere of an e-document and electronic digital signature.

3. IDENTIFICATION AND AUTHENTICATION

3.1. NAMING

3.1.1. Types of names assigned to subordinated CA

A registration certificate issued by subordinated CA contains distinctive names in the DN-name in the format recommended by X.501 "Information technology - Open Systems Interconnection - The Directory: Models" standard of the ITU-T X.500 series of recommended standards in the "Subject" field, consisting of the following components:

Component	Meaning	Length	Obligation
Country name "countryName"	KZ	2 symbols	Obligatory
Administrative-territorial unit "State"	Region, city of republican status, where a subordinated CA is situated	Not more than 32 symbols	Obligatory
Location area "Locality"	City, where a subordinated CA is situated	Not more than 16 symbols	Obligatory
e-mail address (E)	e-mail address of a subordinated CA	Not more than 32 symbols	Obligatory
Personal name "commonName"	Name of a subordinated CA	Not more than 64 symbols	Obligatory

3.1.2. Necessity for use of personal data in the DN-name

The RCA RK issues (resubordinates) registration certificates issued by subordinated CA, which contain personal data in the DN-name, enabling the identification of a subordinated CA and a field of use of registration certificate issued by subordinated CA.

3.1.3. Anonymity or use of pseudonyms of subordinated CA

Anonymity of subordinated CA and use of pseudonyms of subordinated CA is not allowed.

3.1.4. Interpretive rules for DN-names

Distinctive DN-names shall include all the elements specified in the corresponding NCA RK subscriber's registration certificate profile according to the specification of the X.509 standard of the ITU-T X.500 series of recommended standards and RFC-5280.

3.1.5. Necessity for use of unique DN-names

Each unique subordinated CA shall have a unique name in the field "Subject" of the registration certificate.

3.1.6. Recognition, authentication and role of trademarks

The distinctive fields "Subject" and "Issuer" of the registration certificates issued by subordinated CA shall include only officially registered names of legal entities. The RCA RK does not allow the use of trademarks in the distinctive fields for the registration certificate entities.

The use of trademarks in legal entity names in the distinctive field "Subject" by subordinated CA shall be carried out in accordance with the legislation of the Republic of Kazakhstan.

3.2. VERIFICATION (IDENTIFICATION) OF APPLICANTS AT THE TIME OF ISSUANCE (RESUBORDINATION) OF REGISTRATION CERTIFICATES ISSUED BY ACCREDITED CA

The identification of accredited CA shall be carried out on the basis of an application for registration (resubordination) of a registration certificate issued by accredited CA.

Subordinated CA that have a valid registration certificate, registered (resubordinated) by the RCA RK, may request registration (resubordination) of a new registration certificate, upon thier arrival to the RCA RK and providing:

- an application for registration (resubordination) of a registration certificate, accredited by CA;
- a copy of the CA accreditation certificate;
- a registration certificate accredited by CA in a form of an e-document.

The RCA RK registers (resubordinates) registration certificates issued by subordinated CA within 15 working days upon the submission of the above-mentioned documents by accredited CA.

3.2.1. Method of proof of owning the private key

Upon receiving a query for the registration certificate issuance, the NCA RK verifies the fact of ownership referred to the privacy key, corresponding to the public key, which the registration certificate is applied for: when carrying out the identification procedure the NCA RK verifies the application accuracy and availability of the necessary documents, including the certification authority accreditation certificate.

3.2.2. Representation of the applicant's interests by third party

The documents shall be submitted by individuals representing the applicant's interests on the basis of a power of attorney prepared pursuant to a specific form in accordance with the current legislation of the Republic of Kazakhstan. The power of attorney shall be notarized.

3.2.3. Verification (identification) of an applicant

The information referred to in the application submitted by accredited CA for registration (resubordination) of a registration certificate, shall be confirmed by personal arrival of an applicant's representative to the RCA RK upon presentation of the following documents:

- an application for registration (resubordination) of a registration certificate, accredited by CA;
- a copy of the CA accreditation certificate;
- a registration certificate accredited by CA in a form of an e-document.

3.2.4. Unverified subscriber's information

Not applicable.

3.2.5. Verification of authority

While considering an application for resubordination of a registration certificate issued by accredited CA, the RCA RK acts in accordance with Clause 3.2.3. Additional verifications of such authority are not necessary, as it is confirmed by corresponding application and CA accreditation certificate.

At the same time, in the event of doubt concerning such a verification, the RCA RK reserves the right to require the applicant to submit additional documents confirming the information stated in the application, as well as officially request MIC to confirm an applicant's undergoing the CA accreditation procedure.

3.2.6. Cooperation criteria

The RCA RK and applicant may enter into a registration certificate issuance and revocation agreement if the same is necessary for the accelerated registration certificate issuance and revocation.

3.3. VERIFICATION (IDENTIFICATION) OF AN APPLICANT WHEN UNDERGOING THE PROCEDURE OF REISSUANCE OF A REGISTRATION CERTIFICATE ISSUED BY SUBORDINATED CA

The RCA RK does not allow key pair updating in the current subordinate registration certificates issued by subordinated CA. In order to use new key pairs, a subordinated CA shall issue the corresponding registration certificate and complete the registration (resubordination) procedure of the new registration certificate.

In the event of the need to register (resubordinate) the new registration certificate issued by subordinated CA before the expiry of the current registration certificate.

In the event of registration (resubordination) of the new registration certificate upon revocation of existing subordinate registration certificates, a subordinated CA undergoes the identification referred to the applications in accordance with the procedure, described in Clause 3.2 выше.

3.3.1. Identification and authentication of the queries during the scheduled key updating

In this case, the RCA RK verifies the fact of privacy key holding by subscriber according to the same procedure as described in Clause 3.2.1.

3.3.2. Identification and authentication of the queries for the key updating in the certificate upon revocation

In this case, the RCA RK verifies the fact of privacy key holding by subscriber according to the same procedure as described in Clause 3.2.1.

3.4. VERIFICATION (IDENTIFICATION) OF THE RCA RK SUBSCRIBER DURING THE PROCEDURE OF REVOCATION OF A SUBORDINATE REGISTRATION CERTIFICATE ISSUED BY SUBORDINATED CA

An application for revocation of a subordinate registration certificate issued by subordinated CA shall be submitted on paper upon personal arrival of an applicant's representative. The application shall comply with the requirements of the legislation of the Republic of Kazakhstan. The RCA RK verifies (identifies) the identity of an applicant in accordance with the lists of documents given in Clause 3.4.2.

In the event of successful verification (identification) of an applicant's identity and compliance of the documents submitted, the RCA revokes the registration certificate issued by subordinated CA.

3.4.1. Representation of the applicant's interests by third party

The documents shall be submitted by individuals representing the applicant's (legal entity's) interests on the basis of a power of attorney prepared pursuant to a specific form in accordance with the current legislation of the Republic of Kazakhstan. The power of attorney shall be notarized.

3.4.2. Verification (identification) of an applicant

The information referred to in the application submitted by subordinated CA for revocation of a registration certificate, shall be confirmed by personal arrival of an applicant's representative to the RCA RK upon presentation of the following documents:

- an application for revocation of a subordinate registration certificate, authenticated with the seal of a subordinated CA legal entity;
- 3) a power of attorney for the applicant's representative (subordinated CA legal entity) in accordance with Clause 3.4.1. выше; the legal entity's chief executive officer or a person performing the same duties, submits a letter of employment confirmation or a copy of the appointment order (decision, protocol) referred to chief executive officer or a person performing the same duties, authenticated with the subordinated CA legal entity's seal, instead of a power of attorney.
- Hard copies of documents, which verify the applicant's representative's identity (legal entity subordinated CA) in accordance with Clause 3.4.1. выше.

4. OPERATIONAL REQUIREMENTS FOR THE LIFE CYCLE OF A REGISTRATION CERTIFICATE ISSUED BY SUBORDINATED CA

4.1. AN APPLICATION FOR REGISTRATION (RESUBORDINATION) OF A REGISTRATION CERTIFICATE ISSUED BY SUBORDINATED CA

4.1.1. Persons entitled to apply for registration (resubordination) of a registration certificate issued by accredited CA

CA may apply for registration (resubordination) of a registration certificate issued by subordinated CA or for resubordination of an existing registration certificate issued by CA only under the condition that the CA is a CA accredited in the RCA RK PKI.

4.1.2. Procedure for the registration and issuance of the RCA RK registration certificates

All the applicants shall complete the registration process in the RCA RK, consisting of the following steps:

- submission of an application for registration (resubordination) of a registration certificate issued by accredited CA;
- identification and authentication for application in accordance with Clause 3.2 выше;
- submission of the registration certificate issued by subordinated CA, which is a subject of the application for registration (resubordination).

Upon consideration of the documents the RCA RK registers (resubordinates) the registration certificate issued by subordinated CA as an e-document, as well as its copy on paper and adds it to the register of registration certificates.

4.1.3. Procedure for generation of a key pair issuesd by subordinated CA

Applicants (accredited CA) generate their key pairs under their own power in compliance with the requirements of the RCA RK:

- For the key pairs issued in accordance with the RSA procedure:
  - the private key length – 4096 bit;
  - the public key length – 4096 bit.
- For the key pairs issued in accordance with the State Standard 34.310-2004 procedure:
  - the private key length – 256 bit;
  - the public key length – 512 bit.

4.2. PROCESSING OF AN APPLICATION FOR REGISTRATION (RESUBORDINATION) OF A REGISTRATION CERTIFICATE ISSUED BY SUBORDINATED CA

4.2.1. Authentication and identification of an application

Any procedure of identification and authentication during the issuance of a registration certificate shall be performed in the same manner as the original identity verification set out in Section 3.2.

4.2.2. Confirmation of the compliance and validity of an EDS public key

Confirmation of the compliance and validity of an EDS public key shall comply with the provisions of Clause 3.2 выше.

4.2.3. A refusal to accept an application for registration (resubordination) of registration certificates issued by accredited CA

The RCA RK rejects an application for registration (resubordination) of a registration certificate issued by accredited CA, if at least one of the following conditions:

- an accredited CA has not submitted the required documents;
- accredited CA has submitted unreliable information.

4.2.4. Period for consideration of applications for registration (resubordination) of registration certificates

The RCA RK considers applications for the issuance (resubordination) of registration certificates issued by subordinated CA in a period not exceeding 15 calendar days of submission of all the required data.

A motivated answer referred to the refusal of registration (resubordination) of a registration certificate issued by accredited CA shall be provided within 15 working days from the date of submitting the required documents.

4.3. ISSUANCE (RESUBORDINATION) OF SUBORDINATED CA REGISTRATION CERTIFICATES

4.3.1. RCA RK actions during registration (resubordination) of registration certificates

A registration certificate issued by subordinated CA shall be registered (resubordinated) by the RCA RK based on an application. The procedure for registration (resubordination) of a registration certificate requires identification of a subordinated CA upon personal arrival of a subordinated CA representative to the RCA RK.

The RCA RK registers (resubordinates) a registration certificate issued by subordinated CA on the basis of information, included in the application.

4.3.2. Notification for subordinated CA on registration (resubordination) of a registration certificate issued by subordinated CA

An official notice of the fact of registration (resubordination) of a registration certificate means publication of this certificate in the register of registration certificates on the RCA RK Internet resource. In the event of a positive result of processing the application for registration (resubordination) of a registration certificate, an applicant receives the registration certificate issued by subordinated CA signed by the RCA RK registration certificate as a reply.

The RCA RK sends a notice of registration (resubordination) of a registration certificate issued by subordinated CA to the applicant via e-mail. The RCA RK shall not be liable in the event a subordinated CA does not receive such a notice.

4.4. ACCEPTANCE OF A REGISTRATION CERTIFICATE ISSUED BY SUBORDINATED CA

4.4.1. Acceptance of a registration certificate issued by subordinated CA by the RCA RK

The following reaction of a subordinated CA means acceptance of a registration certificate:

- the absence of objections from a subordinated CA to the acceptance of a registration certificate issued by subordinated CA or its contents;
- the of a subordinate registration certificate.

4.4.2. Notification for other parties of registration (resubordination) of registration certificates issued by subordinated CA by the RCA RK

The RCA RK sends a notice to a subordinated CA via e-mail to the address indicated during submission the application.

The RCA RK publishes information on the issuance of a new subordinate registration certificate or resubordination of an existing registration certificate on the RCA RK Internet resource in Section "News", available at http://root.gov.kz/novosti.html.

4.4.3. Publication of a registration certificate by certification authority

The RCA RK places the issued (resubordinated) registration certificates on the RCA RK Internet resource in Section "Register of registration certificates", available at http://root.gov.kz/certificates.html.

4.5. USE OF A KEY PAIR AND REGISTRATION CERTIFICATE ISSUED BY SUBORDINATED CA

4.5.1. Use of private keys and registration certificates issued by subordinated CA

The use of a private key is permitted only upon performance of the following steps:

- a subordinated CA has accepted the requirements hereof;
- The RCA RK has registered (resubordinated) a registration certificate issued by subordinated CA for the corresponding public key in accordance with the current legislation of the Republic of Kazakhstan.

The use of a private key means acceptance by subordinated CA of the Policy of use of the RCA RK registration certificates and these Regulations.

A registration certificate issued by subordinated CA shall be used only in accordance with:

- the current legislation of the Republic of Kazakhstan;
- the Policy of use of the RCA RK registration certificates;

- these Regulations.

The use of registration certificates issued by subordinated CA shall comply with the contents of the "keyUsage" enhancing.

Subordinate CA shall be responsible for the protection of private keys and activation data from unauthorized access in accordance with the requirements of the current legislation of the Republic of Kazakhstan. Subordinate CA are not allowed to use expired private keys or in the case of revocation of a corresponding registration certificate.

4.5.2. Use of public keys and registration certificates issued by subordinated CA by relying parties

Relying parties, CA RK members, shall assume obligations of a relying party, specified in:

- the current legislation of the Republic of Kazakhstan;
- the Policy of use of the RCA RK registration certificates;
- these Regulations.

The decision on trust to the registration certificate issued by subordinated CA can be made upon fulfillment of the following steps by CA RK members.

1. Verify the corresponding e-document, signed by registration certificate(s) issued by subordinated CA.
2. Ensure the validity of a registration certificate issued by subordinated CA, by fulfillment of the following steps:
   a) define the full chain of registration certificates up to the RCA RK root registration certificate;
   б) assess the compliance of all the registration certificates in the chain with the following criteria:
      - a scope in accordance with the corresponding Policy of use of registration certificate;
      - the "keyUsage" and "extendedKeyUsage" fields content of a registration certificate;
   в) ensure, that all the registration certificates in the chain have been signed by the RCA RK;
   г) ensure the validity of each registration certificate at the time of signing the document.

4.6. UPDATE OF A REGISTRATION CERTIFICATE ISSUED BY SUBORDINATED CA

The RCA RK does not provide the data update in a registration certificate issued by subordinated CA, including the validity of a registration certificate. In the event of the need of data update in a registration certificate issued by subordinated CA, it is necessary to request registration (resubordination) of a new valid registration certificate (see Clause 4.1 above) and revoke the old registration certificate (see Clause 4.6.1. ниже).

4.6.1. Grounds for update of a registration certificate

Not applicable.

4.6.2. Who can request update of a registration certificate

The persons, entitled to apply for update of a registration certificate issued by accredited CA are specified in Clause 4.1.1.

4.6.3. Processing of queries for the registration certificate update

The procedure for processing of queries for update of registration certificates is described in Clause 4.1.2.

4.6.4. Notification of the updated registration certificate issuance for the user

Notification of the updated registration certificate issuance for the user is described in Clause 4.3.2.

4.6.5. Procedure for acceptance of the updated registration certificate

Not applicable

4.6.6. Publication of the CA updated registration certificate

The RCA RK places the issued (resubordinated) registration certificates on the RCA RK Internet resource in Section "Register of registration certificates", available at http://root.gov.kz/certificates.html.

4.6.7. Notification of the registration certificate issuance provided by the RCA RK to other entities

Not applicable.

4.7. UPDATING OF KEYS IN REGISTRATION CERTIFICATE

The RCA RK does not allow key updating in registration certificate issued by subordinated CA, including the registration certificate validity. In the event of the need of key updating a subordinated CA shall request registration (resubordination) of a new valid registration certificate (see Clause 4.1 above) and revoke the old registration certificate (see Clause 4.6.1.).

4.7.1. Grounds for key updating in a registration certificate

Not applicable.

4.7.2. Persons, entitled to request a new public key

Persons, entitled to request a new public key are specified in Clause 4.1.1.

4.7.3. Processing of queries for key updating in a registration certificate

The procedure of processing of queries for key updating in a registration certificate is described in Clause 4.1.2.

4.7.4. Notification of a subscriber on the issuance of a registration certificate with updated keys

The notification of a user on the issuance of a registration certificate with updated keys is described in Clause 4.3.2.

4.7.5. Procedure of acceptance of a registration certificate with updated keys

Not applicable.

4.7.6. Publication of a registration certificate with updated keys issued by CA

The RCA RK places the issued (resubordinated) registration certificates on the RCA RK Internet resource in Section "Register of registration certificates", available at http://root.gov.kz/certificates.html.

4.7.7. CA Notification on the issuance of a registration certificate with updated keys of other entities

Not applicable.

4.8. ALTERATION OF A REGISTRATION CERTIFICATE

The RCA RK does not provide the data update in registration certificate issued by subordinated CA, including the validity of a registration certificate. In the event of the need of data alteration in a registration certificate the subordinated CA shall request registration (resubordination) of a new valid registration certificate (see Clause 4.1 above) and revoke the old registration certificate (see Clause 4.6.1.).

4.8.1. Grounds for alteration of a registration certificate

Not applicable.

4.8.2. Who can request for alteration of a registration certificate

Persons, entitled to apply for alteration of a registration certificate issued by accredited CA are specified in Clause 4.1.1.

4.8.3. Processing of queries for alteration of a registration certificate

The procedure of processing of queries for alteration of registration certificates is described in Clause 4.1.2.

4.8.4. Notification of a subscriber on the issuance of an altered registration certificate

The notification of a user on the issuance of an altered registration certificate is described in Clause 4.3.2.

4.8.5. Procedure of acceptance of an altered registration certificate

Not applicable.

4.8.6. Publication of an altered registration certificate issued by CA

The RCA RK places the issued (resubordinated) registration certificates on the RCA RK Internet resource in Section "Register of registration certificates", available at http://root.gov.kz/certificates.html.

4.8.7. CA notification on the issuance of an altered registration certificate to other entities

Not applicable.

4.9. REVOCATION OF A REGISTRATION CERTIFICATE ISSUED BY SUBORDINATED CA

4.9.1. Grounds for revocation of registration certificates issued by subordinated CA

The RCA RK revokes registration certificates issued by subordinated CA before expiry of validity in the following cases:

1) upon request of a registration certificate holder or its representative;
2) establishing the fact of providing invalid information for obtaining a registration certificate;
3) death of a registration certificate holder;
4) change of the registration certificate holder's last name, name or patronymic (if specified in the identity document);
5) change of the name, reorganization, liquidation of the legal entity-the registration certificate holder;
6) in the cases specified in the agreement between a certification authority and a registration certificate holder;
7) according to the court decision in force.

4.9.2. Persons, entitled to apply for revocation of registration certificates issued by subordinated CA

The persons entitled to apply for revocation of registration certificates issued by subordinated CA include:

- subordinated CA;
- authorized representatives of subordinated CA.

4.9.3. Procedures of revocation of a registration certificate for all the members of the RCA RK PKI

Revocation of a registration certificate issued by subordinated CA shall be carried out on the basis of an official letter sent by subordinated CA on paper containing an attached document, confirming the fact of oncoming of one of the cases, specified in Clause 4.7.1 above.

Upon receiving of the required documents the RCA RK verifies the documents no later than 2 working days following the working day of the application submission. In the event of successful consideration of an application, the RCA RK revokes the registration certificate, publishes information on the revoked registration certificate in the RCRL and notifies the subscriber via e-mail. The RCA RK shall not be responsible for the receipt of the notification on revocation of a registration certificate by subscriber.

4.9.4. Application period for revocation of a registration certificate issued by subordinated CA

Subordinate CA shall submit applications for revocation of registration certificates at the appropriate times according to the procedure established by these Regulations.

4.9.5. Period for consideration of applications for revocation of registration certificates issued by subordinated CA

In accordance with the procedure described in Clause 4.9.3. выше.

4.9.6. Requirements for verification of revocation of a registration certificate issued by subordinated CA for relying parties

The CA RK members shall verify the status of registration certificates issued by subordinated CA before making a decision about the use of the above-mentioned registration certificates through verification of availability of the registration certificate issued by subordinated CA in the current RCRL.

The RCA RK provides the necessary mechanisms for verification of the registration certificates status in accordance with these Regulations (see Clause 2.2 выше).

4.9.7. Frequency of publication of RCRL issued by subordinated CA

The RCRL shall be issued and published not less than once every 35 days.

4.9.8. Maximum delay for publication of a RCRL issued by subordinated CA

RCRL issued by subordinated CA shall be published on the RCA RK Internet resource immediately upon generation.

4.9.9. Availability requirement for RCRL

The RCA RK provides continuous availability of the RCRL in accordance with these Regulations (see Clause 2.2 выше).

4.9.10. Requirements for verification of the revocation status online

Not applicable.

4.9.11. Other forms of revocation notifications available

The RCA RK places RCRL on the RCA RK Internet resource in Section "Register of registration certificates", available at http://root.gov.kz/certificates.html.

4.9.12. Specific requirements for the updating of a compromised key pair

The RCA RK subscribers shall be informed on the compromise or suspected compromise of the RCA RK privacy keys via any appropriate means.

In the event of a reasonable suspicion of the privacy key compromise, the subscriber and holder of the corresponding registration certificate shall suspend the registration certificate validity immediately until the circumstances are clarified.

If the fact of compromise of the private key has not been confirmed, the subscriber and holder of the corresponding registration certificate shall be entitled to resume a suspended certificate, otherwise they shall inform the RCA RK immediately.

In this case the RCA RK takes measures and revokes the registration certificate.

In addition, in the event of a private key compromise or dismissal of an employee, who had access to the private keys, the registration certificate holder shall revoke the registration certificates corresponding to these keys and request issuance of new registration certificates for their updating.

4.9.13. Grounds for suspension of a certificate validity

Not applicable.

4.9.14. Who can request suspension of a certificate validity

Not applicable.

4.9.15. Procedure of query for suspension of a certificate validity

Not applicable.

4.9.16. Ranges of a period for suspension of a certificate validity

Not applicable.

4.10. SERVICE FOR VERIFICATION OF THE STATUS OF A REGISTRATION CERTIFICATE ISSUED BY SUBORDINATED CA

4.10.1. Operating characteristics

Information on the status of subscribers' registration certificates issued by subordinated CA shall be available at the addresses specified on the Internet resources of the subordinated CA via the RCRL and OCSP services.

4.10.2. Services' business hours

The RCRL is available continuously 24 hours a day, 7 days a week.

4.10.3. Extra features

Not applicable.

4.11. COMPLETION OF SUBSCRIPTION

The registration certificate issued by subordinated CA certificate shall be considered invalid automatically upon the expiry of the validity period in accordance with Clause 6.3.2. ниже.

Subordinate CA shall be entitled to revoke their registration certificates before the expiry of the validity period (see Clause 4.6.1. выше).

4.12. DEPOSITION AND RESTORATION OF A KEY PAIR

The RCA RK do not perform deposition and restoration of key pairs issued by subordinated CA.

4.12.1. Policy and practice of deposition and restoration of a key pair

Not applicable.

4.12.2. Policy and practice of deposition and restoration of a key pair

Not applicable.

5. ADMINISTRATIVE, OPERATIONAL AND PHYSICAL CONTROLS OF THE RCA RK ASSETS

5.1. PHYSICAL SECURITY CONTROL OF THE RCA RK ASSETS

The RCA RK provides physical security for the RCA RK systems in accordance with the current legislation of the Republic of Kazakhstan. Detailed policies and procedures for the physical security provision measures contain confidential information owned by the RCA RK and therefore can not be published. Section 0 "Not applicable.

Administrative, operational and physical controls" hereof contains an overview of these measures.

The RCA RK provides physical security for the RCA RK systems through organizational, technical and administrative measures aimed at:

physical security provision for the RCA RK employees;

provision of the correct operation of the RCA RK systems hardware, as well as systems for transfer and storage of the RCA RK information and data storage devices relating to the RCA RK;

information security provision by the RCA RK;

performance control of physical security by the RCA RK.

5.1.1. Placement of the RCA RK assets

Buildings where the RCA RK information assets are placed, the following conditions shall be provided:

- physical security provision for the RCA RK activities (see Clause **Ошибка! Источник ссылки не найден.**);
- back-up facilities provision for continuous activity of the RCA RK in cases of emergency.

5.1.2. Physical access to the RCA RK information assets

The RCA RK information assets are protected by at least four successive levels of physical security, characterized by consistently strengthening requirements for physical access to each level in accordance with:

- the RCA RK internal policies of physical security organization and authority separation;
- the internal policies of the organizations, which provide the RCA RK systems placement;
- the legislation of the Republic of Kazakhstan.

Functioning of the safety levels is provided by technical and organizational measures aimed at:

- prevention of unauthorized physical access — via the systems for physical access limitation (tourniquets, lockable doors, security, duty officers);
- automatic fixation of the physical access situations — via video surveillance and recording of the physical access situations for the two levels of maximum physical access limitation (automatic and manual recording);
- reaction of the responsible units to unauthorized attempts to obtain physical access — with the help of security, alarm and video surveillance systems;
- storage security for data storage devices containing the RCA RK key material — via the use of safes and secure uncrackable containers in some physically secure locations, with mandatory recording of the situations of access to the safes and containers, where the RCA RK key material has been stored, as well as with the help of the organizational measures, which guarantee operation of data storage devices only in the presence of the responsible authorized RCA RK employees.

5.1.3. Electric supply and maintenance of microclimate in the area of the RCA RK hardware location

The location area of the hardware, which maintains the RCA RK information assets operation, has been equipped according to the following criteria:

- the electric supply continuity is ensured by systems of main, back-up and emergency electric supply;
- the microclimate, necessary for the RCA RK systems hardware functioning, is ensured by main and reserve systems for temperature, humidity and ventilation control in accordance with the current Standards of the Republic of Kazakhstan, as well as technical and operational documentation of the hardware.

5.1.4. Sensitivity to water exposure

The location area of the RCA RK systems hardware has been defined taking into account minimization of risks of flooding, landslides, mudslides, hurricanes, etc.

5.1.5. Impact of natural disasters on the location area of the hardware

The location area of the hardware for the RCA RK systems has been defined taking into account minimization of risks of natural disasters, such as earthquakes, floods, landslides, mudslides, hurricanes, etc.

5.1.6. Prevention and protection against fire referred to the location area of the RCA RK hardware

The location area of the hardware for the RCA RK information assets provides effective prevention and control of fires, harmful effects of fire and smoke in accordance with the current regulations of the Republic of Kazakhstan.

5.1.7. Maintenance of the RCA RK data storage devices

All the RCA RK data storage devices, including source codes, data, automatic records, back-ups are stored with provision of physical security according to:

- the RCA RK internal policies of physical and information security organization, as well as authority separation;
- the internal policies of the organizations, which provide placement of the NCA RK data storage devices;
- the legislation of the Republic of Kazakhstan.
- The RCA RK protects the RCA RK data storage devices from:
- violation of the above-mentioned rules and regulations;
- damage;
- unauthorized alteration of information;
- disclosure of confidential information.

5.1.8. Disposal of the RCA RK data storage devices and hardware

The RCA RK provides disposal of the data storage devices and hardware in accordance with

- the RCA RK internal policies of physical and information security organization, as well as authority separation;
- the internal policies of the organizations, which provide placement of the NCA RK data storage devices and systems;
- the legislation of the Republic of Kazakhstan;
- technical documentation for the data storage devices and hardware.

All the storage devices, which contained confidential information, shall be made unreadable. The RCA RK provides disposal of the data storage devices for cryptographic hardware (see Clause 6.2.1. ниже).

5.1.9. RCA RK information back-up

The RCA RK carries out back-up procedure for the NCA RK systems software, their data, records, confidential information and RCRL.

The back-up media are stored with provision of physical security for prevention of:

- unauthorized access to the back-ups;
- corruption of the back-ups;
- destruction of the back-ups.

5.2. RCA PK RESPONSIBILITY AND ACTIVITY CONTROL

5.2.1. Distribution of responsible roles

A category of responsible personnel includes the RCA PK employees, having access or controlling the authentication and operations, which may significantly affect the following functions of RCA RK:

- verification of information contained in the applications for registration (resubordination) of registration certificates issued by accredited CA;
- acceptance, refusal of acceptance or other processing types referred to the applications for registration (resubordination) of the registration certificates issued by accredited CA;
- registration (resubordination) or revocation of a subordinate registration certificates.
- The responsible roles include, among others, the following functions:
- support for subordinated CA;
- operations with cryptographic hardware;
- management and provision of information security;
- management and provision of physical security;
- administration of the RCA RK systems software;
- maintenance of the RCA RK systems hardware;
- management and provision of the RCA RK service infrastructure.

The RCA RK provides compliance of employees performing all the responsible roles with competence requirements (see Clause 5.2.3. ниже, as well as Clause 5.3.2. ниже).

5.2.2. Number of personnel required for a particular task

The RCA RK provides the necessary number of units and employees for the provision of internal control system functioning. In the event of vacancy of the full-time equivalent, necessary for the control provision, the RCA RK takes alternative control measures based on the risk assessment.

In particular, the tasks for management of a lifecycle of registration certificates issued by subordinated CA involve participation of the RCA responsible executives and representatives of subordinated CA. The tasks of the RCA RK key material management, access management referred to the RCA RK systems, management of alterations in the

RCA RK systems, the RCA RK systems back-up, etc. also involve participation of at least two employees belonging to two independent units of the RSE STS.

5.2.3. Identification and authentication of a responsible role

Service instructions and qualification requirements have been defined for each role by the RCA RK. The compliance with the qualification requirements is verified in relation to each RCA RK employee before hiring (see Clause 5.3.2. ниже), as well as confirmation of the candidate's identity and other documents collecting in accordance with the legislation of the Republic of Kazakhstan.

Official activities of the RCA RK employees performing responsible roles may be carried out only within the RCA RK physically protected perimeter (see Clause 5.1.2. выше). Access of employees to the protected perimeter allowed upon the employee's identity authentication. Operation of the RCA RK informational systems is also provided by the employees' identity authentication.

5.2.4. RCA RK functions, which require separation of duties

The RCA RK defines incompatible functions, which require separation of duties. They include:

- the RCA RK informational systems administration;
- the RCA RK systems development;
- management of the lifecycle of subordinate registration certificates issued by subordinated CA.

The RCA RK enforces separation of incompatible functions through all its processes.

5.3. SECURITY PROVISION FOR THE RCA RK EMPLOYEES

the RCA RK provides security for the RCA RK employees in accordance with:

- the RCA RK internal policies of physical security organization;
- the internal policies of the organizations, which provide placement of the RCA RK systems and employees;
- the legislation of the Republic of Kazakhstan.

The detailed measures of physical security provision for the RCA RK employees have been formalized and approved in writing, but shall not be published, because they contain the RCA RK confidential information.

5.3.1. Requirements for the experience and qualifications of the RCA RK employees

The RCA RK provides the employees' compliance with minimum requirements for experience and qualifications in accordance with:

- the RCA RK and RSE STS internal recruitment policies and service instructions;
- the internal policies of the organizations, which provide operation of the RCA RK systems;
- the legislation of the Republic of Kazakhstan.

Confirmation of compliance with the requirements for experience and qualifications shall be demonstrated by provision of supporting diplomas, certificates, recommendations, etc., retaining copies in the personnel department.

5.3.2. Procedures of the RCA RK employees' verification

The RCA RK verifies employees before hiring and during the period of the employment contract validity in accordance with:

- the RCA RK and RSE STS internal recruitment policies and service instructions;
- the internal policies of the organizations, which provide operation of the RCA RK systems;
- the legislation of the Republic of Kazakhstan.

The verification includes at least documentary evidence of the following issues:

- compliance with the experience and qualifications requirements (see Clause 5.3.1. выше);
- provision of the necessary verification letters and confirmations in accordance with the legislation of the Republic of Kazakhstan and role of the RCA RK employee.

5.3.3. Requirements for professional development of the RCA RK employees

The RCA RK provides professional development of the employees aimed at competent and high-quality performance of official duties. The professional development of the RCA RK employees shall be carried out through training, additional training and advanced training in accordance with the official duties. The measures for professional development of the employees include taking the required courses and attendance of the training activities.

5.3.4. Requirements for professional development of the RCA RK employees

The frequency of measures for professional development of the RCA RK employees may be defined in accordance with:

- the needs of the RCA RK activities performance aims;

- the internal recruitment policies and service instructions, as well as development budgets for the staff of the RSE STS;
- the legislation of the Republic of Kazakhstan.

5.3.5. Career development of the RCA RK employees

Career development of the RCA RK employees shall be defined in accordance with:

- the needs of the RCA RK activities performance aims;
- the internal recruitment policies and service instructions, as well as plans of the RCA RK and RSE STS;
- the legislation of the Republic of Kazakhstan.

The decisions on the RCA RK employees displacement shall be approved by the RSE STS Director.

5.3.6. RSE STS employee's responsibility for unauthorized actions

The RCA RK and RSE STS employees shall be responsible for compliance with internal regulations in accordance with:

- the internal policies and service instructions of the RCA RK and RSE STS;
- the internal policies of the organizations, which provide operation of the RCA RK systems;
- the legislation of the Republic of Kazakhstan.

Upon detection of unauthorized actions or suspicion of committing unauthorized actions, the person, who found the violation, informs the RCA RK. The RCA RK executive officer decides on the urgent need to block access of a infringer (suspect) to the systems and records the incident. Further activities performed for the incident investigation, as well as determination of the responsibilities shall be carried out in accordance with the procedure of incident management implemented by the RCA RK.

5.3.7. Requirements for independent parties

The RCA RK does not allow independent parties not related to the RCA RK, to perform operations with informational systems, ensuring the RCA RK activities. Independent parties may be present during certain RCA RK procedures performance as participants or observers.

The following organizations are allowed to participate as independent observers:

- competent authorities, relating to the functioning of the RCA RK, the RCA RK PKI or PKI issued by subordinated CA (for example, NSC RK, Prime Minister's Office of the Republic of Kazakhstan, the holders of "E-Notariat", "Treasury-Customer" systems, "electronic government" portal, etc.); as well as
- certification bodies on the basis of services performance agreements and nondisclosure agreements (for example, for certification purposes referred to the RCA RK equipment, WebTrust auditors, etc.).

5.3.8. Documents disclosed by the RCA RK and RSE STS employees

The RCA RK provides the RSE STS employees with a minimum of necessary materials for the purposes of:

- training and professional development in accordance with the service instructions (see Clause 5.3.3. выше);
- the official duties performance.

The materials provision shall be carried out in accordance with:

- the internal policies and service instructions of the RCA RK and RSE STS;
- the internal policies of the organizations, which provide operation of the RCA RK systems;
- the legislation of the Republic of Kazakhstan.

5.4. DOCUMENTATION OF EVENTS (RECORDING) IN THE RCA RK INFORMATIONAL SYSTEM

5.4.1. Types of recorded events

The RCA RK maintains and stores records for the following event types:

Lifecycle management events for the keys obtained by the RCA RK and subordinated CA subject to documentation:

1) transfer of a key pair;
2) restoration of a key pair;
3) taking key pair materials out of operation;
4) annulment of a key pair;
5) identification of a party authorizing operations of key pair lifecycle management;
6) identification of persons having access to the key pair materials;
7) transfer of devices or other means of storage of a key pair for maintenance;
8) a private key compromise;

9) a key pair back-up;
10) Key pair archiving.

Events of the lifecycle of the keys obtained by the RCA RK and the RCA RK customers, subject to recording:
1) issuance of a key pair;
2) use of a key pair.

Lifecycle management events for cryptographic hardware, subject to documentation:
1) issuance of cryptographic hardware;
2) installation of cryptographic hardware.

Events of transfer for storage/issuance after storage of cryptographic hardware, subject to documentation:
1) dismantlement of cryptographic hardware;
2) maintenance of cryptographic hardware;
3) annulment of cryptographic hardware;

Lifecycle management events for cryptographic hardware, subject to documentation:
1) use of cryptographic hardware.

Lifecycle management events for registration certificate, subject to recording/documentation:
1) obtaining of application for issuance/update/revocation/ of a registration certificate;
2) issuance of a registration certificate;
3) distribution of the RCA RK public key;
4) revocation of a registration certificate;
5) generation and issuance of a registration certificate revocation list;

Events, connected with security, subject to recording:
1) critical files recording;
2) actions taken with respect to the sensitive information;
3) alteration of security profiles;
4) use of identification and authentication mechanisms;
5) failures of systems, including software and hardware;
6) actions of employees working in trusted roles and administrators;
7) access to the RCA RK systems and their components.

In the event of inability to insert data in the records of one of the above listed elements, the RCA RK takes alternative technical and organizational measures in order to minimize risks.

The RCA RK does not allow keys and passwords insertion into an explicit form.

5.4.2. Frequency of the control protocol analysis

The RCA RK carries out a daily records analysis for the purposes of the RCA RK internal control system functioning.

5.4.3. Records validity

The RCA RK stores records for at least 90 days, after which the records are subject to archiving and transfer to the archive in accordance with Clause 5.5 ниже.

5.4.4. Records protection

The RCA RK protects the records from unauthorized reviewing, modification, and deletion. The records protection is provided by organizational and technical measures.

5.4.5. Records back-up

The RCA RK carries out the records back-up quarterly. The back-ups shall be stored in accordance with:
the RCA RK and RSE STS internal policies of physical and information security;
the internal policies of the organizations, which provide operation of the RCA RK systems;
the requirements of the legislation of the Republic of Kazakhstan.

5.4.6. Records collection system

Not applicable.

5.4.7. Notification of an entity, who induced the event

Not specified.

5.4.8. Vulnerability analysis

The RCA RK carries out a periodic assessment of vulnerabilities, as well as vulnerabilities, identified in the course of the RCA RK internal control system operation in accordance with:

1) the internal policies of the RCA RK and RSE STS (and among others, in accordance with rules and regulations of the procedure of periodic vulnerability assessments, risk management and incident management);
- the internal policies of the organizations, which provide operation of the RCA RK systems;
- the requirements of the legislation of the Republic of Kazakhstan.

5.5. RECORDS ARCHIVE

5.5.1. Types of archived events

The RCA RK provides archival storage of the following types of information in accordance with the requirements of the current legislation of the Republic of Kazakhstan:

1) event records;
- current, revoked and expired registration certificates issued by subordinated CA;
- current, revoked and expired registration certificates issued by the RCA RK;
- applications for registration (resubordination) and revocation of registration certificates issued by subordinated CA;
- registration certificate revocation lists published by the RCA RK and subordinated CA.

5.5.2. Archive validity

The RCA RK provides continuous operation of the archive in accordance with the requirements of the current legislation of the Republic of Kazakhstan. The duration of the archival data storage shall be defined in accordance with:
- the internal policies of the RCA RK and RSE STS for each data type;
- the internal policies of the organizations, which provide operation of the RCA RK systems;
- the current legislation of the Republic of Kazakhstan.

5.5.3. Archive protection

The RCA RK protects archive materials in accordance with:
- the internal policies of the RCA RK and RSE STS for each data type;
- the internal policies of the organizations, which provide operation of the RCA RK systems;
- the current legislation of the Republic of Kazakhstan.

Only the RCA RK and RSE STS executive officers have access to the archive. The RCA RK uses technical and organizational measures for protection of the archive materials from unauthorized access, modification or deletion.

5.5.4. Archiving conditions

The materials archiving shall be carried out in accordance with:
- the internal policies of the RCA RK and RSE STS for each data type;
- the internal policies of the organizations, which provide operation of the RCA RK systems;
- the legislation of the Republic of Kazakhstan.

5.5.5. Procedure of acceptance and verification of the archive information

The access to the archive materials is limited in accordance with Clause 5.5.3 hereof. The RCA RK executive officers carry out verification of the archive information in accordance with the provisions of Clause 5.7.4. ниже.

5.6. RCA RK KEY UPDATING

The RCA RK updates the RCA RK key pairs and registration certificates upon the expirity of a validity period of the RCA RK registration certificate or in the event of the RCA RK key pair compromise. Provided that the RCA RK:
- terminates the use of old key pairs and corresponding registration certificates;
- generates new key pairs and corresponding root registration certificates.

Generation of the RCA RK key pairs shall be carried out in the presence of an independent party as an observer.

5.7. COMPROMISE AND EMERGENCY RECOVERY OF THE RCA RK KEYS

5.7.1. Procedures for processing of incidents and compromise

The RCA RK provides creation and secure storage of the back-ups of the following critical data in the event of incidents or compromise:
- applications for registration (resubordination) or revocation of registration certificates;
- event records;
- RCRL;

- the RCA RK key pairs.

In the event of incidents in the RCA RK, as well as upon detection of compromise or suspicion of compromise referred to the RCA RK privacy keys, the procedures in accordance with the requirements of the legislation of the Republic of Kazakhstan and internal rules and regulations of RCA RK shall be conducted for the purposes of:

- assessment and categorization of the event;
- measures taken to prevent and eliminate the event consequences in accordance with the RCA RK risk assessment.

5.7.2. Damage of computing, software resources and / or data

Damage of the RCA RK computing, software resources and / or data shall be considered as incidents and processed in accordance with the provisions Clause 5.7.1. вышегеreof.

5.7.3. The RCA RK privacy key compromise

The RCA RK provides the internal control system operation, which includes monitoring for possible compromise of the RCA RK privacy keys. In the event of compromise detection or existence of reasonable suspicions of compromise referred to the RCA RK privacy keys, the RCA RK employee takes the necessary measures in accordance with the Plan of continuity and restoration of the RCA RK and RCA RK activities.

In the event of the need to reissue the RCA RK key pairs, the procedure described in Clause 6.1 ниже shall be carried out. In this case a notification of all the subordinated CA and members of the RCA RK PKI on the fact of the RCA RK key pair reissuance shall be provided.

5.7.4. Potential for continuous operations after incidents

The RCA RK has approved and tested the detailed Plan of continuity and restoration of the activity of the Root Certification Authority of the Republic of Kazakhstan and National certification authority of the Republic of Kazakhstan (hereinafter referred to as the "Plan"), aimed at mitigating the consequences of threats, including natural catastrophes. The Plan shall be regularly reviewed for the purposes of update in accordance with the RCA RK internal risk assessment procedures.

The RCA RK has back-up objects aimed at provision of the continuity of the RCA RK services and key functions.

The time period required to restore the RCA RK critical services, in the event of external and / or internal threats, being able to some extent affect the performance of the RCA RK:

- The target time for a full restoration of the RCA RK (RTO) = 2 months 4 hours 25 minutes 39 seconds;
- The partial restoration time of the RCA RK (pRTO) = 2 hours 10 minutes;
- The mean time between failures = depending on the emerging threat.

For the purposes of testing of the continuous operation potential, the RCA RK regularly transfers the processing from the main object to the reserved one.

5.8. THE RCA RK ACTIVITY TERMINATION

In the event of necessity to terminate the RCA RK activities, the RCA RK shall take all measures necessary for advance notification of the subordinated CA and RCA RK PKI subscribers and members. Next the RCA RK shall develop a plan of termination of activities aimed at minimization of inconveniences for the subordinated CA and RCA RK PKI and members. The termination plan may include the following issues:

- Notification containing information on the RCA RK status for the parties, affected by termination of the RCA RK activities, including the RCA RK PKI subscribers and members;
- storage of the RCA RK archives in accordance with the requirements of the legislation of the Republic of Kazakhstan and corresponding Policy of use of registration certificates;
- continuation of support services for the subordinated CA;
- continuation of service verification of revocation and the RCRL issuance;
- revocation of the current registration certificates issued by subordinated CA, which have not been revoked earlier, when appropriate;
- issuance of the updated registration certificates by certification authority-successor;
- further location of the RCA RK privacy keys and cryptographic modules, containing these privacy keys;
- provisions necessary for the services transmission by the RCA RK to its successor.

6. TECHNICAL PROTECTION CONTROL OF THE RCA RK

6.1. ISSUE AND INSTALLATION OF KEY PAIRS OF THE RCA RK

6.1.1. Key pair generation

Subordinate CAs generate their key pairs by themselves, as well as determine policy concerning their subscribers' key pairs generation.

The RCA RK generates all the key pairs used in the RCA RK. Generation of key pairs is carried out by means of cryptographic modules that are certified to meet the applicable standards of the Republic of Kazakhstan ST RK 1073-2007 at a level not lower than the third one.

Generation of key pairs of the RCA RK is carried out exclusively in accordance with the approved internal regulations, with the participation of competent senior officials and under the supervision of an independent party. Ceremony of the RCA RK key pairs generation is recorded with the relevant protocol signed by all participants of the ceremony. The protocols are stored and archived in accordance with the applicable legislation of the Republic of Kazakhstan and the internal regulations of the RCA RK.

A process of generating a key pair is protected from electromagnetic radiation emissions. This requirement is implemented by external physical protection of "Certex HSM" hardware and software complex using Lampertz 9.3 secure safe box. This safe box protects against electromagnetic radiation emissions with the external capacity of less than 70 decibels.

6.1.2. Private Key Delivery of subordinated CA in the RCA RK

For subordination of CA registration certificate, CA private key is not required, in this regard, private key delivery in the RCA RK is not carried out.

6.1.3. Public Key Delivery of subordinated CA in the RCA RK

A public key of subordinated CA is available in the RCA RK as part of a registration certificate of the subordinated CA during registration (resubordination) of the registration certificate of subordinated CA.

6.1.4. RCA RK public key transfer to relying parties

RCA RK public key is available as a part of a RCA RK root registration certificate on the Internet resource of the RCA RK provides organizational and technical measures to ensure the integrity and validity of the RCA RK public key.

6.1.5. Purposes of key usage

In accordance with 1.4 hereof

6.1.6. Key size

Key pairs of subordinate CAs are issued in line with the RSA algorithm and have the following sizes:
private key - 4096 bits;
public key - 4096 bits.
Also, RCA RK issues key pairs of subordinated CA according to the algorithm of GOST 34.310-2004, and they have the following sizes:
private key - 256 bits;
public key - 512 bits.

6.1.7. Parameters of public key generation

Parameters of public key generation are specified in 6.1.1.

6.2. PROTECTION CONTROLS OF PRIVATE KEYS OF THE RCA RK AND SUBORDINATE CAS, AS WELL AS MANAGING LIFE CYCLE OF CRYPTOGRAPHIC HARDWARE OF THE RCA RK

The RCA RK supports inner control environment in order to protect RCA RK private keys and to secure life cycle management of the RCA RK cryptographic hardware.

6.2.1. Standards and control of cryptographic hardware

The RCA RK cryptographic hardware is certified for compliance with the applicable in the Republic of Kazakhstan standards ST RK 1073-2007, defining general technical requirements for the means of cryptographic information protection for the compliance not below the third level of security.

The RCA RK is implementing a number of technical and organizational measures to ensure the confidentiality and integrity of the cryptographic hardware during transporting, pre-commissioning and operation in primary and backup the RCA RK facilities. The RCA RK also implements a number of technical and organizational measures to ensure operation and maintenance of cryptographic hardware in strict accordance with its technical and operational documentation and internal rules of physical security in accordance with paragraph 5.1 hereof and the rules of procedure in accordance with paragraph 5.2 hereof.

The RCA RK cryptographic hardware is stored and used only in designated protected the RCA RK facilities. Putting the RCA RK cryptographic hardware out of operation for repair work is accompanied by the guaranteed cleaning and, if possible, physical destruction of the memory storage devices. Decommission of the RCA RK cryptographic hardware is accompanied by physical destruction of the cryptographic hardware in secure environment.

Arrangements for reception, maintenance and decommissioning of the RCA RK cryptographic hardware are carried out in the presence of senior officials included in a list of trusted roles in accordance with paragraph 5.2 hereof.

6.2.2. Sharing the RCA RK private key between responsible parties under the scheme of m of n

Cryptographic operations carried out manually and requiring the use of the RCA RK private keys are made using a backup copy of the RCA RK private key, protected by means of the shared secret. To do this, the information needed to restore a backup copy of any RCA RK private key ("secret") is shared into n parts. To successfully restore a backup copy of the RCA RK private key at least m parts of the secret are required. When generating a secret value, m and n are defined according to the formula: $n > m + 1$.

Parts of the secret are kept by responsible participants of the ceremony of generating RCA RK key pairs in accordance with the legal requirements of Kazakhstan and internal regulatory documentation of the RCA RK in accordance with paragraph 6.4.1. ниже.

6.2.3. Depositing private keys of subordinate CAs

RCA RK does not deposit private keys of subordinate CAs.

6.2.4. Backing up RCA RK private key

In case of damage or inaccessibility of the RCA RK private keys, backup copies are created when generating RCA RK key pairs. Backup copy of the RCA RK private key is protected by a secret in accordance with paragraph 6.2.2 hereof.

6.2.5. Archiving RCA RK private key

Archiving RCA RK private keys if the registration certificate expired.

6.2.6. Importing and exporting RCA RK private keys stored in cryptographic modules

RCA RK key material outside the cryptographic module exists only in encrypted form to ensure the integrity and confidentiality of the RCA RK key material.

Exporting RCA RK key material from cryptographic modules is possible only as a backup copy of the private key in accordance with paragraph 6.2.4 hereof.

6.2.7. Storing RCA RK private key in a cryptographic module

Cryptographic modules that store RCA RK private keys, do not allow by hardware storing key material in unencrypted form, including RAM.

Private keys of subordinate CAs must be stored in approved protected media, in accordance with the requirements of the PKCS # 11 standard.

6.2.8. Methods of activation of the RCA RK private key

RCA RK private keys are manually activated before use in accordance with the provisions documented in paragraph 6.2.2 hereof.

6.2.9. Method of deactivation of a private key

RCA RK private key deactivation is not carried out due to its safe storing on RCA RK hardware cryptographic module.

6.2.10. Method of destruction of the RCA RK private key and subordinate

All parts of decommissioned RCA RK private keys are disposed with guaranteed impossibility of being restored. RCA RK private key destruction procedure is carried out by authorized personnel in the presence of an independent observer.

The destruction of private keys of subordinate CAs is the responsibility of subordinate CAs.

6.2.11. Estimation of cryptographic modules of the RCA RK and subordinate CAs

All cryptographic modules used by RCA RK, are certified for compliance with the applicable standard of the Republic of Kazakhstan ST RK 1073-2007 not lower than the third level. The use of non-certified cryptographic modules is not allowed in accordance with the internal regulations of the RCA RK, these Regulations and Policy of registration certificates implication.

6.3. OTHER ASPECTS OF THE RCA RK KEY PAIR MANAGEMENT

6.3.1. Public keys archiving

All public keys of the RCA RK and subordinate CAs for which RCA RK ever registered (reassigned) registration certificates are archived as parts of the relevant registration certificates in accordance with the provisions of paragraph 5.5 hereinabove.

6.3.2. Validity of registration certificates and use of key pairs

RCA RK registration certificates are generated for no more than 10 years. Registration certificates of subordinate CAs should be issued with a validity period of 5 years. In case of revocation of registration certificates of the RCA RK or subordinate CAs validity period ends at the time of the revocation. Usage of key pairs of revoked registration certificates of the RCA RK or subordinate CAs is not allowed.

6.4. ACTIVATION DATA

6.4.1. Generating and installing activation data of private keys

Generation of the RCA RK private keys is accompanied by creation of a "secret" on protected media for key information in accordance with the procedure described in paragraph 6.2.2. выше. Usage of "secret" requires two-factor authentication: use of the media with a part of the secret and the corresponding unique PIN-code. Responsible participants if a ceremony of generating RCA RK private keys are selected on the basis of compliance with the principle of separation of powers and independence. Activation data of each of the secret, entrusted to the responsible party, is entered directly by the responsible party and cannot be disclosed to the other responsible parties.

6.4.2. Activation data protection

Responsible participants of a ceremony of the RCA RK key pairs generation accept in written form the responsibility for storing of the secret entrusted to them and the activation data.

6.4.3. Other aspects of activation data

Activation data of the RCA RK private keys is decommissioned with the use of procedures protecting against loss, theft, modification, disclosure or unauthorized use of private keys that are activated by this data. Activation data that is not to be further stored is decommissioned by physical destruction.

6.5. COMPUTER PROTECTION CONTROLS

6.5.1. Special technical requirements of computer protection

Protection of the RCA RK technical devices is provided by:

- organizational and technical security measures (including access control, software update management, virus protection and so on.);
- events logging.

6.5.2. Computer protection assessment

The RCA RK uses certified computer security tools, which indicates a successful assessment of the high level of security.

The RCA RK carries out periodic assessments of vulnerabilities in the infrastructure with risk assessment and subsequent treatment of risks.

6.6. SECURITY LIFE CYCLE CONTROLS

6.6.1. System development control

The procedure of development of new RCA RK software is defined in Regulation of Software Development of the RCA RK.

6.6.2. Safety management control

The RCA RK provides functioning of safety management controls in accordance with the requirements of ST RK ISO/IEC 27001.

6.6.3. Life cycle safety management

The RCA RK provides functioning of safety management controls in accordance with the requirements of the ST RK ISO/IEC 27001.

6.7. NETWORKS PROTECTION CONTROLS

The RCA RK provides protection of internal networks, as well as safety of data transmitted by external networks. The RCA RK provides organizational and technical measures against unauthorized access and attacks on their networks. Policies and procedures for network security monitoring activities are documented and approved, but not published because they contain confidential the RCA RK information.

7. PROFILES OF REGISTRATION CERTIFICATE OF SUBORDINATE CA AND RCRL

7.1. PROFILES OF REGISTRATION CERTIFICATE OF SUBORDINATE CA

7.1.1. Profiles of RSA registration certificate for subordinate CA

Field	Description	OID, criticality	Content
Basic fields of a registration certificate in X.509 format			
Version	Version of X.509 standard	–	V3
SerialNumber	Registration certificate serial number has to be a positive integer (20 bytes) and to meet the requirements of 4.1.2.2 of RFC5280 standard	–	–
SignatureAlgorithm	Signature Algorithm	1.2.840.113549.1.1.11	sha256WithRSAEncryption
Subject	Data on the owner of a registration certificate	C=2.5.4.6 L=2.5.4.7 S=2.5.4.8 O=2.5.4.10 CN =2.5.4.3	L = Subordinate CA's city (required) S = Subordinate CA's state (required) C = KZ (required) O = Legal name of organisation that possesses Subordinate CA (required) CN = Subordinate CA's name (required)
Validity from	Valid from date	UTC TIME	Valid from: YYMMDDHHMMSSZ GMT
Validity to	Expiry date	UTC TIME	Expires on: YYMMDDHHMMSSZ GMT
Issuer	Data on the issuer of a registration certificate	CN =2.5.4.3 O=2.5.4.10 C=2.5.4.6	CN = НЕГІЗГІ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA) O = РМК "МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ" C = KZ
PublicKey	Public key value (4096 bits)	1.2.840.113549.1.1.1	–
Additional fields of a registration certificate in X.509 format			
Subject Key Identifier	Subject Key Identifier (4 bytes) Key ID on HSM	2.5.29.14	–
Authority Key Identifier	Subject Key Identifier (4 bytes) Key ID on HSM	2.5.29.35	–
Basic Constraints	Basic Constraints	2.5.29.19, critical	Subject type = CA; Constraint for length = Absent
Key Usage	Key Usage	2.5.29.15, critical	Registration certificate signing, Independent Certificate Revocation List Signing (CRL), Certificate Revocation List Signing (CRL)
Certificate Policy	Registration Certificate Policy	2.5.29.32	[1]Registration Certificate Policy: Policy ID = value [1.1]Policy qualifier information: Policy qualifier ID = CPS Qualifier:
Certificate Authority Information Access	Certificate Authority Information Access	1.3.6.1.5.5.7.1.1	[1]Certificate Authority Data Access Access Method = Certification Authority Supplier Additional name: URL=http://root.gov.kz/cert/root_rsa.cer
Crl Distribution Points	Distribution point of Revocation List	2.5.29.31	[1]Distribution point of Revocation List (CRL)

			Distribution point name: Full name: URL=http://crl.root.gov.kz/rsa.crl URL=http://crl1.root.gov.kz/rsa.crl
Digital Signature	CA Digital Signature (4096 bits)	1.2.840.113549.1.1.11	sha256WithRSAEncryption

7.1.2. Profiles of GOST registration certificate for EDS of a subordinate CA

Field	Description	OID, criticality	Content
Basic fields of a registration certificate in X.509 format			
Version	Version of X.509 standard	–	V3
Serial Number	Registration certificate serial number has to be a positive integer (20 bytes) and to meet the requirements of 4.1.2.2 of RFC5280 standard	–	–
Signature Algorithm	Signature Algorithm	1.2.398.3.10.1.1.1.2	GOST 34.310-2004
	Hash-coding algorithm	1.2.398.3.10.1.3.1.1.0	Hash-coding algorithm GOST 34.311-95
Subject	Data on the owner of a registration certificate	C=2.5.4.6 L= 2.5.4.7 S=2.5.4.8 O=2.5.4.10 CN =2.5.4.3	L = Subordinate CA's city (required) S = Subordinate CA's state (required) C = KZ (required) O = Legal name of organisation that possesses Subordinate CA (required) CN = Subordinate CA's name (required)
Validity from	Valid from date	UTC TIME	Valid from: YYMMDDHHMMSSZ GMT
Validity to	Expiry date	UTC TIME	Expires on: YYMMDDHHMMSSZ GMT
Issuer	Data on the issuer of a registration certificate	CN =2.5.4.3 O=2.5.4.10 C=2.5.4.6	CN = НЕГІЗГІ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST) (mandatory field) O = РМК "МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ" (mandatory field) C = KZ(mandatory field)
Public Key	Public key value (512 bits)	1.2.398.3.10.1.1.1.1 with the parameters 1.2.398.3.10.1.1.1.1 1.2.398.3.10.1.3.1.1.0	GOST 34.310-2004
Additional fields of a registration certificate in X.509 format			
Subject Key Identifier	Subject Key Identifier (4 bytes) Key ID on HSM	2.5.29.14	–
Authority Key Identifier	CA Key Identifier (4 bytes) Key ID on HSM	2.5.29.35	–
Basic Constraints	Basic Constraints	2.5.29.19, critical	Subject Type = Certificate Authority Constraint for length = Absent
Key Usage	Key Usage	2.5.29.15, critical	Registration certificates signing, Independent Certificate Revocation List Signing (CRL), Certificate Revocation List Signing (CRL)
Certificate Policy	Registration Certificate Policy	2.5.29.32	[1]Registration Certificate Policy: Policy ID = value [1.1]Policy qualifier information: Policy qualifier ID = CPS Qualifier:
Certificate Authority Information Access	Certificate Authority Information Access	1.3.6.1.5.5.7.1.1	[1]Certificate Authority Data Access Access Method = Certification Authority Supplier

			Additional name: URL=http://root.gov.kz/cert/root_gost.cer
Crl Distribution Points	2.5.29.31	Distribution point of Revocation List	[1]Distribution point of Revocation List (CRL) Distribution point name: Full name: URL=http://crl.root.gov.kz/gost.crl URL=http://crl1.root.gov.kz/gost.crl
Digital Signature	CA Digital Signature (512 bits)	1.2.398.3.10.1.1.1.2	–

7.1.3. Profile of revoked registration certificate for EDS in X.509 format

Name	Content
Version — Version	V2
Issuer — RCRL Issuer	CN = НЕГІЗГІ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA) O = РМК "МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ" C = KZ
thisUpdate — RCRL Issuing Time	Valid from: YYMMDDHHMMSSZ
nextUpdate — Next RCRL Update	Valid to: YYMMDDHHMMSSZ
signatureAlgorithm — Signature Algorithm	sha256RSA
Main constraints for subject type	Subject
Main constraints for route length	—

7.1.4. Processing critical extension semantics

Not applicable.

7.2. OCSP PROFILE

The RCA RK does not use OCSP.

7.2.1. Version

Not applicable.

7.2.2. OCSP extensions

Not applicable.

8. COMPLIANCE AUDIT

The internal control environment of the RCA RK is checked for compliance with the international standard WebTrust. The audit is carried out by independent auditing companies, licensed by the owner of WebTrust standard.

All subordinate CAs have to provide a certificate of successful certification in accordance with international standard WebTrust to the RCA RK at least once a year. If there is no compliance with the requirements of the standard registration certificate of a subordinate CA will be revoked.

8.1. PERIODICITY OF AUDIT

Audit of the NVC RK internal control environment for compliance with the international standard WebTrust (external audit) shall be held not less than once a year.

8.2. AUDITORS AND THEIR QUALIFICATIONS

Audit of the RCA RK internal control environment for compliance with the international standard WebTrust is carried out by independent audit organizations that have a license from the owner of the WebTrust international standard for carrying out the certification audit for compliance with the international standard WebTrust. License by WebTrust standard owner shall be issued after verification of qualification of the audit organization.

8.3. RELATIONS BETWEEN NVC RK AND AUDITING COMPANIES

Audit companies engaged in auditing internal control environment of the RCA RK for compliance with the WebTrust international standard, are independent of the RSE STS and the Owner.

8.4. AUDIT OBJECTIVES

Audit of internal control environment of RCA is conducted in accordance with WebTrust international standard for Certification Authorities. The scope of inspections includes the following sections of WebTrust international standard:

1) Disclosure of business practices of the RCA RK;
- registration certificates policy appliance management;
- registration certificates instruction management.

The RCA RK environment controls:
- information protection management;
- classification of the assets and managing them;
- personnel protection;
- physical protection management;
- the RCA RK activity management;
- access management;
- system development and maintenance management;
- business continuity management;
- monitoring and managing compliance with requirements;
- logging.

Controls of life cycle of the RCA RK registration certificates.
- the RCA RK keys generation;
- storing, backup copying and restoring RCA RK keys;
- distribution of the RCA RK public keys;
- the RCA RK keys usage;
- archiving and decommissioning RCA RK keys;
- controls of compromise of the RCA RK keys;
- the RCA RK CIPF life cycle management.

controls of life cycle management of registration certificates of subordinate CAs.

8.5. MEASURES TAKEN AFTER EXPOSURE OF DEFICIENCIES AND VIOLATIONS

Based on the results of inspections of the RCA RK internal control environment for compliance with the international standard WebTrust licensed audit companies provide to MIC RK a final report containing a list of

identified deficiencies or violations, as well as the risks connected with these deficiencies or violations and recommendations for their elimination. On the basis of the final report of the audit, officials of the RCA RK make a plan to eliminate deficiencies and violations, indicating deadlines, responsible persons and results of the plan implementation. The plan is approved by the responsible persons of the MIC RK. MIC RK controls implementation of the plan for elimination deficiencies and violations

RCA RK provides to MIC RK information on the elimination of the identified deficiencies in accordance with the plan for eliminating deficiencies and violations. RCA RK provides to independent licensed auditors the information about how to eliminate the previously identified deficiencies at the next annual audit of internal control environment of the RCA RK.

8.6. MESSAGE ABOUT RESULTS

Message about audit results is defined in cl. 8.5.

9. LEGAL AFFAIRS

9.1. SERVICE FEE

RCA RK does not charge for the provision of public services by RCA RK PKI.

- registration of applications on reassignment, suspension or revocation of registration certificates of subordinate CAs;
- registration of registration certificates of subordinate CAs;
- revocation of registration certificates of subordinate CAs;
- RCRL release;
- proof of ownership, authenticity and validity of the issued registration certificates by the official appeals of the RCA RK PKI participants (see 9.12 ниже).

9.1.1. Registration certificate issue and update fee

Registration certificates issue is free.

9.1.2. Registration certificate access fee

Registration certificate access is free.

9.1.3. Registration certificate status information access fee

Access to the RCRL information is free.

9.1.4. Fee for other services

Not applicable.

9.1.5. Refund policy

Not applicable.

9.2. FINANCIAL LIABILITY

9.2.1. Insurance protection

The RCA RK does not provide insurance protection to any of the RCA RK PKI participants.

9.2.2. Other financial liability

Not applicable.

9.2.3. Scope of insurance and guarantees for end entities

Not applicable.

9.3. PRIVACY OF THE RCA RK INFORMATION

9.3.1. RCA RK confidential information

The RCA RK in the course of business processes, receives, uses and stores private information, and the RCA RK shall take all necessary measures to protect it in accordance with the current legislation of the Republic of Kazakhstan. The RCA RK information not considered private.

9.3.2. Information outside confidential

The RCA RK participants recognize that registration certificates, information about their revocation or other information on the status of a registration certificate, a public part of the Register of registration certificates and information contained therein is not considered as confidential information.

9.3.3. Responsibility for RCA RK confidential information protection

The RCA RK is responsible for the protection of the processed, received, used and stored confidential information in accordance with the current legislation of the Republic of Kazakhstan.

9.4. PRIVACY OF PERSONAL DATA

9.4.1. Ensuring confidentiality of personal data of the RCA RK and subordinate CAs.

The RCA RK protects personal data in accordance with the current legislation of the Republic of Kazakhstan. RCA RK does not disclose information that identifies applicants for registration (resubmission) of registration certificates of accredited CAs. In case theRCA RK stops its activity, personal data of subscribers and applicants are transmitted to a successor CA in accordance with the provisions listed in 5.8 выше.

9.4.2. Information considered as personal data

The RCA RK considers as personal data any information on accredited CAs, subordinate CAs and their subscribers, not available on public sources and from the content of registration certificates issued in accordance with the current legislation of the Republic of Kazakhstan.

9.4.3. Information not considered as personal data

The RCA RK does not consider as personal data the information contained in the registration certificate of subordinate CAs and its subscribers, as well as other information, subject to mandatory publication in accordance with the current legislation of the Republic of Kazakhstan. Using of registration certificates by subordinate CAs and their subscribers suggests acceptance hereof and consent to the publication of data, not considered to be confidential.

9.4.4. Responsibility for confidential information protection of subordinate CAs

All employees of the RCA RK, working with personal data of subscribers, are responsible for protection of personal data of subordinate CAs in accordance with the current legislation of the Republic of Kazakhstan.

9.4.5. Notification and consent to the use of personal data

Provision of personal data in the RCA RK means consent to the use of personal data in order to provide services of CA and RCA RK in accordance with the current legislation of the Republic of Kazakhstan.

9.4.6. Disclosure of personal data of subordinate CAs to law enforcement and judicial authorities

The RCA RK provides confidential information on the personal data of subordinate CAs to law enforcement and judicial authorities in accordance with applicable legislation of the Republic of Kazakhstan.

9.4.7. Other bases for disclosure pf personal data of subordinate CAs

Not applicable.

9.5. INTELLECTUAL PROPERTY RIGHTS

The RCA RK retains the intellectual property rights for the registration certificates of subordinate CAs that it registers (reassigns), and for the information about their status. At the same time RCA RK does not prohibit copying and distribution of registration certificates of subordinate CAs on a nonexclusive free-of-charge basis, subject to the conditions of completeness of copying registration certificates in accordance with the terms of the agreement, made with subordinate CAs. RCA RK also does not prohibit the use of information on the status of the registration certificates of subordinate CAs for the implementation of the relying party functions.

Subordinate CAs recognize the intellectual property rights of the RCA RK for this Policy and other documentation of NVC RK, regulating the activities of the RCA RK and subordinate CAs.

Subordinate CAs retain all the rights for all trade and similar brands and names contained in the application for the issuance (reassignment) of registration certificates and distinctive (DN-) names in the issued registration certificate of subordinate CAs.

Key pairs that correspond to the registration certificate issued or reassigned by RCA RK, are the property (including intellectual) of the correspondent participants of the RCA RK PKI, regardless of the physical media in which

these key pairs are stored and protected. In particular, public keys, RCA RK registration certificates and parts of the secret of private RCA RK keys are the property (including intellectual property) of the RCA RK.

9.6. RESPONSIBILITIES

9.6.1. RCA RK responsibilities

The RCA RK is responsible for:

1) creation of electronic digital signature keys taking measures to protect private key of electronic digital signature against unauthorized access;

2) issue, registration, revocation, storage of registration certificates, maintaining the register of registration certificates issued in the established order;

2-1) approval of rules of application a registration certificate for each type of registration certificate;

3) accounting of valid and revoked registration certificates;

4) proof of ownership and validity of public key of electronic digital signature, registered by certification authority in accordance with the legislation of the Republic of Kazakhstan;

RCA RK is obliged to take all necessary measures to prevent the loss, modification, and falsification of stored electronic digital signature public keys.

For not fulfilling the obligations provided for in paragraph above, RCA RK is responsible in accordance with the current legislation of the Republic of Kazakhstan.

9.6.2. CA responsibilities

CA is responsible for:

- documents acceptance and check;
- applier's identification;
- issue of a reassigned registration certificate to an applier;
- storing the documents for appliers' registration certificates issue.

9.6.3. Subscriber's responsibilities

The owner of the registration certificate shall have the right to require revocation of the registration certificate in cases where it involves violation of the access to the electronic digital signature private key corresponding to the public key specified in the registration certificate.

The owner of the registration certificate has to:

1) provide reliable information to a certifying center;

2) use the private key corresponding to the public key listed in the registration certificate;

3) take measures to protect his electronic digital signature private key from unauthorized access and use, as well as to store public keys in accordance with the legislation of the Republic of Kazakhstan.

9.6.4. Responsibilities of relying parties

Not applicable.

9.6.5. Responsibilities of other participants

Not applicable.

9.7. GUARANTEES REVOCATION

Not applicable.

9.8. LIMITATION OF LIABILITY

Not applicable.

9.9. GUARANTEES

9.9.1. RCA RK guarantees

The RCA RK guarantees:

- absence in the issued or reassigned registration certificates of subordinate CAs of intentional falsification of facts, input there or known by RCA RK;
- absence in the information of the issued or reassigned registration certificates of RCA RK and subordinate CAs of accidental mistakes made by RCA RKTC due to negligence in the processing of applications for registration (reassignment) or during registration (reassignment) of registration certificates;
- compliance of registration certificates of the RCA RK and subordinate CAs with the requirements of the legislation of the Republic of Kazakhstan, the essential requirements of the corresponding Policy to apply the registration certificates and these Regulations;
- compliance of services of registration certificates revocation with the requirements of current legislation of the Republic of Kazakhstan, the essential requirements of the corresponding Policy to apply the registration certificates and these Regulations in all material aspects.

In addition, RCA RK is obliged to ensure conditions for implementation of guarantees and assurances of subscriber and relying party, as set before in these Rules, in 9.9.2. ниже and in 9.9.3. ниже.

9.9.2. Guarantees of subordinate CAs

Subordinate CAs guarantee the realization of the following conditions:

3. for each EDS formed using the private key that matches the public key listed in the registration certificate of the subordinate CA that:

- this EDS belongs to the subordinate CA;
- the corresponding registration certificate was accepted by a subscriber;
- the corresponding registration certificate has not expired, was not revoked, and its validity is not suspended at the time of formation of the EDS;
- their private keys are protected, and no unauthorized person have never had access to them;
- all the information provided by the subordinate CA for the application for registration (reassignment) of the registration certificate is accurate;
- all the information contained in the registration certificate of the subordinate CA, is reliable;
- the registration certificate is being used in accordance with:
    - the current legislation of the Republic of Kazakhstan;
    - essential requirements of the Policy to apply registration certificates of the RCA RK;
    - essential requirements hereof;
- subscribers of the subordinate CA are not certifying authorities and do not use private keys that correspond to the public keys specified in the registration certificate, for electronic digital signature of any of the registration certificates (or any other format of the public key certificates) or lists of revoked registration certificates.

In addition, the subordinate CA is obliged to comply with the conditions of guarantees and assurances of the relying party set before in these Regulations in 9.9.3. ниже.

9.9.3. Guarantees of relying parties

Relying parties guarantee the use of the RCA RK registration certificate in accordance with these Regulations and the current legislation of the Republic of Kazakhstan

9.10. VALIDITY PERIOD AND PROCEDURE OF TERMINATION

9.10.1. Entry into legal force

These Regulations come into effect immediately upon publishing them on the RCA RK Internet resource.

9.10.2. Procedure of termination

These Regulations remain in effect until replacement by a new version over the functioning of the RCA RK. Replacement by a new version is carried out in accordance with 1.6 выше.

9.10.3. Legal consequences of termination

Starting upon termination hereof, subordinate CAs and RCA RK participants are contingent with the latest version hereof for all registration certificates until the expiration of each of the registration certificates.

9.11. INDIVIDUAL NOTIFICATIONS AND INTERACTION WITH THE PARTICIPANTS

The RCA RK uses any of the available methods of the official notification of participants of the RCA RK PKI, subordinate CAs and participants of PKI of subordinate CAs.

Questions of interaction of the RCA RK PKI participants with each other are not regulated.

9.12. AMENDMENTS

9.12.1. Making amendments

Amendments to the Regulations are prepared by PLI service and documented in the form of a separate document containing either the text of the Regulation or notification of changes and additions to its actual text.

Publication of an actual edition of the Regulations or the notification about changes and additions made to it is carried out on the official web-site of the RCA RK at: http://root.gov.kz.

9.12.2. Mechanism and period of notice

The RCA RK retains the right to make minor changes and additions to these Regulations without prior notice, including, but without limitation to correcting typos, change of addresses, links and contact information. Decisions about whether these changes and additions are significant or not are accepted purely at discretion of the RCA RK.

9.12.3. Reasons for which the object identifier is to be changed

If, due to amendments and additions to these Rules RCA RK determined the need to change the object identifiers in the relevant Policy to apply registration certificates, new object identifiers for each type of registration certificate shall be specified in the actual text hereof, which must come into effect simultaneously with changes and amendments to these Regulations

9.13. PROCEDURE OF SETTLEMENT OF DISAGREEMENTS

Disagreements occurring in the course of business or provision of public services should be settled by agreement of the parties and the parties should take all efforts to settle the disagreement. Unsettled disagreements are dealt with in the courts of Astana in accordance with the legislation of the Republic of Kazakhstan.

9.14. APPLICABLE LEGISLATION

Validity, interpretation hereof shall be in accordance with the applicable legislation of the Republic of Kazakhstan.

9.15. COMPLIANCE WITH THE APPLICABLE LEGISLATION

Validity, interpretation hereof shall be in accordance with the applicable legislation of the Republic of Kazakhstan.

9.16. OTHER REGULATIONS

9.16.1. Completeness of the agreement

Not stipulated.

9.16.2. Assignment of rights

Not applicable.

9.16.3. Divisibility

In case a part of the provisions hereof is found to be unenforceable by a court or an authorized state body, the rest of it remains in force.

9.16.4. Right of use (attorney compensation and abandonment of rights)

Not stipulated.

9.16.5. Force majeure

Not stipulated.

9.17. OTHER PROVISIONS

Not stipulated.