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, «__» _____

POLICY FOR USE OF REGISTRATION CERTIFICATES OF SUBSCRIBERS OF THE ROOT CERTIFICATION AUTHORITY OF THE REPUBLIC OF KAZAKHSTAN (CERTIFICATE POLICY)

Version 2.0

Astana, 2016

VERSION CONTROL

No.	Status	Date	Author	Revision description
2.0				
1.0				

CONTENTS

TERMS AND ABBREVIATIONS

This document uses the following terms:

Term	Definition
Policy	Policy of use of a registration certificates of subscribers of the Root Certification Authority of the Republic of Kazakhstan (Certificate Policy)
Registration certificate	Document on paper or an e-document, issued by the certification authority for confirmation of compliance to EDS requirements, specified by regulatory legal acts of the Republic of Kazakhstan

This Policy uses the following abbreviations:

Abbreviation	Definition
RFC	(Request for Comments) Document from series of numbered information documents of the Internet, containing technical specifications and standards, widely applied in the world network
TSP	(Time Stamp Protocol) Cryptographic protocol, which allows to create evidence of fact of e-document existence for the time being
WebTrust	International standard "Trust Service Principles and Criteria for Certification Authorities Version 2.0" ("Trust Service Principles and Criteria for Certification Authorities Version 2.0")
PKI	(Public Key Infrastructure) Complex of informational systems, organizational and technical arrangements, aimed to control of a registration certificates in accordance with the law of the Republic of Kazakhstan concerning e-document and electronic digital signature
RCA RK	(Root Certification Authority of the Republic of Kazakhstan) Certification Authority conforming the compliance and validity of public keys of electronic digital signature of certification authorities
MIC RK	(Ministry of Information and Communication of the Republic of Kazakhstan)
NCA RK	(National Certification Authority of the Republic of Kazakhstan) Certification authority, which services SUBSCRIBERS of "electronic government", state and non-state informational systems
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)
RK	Republic of Kazakhstan
RCRL	(Registration Certificate Revocation List) A list of all the NCA RK subscriber's registration certificates, revoked by the time the RCRL has been issued
CA	Certification Authority

1. INTRODUCTION

This document contains the Policy for use of a registration certificates of subscribers of the Root Certification Authority of the Republic of Kazakhstan (Certificate policy) (hereinafter referred to as the Policy). Policy defines activity of the Root Certification Authority of the Republic of Kazakhstan (hereinafter referred to as the RCA RK) concerning services, related to the lifecycle of a registration certificates RCA RK and registration certificates of subordinated certification authorities (hereinafter referred to as the CA), as well as sets legal and technical requirements for subordinated CA necessary for issuance, revocation and use of a registration certificates. Policy defines the types of a registration certificates, issued by RCA RK, the scope of their application, as well as the related verification procedures.

RCA RK was established in order to conform the compliance and validity of public keys of electronic digital signature hereinafter referred to as the EDS) of the CA. RCA RK operates in accordance with the following regulatory legal acts of the RK:

- Law of the RK No. 370-II "Concerning e-document and electronic digital signature" dated January 7, 2003;
- Law of the RK "On informatization" dated November 24, 2015;
- Order No. 1184 of the Minister of Investments and Development of the RK "On Approval of the Model Regulation of Certification Authority" dated December 9, 2015;
- Order No. 727 of the Acting Minister of Investments and Development of the RK "On Approval of the Rules for issue, storage, revocation of a registration certificates and confirmation of the compliance and validity of public key of electronic digital signature by the Root Certification Authority of the RK, Certification Authority of State Bodies and National Certification Authority of the RK" dated June 26, 2015;
- Government Regulation of the RK No. 1222 "On Approval of Rules for Accreditation of Certification Authorities" dated November 19, 2010;
- ST RK 1073-2007. Means of cryptographic information protection. General requirements.

This Policy meets the requirements of the following standards that are relevant at the time of publication of the Policy:

- principles and criteria of international standard WebTrust 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 Publicly-Trusted Certificates, version 1.1.9;
- recommendations of guideline for the policy development of use of a registration certificates and instructions for use of the registration certificates of public key infrastructure in accordance with standard X.509 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" hereinafter referred to as the "RFC 3647").

1.1. OVERVIEW

This Policy is applicable to all subscribers of the Certification Authorities System of the Republic of Kazakhstan, hereinafter referred to as the CAS RK), who use registration certificates issued by the subordinated CA (RCA RK issues registration certificates only to subordinated CA RCA RK on the condition of their accreditation by the authorized body. RCA RK does not issue registration certificates to end-users, but only certifies subordinated CA).

This Policy is directed to:

- Subordinated CA;
- Relying Parties;
- Holders of Registration Certificates;

This Policy consists of 9 sections. Policy is a high-level document belonging to RCA RK; more detailed information is set out in Rules for use of a registration certificates of the Root Certification Authority of the Republic of Kazakhstan (Certificate Practice Statement) (hereinafter referred to as the Rules). In order to retain the conformity of Policy structure to principles and criteria of international standard WebTrust and recommendations RFC 3647 section, the PKI RCA RK that are not applicable to practices contain mark "not applicable" or "not stipulated".

1.2. NAME AND IDENTIFICATION OF THE DOCUMENT

Name of this document	Policy of use of a registration certificates of subscribers of the Root Certification Authority of the Republic of Kazakhstan (Certificate policy)
Document Version	2.0
Bring into force	by Order of the Director RSE "STS" No. ___ dated day-month-year.
Link to the active version of the document	http://root.gov.kz

1.3. SUBSCRIBERS OF PKI RCA RK

1.3.1. RCA RK

The RCA RK is the Certification Authority that issues (resubordinates) registration certificates to accredited CA.

The RCA RK carries out activities directly related to CA RK, which is:

- receipt and processing of requests for issuing (resubordination) and registration certificates revocation of accredited CA;
- issuing (resubordination) and registration certificates revocation of accredited and subordinated CA;
- publication and support of subordinated Registration Certificate Revocation Lists of subordinated CA hereinafter referred to as the RCRL);
- support of a registration certificates' register;
- storage of a registration certificates.

1.3.2. Accredited CA

Accredited CA is CA that officially designated as the authorized body in the field of informatization by the competent CA in providing services in accordance with the law of the Republic of Kazakhstan.

1.3.3. Subordinated CA

Subordinated CA is accredited CA.

1.3.4. Subscribers of subordinated CA

Subscriber of subordinated CA is a holder of a registration certificate, a person or an entity on behalf of which the registration certificate of the subscriber was issued by the subordinated CA, lawfully in possession of the private key corresponding to the public key specified in the registration certificate of subscriber.

1.3.5. Relying parties

Relying party is an entity which takes action based on the subscriber's registration certificate issued by the subordinated CA. Relying party can be a subordinated CA or a subscriber of subordinated CA.

1.3.6. CAS RK

In order to create the foundation of a common trust space between the subscribers of information exchange in the Republic of Kazakhstan the infrastructure of the CA RK system is functioning. Subscribers of the CAS RK are:

- RCA RK;
- subordinated CA, including:
  - NCA RK;
  - CA SB RK;
- holders of a registration certificates of subordinated CA.

See more information in the Regulations.

1.4. USE OF REGISTRATION CERTIFICATE OF SUBORDINATED CA

1.4.1. Use of a registration certificates of subordinated CA

Registration certificates of subordinated CA are applicable for the following purposes:

- issuance and revocation of a registration certificates for applicants of subordinated CA;
- conforming the compliance and validity of public key of EDS by the verification.

1.4.2. Requirements for use of a registration certificates of subordinated CA

The use of a registration certificates of the subordinated CA should not contradict the current legislation of the Republic of Kazakhstan, as well as the requirements of this Policy.

See more information in the Regulations.

1.5. POLICY MANAGEMENT

1.5.1. Organization that administers the document

Name of the organization	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
Actual address	16, Kuyshi Dina str., Astana, Republic of Kazakhstan, 010000
Legal address	1/1, Zhirentaeva str, Astana, Republic of Kazakhstan, 010000
Electronic mail address	info@sts.kz
Reception phone number	+7(7172) 55 99 22
Chancellery phone number	+7(7172) 55 81 15
Technical support phone number	8-800-080-7777

1.5.2. Contact person

Name of subdivision	Department of Infrastructure Solutions
Position name	Chief Specialist of cross-border and interdepartmental cooperation sector of Public Key Infrastructure Service of Infrastructure Solutions Department RSE "STS"
Electronic mail address	b_kenzhebulatov@sts.kz
Contact phone number	+7(7172) 55 99 99 (ex.398)

1.5.3. Person who determines the compliance of the CA with requirements of policy

Position name	Director of RSE "STS"
Electronic mail address	info@sts.kz
Contact phone number	+7(7172) 55 99 22

Director of RSE "STS" is responsible for the conformity assessment of this Policy to the Rules.

Director of RSE "STS" is responsible for defining the general requirements for public key infrastructure to this Policy.

1.5.4. Policy qualification procedure

Proposals for alterations or additions to the Policy are introduced by the executive officials of the RCA RK and approved by the order of Director of RSE "STS" or another authorized person. Alterations or additions to the Policy are accompanied by the verification of Rules for use of a registration certificates of the RCA RK for compliance with the new version of the Policy and, if necessary, Rules for use of a registration certificates of the RCA RK are brought into compliance with new version of the Policy.

Approved, modified or amended Policy is published on the Internet resource of the RCA RK as a separate document containing the full text of the Policy or notifications of making alterations or alterations themselves specifying the sequential increasing number of Policy Version. All the repealed Policy Versions remain published on the Internet resource of the RCA RK. All the repealed Policy Versions are provided with a mark stating the approval dates of Policy and a link to the current Policy Version.

2. LIABILITY REGARDING PUBLICATION AND STORAGE

2.1. STORAGE AND PUBLIC INFORMATION ACCESSIBILITY

RCA RK provides public accessibility 24-h/7-day of the following materials on the official Internet resource of the RCA RK:

- root registration certificate of the RCA RK by RSA algorithm available at http://root.gov.kz/cert/root_rsa.cer;
- root registration certificate of the RCA RK by GOST algorithm available at http://root.gov.kz/cert/root_gost.cer;
- object identifiers of the Republic of Kazakhstan;
- RCRL;
- Policy of use of a registration certificates of the RCA RK;
- These Rules.

RCRL retention period in the registration certificates' register is not less than five years, at the same time revoked registration certificates are in RCRL until the expiry date of a registration certificate.

Upon the expiry of storage period of RCRL in the registration certificates' register RCRL (out-of-date) goes to the archive storage in accordance with the applicable legislation of the Republic of Kazakhstan.

2.2. PUBLICATION OF INFORMATION ON REGISTRATION CERTIFICATES

RCRL of the RCA RK is available in electronic format and in format specified by the RFC 5280 recommendations (Certificate and Certificate Revocation List (CRL) Profile), as well as by these Rules. RCA RK publishes the following types of RCRL:

- RCRL for RSA registration certificates available at: http://crl.root.gov.kz/rsa.crl;
- RCRL for GOST registration certificates available at: http://crl.root.gov.kz/gost.crl.

2.3. PERIOD OF INFORMATION PUBLICATION

RCRL is issued and published not less than 1 time per 35 days. The period of validity of RCRL is not more than 35 days.

2.4. CONTROL OF ACCESS TO PUBLIC INFORMATION

The RCA RK implements the information and physical security measures as to prevent unauthorized entering, altering or deleting the information contained in RCRL and information system of the RCA RK.

3. IDENTIFICATION AND AUTHENTICATION

3.1. NAMING

All registration certificates of subordinated CA shall contain the distinguished names in DN-name in the format recommended by the standard X.501 "Information technology - Open Systems Interconnection - The Directory: Models" of a series of recommended standards ITU-T X.500.

See more information in the Regulations.

3.2. VERIFICATION (IDENTIFICATION) OF APPLICANTS IN THE ISSUANCE (RESUBORDINATION) OF REGISTRATION CERTIFICATES OF ACCREDITED CA

Identification of accredited CA is carried out on the basis of an application for registration (resubordination) of a registration certificate of accredited CA. The application should comply with the requirements of the legislation of the Republic of Kazakhstan.

More information is set out in the Regulations.

3.3. VERIFICATION (IDENTIFICATION) OF APPLICANT IN THE REISSUE OF REGISTRATION CERTIFICATE OF SUBORDINATED CA

The RCA RK excludes the replacement of key pairs in the current subordinated registration certificates of subordinated CA.

See more information in the Regulations.

3.4. VERIFICATION (IDENTIFICATION) OF RCA RK SUBSCRIBER IN THE REVOKE OF SUBORDINATED REGISTRATION CERTIFICATE OF SUBORDINATED CA

Revoke of the registration certificate is carried out on basis of application. The application should comply with the requirements of legislation of the Republic of Kazakhstan.

See more information in the Regulations.

4. OPERATIONAL REQUIREMENTS FOR THE LIFECYCLE OF REGISTRATION CERTIFICATE OF SUBORDINATED CA

4.1. APPLICATION FOR REGISTRATION (RESUBORDINATION) OF REGISTRATION CERTIFICATE OF SUBORDINATED CA

Accredited CA may apply for registration (resubordination) of the registration certificate of subordinated CA.

See more information in the Regulations.

4.2. PROCESSING OF APPLICATION FOR REGISTRATION (RESUBORDINATION) OF REGISTRATION CERTIFICATE OF SUBORDINATED CA

See more information in the Regulations.

4.3. ISSUE (RESUBORDINATION) OF REGISTRATION CERTIFICATES OF SUBORDINATED CA

The registration certificate of subordinated CA is registered (resubordinated) by the RCA RK based on the application.

See more information in the Regulations.

4.4. ADOPTION OF REGISTRATION CERTIFICATE OF SUBORDINATED CA

The RCA RK publishes information about the issue of a new subordinated registration certificate or resubordination of the existing registration certificate on the Internet resource of the RCA RK in the "News" section available at http://root.gov.kz/novosti.html.

See more information in the Regulations.

4.5. USE OF KEY PAIR AND REGISTRATION CERTIFICATE OF SUBORDINATED CA

The registration certificate of subordinated CA should be used only in accordance with:

- the current legislation of the Republic of Kazakhstan;
- this Policy;

The responsibility of subordinated CA is to protect the private keys and activation data from unauthorized access in accordance with the requirements of current legislation of the Republic of Kazakhstan. Subordinated CA shall not be entitled to use the time-expired private keys or in the case of revocation of the corresponding registration certificate.

See more information in the Regulations.

4.6. RENEWAL OF REGISTRATION CERTIFICATE OF SUBORDINATED CA

The RCA RK excludes the data alteration in the registration certificate of subordinated CA, including the period of validity of a registration certificate.

See more information in the Regulations.

4.7. RESUBORDINATION OF REGISTRATION CERTIFICATE

See more information in the Regulations.

4.8. ALTERATION OF CERTIFICATE

See more information in the Regulations.

4.9. REVOCATION OF REGISTRATION CERTIFICATE OF SUBORDINATED CA

Revocation of a registration certificate of subordinated CA is carried out on basis of an official letter from subordinated CA on paper.

See more information in the Regulations.

4.10. SERVICES OF STATUS VERIFICATION OF A REGISTRATION CERTIFICATE OF SUBORDINATED CA

See more information in the Regulations.

4.11. TERMINATION OF SUBSCRIPTION

Subordinated CA has a right to revoke their registration certificates before its expiry.

See more information in the Regulations.

4.12. DEPOSITION AND RESTORATION OF A KEY PAIR

The RCA RK does not carry out the deposition and restoration of key pairs of subordinated CA.

5. MANAGEMENT, OPERATIONAL AND PHYSICAL CONTROL OF RCA RK ASSETS

5.1. PHYSICAL SECURITY CONTROL OF RCA RK ASSETS

RCA RK provides physical security of the RCA RK systems in accordance with the current legislation of the Republic of Kazakhstan. Detailed policies and procedures of physical security arrangements contain confidential information of the RCA RK therefore not published.

See more information in the Regulations.

5.2. RESPONSIBILITY AND CONTROL IN THE ACTIVITIES OF THE RCA RK

The RCA RK provides the necessary number of subdivisions and employees for the internal control system operation. The RCA RK takes alternative control measures based on risk assessment in case of vacancy of staffing position necessary for monitoring.

See more information in the Regulations.

5.3. SECURITY PROTECTION OF RCA RK EMPLOYEES

The RCA RK provides security of the RCA RK employees in accordance with:

- internal policies of the RCA RK on organization of physical security;
- legislation of the Republic of Kazakhstan.

See more information in the Regulations.

5.4. DOCUMENTING OF EVENTS (LOGGING) IN RCA RK INFORMATION SYSTEM

The RCA RK carries out the log keeping and storage for the following event types:

- Lifecycle events of the RCA RK keys and subordinated CA;
- Lifecycle events of the RCA RK keys and RCA RK clients;
- Lifecycle management events of cryptographic hardware;
- Events of deposit/receipt of cryptographic hardware;
- Events of application for issuance of a registration certificate;
- Lifecycle management events of a registration certificate;
- Events related to security.

If the logging of any of above-listed items is found impossible, the RCA RK uses alternative technical and organizational measures in order to minimize risks.

The RCA RK excludes recording in an explicit form of keys and passwords.

See more information in the Regulations.

5.5. ARCHIVES

The RCA RK provides archive storage of the following types of information in compliance with the current statutory requirements of the Republic of Kazakhstan:

- event logs;
- current, revoked and expired registration certificates of subordinated CA;
- current, revoked and expired registration certificates of the RCA RK;
- applications for registration (resubordination) and registration certificates revocation of subordinated CA;
- Registration Certificate Revocation Lists of the RCA RK and subordinated CA.

See more information in the Regulations for use of subscribers' registration certificates of Root Certification Authority of the Republic of Kazakhstan.

5.6. KEY CHANGE OF THE RCA RK

The RCA RK carries out a change of key pairs and registration certificates of the RCA RK upon the expiration of a registration certificate of the RCA RK or in the case of compromise of key pairs of the RCA RK.

See more information in the Regulations for use of subscribers' registration certificates of Root Certification Authority of the Republic of Kazakhstan.

5.7. COMPROMISE AND DISASTER RECOVERY OF KEYS OF THE RCA RK

The procedures take place upon events in RCA RK, as well as if found the compromise or suspected of compromise of the RCA RK private keys in accordance with the requirements of legislation of the Republic of Kazakhstan and internal rules of the RCA RK in order to:

- assess and categorize the event;
- take preventive or recovery measures for events consequences in accordance with the risk assessment of the RCA RK.

See more information in the Regulations.

5.8. CESSATION OF ACTIVITIES OF THE RCA RK

In case of need to cease the activities of the RCA RK, the RCA RK takes all measures necessary for advance notification of subordinated CA and subscribers of the PKI RCA RK on this matter.

See more information in the Regulations.

6. TECHNICAL SAFETY CONTROL OF THE RCA RK

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

Subordinated CA generate their key pairs on their own, as well as individually determines policy in relation to generation of key pairs of its subscribers.

The RCA RK individually generates all key pairs used in the RCA RK. Generation of key pairs is carried out by means of cryptographic modules certified for compliance with the applicable standard of the Republic of Kazakhstan ST RK 1073-2007 at the level not lower than the third.

Generation of key pairs of the RCA RK is carried out solely in accordance with the approved internal rules with the participation of competent executive officials and under the supervision of an independent party. Generation ceremony of key pairs of the RCA RK is recorded officially by the relevant protocol under the signature of all participants of the ceremony. Protocols are stored and archived in compliance with the current statutory requirements of the Republic of Kazakhstan and internal rules of the RCA RK.

See more information in the Regulations.

6.2. SECURITY CONTROL OVER THE PRIVATE KEYS OF THE RCA RK AND SUBORDINATED CA, AS WELL AS LIFECYCLE MANAGEMENT OF CRYPTOGRAPHIC HARDWARE OF THE RCA RK

The RCA RK maintains inner control environment in order to protect private keys of the RCA RK and safe lifecycle management of cryptographic hardware of the RCA RK.

Cryptographic hardware of the RCA RK is certified for compliance with the applicable standard in the Republic of Kazakhstan ST RK 1073-2007, defining the general technical requirements to the means of cryptographic information protection for compliance not lower than the third level of security. All cryptographic modules used by RCA RK are certified against the requirements of applicable standard in force of the Republic of Kazakhstan ST RK 1073-2007 not lower than by the third level. Use of non-certified cryptographic modules is not allowed in accordance with the internal rules of the RCA RK, this Policy and Rules.

The RCA RK implements a number of technical and organizational measures to ensure the confidentiality and integrity of cryptographic hardware during transportation, commissioning works and operation at the main and reserve facilities of the RCA RK. The RCA RK also implements a number of technical and organizational measures to ensure the operation and maintenance of cryptographic hardware in strict accordance with its technical and operational documentation, as well as the internal rules of physical security and rules of procedure.

See more information in the Regulations.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT OF RCA RK

See more information in the Regulations.

6.4. ACTIVATION DATA

See more information in the Regulations.

6.5. COMPUTER SECURITY CONTROL

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

The RCA RK performs periodic vulnerability assessments in the infrastructure with risk assessment and further risk handling.

See more information in the Regulations.

6.6. SAFETY LIFECYCLE CONTROL

The RCA RK provides functioning of safety management control in accordance with the requirements of ST RK ISO/MEK 27001 standard.

See more information in the Regulations.

7. PROFILES OF A REGISTRATION CERTIFICATE OF SUBORDINATED CA AND RCRL

7.1. PROFILE OF A REGISTRATION CERTIFICATE OF SUBORDINATED CA

The RCA RK issues registration certificates in electronic format in the format based on the recommendations of X.509v3 and RFC 5280.

See more information in the Regulations for use of subscribers' registration certificates of Root Certification Authority of the Republic of Kazakhstan.

7.2. PROFILE OF OCSP

The RCA RK does not use OCSP.

8. COMPLIANCE AUDIT

Inner control environment of the RCA RK is verified for compliance with the requirements of international standard WebTrust. The independent audit companies licensed by the owner of standard WebTrust carry out verifications.

All subordinated CA shall provide to RCA RK certificates of successful certification for compliance with the requirements of international standard WebTrust at least once a year. The absence of timely confirmation of compliance with the requirements of standard entails the revoke of a registration certificate of subordinated CA.

8.1. AUDIT PERFORMANCE PERIODICITY

Audit of inner control environment of the RCA RK for compliance with requirements of the international standard WebTrust (external audit) is carried out not less than once a year.

8.2. AUDITORS AND THEIR QUALIFICATION

Independent audit organizations licensed by the owner of international standard WebTrust to conduct certification audit for compliance with the international standard WebTrust perform audit of inner control environment of the RCA RK for compliance with requirements of international standard WebTrust.

8.3. RELATIONS BETWEEN THE RCA RK AND AUDIT ORGANIZATIONS

Audit companies verifying the inner control environment of the RCA RK for compliance with requirements of international standard WebTrust are independent of the RCA RK, RSE "STS" and MIC RK.

8.4. AUDIT TASKS

Audit of inner control environment of the RCA is carried out in accordance with international standard WebTrust for Certification Authorities. The scope of verifications includes the following sections of the international standard WebTrust:

1) Disclosure of business practices of the RCA RK;

2) Environmental control of the RCA RK;
3) Keys lifecycle control of the RCA RK;
4) Lifecycle management control of a registration certificates of subordinated CA.

See more information in the Regulations.

8.5. MEASURES ATTEMPTED IN THE DETECTION OF DEFECTS AND VIOLATIONS

See more information in the Regulations for use of subscribers' registration certificates of the Root Certification Authority of the Republic of Kazakhstan.

8.6. NOTIFICATION OF THE RESULTS

See more information in the Regulations for use of subscribers' registration certificates of Root Certification Authority of the Republic of Kazakhstan.

9. LEGAL AFFAIRS

9.1. PAYMENT FOR SERVICES

The RCA RK does not charge for the service provision of the PKI RCA RK.
See more information in the Regulations.

9.2. FINANCIAL LIABILITY

The RCA RK does not give the insurance coverage to any of the subscribers of the PKI RCA RK.

See more information in the Regulations.

9.3. INFORMATION CONFIDENTIALITY OF THE RCA RK

The RCA RK in the course of its activities processes, receives, uses and stores confidential information, at the same time the RCA RK takes all necessary measures for its protection in accordance with the current legislation of the Republic of Kazakhstan. Information of the RCA RK shall not be regarded as confidential.

See more information in the Regulations.

9.4. CONFIDENTIALITY OF PERSONAL DATA

The RCA RK provides protection of personal data in accordance with the current legislation of the Republic of Kazakhstan. The RCA RK does not disclose information that identifies the applicants for registration (resubordination) of a registration certificates of accredited CA.

See more information in the Regulations.

9.5. INTELLECTUAL PROPERTY RIGHTS

The RCA RK reserves the intellectual property rights to registration certificates of subordinated CA, which it registers (resubordinates), and information on their status. At the same time the RCA RK does not prohibit copying and distribution of a registration certificates of subordinated CA on non-exclusive non-repayable basis, subject to the conditions of completeness of copying and use of a registration certificates in accordance with the terms of concluded contracts with subordinated CA. The RCA RK also does not prohibit the use of information on the status of a registration certificates of subordinated CA to perform functions of relying party.

Subordinated CA recognizes the intellectual property right of the RCA RK of this Policy and other documentation of the RCA RK regulating the activities of the RCA RK and subordinated CA.

Subordinated CA retains all the rights to all trade and the like brands and names contained in the applications for registration (resubordination) of a registration certificates and distinguished (DN-) names in the issued registration certificates of subordinated CA.

Key pairs that correspond to the registration certificates issued or resubordinated by RCA RK constitute property (including intellectual) of the respective subscribers of PKI RCA RK regardless of physical media, which store these key pairs and through which they are protected. In particular, public keys of a registration certificates of the RCA RK and parts of private key secret of the RCA RK are the property (including intellectual) of the RCA RK.

9.6. RESPONSIBILITIES

See more information in the Regulations.

9.7. WARRANTIES REVOCATION

See more information in the Regulations.

9.8. LIABILITY RESTRICTION

See more information in the Regulations.

9.9. WARRANTIES

See more information in the Regulations.

9.10. VALIDITY AND TERMINATION PROCEDURE

This Policy becomes effective on the date of its publication in the Internet resource of the RCA RK. This Policy remains in effect until the replacement of new version over the functioning of the RCA RK.

9.11. PERSONAL NOTIFICATIONS AND INTERACTION WITH SUBSCRIBERS

The RCA RK uses any available methods of formal notification of subscribers of the PKI RCA RK, subordinated CA and subscribers of the PKI of subordinated CA.

9.12. AMENDMENTS

The Public Key Infrastructure Service prepares alterations and additions to the Policy that presented in a form of separate document containing either actual text of the Policy or notification of alterations and additions to its actual text.

Publication of actual version of the Policy or notifications of alterations and additions is made on the official Internet resource of the RCA RK at: http://root.gov.kz.

9.13. DISPUTE SETTLEMENT PROCEDURE

Disputes arising in the course of activities or provision of public services shall be settled as agreed by the parties, and the parties shall take best efforts to solve any emerged disputes. Unsettled disputes shall be reviewed in the court of Astana in accordance with the legislation of the Republic of Kazakhstan.

9.14. CURRENT LEGISLATION

See more information in the Regulations.

9.15. COMPLIANCE WITH CURRENT LEGISLATION

See more information in the Regulations.

9.16. OTHER REGULATIONS

See more information in the Regulations.

9.17. OTHER PROVISIONS

See more information in the Regulations.