REPUBLICAN STATE ENTERPRISE ON THE RIGHT OF ECONOMIC USE "STATE TECHNICAL SERVICE" OF THE MINISTRY OF INFORMATION AND COMMUNICATION LINES 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, «13» 09 _____

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

Version 2.0

Astana, 2016

VERSION CONTROL

No.	Status	Date	Author	Revision Description
2.0	Current	13.09.2016	Dosanov G.K.	Policy are brought into compliance with the requirements of the international standard Web Trust
1.0	Terminated	22.05.2015	Seifullina A.O.	-

Contents

TERMS AND ABBREVIATIONS

The following terms are used herein:

Term	Definition
Policy	Policy for use of registration certificates of subscribers of the Root Certification Authority of the Republic Kazakhstan
Registration Certificate	A paper document or an e-document issued by the Certification Authority to confirm the compliance with the EDS requirements specified by laws and regulations of the Republic of Kazakhstan
Internal Control Environment	Complex of process controls used by the RK NCA
RK NCA Work Log	The RK NCA IS record file containing events in a chronological order
Internet Resource of the RK NCA	Internet resource of the RK NCA www.pki.gov.kz
Key Pair	A set consisting of two keys: private (secret) key and public key
EDS Public Key	A sequence of electronic digital symbols available to anyone and is designed to confirm the EDS compliance in e-document
Registration Certificate	A paper document or an e-document issued by the certification authority to confirm the EDS compliance to the requirements specified by laws and regulations of the Republic of Kazakhstan

The following abbreviations are used herein:

Abbreviation	Definition
RFC	(Request for Comments) Document from series of numbered Internet information documents containing technical specifications and standards, widely applied in the world network
TSP	(Time Stamp Protocol) A cryptographic protocol allowing to create a fact existence proof for the e-document at a certain moment of time
OCSP	(Online Certificate Status Protocol) Protocol of certificate status inspection
WebTrust	"Trust Service Principles and Criteria for Certification Authorities Version 2.0" International Standard
PKI	(Public Key Infrastructure) A complex of informational systems, organizational and technical arrangements aimed at control of registration certificates in accordance with the legislation of the Republic of Kazakhstan concerning e-document and electronic digital signature
RK RCA	(Root Certification Authority of the Republic of Kazakhstan) Certification Authority confirming the ownership and validity of public keys of electronic digital signature of certification authorities
RK NCA	(National Certification Authority of the Republic of Kazakhstan) A certification authority serving the participants of "e-government", state and non-state informational systems
STS RSE	("State Technical Service" Republican State Enterprise on the Right of Economic Use of the Ministry of Information and Communications of the Republic of Kazakhstan)
RK MIC	Ministry of Information and Communications of the Republic of Kazakhstan
RK	Republic of Kazakhstan
RCRL	(Registration Certificate Revocation List) A list of all the RK NCA subscribers' registration certificates withdrawn by the time the RCRL has been issued
CA	Certification Authority

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
IS	Informational System
OCSP	(Online Certificate Status Protocol) Protocol of the certificate status inspection

1. INTRODUCTION

The present document contains the Policy for use of registration certificates of subscribers of the National Certification Authority of the Republic of Kazakhstan (hereinafter referred to as the Policy). The Policy specifies the RK NCA activity concerning services connected with the life-cycle of the RK NCA registration certificates and is applied to all RK NCA PKI subscribers and members.

The National Certification Authority of the Republic of Kazakhstan has been established for the purposes to provide registration certificates to individuals and legal entities. The National Certification Authority of the Republic of Kazakhstan conducts its activities in accordance to the following laws and regulations of the Republic of Kazakhstan, internal and public documents:

- Law of the Republic of Kazakhstan "On Informatization" dated November, 24, 2015;
- Law of the Republic of Kazakhstan "On Electronic Document and Electronic Digital Signature" dated January, 7, 2003;
- Law of the Republic of Kazakhstan "On Personal Data and Their Security" dated May, 2, 2013;
- Order issued by the Acting Minister of Investments and Development of the Republic of Kazakhstan "On Adoption of Regulations for Issue, Storage, Withdrawal of Registration Certificates and Confirmation of Accessory and Validity of a Public Key for the Electronic Digital Signature by the Root Certification Authority of the Republic of Kazakhstan, a Certification Authority of State Authorities and the National Certification Authority of the Republic of Kazakhstan" No. 727 dated June, 26, 2015
- Order issued by the Minister of Investments and Development of the Republic of Kazakhstan "On Approval of the Standard for the State Service Named "Issuance and Withdrawal of Registration Certificate of the National Certification Authority of the Republic of Kazakhstan" No. 491 (hereinafter referred to as the Standard) dated April, 24, 2015;
- Order issued by the Minister of Investments and Development of the Republic of Kazakhstan "On Approval of the Procedure for the State Service Named "Issuance and Withdrawal of a Registration Certificate of the National Certification Authority of the Republic of Kazakhstan" No. 601 dated May, 25, 2015;
- Order issued by the Minister of Investments and Development of the Republic of Kazakhstan "On Approval of Rules for Verification of Electronic Digital Signature" No. 1187 dated December, 9, 2015;
- Order issued by the Minister of Investments and Development of the Republic of Kazakhstan "On Approval of the Standard Statute of a Certification Authority" No. 1184 dated December, 9, 2015;
- ST RK 1073-2007 "Cryptographic information protection facilities. General requirements";
- Liaison protocol of the Republican State Enterprise on the Right of Economic Use "State Technical Service" of the Committee of Communication, Informatization and Information of the Ministry of Investments and Development of the Republic of Kazakhstan and the Republican State Enterprise on the Right of Economic Use "Public Service Center" of the Ministry of Investments and Development of the Republic of Kazakhstan on rendering the state services "Issuance and Withdrawal of Registration Certificate of the National Certification Authority of the Republic of Kazakhstan";
- Registration Certificate Practice Statement for the RK NCA subscribers (Certificate practice statement).

The present Policy corresponds to the requirements of the following standards effective as of the date of the Policy publication:

- 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 Publicly-Trusted Certificates, version 1.1.9;
- Recommendations to the guidelines on development of the policies for use of registration certificates and instructions on use of registration certificates of public key infrastructure in accordance to the standard X.509 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" (hereinafter referred to as "RFC 3647").

1.1. Review

The present Policy shall be applied to all Subscribers and participants of the RK NCA PKI.

The present Policy consists of 9 sections. The Policy is a high-level document belonged to the RK NCA, more detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan. To secure the structure conformance to the rules, principles and criteria of the WebTrust International Standard and RFC 3647 Recommendations the sections Not applicable to the RK NCA PKI practices contain the note "Not applicable" or "Not stipulated".

1.2. Name and Identification of the Document

Name of the Present Document	Policy for Use of Registration Certificates of the National Certification Authority of the Republic of Kazakhstan
Version of the Document	2.0
Effected from	By Order of the Director of STS RSE No. 01-04/211 dated 13.09.2016
Link to the Current Version of the Document	http://pki.gov.kz/images/PPRS%20v2/Policy_13.09.16_En.pdf

1.3. Participants of the RK NCA PKI

1.3.1. RK NCA

The RK NCA is a certification authority issuing registration certificates. No other certification authorities are allowed in the RK NCA PKI.

The RK NCA performs the activity directly connected with the PKI, i.e.:

- receipt and process of the applications for issuance and withdrawal of registration certificates;
- issuance and withdrawal of registration certificates of the RK NCA subscribers;
- publication and support of the RCRL and intermediate lists (hereinafter referred to as the delta RCRL);
- process of any applications for the RCRL service;
- putting of the TSP time stamp.

1.3.2. Registration Authorities

Branches of State-owned corporation and the subdivision of STS RSE perform the function of the registration authorities in the RK NCA PKI. The State-owned corporation and STS RSE cooperate on basis of the Liaison Protocol of STS RSE and State-owned corporation for rendering the state services named "Issuance and Withdrawal of the RK NCA Registration Certificate".

More detailed information is specified in the Registration Certificate Practice Statement of subscribers of the National Certification Authority of the Republic of Kazakhstan.

1.3.3. NCA RK Subscribers

A subscriber of the RK NCA is an owner of the RK NCA registration certificate, an individual or a legal entity with a registration certificate issued in its name, who validly possesses a private key corresponding to the public key specified in the registration certificate.

1.3.4. Relying Parties

A relying party is an entity fulfilling any actions based on the registration certificate issued by the RK NCA. A dependent party can be a subscriber of the RK NCA.

1.3.5. Other Members

Not applicable.

1.4. Use of a Registration Certificate of the RK NCA Subscriber

1.4.1. Permitted Use Methods of Registration Certificates for the RK NCA Subscribers

Registration certificates of the RK NCA subscribers are applied for the following purposes:

1. signing any electronic documents with an electronic digital signature;
2. verification of an electronic digital signature;
3. authentication of the RK NCA subscribers in state and non-state IS of the Republic of Kazakhstan;
4. security of information transfer path between a user and the Internet Resource (SSL).

1.4.2. Use Methods of Registration Certificates Forbidden for the RK NCA Subscribers

Use methods for registration certificates of the RK NCA subscribers shall not contradict to the current legislation of the Republic of Kazakhstan, and the requirements hereof.

More detailed information is specified in the Registration Certificate Practice Statement for Subscribers of the National Certification Authority of the Republic of Kazakhstan.

1.5. Policy Management

1.5.1. Organization managing the document

Name of the Organization	"State Technical Service" Republican State Enterprise on the Right of Economic Use of the Ministry of Information and Communications of the Republic of Kazakhstan
Business Address	16 Kuishi Dina St., Astana, Republic of Kazakhstan, 010000
Registered Office	1/1, Zhirentayeva St., Astana, Republic of Kazakhstan, 010000
E-mail	info@sts.kz
Reception Number	+7(7172) 55 99 22
Administrative Office Number	+7(7172) 55 81 15
Technical Support Number	8-800-080-7777

1.5.2. Contact Person

Division Name	Department of Infrastructure Solutions
Position Name	Director of the STS RSE
E-mail	+7(7172) 55 99 99 (int.399)
Contact Number	info@pki.gov.kz

1.5.3. Person Assessing the CA Correspondence to the Policy Requirements

The CA correspondence to the Policy requirements shall be determined by the STS RSE employees.

1.5.4. Procedure for the Rules Qualification

Any alterations or amendments hereto shall be made after their check for correspondence to the Registration Certificate Practice Statement of the RK NCA. Any proposals for alterations or amendments to the Policy shall be made by the RK NCA authorized employees of and approved by the Order of the Director of the STS RSE or an authorized deputy.

The amended or added Policy approved shall be published on the RK NCA Internet resource in the form of a single document containing the complete text of the Policy, or notice on amendments and amendments themselves with an increased version number of the Policy. All outdated versions of the Policy shall be also kept published on the RK NCA Internet resource. All outdated versions of the Policy shall be provided with a mark with specification of the time interval available for effectiveness of the Policy version and a link to the effective version of the Policy.

2. RESPONSIBILITY FOR PUBLICATION AND STORAGE

2.1. Storage and Availability of Public Information

The RK NCA provides public availability of the following materials on the RK NCA Internet resource during twenty-four hours seven days a week:

- Root registration certificate of the RK NCA under the RSA algorithm;
- Root registration certificate of the RK NCA under the GOST algorithm;
- Root registration certificate of the RK RCA under the RSA algorithm;
- Root registration certificate of the RK RCA under the GOST algorithm;
- Policy for use of registration certificates of the RK NCA subscribers;
- Present Policy;
- User agreement;
- List of registration certificates withdrawn;
- Delta RCRL;
- OCSP Services;
- TSP Service.

2.2. Publication of Information on Registration Certificates

The RK NCA RCRL is provided in an electronic form and in the format specified by the RFC 5280 recommendations and the present Policy. The RK NCA publishes the following types of RCRL:

1. RCRL for registration certificates under the RSA algorithm;
2. RCRL for registration certificates under the GOST algorithm.

The RK NCA also provides a service for an anonymous verification of the RK NCA subscriber's registration certificate status via OCSP service. The RK NCA provides a service for an anonymous stamping of a “Time Stamp” for the RK NCA subscribers via TSP service.

More detailed information is specified in the Registration Certificate Practice Statement for subscribers of the National Certification Authority of the Republic of Kazakhstan.

2.3. Period for the Information Publication

The RCRL shall be published once daily. The RCRL validity period is 25 hours.

More detailed information is specified in the Registration Certificate Practice Statement for subscribers of the National Certification Authority of the Republic of Kazakhstan.

2.4. Control of Access to Public Information

The RK NCA has implemented information and physical security measures to prevent unauthorized introduction, alteration or deletion of the information contained in the RCRL and the RK NCA PKI.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Naming

A registration certificate of the RK NCA subscriber shall contain distinctive names in a DN-name in the form recommended by X.501 Standard «Information technology - Open Systems Interconnection - The Directory: Models» from the series of the ITU-T X.500 recommended standards

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

3.2. Verification (Identification) of Customers at the Time of Issuance of a RK NCA Subscriber's Registration Certificate.

The ownership and validity of the RA EDS public key shall be confirmed on the basis of an application for the RK NCA registration certificates.

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

3.3. Verification (Identification) of Customers at the Time of Re-Issuance of the Registration Certificate of the RK NCA subscriber.

The RK NCA does not allow to reissue registration certificates of the RK NCA subscriber identical to the issued ones when they were lost or damaged.

More detailed information is specified in the Registration Certificate Practice Statement of the National Certification Authority of the Republic of Kazakhstan.

3.4. Verification (Identification) of Customers at the Time of Withdrawal of Registration Certificates.

A registration certificate can be withdrawn based on an application. The application shall meet the requirements of the legislation of the Republic of Kazakhstan.

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

4. OPERATIONAL REQUIREMENTS TO THE LIFE CYCLE OF A REGISTRATION CERTIFICATE OF THE RK NCA SUBSCRIBER

4.1. Application Procedure for the RK NCA Registration Certificate Issuance

The RK NCA registration certificate issue can be applied by:

- individuals;
- legal entities;
- individuals who are non-residents;
- legal entities who are non-residents;
- participants of Treasure-Client IS.

4.2. Process of the Application for the RK NCA Registration Certificate Issuance

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

4.3. RK NCA Registration Certificate Issuance

The RK NCA registration certificate shall be issued by the RK NCA based on the application filed through the RK NCA IS.

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

4.4. RK NCA Registration Certificate Receipt

The RK NCA sends a notice to a RK NCA subscriber via e-mail to the address specified when applying for the RK NCA registration certificate issuance.

The RK NCA does not notify the relying parties about the RK NCA registration certificate issuance.

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

4.5. Use of a Key Pair and Registration Certificate of the RK NCA Subscriber

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

4.6. RK NCA Registration Certificate Update

The RK NCA does not update, renew, change and amend the data in the structure of registration certificates of the RK NCA subscriber.

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

4.7. Registration Certificate Reassignment

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

4.8. Change of Registration Certificates

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

4.9. Termination of a Registration Certificate of the RK NCA Subscriber

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

4.10. Verification Services for the RK NCA Subscribers' Registration Certificate Status.

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

4.11. Subscription Expiry

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

4.12. Deposition and Recovery of a Key Pair

The RK NCA does not allow deposition and recovery of key pairs of subscribers and the RK NCA.

5. MANAGEMENT, OPERATION AND PHYSICAL CONTROLS

5.1. Physical Security Control of the RK NCA Assets

The RK NCA provides physical safety of the RK NCA systems in accordance with the effective legislation of the Republic of Kazakhstan. Detailed safety policies and procedures contain the RK NCA confidential information, and therefore cannot be published.

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

5.2. Responsibility and Control of the RK NCA Activity

The STS RSE provides a required number of departments and employees for functioning the internal control system. The STS RSE takes alternative control measures based on risk assessment in case of a vacancy in the staff position necessary for monitoring.

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

5.3. RK NCA Employees' Security Measures

The STS RSE ensures the safety of the STS RSE employees in accordance with:

- the RK NCA internal physical safety policies;
- internal policies of the organizations placing the RK NCA systems and employees;
- legislation of the Republic of Kazakhstan.

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

5.4. Documenting Events (Logging) in the RK NCA IS.

The RK NCA shall keep the logs for the following types of events:

1) life cycle management events for the RK NCA key pairs, including generation;
2) life cycle management events for the RK NCA registration certificates;
3) events connected with the RK NCA physical and informational safety;

The RK NCA does not allow recording any keys and passwords in an explicit form;

5.5. Archive of Records

The RK NCA provides archive storage for the following types of information in accordance with the requirements of the effective legislation of the Republic of Kazakhstan.

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

5.6. Issuance of the RK NCA Keys

The RK NCA issues key pairs and the RK NCA registration certificates after expiration of a root registration certificate or in case of compromise of key pairs.

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

5.7. Compromise and Emergency Recovery of the RK NCA Keys

The RK NCA has the procedures for any facts of the RK NCA incidents, and of compromise or suspicion to compromise of private keys, in accordance with the requirements of the Republic of Kazakhstan.

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

5.8. Termination of the RK NCA Activity

In the case when it is necessary to terminate the activities of the RK NCA, the RK NCA takes all measures required to notify the RK NCA PKI subscribers and the participants in advance.

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

6. RK NCA TECHNICAL SAFETY CONTROL

6.1. Issuance and Installation of the RK NCA Key Pairs and the RK NCA Subscribers

The RK NCA generates all key pairs used in the RK NCA PKI. Key pairs are generated with the help of cryptographic modules certified in accordance with the effective standard of the Republic of Kazakhstan ST RK 1073-2007 under the level equal or higher than the second level.

Generation of key pairs of the RK NCA 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 RK NCA key pairs generation is documented with the relevant protocol signed by all participants in the procedure. Protocols are stored and archived in accordance with the applicable legislation of the Republic of Kazakhstan and the internal regulations of the RK NCA.

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

6.2. Controls for Security of the RK NCA Private Keys and RK NCA subscribers, and for Management of the RK NCA Cryptographic Hardware Life Cycle.

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

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

6.3. Other Aspects of the RK NCA Key Pair Management

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

6.4. Activation Data

In order to ensure confidentiality, integrity and availability of private keys, the RK NCA applies data protection activation keys.

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

6.5. Computer Security Control

The RK NCA uses certified computer security tools proving a successful assessment of the high level of security.

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

6.6. Security Lifecycle Control

The RK NCA develops its own software. The RK NCA uses internal controls to determine the requirements for the system upgrades and testing.

The RK NCA internal control system provides separation of the development environment and production environment, as well as separation of powers of the employees with conflict roles of developers and system administrators.

6.7. Networks Security Controls

The RK NCA provides security of internal networks, as well as security of data transmitted over the external networks.

The RK NCA provides organizational and technical measures against unauthorized access and attacks on its networks. Policies and procedures for network security monitoring activities are documented and approved, but not published because they contain confidential information of the RK NCA.

7. PROFILES OF REGISTRATION CERTIFICATES OF THE RK NCA SUBSCRIBERS

7.1. Structure of a Registration Certificate of the RK NCA Subscriber

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

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

7.2. OCSP PROFILE

The OCSR service version used by the RK NCA for registration certificate status check, meets the RFC 6960requirements.

Extensions processed by the OCSP service, as well as their criticality, meet the RFC 6960 recommendations.

7.2.1. VERSION NUMBER

To check registration certificate status, the RK NCA uses OCSP v.1.

7.2.2. OCSR EXTENSIONS

Extensions processed by the OCSP service, as well as their criticality, meet the RFC 6960 recommendations.

8. COMPLIANCE AUDIT

The internal control environment of the RK NCA is checked for compliance with the WebTrust International Standard. The audit is carried out by independent auditing companies licensed by the owner of the WebTrust Standard.

8.1. Periodicity and Grounds of Inspections

The RK NCA internal control environment for compliance with the WebTrust International Standard (external audit) shall be audited not less than once a year.

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

8.2. Auditors and Their Qualifications

The RK NCA internal control environment for compliance with the WebTrust International Standard shall be audited by independent companies licensed by the owner of the WebTrust International Standard to carry out the certification audit for compliance with the WebTrust International Standard. More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

8.3. Relations between the RK NCA and Auditing Companies

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

8.4. Audit Tasks

The RK NCA internal control environment shall be audited in accordance with the WebTrust International Standard for Certification Authorities. The scope of inspections includes the following sections of the WebTrust International Standard:

1) disclosure of business practices of the RK NCA;
2) RK NCA environment controls;
3) controls of the RK NCA keys life cycle;
4) controls of the RK NCA subscribers' keys life cycle;
5) controls of life cycle management of the RK NCA registration certificates.

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

8.5. Measures Taken when any Shortcomings and Violations have been Identified

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

8.6. Notification on the Results

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

9. LEGAL ACTIVITIES

9.1. Payment for Services

The STS RSE and the State Corporation do not charge any payment for provision of public services.

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

9.2. Financial Liability

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

9.3. RK NCA Information Privacy

The RK NCA receives, uses and stores private information in the course of its business processes, and the RK NCA takes all necessary measures to protect it in accordance with the current legislation of the Republic of Kazakhstan. The RK NCA information shall not be considered as confidential.

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

9.4. Confidentiality of Personal Data of the RK NCA Subscribers

The RK NCA protects personal data of the RK NCA subscriber in accordance with the current legislation of the Republic of Kazakhstan.

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

9.5. Intellectual Property Rights

The RK NCA retains the intellectual property rights for the registration certificates it produces, and for the information about their status. At the same time the RK NCA does not prohibit to copy and to distribute registration certificates on a nonexclusive free-of-charge basis, subject to the conditions of completeness of use and copy of the registration certificates in accordance with the terms of the user agreements concluded. The RK NCA does not prohibit use of information on the status of the registration certificates for implementation of the relying party's functions.

The IS members served by the RK NCA recognize the intellectual property rights of the RK NCA for this Policy and other documentation of the RK NCA regulating the CA activities.

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

Key pairs corresponding to the registration certificate issued by the RK NCA, are the property (including intellectual) of the correspondent participants of the RK NCA PKI, regardless of the physical media in which these key pairs are stored and protected. In particular, public keys, registration certificates and parts of the secret of RK NCA private keys are the property (including intellectual property) of the RK NCA.

9.6. Duties

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

9.7. Revocation of Guarantees

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

9.8. Liability Limitations

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

9.9. Guarantees

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

9.10. Validity Period and Procedure of Expiration

This policy comes into effect immediately upon signing and publishing it on the RK NCA Internet resource.

9.11. Individual Notices and Interaction with the Participants

The RK NCA uses any available methods of the official notification of participants of the RK NCA PKI

.

9.12. Amendments

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

9.13. Dispute Settlement Procedure

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

9.14. Governing Law

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

9.15. Accordance with Governing Law

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

9.16. Other Directives

More detailed information is specified in the Registration Certificate Practice Statement for the subscribers of the National Certification Authority of the Republic of Kazakhstan.

9.17. Other Regulations

Not provided.