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, « 13 » 09

REGISTRATION CERTIFICATE PRACTICE STATEMENT OF THE NATIONAL CERTIFICATION AUTHORITY OF THE REPUBLIC OF KAZAKHSTAN (CERTIFICATE PRACTICE STATEMENT)

Version 2.0

Astana, 2016

VERSION CONTROL

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

Table of Contents

1. INTRODUCTION

The National Certification Authority of the Republic of Kazakhstan was created in order to provide registration certificates to individuals and legal entities.

The National Certification Authority of the Republic of Kazakhstan operates in accordance with the following laws and regulations of the Republic of Kazakhstan, internal and public documents:

1) Law of the Republic of Kazakhstan "On Informatization" dated November, 24, 2015;

2) Law of the Republic of Kazakhstan "On Electronic Document and Electronic Digital Signature" dated January, 7, 2003;

3) Law of the Republic of Kazakhstan "On Personal Data and Their Security" dated May, 2, 2013;

4) 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;

5) Order issued by the Minister of Investments and Development of the Republic of Kazakhstan "On Approval of the Standard for the State Service Named "Issue 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;

6) 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;

7) 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;

8) 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;

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

10) Recommended RFC 3647 Standard Certificate Policy and Certification Practices Framework related to the IETF series of international standards (hereinafter referred to as "RFC 3647");

11) ITU-T X.500 series of recommended standards;

12) RFC 5280 Certificate and Certificate Withdrawal List Profile recommended standard (hereinafter referred to as "RFC 5280");

13) 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 "Issue and Withdrawal of Registration Certificate of the National Certification Authority of the Republic of Kazakhstan";

14) Policy on use of the RK NCA subscribers' registration certificates (Certificate policy).

National Certification Authority of the Republic of Kazakhstan issuances registration certificates according to the following templates:

- registration certificates for individuals (applicable to signature and authentication);
- registration certificates for legal entities – first head (applicable to signature and authentication);
- registration certificates for legal entities – employee with the right of signature (applicable to signature and authentication);
- registration certificates for legal entities - HR officer (applicable to signature and authentication);
- registration certificates for legal entities - employee with the right to sign the financial documents officer (applicable to signature and authentication);
- registration certificates for legal entities – employee of the organization (applicable to signature and authentication);
- registration certificates for legal entities - the Treasury-Client information system participant (applicable to signature and authentication);
- SSL registration certificates for individuals;
- SSL registration certificates for legal entities.

1.1. DEFINITIONS AND ABBRETHROUGHTIONS

The following definitions are used herein:

№	Term	Definition
1.	Assets	The STS RSE resources aimed at ensuring the continuity of the RK NCA work
2.	Internal control environment	Complex of process controls used by the RK NCA
3.	RK NCA Work Log	The RK NCA IS record file containing events in a chronological order
4.	EDS private key	A sequence of digital symbols known to the registration certificate holder and intended to create a digital signature with the use of EDS instruments
5.	Applicant	An individual or legal entity (branch/representative office) submitting documents for issuance or withdrawal (cancelation) of a registration certificate before the registration certificate has been registered or declared invalid (cancelled)
6.	RK NCA Internet resource	RK NCA Internet resource www.pki.gov.kz
7.	Key pair	A set consisting of two keys: a privacy (secret) key and a public key
8.	EDS public key	A sequence of electronic digital symbols available to anyone and is designed to confirm the EDS compliance in e-document
9.	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 abbrethroughtions are used herein:

№	Abbrethroughtion	Definition
1.	TSP	(Time Stamp Protocol) cryptographic protocol allowing to create a fact existence proof for the e-document at a certain moment of time
2.	WebTrust	"Trust Service Principles and Criteria for Certification Authorities Version 2.0" International standard
3.	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
4.	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
5.	RK MIC	Ministry of Information and Communications of the Republic of Kazakhstan
6.	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
7.	STS RSE	State Technical Service Republican State Enterprise on the Right of Economic Use, Ministry of information and communications of the Republic of Kazakhstan
8.	RCRL	(Registration Certificate Revocation List) A list of all the RK NCA subscribers' registration certificates withdrawn by the time the RCRL has been issued
9.	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.
10.	IS	Information System
11.	OCSP	(Online Certificate Status Protocol) Protocol of the certificate status inspection

1.2. OVERVIEW

This RK NCA Certificate Practice Statement (hereinafter referred to as the "Certificate Practice Statement") defines the RK NCA activity with respect to the services related to the lifecycle of registration certificates issued by the RK NCA, and the RK NCA subscribers, and are applicable to all RK NCA PKI participants using the RK NCA subscriber's registration certificates.

This Certificate Practice Statement has been drafted in accordance with the following recommended 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 of the guidelines for development of application policies and instructions for application of the Public key infrastructure registration certificates in accordance with the RFC 3647 International Standard "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

In accordance with the above mentioned standards, this Certificate Practice Statement describes the service provision practice in relation to the RK NCA subscriber's registration certificates, as well as safety checks, used to protect the RK NCA PKI. In order to maintain compliance with the structure of the Certificate Practice Statement the principles and criteria of the WebTrust International Standard and RFC 3647 recommendations are not applicable to the RK NCA PKI practices, contain a "not applicable" or "not specified" mark.

This Certificate Practice Statement describes the RK NCA activities, applicable to the RK NCA subscriber's registration certificates in accordance with the requirements set out in the Policy on use of registration certificates of subscribers of the National Certification Authority (Certificate policy). The RK NCA activities comply with the following standards relevant at the time of publication of the Certificate Practice Statement:

- 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 to Issuance and Management of Publicly-Trusted Certificates, version 1.1.9.

1.3. NAME AND IDENTIFICATION OF THE DOCUMENT

Name of the document: Certificate Practice Statement of National Certification Authority of the Republic of Kazakhstan.

Document version: 2.0.

Put into effect by Order of the STS RSE Director No. 01-04/211. dated 13.09.2016

Current version of this Certificate Practice Statement has been published on the RK NCA Internet resource.

1.4. RK NCA PKI PARTICIPANTS

1.4.1. RK NCA

The RK NCA is a certification authority issuing registration certificates for use in accordance with the provisions of Clause **Ошибка! Источник ссылки не найден.** hereof. Other certification authorities are not allowed in the RK NCA PKI.

The RK NCA carries out activities directly related to the PKI, i.e.:

- receipt and process of applications for the issuance and withdrawal of registration certificates;
- issuance and withdrawal of the RK NCA subscriber's registration certificates;
- publication and support for the RCRL and intermediate lists;
- process of the applications for the OCSP service;
- putting of the TSP time stamp.

1.4.2. Registration Authorities

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

Functions of a registration authority:

1) an operator of the State Corporation shall carry out:

- personal verification (identification) of a Customer and verification of the documents submitted;
- confirmation of the Customer's e-application through authorization with the help of a personal EDS in the event of successful personal verification (identification) of a Customer and conformity of the

documents provided, as well as sending an e-application to the RK NCA IS;

- entry of registration certificates into the Customer's ID card containing electronic data storage device (chip);
- issuance of a document receipt to the Customer;
- withdrawal of registration certificates from the RK NCA subscriber's ID card;
- filling in an e-application form for registration certificate withdrawal and confirmation of the e-application through authorization with the help of a personal EDS, as well as sending it to the RK NCA IS.

2) the STS RSE executive officer shall carry out:

- personal verification (identification) of a Customer and verification of the documents submitted;
- confirmation of a Customer's e-application through authorization with the help of a personal EDS in the event of successful personal verification (identification) of a Customer and conformity of the documents provided, as well as sending an e-application to the RK NCA IS;
- filling in an e-application form for registration certificate withdrawal and confirmation of the e-application through authorization with the help of a personal EDS, as well as sending it to the RK NCA IS.

1.4.3. RK NCA 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.

1.4.4. 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.

1.4.5. Other Participants

Not applicable.

1.5. USE OF A REGISTRATION CERTIFICATE OF THE RK NCA SUBSCRIBER

1.5.1. 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).

1.5.2. 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.

The RK NCA and IS subscribers are not allowed to use the RK NCA subscriber's registration certificates in the following events:

1) upon expiry of a validity period of the RK NCA subscriber's registration certificate;
2) in the event of the RK NCA subscriber's registration certificate withdrawal;
3) in the event of compromise suspicion of the private key certified by the RK NCA subscriber's registration certificate;
4) in the event of discovered compromise of the private key certified by the RK NCA subscriber's registration certificate;
5) in the events not related to the methods of use permitted for RK NCA subscribers' registration certificate

1.6. CERTIFICATE PRACTICE STATEMENT MANAGEMENT

1.6.1. Organization managing the document

Republican State Enterprise on the Right of Economic Use "State Technical Service"
Registered office: 1/1, Zhirentayeva St., Astana, Republic of Kazakhstan, 010000;
Business address: 16 Kuishi Dina St., Astana, Republic of Kazakhstan, 010000

1.6.2. Contact person

Chief Specialist of the State Body Certification Authority Division, Public Key Infrastructure Service, Infrastructure Solution Department, STS RSE is Dossanov G.K., tel. 55-99-99 (int. 391), e-mail – info@pki.gov.kz

1.6.3. Person Assessing the CA Complience to the Policy Requirements

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

The STS RSE Director shall be also responsible for confirmation of the compliance of this Certificate Practice Statement with the Policy on use of the RK NCA subscriber's registration certificates (certificate policy).

1.6.4. Certificate Practice Statement Qualification Procedure

Development, support and update hereof shall be carried out by the STS RSE.

Reference Details:

- Registered office: 1/1, Zhirentayeva St., Astana, Republic of Kazakhstan, 010000;
- Business address: 16 Kuishi Dina St., Astana, Republic of Kazakhstan, 010000;
- STS RSE e-mail address: info@pki.gov.kz;
- tel. 55 99 99.

Any alterations or amendments hereto shall be made after their check for correspondence to the Rules of Use of the RK NCA Registration Certificates. 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 available at http://pki.gov.kz/cert/pki_rsa.cer;
- Root registration certificate of the RK NCA under the GOST algorithm available at http://pki.gov.kz/cert/pki_gost.cer;
- Root registration certificate of the RK RCA under the RSA algorithm available at http://root.gov.kz/cert/root_rsa.cer;
- Root registration certificate of the RK RCA under the GOST algorithm available at http://root.gov.kz/cert/root_gost.cer;
- Policy on use of registration certificates of the RK NCA subscribers;
- This Certificate Practice Statement;
- User agreement;
- RCRL available for download at http://crl.pki.gov.kz/ and http://crl1.pki.gov.kz/;
- RCRL delta available for download at http://crl.pki.gov.kz/ and http://crl1.pki.gov.kz;
- OCSP services available at http://ocsp.pki.gov.kz;
- TSP service available at http://tsp.pki.gov.kz.

Upon the expiry of a validity period of the RCRL, the RCRL validity in the register of registration certificates shall be five years, and the withdrawn registration certificates shall be included into the RCRL until the expiry of the validity period of the registration certificate.

2.2. PUBLICATION OF INFORMATION ON REGISTRATION CERTIFICATES

2.2.1. RK NCA RCRL

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 available at:
- http://crl.pki.gov.kz/rsa.crl - RCRL for RSA registration certificates;
- http://crl1.pki.gov.kz/rsa.crl - reserve RCRL for RSA registration certificates;
- http://crl.pki.gov.kz/d_rsa.crl - RCRL delta for RSA registration certificates;
- http://crl1.pki.gov.kz/d_rsa.crl- reserve RCRL delta for RSA registration certificates.

2) RCRL for registration certificates under the GOST algorithm available at:
- http://crl.pki.gov.kz/gost.crl - RCRL for GOST registration certificates;
- http://crl1.pki.gov.kz/gost.crl - reserve RCRL for GOST registration certificates;
- http://crl.pki.gov.kz/d_gost.crl - RCRL delta for GOST registration certificates;
- http://crl1.pki.gov.kz/d_gost.crl - reserve RCRL delta for GOST registration certificates.

2.2.2. RK NCA OCSP Service

RK NCA also provides a service for an anonymous verification of the RK NCA subscriber's registration certificate status through OCSP service available at http://ocsp.pki.gov.kz.

2.2.3. RK NCA TSP Service

RK NCA provides a service for an anonymous stamping of a “Time Stamp” for the RK NCA subscribers through TSP service, available at http://tsp.pki.gov.kz.

2.3. PERIOD FOR THE INFORMATION PUBLICATION

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

The RK NCA also publishes the RCRL update as a separate RCRL delta containing a list of registration certificates withdrawn since the release of the last main RCRL. The RCRL delta shall be generated every hour and be valid until the next RCRL delta release, but not more than 2 hours from the moment of its publication.

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

3.1.1. Types of Names Assigned to the RK NCA Subscriber

The RK NCA subscriber's registration certificate shall contain distinctive names in the DN-name in the format recommended by X.501 Standard "Information technology - Open Systems Interconnection - The Directory: Models" of the ITU-T X.500 series of recommended standards in the "Subject" field, referred to in Clauses 7.1.3. - 7.1.10. hereof shall identify the subscriber clearly and shall not be misleading for the relying parties.

3.1.2. Necessity for Use of Personal Data in the DN-name

The RK NCA issuances the RK NCA subscriber's registration certificates which contain personal data in the DN-name enabling the identification of a RK NCA subscriber and a field of use of a RK NCA subscriber's registration certificate.

3.1.3. Anonymity or Use of Pseudonyms by the RK NCA Subscribers

Anonymity or use of pseudonyms by subscribers shall not be allowed.

3.1.4. Interpretation Rules for DN-Names

The distinctive DN-names shall include all elements specified in the corresponding RK NCA 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. The RK NCA fills the "Subject" field with the RK NCA subscriber's personal data obtained from the state database of individuals and state database of legal entities on the basis of the identifying information submitted by the Customer.

3.1.5. Necessity of Use of Unique DN-Names

Each unique RK NCA subscriber shall have a unique name of a RK NCA subscriber's registration certificate in the "Subject" field, referred to in Clauses 7.1.3-7.1.10 hereof.

3.1.6. Recognition, Authentication and Function of Trademarks

The distinctive fields "Subject" and "Issuer" of the RK NCA registration certificates shall include only officially registered names of legal entities. The RK NCA does not allow the use of trademarks in the distinctive fields "Subject" and "Issuer" of the registration certificates.

The RK NCA shall use trademarks in the legal entity names in the "Subject" distinctive field b in accordance with the current legislation 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 a customer's application for RK NCA registration certificates executed through RK NCA IS, and include the following steps:

1) when applying for registration certificates for the Customer's computer facilities:

- In the event of availability of the Customer's data in the "Individuals" state database and (or) "Legal entities" state database (hereinafter referred to as I/LE SDB) the RK NCA IS registers an electronic application within 5 minutes and upon its confirmation through authorization of the electronic digital signature by a legal entity's first head or a person performing the same duties (for the legal entity's employees), sends the application for registration certificate issuance to the Customer for its further submission to the RA;
- the RA responsible officer carries out a receipt of an application, personal verification (identification) of the Customer and application within 20 minutes;
- in the event of a successful personal verification (identification) of the Customer and compliance of the application submitted, the RA responsible officer provides the Customer's e-mail application confirmation through authorization with a personal EDS, its sending to the RK NCA IS within 15 minutes;
- in the event of a successful verification of the Customer's electronic application certified by RA

responsible officer's EDS, the RK NCA IS sends an e-mail notification to the Customer on a successful registration certificate issuance with a link to its installation within 7 hours.

2) when applying for the registration certificates for ID card, containing an electronic data storage device (a chip) (hereinafter referred to as "ID card") and (or) sim-card containing the cryptographic information protection facilities (hereinafter referred to as a "sim-card"):

- the RA responsible officer carries out a personal verification (identification) of the Customer within 1 minute from receipt of the ID card and (or) sim-card provided by the Customer;
- in the event of a successful personal verification (identification) of the Customer, the RA responsible officer selects an appropriate public service, enters its personal account, fills in forms of electronic application for the registration certificate issuance and sends it through the "electronic government" gateway (hereinafter referred to as EGG) to the I/LE SDB within 5 minutes;
- in the event of the Customer's data availability in the I/LE SDB, the RA responsible officer receives a message about the Customer's data availability and continues further filling of the electronic application within 2 minutes;
- the RA responsible officer provides the Customer with a personal ID card and (or) sim-card to enter a PIN code within 1 minute;
- the RA responsible officer registers the electronic application in the RK NCA IS and receives an application for the registration certificate issuance within 2 minutes;
- the RA responsible officer receives from the Customer a signed application for the registration certificate issuance within 1 minute;
- upon receiving the application signed by the Customer the RA responsible officer provides the electronic application confirmation through authorization with a personal EDS and the electronic application sending to the RK NCA IS within 4 minutes;
- in the event of a successful verification of the electronic application certified with a personal EDS by the RK NCA IS, the RA responsible officer records the registration certificates at the Customer's ID card and (or) sim-card within 4 minutes.

3.2.1. Method of Proof of the Private Key Ownership

Upon receipt of an application for the registration certificate issuance, the RK NCA verifies the fact of the private key ownership corresponding to the public key for which the registration certificate is applied for: for identification the RK NCA verifies the application accuracy and availability of the necessary documents.

3.2.2. Representation of the Customer's Interests by a Third Party

The legal entity's first head or a person performing the same duties, shall have the right to transfer the authority to use the EDS to the legal entity's employee or authorized person, on the basis of a Power of Attorney for a single issuance or withdrawal of the RK NCA registration certificates, in accordance with Annex 3 to the Standard for the public service "Issuance and Withdrawal of Registration Certificate by the National Certification Authority of the Republic of Kazakhstan".

3.2.3. Unverified Subscriber's Information

Not available.

3.2.4. Verification of Authorities

While reviewing applications for the certificate issuance to an individual authorized to represent a legal entity, the RK NCA acts in accordance with Clause 3.2. Additional verifications of such authority are not necessary, as it is confirmed by the appropriate application and attached documents.

At the same time, in the event of doubt concerning such a verification, the RK NCA reserves the right to require from the applicant to submit additional documents confirming the information stated in the application.

3.2.5. Cooperation Criteria

The NCA and a registration certificate holder may enter into registration certificate issuance and withdrawal agreements if they Are necessary for the registration certificate issuance and withdrawal.

3.2.6. Verification (identification) of the Customer (Nonresident Individual)

The information specified in the application submitted by a nonresident individual for the registration certificate issuance may be confirmed by personal arrival of the Customer or the Customer's representative to the RA and presentation of the following documents:

1) an application for issuance of the RK NCA registration certificates submitted by an individual obtained

from the portal or through the integrated information system (hereinafter referred to as the "IIS") of the State Corporation which contains a unique number;

2) an identity document of the Customer's representative;

3) a Power of Attorney for the Customer's representative (individual) certified by a notary, with an indication of the authority to submit documents for the RK NCA registration certificate issuance and sign the relevant documents for the execution of the order specified by the Power of Attorney – when the Customer's interests are represented by any third party;

4) one of the following documents containing a Unique Identification Number and confirming that this nonresident has been registered in the territory of the Republic of Kazakhstan:

- a resident permit in the Republic of Kazakhstan;
- a stateless person's card;
- a foreigner's registration certificate.

3.2.7. Verification (Identification) of the Customer (Individual)

The information referred to in the application for the RK NCA registration certificate issuance submitted by an individual may be confirmed by personal arrival of the Customer or the Customer's representative to the RA and presentation of the following documents:

1) an application for the RK NCA registration certificate issuance submitted by an individual obtained from the portal or through the IIS of the State Corporation which contains a unique number;

2) an identity document of the Customer;

3) a Power of Attorney for the Customer's representative (individual) certified by a notary, with an indication of the authority to submit documents for the RK NCA registration certificate issuance and sign the relevant documents for execution of the order specified by the Power of Attorney – when the Customer's interests are represented by any third party.

3.2.8. Verification (Identification) of the Customer (individual entrepreneurs operating in the form of a joint enterprise)

The information referred to in the application for the RK NCA registration certificate issuance submitted by an individual entrepreneurs operating in the form of a joint enterprise, may be confirmed by personal arrival of the Customer or the Customer's representative to the RA and presentation of the following documents:

1) an application for the RK NCA registration certificate issuance (submitted by a legal entity and an individual entrepreneur operating in the form of a joint enterprise), obtained from the portal or through the IIS of the State Corporation which contains a unique number;

2) an identity document of the Customer's representative;

3) a Power of Attorney for the Customer's representative (individual) certified by a notary, with an indication of the authority to submit documents for the RK NCA registration certificate issuance and sign the relevant documents for the execution of the order specified by the Power of Attorney – when the Customer's interests are represented by any third party;

4) a certificate of an individual entrepreneur registration.

3.2.9. Verification (Identification) of the Customer (Legal Entity)

The information referred to in the application for the RK NCA registration certificate issuance submitted by a legal entity, may be confirmed by personal arrival of the Customer or the Customer's representative to the RA and presentation of the following documents:

1) an application for the RK NCA registration certificate issuance (submitted by a legal entity and individual entrepreneur operating in the form of a joint enterprise), obtained from the portal or through the IIS of the State Corporation which contains a unique number;

2) an identity document of the Customer's representative;

3) a Power of Attorney for a single issuance or withdrawal of the RK NCA registration certificates submitted by a legal entity in accordance with Clause 3.2.1 hereof;

4) a verification letter or certificate (if available) of registration (reregistration) of a Customer's legal entity as a legal entity.

5) in order to obtain registration certificates for the legal entity's employee before applying to the State Corporation or to the Service provider, the legal entity's first head or a person performing the same duties confirms an application for the registration certificate issuance submitted by a legal entity's employee through the portal through its authorization with a personal electronic digital signature;

6) the legal entity's first head or a person performing the same duties, submits a letter of employment confirmation or a copy of the appointment order (decision, protocol) referred to the first head or a person performing the same duties certified with the legal entity's seal (if available), instead of the Power of Attorney.

3.2.10. Verification (Identification) of the Customer (Nonresident Legal Entity)

The information referred to in the application submitted by a nonresident legal entity for the registration certificate issuance may be confirmed by personal arrival of the Customer or the Customer's representative to the RA and presentation of the following documents:

1) an application for the RK NCA registration certificate issuance (submitted by a legal entity and individual entrepreneur operating in the form of a joint enterprise) obtained from the portal or through the IIS of the State Corporation which contains a unique number;

2) an identity document of the Customer;

3) a Power of Attorney for a single issuance or withdrawal of the RK NCA registration certificates submitted by a legal entity in accordance with Clause 3.2.1 hereof;

4) one of the following documents containing a Unique Identification Number and confirming that this representative of the nonresident legal entity has been registered in the territory of the Republic of Kazakhstan:

- a resident permit in the Republic of Kazakhstan;
- a stateless person's card;
- a foreigner's registration certificate.

5) one of the following documents containing a Business Identification Number and confirming that this nonresident legal entity has been registered in the territory of the Republic of Kazakhstan:

- a verification letter or certificate (if available) of record registration (reregistration) of a branch, representative office – for nonresident legal entities carrying out activities in the Republic of Kazakhstan through branches and representative offices (with establishment of a permanent establishment);
- a registration certificate for nonresident legal entities:
- representing tax agents in accordance with Clause 5 Article 197, the Code of the Republic of Kazakhstan dated December 10, 2008 “On Taxes and other Obligatory Payments to the Budget” (the Tax Code) (hereinafter referred to as the “Tax Code”);
- holding taxable activities and assets in the Republic of Kazakhstan;
- being diplomatic and equivalent representative offices of foreign states accredited in the Republic of Kazakhstan;
- carrying out activities through a dependent agent which is regarded as a personal permanent establishment in accordance with Clause 8 Article 191 of the Tax Code;
- carrying out activities through a permanent establishment without opening a branch, representative office;
- opening current accounts with non-resident banks.

6) the legal entity's first head or a person performing the same duties submits a letter of employment confirmation or a copy of the appointment order (a decision, protocol) for the first head or a person performing the same duties certified with the legal entity's seal (if available), instead of the Power of Attorney.

3.2.11. Verification (Identification) of the Customer (“Treasury-Customer” IS Participant)

The information referred to in the application for the registration certificate issuance for the “Treasury-Customer” IS participants may be confirmed by personal arrival of the Customer or the Customer's representative to the RA and presentation of the following documents:

1) an application for the RK NCA registration certificate issuance (submitted by a legal entity for the “Treasury-Customer” IS users) according to the form, obtained from the portal or through the IIS of the State Corporation which contains a unique number;

2) an identity document of the Customer's representative;

3) a Power of Attorney for a single issuance or withdrawal of the RK NCA registration certificates submitted by a legal entity, in accordance with Clause 3.2.1 hereof;

4) an agreement or a supplementary agreement for EDS application between the Ministry of Finance Treasury Committee of the Republic of Kazakhstan and a Customer executed in hard copy (if the date of signing the agreement and the date of the agreement or the supplementary agreement submission to the RK NCA exceeds 3 working days, excluding the day of signing the agreement (supplementary agreement), this agreement shall be rejected).

3.2.12. Verification (Identification) of the Customer (individual who is a Holder of an Internet Resource Domain Name)

The information referred to in the application for the SSL registration certificate issuance for individuals who are holders of an Internet resource domain name may be confirmed by personal arrival of the Customer or the Customer's representative to the RA and presentation of the following documents:

1) an application for the SSL registration certificate issuance by the RK NCA (submitted by an individual), obtained from the portal or through the IIS of the State Corporation which contains a unique number;

2) an identity document of the Customer;

3) a Power of Attorney for the Customer's representative (individual) certified by a notary, with an indication of the authority to submit documents for the RK NCA registration certificate issuance and sign the relevant documents for the execution of the order, specified by the Power of Attorney – when the Customer's interests are represented by any third party;

4) a copy of one of the following supporting documents confirming the right to hold an Internet resource domain name:

- a certificate of holding a domain name issued by the Kazakhstan Network Information Center;
- an extract from the WHOIS (a domain name search in the. KZ and. ҚАЗ area).

3.2.13. Verification (Identification) of the Customer (legal entity which is an Internet resource domain name holder)

The information referred to in the application for the SSL registration certificate issuance for legal entities which are holders of an Internet resource domain name may be confirmed by personal arrival of the Customer or the Customer's representative to the RA and presentation of the following documents:

1) an application for the SSL registration certificate issuance by the RK NCA (submitted by a legal entity), obtained from the portal or through the IIS of the State Corporation which contains a unique number;

2) an identity document of the Customer's representative;

3) a Power of Attorney for a single issuance or withdrawal of the RK NCA registration certificates submitted by a legal entity, in accordance with Clause 3.2.1 hereof;

4) a copy of one of the following supporting documents confirming the right to hold an Internet resource domain name:

- a certificate of holding a domain name issued by the Kazakhstan Network Information Center;
- an extract from the WHOIS (a domain name search in the. KZ and. ҚАЗ area).

3.3. VERIFICATION (IDENTIFICATION) OF THE CUSTOMER AT THE TIME OF SECOND ISSUANCE OF THE RK NCA SUBSCRIBER'S REGISTRATION CERTIFICATE

The RK NCA does not provide the second issuance of the RK NCA subscriber's registration certificates identical to the previously issued RK NCA registration certificates in the case of any loss or damage.

In the event of the second application through the RK NCA IS the Customer (except for the "Treasury-Customer" IS Participants) sends an application in the form of an electronic document containing a public key (keys) certified with the current Customer's electronic digital signature.

If the Customer holds current registration certificates, it is possible to provide the registration certificate second issuance before the expiry of the term without any documents submission to the RA, through online submission through personal account and application authorization with a personal EDS:

1) the Customer enters its personal account with the help of its current RK NCA subscriber's registration certificate, fills in the application forms for the registration certificate issuance and sends the application through a gateway to the state databases;

2) In the event of availability of the Customer's data in the I/LE SDB state databases, the RK NCA IS displays a notice on the Customer's data availability and continues further filling of the forms within 5 minutes;

3) The RK NCA IS issuances the registration certificates and sends a notification of a successful registration certificate issuance with a link to its installation within 1 business day to the Customer's e-mail.

In the event of the registration certificate issuance upon withdrawal of the previous RK NCA registration certificates, the RK NCA subscriber shall undergo a personal verification (identification) of a Customer in accordance with the procedure described in Clause 3.2 hereof.

3.3.1. Identification and Authentication of the Applications at the Time of the Scheduled Key Replacement

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

3.3.2. Identification and Authentication of the Applications for the Key Replacement in the Certificate upon Withdrawal

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

3.4. VERIFICATION (IDENTIFICATION) OF THE RK NCA SUBSCRIBER AT THE TIME OF THE REGISTRATION CERTIFICATE WITHDRAWAL

At the time of the RK NCA subscriber's registration certificates withdrawal:

1) when submitting an application for the registration certificate withdrawal, if the current Customer's EDS is available:

- The RK NCA IS registers an electronic application signed with the Customer's EDS within 5 minutes;
- The RK NCA IS carries out a verification of the electronic application certified with the Customer's EDS and withdrawal of the Customer's registration certificates with sending a notice on a successful registration certificate withdrawal within 1 business day to the Customer's e-mail address.

2) when submitting an application for the registration certificate withdrawal:

- the RA responsible officer carries out a personal verification (identification) of a Customer and an application within 5 minutes since the Customer's application has been submitted;
- in the event of a successful personal verification (identification) of the Customer and compliance of the application submitted, the RA responsible officer selects an appropriate public service, enters its personal account, fills in a form of electronic application for the registration certificate withdrawal, confirms it through authorization with a personal EDS and sends it to the RK NCA IS within 15 minutes;
- in the event of a successful verification of the electronic application certified with the RA responsible officer's EDS, the RK NCA IS withdraws the Customer's registration certificates and sends a notice on successful registration certificate withdrawal within 1 business day to the Customer's e-mail address.

3.4.1. Representation of the Customer's Interests by any Third Party

The legal entity's first head or a person performing the same duties shall have the right to transfer the authority to use the EDS to the legal entity's employee or authorized person, on the basis of a Power of Attorney for a single issuance or withdrawal of the RK NCA registration certificates, in accordance with Annex 3 to the Standard for the public service "Issuance and Withdrawal of Registration Certificate by the National Certification Authority of the Republic of Kazakhstan".

3.4.2. Verification (Identification) of the RK NCA Subscriber (Individual)

The information referred to in the application submitted by an individual for the registration certificate withdrawal may be confirmed by personal arrival of a RK NCA subscriber, or a RK NCA subscriber's representative to the RA and presentation of the following documents:

1) an application for the RK NCA registration certificate withdrawal submitted by an individual, obtained from the portal or through the IIS of the State Corporation;

2) an identity document of the Customer;

3) a Power of Attorney for the Customer's representative (individual) certified by a notary, with an indication of the authority to submit documents for the RK NCA registration certificate withdrawal and sign the relevant documents for the execution of the order, specified by the Power of Attorney – when the Customer's interests are represented by any third party.

3.4.3. Verification (Identification) of the RK NCA Subscriber (Nonresident Individuals)

The information referred to in the application submitted by an individual for the registration certificate withdrawal may be confirmed by personal arrival of a RK NCA subscriber, or a RK NCA subscriber's representative to the RA and presentation of the following documents:

1) an application for the RK NCA registration certificate withdrawal submitted by an individual-nonresident obtained from the portal or through the IIS of the State Corporation;

2) an identity document of the Customer;

3) a Power of Attorney for the Customer's representative (individual) certified by a notary, with an indication of the authority to submit documents for the RK NCA registration certificate withdrawal and sign the relevant documents for the execution of the order, specified by the Power of Attorney – when the Customer's interests are represented by any third party.

3.4.4. Verification (Identification) of the RK NCA Subscriber (Individual Entrepreneurs Operating in the Form of a Joint Enterprise)

The information referred to in the application submitted by an individual entrepreneur operating in the form of a joint enterprise for the registration certificate withdrawal may be confirmed by personal arrival of a RK NCA subscriber, or a RK NCA subscriber's representative to the RA and presentation of the following documents:

1) an application for the RK NCA registration certificate withdrawal submitted by an individual entrepreneur operating in the form of a joint enterprise, obtained from the portal or through the IIS of the State Corporation certified with the legal entity's seal (if available), or an extract from the order on the Customer termination. in the event of submission of an extract from the order on termination, the first head's signature and organization's seal are not necessary;

2) an identity document of the Customer's representative;

3) a Power of Attorney for the Customer's representative (individual) certified by a notary, with an indication of the authority to submit documents for the RK NCA registration certificate withdrawal and sign the relevant documents for the execution of the order, specified by the Power of Attorney – when the Customer's interests are represented by any third party.

3.4.5. Verification (Identification) of the RK NCA Subscriber (legal entity)

The information referred to in the application submitted by a legal entity for the registration certificate withdrawal may be confirmed by personal arrival of a RK NCA subscriber, or a RK NCA subscriber's representative to the RA and presentation of the following documents:

1) an application for the RK NCA registration certificate withdrawal submitted by a legal entity, obtained from the portal or through the IIS of the State Corporation certified with the legal entity's seal (if available), or an extract from the order on the Customer termination. in the event of submission of an extract from the order on termination, the first head's signature and organization's seal are not necessary;

2) an identity document of the Customer's representative;

3) a Power of Attorney for a single issuance or withdrawal of the RK NCA registration certificates submitted by a legal entity, in accordance with Clause 3.4.1 hereof.

3.4.6. Verification (Identification) of the RK NCA Subscriber (nonresident legal entity)

The information referred to in the application submitted by a nonresident legal entity for the registration certificate withdrawal may be confirmed by personal arrival of a RK NCA subscriber, or a RK NCA subscriber's representative to the RA and presentation of the following documents:

1) an application for the RK NCA registration certificate withdrawal submitted by a nonresident legal entity, obtained from the portal or through the IIS of the State Corporation certified with the legal entity's seal (if available), or an extract from the order on the Customer termination. in the event of submission of an extract from the order on termination, the first head's signature and organization's seal are not necessary;

2) an identity document of the Customer's representative;

3) a Power of Attorney for a single issuance or withdrawal of the RK NCA registration certificates submitted by a legal entity, in accordance with Clause 3.4.1 hereof.

3.4.7. Identification of the Customer (“Treasury-Customer” IS Participant)

The information referred to in the application for the registration certificate withdrawal for the “Treasury-Customer” IS users may be confirmed by personal arrival of a RK NCA subscriber, or a RK NCA subscriber's representative to the RA and presentation of the following documents:

1) an application for the RK NCA registration certificate withdrawal submitted by “Treasury-Customer” IS participant, obtained from the portal or through the IIS of the State Corporation certified with the legal entity's seal (if available), or an extract from the order on the Customer termination. in the event of submission of an extract from the order on termination, the first head's signature and organization's seal are not necessary;

2) an identity document of the Customer's representative;

3) a Power of Attorney for a single issuance or withdrawal of the RK NCA registration certificate submitted by a legal entity, in accordance with Clause 3.4.1 hereof.

3.4.8. Verification (Identification) of the Customer (Individual who is a Holder of an Internet Resource Domain Name)

The information referred to in the application for the SSL registration certificate withdrawal for the individual who is a holder of an Internet resource domain name may be confirmed by personal arrival of a RK NCA subscriber or a RK NCA subscriber's representative to the RA and presentation of the following documents:

1) an application for the RK NCA registration certificate withdrawal submitted by an individual - holder domain name Internet resource, obtained from the portal or through the IIS of the State Corporation;

2) an identity document of the Customer;

3) a Power of Attorney for the Customer's representative (individual) certified by a notary, with an

indication of the authority to submit documents for the RK NCA registration certificate withdrawal and sign the relevant documents for the execution of the order, specified by the Power of Attorney – when the Customer's interests are represented by any third party.

3.4.9. Verification (Identification) of the Customer (Legal Entity which is a Holder of an Internet Resource Domain Name)

The information referred to in the application for the SSL registration certificate withdrawal for legal entity which is a holder of an Internet resource domain name may be confirmed by personal arrival of a RK NCA subscriber or a RK NCA subscriber's representative CA presentation of the following documents:

1) an application for the RK NCA registration certificate withdrawal submitted by a legal entity - Internet resource domain name holder, obtained from the portal or through the IIS of the State Corporation certified with the legal entity's seal (if available), or an extract from the order on the Customer termination. in the event of submission of an extract from the order on termination, the first head's signature and organization's seal are not necessary;

2) an identity document of the Customer's representative;

3) a Power of Attorney for a single issuance or withdrawal of the RK NCA registration certificate submitted by a legal entity, in accordance with Clause 3.4.1 hereof.

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

4.1. APPLICATION PROCEDURE FOR THE NCA PK REGISTRATION CERTIFICATE ISSUANCE

4.1.1. Persons Entitled to Apply for the RK NCA Subscriber's Registration Certificate Issuance

An application for the RK NCA subscriber's registration certificate issuance may be submitted by:

- individuals;
- legal entities;
- nonresident individuals;
- nonresident legal entities;
- a "Treasury-Customer" IS participant.

4.1.2. Registration Procedure and Associated Responsibilities

The Customer's registration in the RK NCA shall be carried out in accordance with Clause 3.2 hereof.

4.1.3. The procedure for generating the RK NCA subscriber's key pairs

The Customers and the RK NCA subscribers generate their key pairs through the RK NCA Internet resource, through the personal account or application submission service for the RK NCA registration certificate issuance, or in the case of a personal address to the RA in the event of EDS placing at the ID card in accordance with Clause 6.1.2. hereof.

4.2. PROCESS OF THE RK NCA SUBSCRIBER'S APPLICATION FOR THE REGISTRATION CERTIFICATE ISSUANCE

4.2.1. Authentication and Identification of the Application

Any procedure of identification and authentication at the time of the registration certificate issuance shall be carried out according to the same procedure as the original identity verification set out in Section 3.2.

4.2.2. Confirmation of the EDS Public Key Ownership and Validity

Confirmation of the EDS public key ownership and validity shall be carried out in accordance with Clause 3.2 hereof. If the current registration certificate is available, the information actuality confirmation is not necessary, and all the actions for the new registration certificate issuance shall be carried out through the RK NCA IS, no need in the personal arrival to the RA.

4.2.3. Refusal to Accept the Customer's Application for the RK NCA Registration Certificate Issuance

The RK NCA refuses to the Customer:

- to issue the holder's registration certificate in the event of his / her failure to submit the necessary information and of submission of false information;
- to withdraw the holder's registration certificate in the event of improper execution of the relevant application for the holder's registration certificate withdrawal and the expiry of the holder's registration certificate.

4.2.4. Term for Review of the Applications for the RK NCA Subscribers' Registration Certificate Issuance

The period for the public service delivery by the RK NCA from the moment of the document package submission to the RA is 1 business day.

4.3. RK NCA SUBSCRIBERS' REGISTRATION CERTIFICATE ISSUANCE

4.3.1. RK NCA Actions in the Course of the RK NCA Subscribers' Registration Certificate Issuance

The RK NCA subscriber's registration certificate is issued by the RK NCA on the basis of an application, executed through the RK NCA IS. The procedure of the RK NCA subscriber's registration certificate issuance requires one of the confirmation forms:

- in the event of unavailability of the current RK NCA subscriber's registration certificate- confirmation of the EDS public key ownership and validity by the CA operator;
- If the current RK NCA subscriber's registration certificate is available - signing of the application with a current EDS and relevant subscriber's registration certificate.

The RK NCA generates key pairs and relevant RK NCA subscriber's registration certificate on the basis of information submitted in the application.

4.3.2. Notice on the RK NCA Subscriber's Registration Certificate Issuance for the RK NCA Subscribers

An official notice on the fact of registration certificate issuance means publication of this registration certificate in the register of registration certificates. In the event of a positive result of processing the application for the registration certificate issuance, the Customer receives an issued registration certificate as a reply.

The RK NCA may send a notice on RK NCA subscriber's registration certificate issuance to the Customer through e-mail. The RK NCA shall not be liable in the event the RK NCA subscriber does not receive such a notice.

4.4. RK NCA SUBSCRIBER'S REGISTRATION CERTIFICATE ACCEPTANCE

4.4.1. RK NCA Subscriber's Registration Certificate Acceptance

Acceptance of the RK NCA registration certificates by a subscriber:

- key pairs installation;
- absence of the Customer's objections against the acceptance of the RK NCA registration certificates or its content;
- the registration certificate application by the RK NCA subscriber.

4.4.2. RK NCA Notice on the RK NCA Subscriber's Registration Certificate Issuance to Relying Parties

The RK NCA sends a notice to the RK NCA subscriber through e-mail to the address indicated when submitting an application for the RK NCA registration certificate issuance.

The RK NCA does not notify the relying parties on the RK NCA subscriber's registration certificate issuance.

4.4.3. Registration Certificate Publication by Certification Authority

The RK NCA places the issued (reassigned) registration certificates on the home page of the RK NCA Internet resource in the “Root Certificates” Section.

4.5. USE OF THE RK NCA SUBSCRIBER'S KEY PAIRS AND REGISTRATION CERTIFICATE

4.5.1. Use of the Private Keys and Registration Certificates by the RK NCA Subscribers

The RK NCA subscriber may use the private key upon review and full acceptance of the requirements specified in:

1) the current legislation of the Republic of Kazakhstan;
2) the user agreement;
3) Policy on use of the RK NCA subscriber's registration certificates;
4) this Certificate Practice Statement.

The RK NCA subscriber shall use the RK NCA registration certificates in accordance with the policy on use indicated in the “Key Usage” and “ExtendedKeyUsage” fields in accordance with Clause 7.1.3-7.1.10. hereof.

Use of the RK NCA registration certificates by subscribers constitutes acceptance of the provisions hereof and consent to the publication of the data not considered confidential.

The RK NCA subscriber shall take measures to protect the EDS private key owned by it against unauthorized access and use, as well as store the public keys in accordance with the procedure established by the current legislation of the Republic of Kazakhstan.

4.5.2. Use of Public Keys and the RK NCA Subscriber's Registration Certificates by Relying Parties

The RK NCA PKI participants accept liabilities, provided in:

- the current legislation of the Republic of Kazakhstan;
- Policy on use of the RK NCA subscriber's registration certificates;
- this Certificate Practice Statement.

Before making a decision on the credibility to the RK NCA subscriber's registration certificate, the RK NCA PKI participants shall fulfill the following steps:

1) check the corresponding electronic document signed by the RK NCA subscriber's registration certificate (certificates);

2) verify the RK NCA subscriber's registration certificate validity, by fulfillment the following steps:

- define the full chain of the RK NCA subscriber's registration certificates up to the RK RCA root registration certificate;
- assess the compliance of all the RK NCA subscriber's registration certificates in the chain with the following criteria:
- a scope in accordance with this Certificate Practice Statement;
- the "keyUsage" and "extendedKeyUsage" fields content of the registration certificate in accordance with Clause 7.1.3-7.1.10. hereof;
- make sure that all the RK NCA subscriber's registration certificates in the chain have been signed by RK RCA.

The information systems relating to the RK NCA PKI participants, shall carry out the appropriate verification in accordance with "Guidelines on interaction of information systems with the RK NCA", available at the RK NCA Internet resource.

4.6. RK NCA SUBSCRIBER'S REGISTRATION CERTIFICATE UPDATE

The RK NCA does not provide the data update, increase of the validity, alterations and amendments to the RK NCA subscriber's registration certificate structure.

In the event of an update of the personal data contained in the RK NCA subscriber's registration certificates, it is necessary to revoke the RK NCA subscriber's registration certificate in accordance with Clause 4.9 hereof and receive a new RK NCA registration certificate issued in accordance with Clause 4.1 hereof.

4.6.1. Grounds for the Certificate Update

The RK NCA does not deliver any services for the registration certificates update.

In the event of an update of the personal data contained in the RK NCA subscriber's registration certificates, it is necessary to revoke the RK NCA subscriber's registration certificate in accordance with Clause 4.9 hereof and receive a new RK NCA registration certificate issued in accordance with Clause 4.1 hereof.

4.6.2. Persons Entitled to Apply for the Certificate Update

The RK NCA does not deliver any services for the registration certificates update.

In the event of an update of the personal data contained in the RK NCA subscriber's registration certificates, it is necessary to revoke the RK NCA subscriber's registration certificate in accordance with Clause 4.9 hereof and receive a new RK NCA registration certificate issued in accordance with Clause 4.1 hereof.

4.6.3. Processing of Applications for the Certificate Update

The RK NCA does not deliver any services for the registration certificates update.

In the event of an update of the personal data contained in the RK NCA subscriber's registration certificates, it is necessary to revoke the RK NCA subscriber's registration certificate in accordance with Clause 4.9 hereof and receive a new RK NCA registration certificate issued in accordance with Clause 4.1 hereof.

4.6.4. Notice on the Updated Certificate Issuance for the User

The RK NCA does not deliver any services for the registration certificates update.

In the event of an update of the personal data contained in the RK NCA subscriber's registration certificates, it is necessary to revoke the RK NCA subscriber's registration certificate in accordance with Clause 4.9 hereof and receive a new RK NCA registration certificate issued in accordance with Clause 4.1 hereof.

4.6.5. Procedure for Acceptance of the Updated Certificate

The RK NCA does not deliver any services for the registration certificates update.

In the event of an update of the personal data contained in the RK NCA subscriber's registration

certificates, it is necessary to revoke the RK NCA subscriber's registration certificate in accordance with Clause 4.9 hereof and receive a new RK NCA registration certificate issued in accordance with Clause 4.1 hereof.

4.6.6. CA Updated Certificate Publication

The RK NCA does not deliver any services for the registration certificates update.

In the event of an update of the personal data contained in the RK NCA subscriber's registration certificates, it is necessary to revoke the RK NCA subscriber's registration certificate in accordance with Clause 4.9 hereof and receive a new RK NCA registration certificate issued in accordance with Clause 4.1 hereof.

The RK NCA places the issued (reassigned) registration certificates on the home page of the RK NCA Internet resource in the "Root Certificates" Section.

4.6.7. RK NCA Notice on the Certificate Issuance to Other Entities

Not applicable.

4.7. REGISTRATION CERTIFICATE REASSIGNMENT

Not applicable.

4.7.1. Grounds for the Registration Certificate Reassignment

Not applicable.

4.7.2. Persons Entitled to Request a New Public Key

Not applicable.

4.7.3. Processing of the Applications for the Registration Certificate Reassignment

Not applicable.

4.7.4. Notice on Issuance of the Registration Certificate Containing Replaced Keys for the Subscriber

Not applicable.

4.7.5. Procedure for Use of the Registration Certificate Containing Replaced Keys

Not applicable.

4.7.6. Publication of the CA Registration Certificate Containing Replaced Keys

Not applicable.

4.7.7. Notice on the Registration Certificate Issuance to Other Entities Produced by the RK NCA

Not applicable.

4.8. ALTERATION OF THE REGISTRATION CERTIFICATE

The RK NCA does not allow the key replacement in the registration certificate of the assigned CA, including the registration certificate validity period. In the event of a key replacement necessity the CA assigned shall request for a registration (reassignment) of a new current 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 the Registration Certificate

The RK NCA does not deliver any services for the registration certificates alteration.

4.8.2. Persons Entitled to Apply for the Registration Certificate Alteration

The RK NCA does not deliver any services for the registration certificates alteration.

In the event of a key replacement necessity the CA assigned shall request for a registration (reassignment) of a new current registration certificate (see Clause 4.1 above) and revoke the old registration certificate (see Clause 4.6.1).

4.8.3. Processing of Applications for the Registration Certificate Alteration

The RK NCA does not deliver any services for the registration certificates alteration.

In the event of a key replacement necessity the CA assigned shall request for a registration (reassignment) of a new current registration certificate (see Clause 4.1 above) and revoke the old registration certificate (see Clause 4.6.1).

4.8.4. Notice on issuance of the altered registration certificate for the subscriber

The RK NCA does not deliver any services for the registration certificates alteration.

In the event of a key replacement necessity the CA assigned shall request for a registration (reassignment) of a new current registration certificate (see Clause 4.1 above) and revoke the old registration certificate (see Clause 4.6.1).

4.8.5. The procedure for acceptance of the altered registration certificate

Not applicable.

4.8.6. Publication of the altered CA registration certificate

The RK NCA does not deliver any services for the registration certificates alteration.

In the event of a key replacement necessity the CA assigned shall request for a registration (reassignment) of a new current registration certificate (see Clause 4.1 above) and revoke the old registration certificate (see Clause 4.6.1).

The RK NCA places the issued (reassigned) registration certificates on the home page of the RK NCA Internet resource in the “Root Certificates” Section.

4.8.7. CA Notice on the Altered Registration Certificate Issuance to Other Entities

Not applicable.

4.9. RK NCA SUBSCRIBER'S REGISTRATION CERTIFICATE WITHDRAWAL

4.9.1. Grounds for the RK NCA Subscribers' Registration Certificate Withdrawal

The RK NCA withdraws the RK NCA subscriber's registration certificates before the expiry of the term in the following cases:

- at the request of the registration certificate holder or its representative;
- establishing the fact of providing false information for the registration certificate issuance;
- the registration certificate holder's death;
- change of the registration certificate holder's name, surname or patronymic (if specified in an identity document);
- change of the name, reorganization, liquidation of a legal entity-registration certificate holder;
- under the agreement between the certification authority and a registration certificate holder;
- according to the court decision in force.

4.9.2. Persons Entitled to Apply for the RK NCA Subscribers' Registration Certificate Withdrawal

The persons entitled to apply for the RK NCA subscribers' registration certificate withdrawal are as follows:

- The RK NCA subscribers;
- The RK NCA subscribers' representatives.

4.9.3. Procedures for the Registration Certificate Withdrawal for the RK NCA Subscribers

The RK NCA subscriber's registration certificate withdrawal shall be carried out by subscriber itself through the RK NCA IS, through the “Personal account”. The RK NCA subscriber may also revoke the registration certificate through the CA.

Upon the necessary documents receipt the CA operator carries out a personal verification (identification) of the subscriber and verification of the documents within 20 minutes. In the event of a successful verification, the CA operator fills in an electronic application form for the registration certificate withdrawal and confirms the e-application through authorization with the help of a personal EDS, sends it to the RK NCA IS and issuances a document receipt to the subscriber or its representative.

4.9.4. Term for Submission of the Application for the RK NCA Subscriber's Registration Certificate Withdrawal

The RK NCA subscribers shall be responsible for the timely submission of the applications for registration certificate withdrawal.

4.9.5. Term for Consideration of the Application for the RK NCA Subscriber's Registration Certificate Withdrawal

Upon receipt an application for the registration certificate withdrawal the RK NCA considers and process it within 1 business day. In the event of a successful consideration of the application, the RK NCA IS carries out the registration certificate withdrawal, publishes information about the withdrawn registration certificate in the RCRL and notifies the subscriber through e-mail. The RK NCA shall not be responsible for the failure of the registration certificate withdrawal notice delivery.

4.9.6. Requirements to Verification of the RK NCA Subscriber's Registration Certificate Withdrawal for the Relying Parties

The RK NCA PKI participants shall verify the status of the RK NCA subscriber's registration certificates before making a decision on the application of the mentioned RK NCA subscriber's registration certificates, through one of the following methods:

- verification of the RK NCA subscriber's registration certificate availability in the current RCRL;
- verification of the RK NCA subscriber's registration certificate status through the OCSP services.

The RK NCA provides the necessary mechanisms for verification of the RK NCA subscriber's registration certificate status.

4.9.7. RCRL Issuance Frequency

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

The RK NCA also publishes the RCRL update as a separate RCRL delta containing a list of the registration certificates, withdrawn since the release of the last main RCRL. The RCRL delta shall be generated every hour and be valid until the next RCRL delta release, but not more than 2 hours from the moment of its publication.

4.9.8. RCRL Maximum Delay

The RCRL of the RK NCA subscribers shall be published immediately after generation to the addresses specified in Clause 2.2.1 hereof.

4.9.9. Requirement to the Availability of the RCRL and Information on the RK NCA Subscriber's Registration Certificate Status

The RK NCA provides continuous availability of the RCRL service and information on the RK NCA subscriber's registration certificate status in accordance with this Certificate Practice Statement.

4.9.10. Requirements to Verification of the Withdrawal Status Online

Not applicable.

4.9.11. Other Forms of Withdrawal Notices Available

The RK NCA places the RCRL on the home page of the RK NCA Internet resource in the “Certificate Withdrawal List” Section.

4.9.12. Specific Requirements to the Replacement of a Compromised Key Pair

The RK NCA subscribers shall be informed of a compromise or a suspected compromise of the RK NCA private keys through any appropriate means.

In the event of reasonable suspicion of the private key compromise, the subscriber and holder of the corresponding registration certificate shall revoke the RK NCA registration certificate immediately in accordance with Clause 4.9 and request the issuance of new registration certificates for their replacement.

4.9.13. Grounds for Termination of a Registration Certificate

Not applicable.

4.9.14. Persons Entitled to Request the Termination of a Registration Certificate

Not applicable.

4.9.15. Procedure for Application to Terminate a Registration Certificate

Not applicable.

4.9.16. Suspension Period for a Registration Certificate

Not applicable.

4.10. SERVICES FOR VERIFICATION OF THE RK NCA SUBSCRIBERS' REGISTRATION CERTIFICATE STATUS

4.10.1. Operating Characteristics

The information on the RK NCA subscriber's registration certificate status is available at the addresses, specified in Clause 2.2.1 hereof through the RCRL and OCSP services.

4.10.2. Services' Business Hours

The services for verification of the RK NCA subscriber's registration certificate status are available continuously 24 hours a day, 7 days a week, with a total downtime of not more than 1.5 hours per quarter.

4.10.3. Extra Features

Not applicable.

4.11. EXPIRY OF THE PERIOD OF THE RK NCA SUBSCRIBER'S REGISTRATION CERTIFICATE VALIDITY.

The RK NCA subscriber's registration certificate shall be considered invalid upon the expiry of period of its validity in accordance with Clause 6.3.2 hereof.

The RK NCA subscriber shall be entitled to revoke the RK NCA subscriber's registration certificate before the expiry of period of its validity in accordance with Clause 3.4 hereof.

4.12. DEPOSITION AND RESTORATION OF COMPLEMENTARY KEYS

The RK NCA shall not allow deposition and restoration of the key pairs owned by subscribers and the RK NCA.

4.12.1. Policy and Practice of Deposition and Restoration of Key Pairs

Not applicable.

4.12.2. Policy and Practice of Encapsulation and Restoration of Key Pairs

Not applicable.

5. ADMINISTRATIVE, OPERATIONAL AND PHYSICAL CONTROLS

5.1. PHYSICAL SECURITY CONTROL OF THE RK NCA ASSETS

The RK NCA provides physical security for the RK NCA 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 RK NCA and therefore cannot be published. The “

Administrative, operational and physical controls" Section of this Certificate Practice Statement provides an overview of these measures.

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

- physical security provision for the RK NCA employees;
- provision of the correct operation of the RK NCA systems hardware, as well as systems for transmission and storage of the RK NCA information and data storage devices relating to the RK NCA;
- information security provision for RK NCA;
- performance control of the RK NCA physical security.

5.1.1. Location of the RK NCA Assets

In the buildings where the RK NCA information assets are located the following conditions shall be provided:

- physical security for the RK NCA activities in accordance with Clause 5.1 hereof;
- back-up facilities for continuous activity of the RK NCA in cases of emergency.

5.1.2. Physical Access to the RK NCA information assets

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

The safety levels functioning is provided by technical and organizational measures aimed at:

- prevention of unauthorized physical access - through the systems for physical access limitation (tourniquets, lockable doors, security, duty officers);
- automatic fixation of the physical access situations - through 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 RK NCA key material - through the use of safes and secure uncrackable containers in physically secure locations, with mandatory logging of the situations of access to the safes and containers, where the RK NCA 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 RK NCA employees.

5.1.3. Electric Supply and Maintenance of a Microclimate in the Area of the RK NCA Hardware Location

The location area of the hardware which maintains the RK NCA 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 RK NCA 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. Water Exposure

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

5.1.5. Impact of Natural Disasters on the Hardware Location Area

The location area of the RK NCA information assets hardware 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 in the Location Area of the Hardware

The location area of the RK NCA systems hardware 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 RK NCA data storage devices

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

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

5.1.8. Disposal of the RK NCA Data Storage Devices and Hardware

The RK NCA provides disposal of the data storage devices and hardware in accordance with technical documentation for the data storage devices and hardware, as well as other requirements.

All the storage devices which used to contain confidential information, shall be made unreadable. RK NCA provides disposal of the data storage devices for cryptographic hardware in accordance with Clause 6.2.1 hereof.

5.1.9. RK NCA Information Back-Up

The RK NCA carries out back-up of the RK NCA systems software, their data, logs, confidential information and RCRL.

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

1) unauthorized access to the back-ups;
2) corruption of the back-ups;
3) destruction of the back-ups.

5.2. RK NCA RESPONSIBILITY AND ACTIVITY CONTROL

5.2.1. Distribution of Responsible Roles

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

- verification of information contained in the applications for the registration certificate issuance;
- acceptance, refusal of acceptance or other processing types referred to the applications for issuance or withdrawal of the registration certificates;
- issuance or withdrawal of the registration certificates.

The responsible roles include but are not limited to the following functions:

- the RK NCA subscribers support;
- operations with cryptographic hardware;
- management and provision of information security;
- management and provision of physical security;
- administration of the RK NCA systems software;
- maintenance of the RK NCA systems hardware;
- management and provision of the RK NCA service infrastructure.

The RK NCA provides compliance of employees performing all the responsible roles with competence requirements in accordance with Clause 5.3.1 and Clause 5.3.2 hereof.

5.2.2. Number of Personnel Required for a Particular Task

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

In particular, the tasks of the RK NCA subscriber's registration certificates lifecycle management involve participation of at least two independent parties - the CA operator and the STS RSE executive officer. The tasks of the RK NCA key material management, access management referred to the RK NCA IS, management of alterations

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

5.2.3. Identification and Authentication of a Responsible Role

Official activities of the STS RSE employees performing responsible roles may be carried out only within the STS RSE physically protected perimeter in accordance with Clause 5.1.2 hereof. Access of employees to the protected perimeter allowed upon the employee's identity authentication. Operation of the RK NCA IS may also be allowed upon the STS RSE employees' identity authentication.

5.2.4. RK NCA PKI functions requiring separation of duties

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

- the RK NCA IS administration;
- the RK NCA systems development;
- the RA operators work.

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

5.3. SECURITY PROVISION FOR THE RK NCA EMPLOYEES

The STS RSE provides security for the STS RSE employees in accordance with:

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

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

5.3.1. Requirements to Experience and Qualifications of the RK NCA Employees

The STS RSE provides the employees compliance with the minimum requirements for experience and qualifications in accordance with:

- the STS RSE internal recruitment policies and service instructions.
- the internal policies of the organizations which provide operation of the RK NCA IS;
- 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 STS RSE Employees' Verification

The STS RSE verifies employees before employment and during the period of the employment contract validity in accordance with:

- the internal recruitment policies and service instructions of the STS RSE or State Corporation;
- the internal policies of the organizations which provide operation of the RK NCA IS;
- the current legislation of the Republic of Kazakhstan.

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

- compliance with the experience and qualifications requirements in accordance with Clause 5.3.1 hereof;
- provision of the necessary verification letters and confirmations in accordance with the current legislation of the Republic of Kazakhstan and role of the STS RSE employee.

5.3.3. Requirements to Professional Development of the STS RSE Employees

The STS RSE provides professional development of the employees aimed at competent and high-quality performance of official duties. The professional development of the STS RSE 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. Frequency of Professional Development of the STS RSE Employees

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

- the needs of the RK NCA activities performance aims;
- the internal recruitment policies and service instructions;
- the legislation of the Republic of Kazakhstan.

5.3.5. Frequency and Sequence of Career Development of the STS RSE Employees

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

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

The decisions on the STS RSE employees' displacement shall be approved by the STS RSE Director or an authorized deputy.

5.3.6. STS RSE Employees' Responsibility for Unauthorized Actions

The STS RSE employees, as well as the CA operators shall be responsible for compliance with internal regulations in accordance with:

- the internal policies and service instructions for the STS RSE or State Corporation employees;
- the internal policies of the organizations which provide operation of the RK NCA systems;
- the legislation of the Republic of Kazakhstan.

Upon detection of unauthorized actions or suspicion of committing unauthorized actions, the person, who found a violation, informs the STS RSE information security department. The executive officer of the STS RSE information security department 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, established by the above-mentioned rules and regulations.

5.3.7. Requirements to the Independent Parties

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

The following organizations are allowed to participate as independent observers:

- the competent authorities relating to the RK NCA PKI or RK RCA PKI functioning (for example, RK NSC, Prime Minister's Office of the Republic of Kazakhstan, etc.);
- certification bodies on the basis of services performance agreements and nondisclosure agreements (for example, for certification purposes referred to the RK NCA equipment, WebTrust auditors, etc.).

5.3.8. Documents Disclosed by Employees of the RK NCA and STS RSE

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

- training and professional development in accordance with service instructions contained in Clause 5.3.3 hereof;
- the official duties performance.

The materials provision shall be carried out in accordance with:

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

5.4. DOCUMENTATION OF EVENTS (LOGGING) IN THE RK NCA IS

5.4.1. Types of the events logged

The RK NCA maintains and stores logs for the following event types:

1) lifecycle management events for the RK NCA key pairs, including generation;
2) lifecycle management events for the RK NCA registration certificates, including:
   - application for the issuance and withdrawal of the RK NCA registration certificate;
   - successful or unsuccessful processing of applications for the issuance and withdrawal of the RK NCA registration certificates;
   - generation and publication of the RCRL.
3) the events related to the provision of physical and information security by the RK NCA:
   - update or modification of the RK NCA systems;
   - access management referred to the RK NCA systems or changing of the access management policies

(including the users' roles and profiles);
- the information security events (including attempts to obtain access to the RK NCA confidential information and systems - both successful and unsuccessful);
- software and hardware failures and mistakes of the RK NCA IS;
- The RK NCA does not allow the explicit recording of keys and passwords.

5.4.2. Frequency of the Control Protocol Analysis

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

A verification of integrity, unauthorized activity and alterations in archive logs of events of the CA by calculating the checking sum and printing the data received shall be carried out on a continuous basis, but not less than half-yearly.

5.4.3. Logs Validity

The RK NCA stores the logs within for at least 90 days, after which the logs are subject to archiving and copying to a dedicated server with the help of regular means of the operating system in accordance with Clause 5.5 hereof.

5.4.4. Logs Protection

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

5.4.5. Logs Back-Up

The RK NCA carries out the logs back-up quarterly. The back-ups are stored providing their integrity.

5.4.6. Log Collection System (Internal and External)

The key events from the RK NCA external systems are further forwarded to a dedicated log collection system – "Syslog Server" for further analysis in the automatic mode by security system.

5.4.7. Notice to the Subject Induced an Event

Not specified.

5.4.8. Vulnerability Analysis

The RK NCA carries out a periodic assessment of vulnerabilities, as well as vulnerabilities, identified in the course of the RK NCA internal control system operation in accordance with:
- the STS RSE internal policies (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 RK NCA systems;
- the requirements of the legislation of the Republic of Kazakhstan.

5.5. RECORDS ARCHIVE

5.5.1. Types of the Events to be Archived

The RK NCA provides archival storage for the following types of information in accordance with the requirements of the current legislation of the Republic of Kazakhstan:
- event logs;
- current and withdrawn subscribers' registration certificates;
- current and withdrawn RK NCA registration certificates;
- applications for issuance and withdrawal of the subscribers' registration certificates;
- withdrawn registration certificate lists owned by subscribers and the RK NCA.

5.5.2. Archive Validity

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

- the current legislation of the Republic of Kazakhstan.

5.5.3. Archive Protection

The RK NCA protects archive materials in accordance with:

- the STS RSE internal policies for each data type;
- the internal policies of the organizations which provide operation of the RK NCA systems;
- the current legislation of the Republic of Kazakhstan.

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

5.5.4. Archive Back-Up

The data stored in the archive, are subject to back-up in accordance with the requirements for the periodic back-up. The archive back-ups are stored in a physically protected storage location in accordance with the current legislation of the Republic of Kazakhstan.

5.5.5. Requirements to the Record Time Marking

The RK NCA conducts automatic registry of the archive materials with automatic indication of the archive entry date. The registry of the archive materials shall be signed with the RK NCA root certificate.

5.5.6. Archive Data Collection System (Internal and External)

The RK NCA provides archive data collection in accordance with:

- the STS RSE internal policies for each data type;
- the internal policies of the organizations which provide operation of the RK NCA systems;
- the current legislation of the Republic of Kazakhstan.

5.5.7. Archiving Conditions

The materials archiving shall be carried out in accordance with:

- the STS RSE internal policies for each data type;
- the internal policies of the organizations which provide operation of the RK NCA systems;
- the legislation of the Republic of Kazakhstan.

5.5.8. Procedure for Acceptance and Verification of Archive Information

The access to the archive materials is limited in accordance with Clause 5.5.3 hereof. The STS RSE executive officers carry out verification of the archive information in accordance with Clause 5.7 hereof.

5.6. ISSUANCE OF THE RK NCA KEYS

The RK NCA issuances the RK NCA key pairs and registration certificates upon expiry of the root registration certificate or in the event of key pairs compromise. In which case RK NCA:

- terminates application of the old key pairs and corresponding registration certificates;
- generates new key pairs and corresponding root registration certificates.

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

5.7. COMPROMISE AND DISASTER RECOVERY OF THE RK NCA KEYS

5.7.1. The procedures for processing of incidents and compromise

The RK NCA provides creation, and secure storage of the critical data back-ups in the event of incidents or compromise:

- applications for issuance and alteration of the registration certificate status;
- event logs;
- withdrawn registration certificate lists;
- the RK NCA key pairs.

In the event of incidents in the RK NCA, as well as upon detection of compromise or suspicion of compromise of the RK NCA private keys, the procedures in accordance with the requirements of the legislation of the Republic of Kazakhstan and internal rules and regulations of the RK NCA 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 RK NCA risk assessment.

5.7.2. Damage of Computing, Software Resources and / or Data

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

5.7.3. RK NCA Private Key Compromise

The RK NCA provides the internal control system operation which includes monitoring for possible compromise of the RK NCA the private keys. In the event of compromise detection or presence of reasonable suspicions of compromise referred to the RK NCA private keys the Plan of continuity and recovery of the RK RCA and the RK NCA activities shall be applied.

If it is necessary to reissuance the RK NCA key pairs, the procedure described in Clause 6.1 hereof shall be carried out. In this case a notice on the RK NCA key pairs reissuance shall be send to all the RK NCA PKI participants.

5.7.4. Potential for Continuous Operations after Incidents

The RK NCA has approved and tested the detailed Plan for activities recovery, aimed at mitigating the consequences of threats, including natural catastrophes. The Plan for activities recovery shall be regularly reviewed for the purposes of update in accordance with the RK NCA internal risk assessment procedures.

The RK NCA has back-up systems aimed at provision of the continuity of the RK NCA services and key functions. The information contained in the RK NCA main system is synchronized with back-up systems online.

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

- The target time for a full recovery of the RK NCA IS (RTO) = 2 months 4 hours 25 minutes 39 seconds;
- The partial recovery time of the RK NCA IS (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, RK NCA regularly tests the Plan of continuity and recovery of the RK RCA and the RK NCA activities shall be applied.

5.8. RK NCA ACTIVITY TERMINATION

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

- a notice containing information on the RK NCA status for the parties, affected by termination of the RK NCA activities, including the RK NCA PKI subscribers and participants;
- storage of the RK NCA archives in accordance with the requirements of the legislation of the Republic of Kazakhstan and corresponding policy on use referred to the subscribers' registration certificates;
- continuation of support services for the subscribers and customers;
- continuation of withdrawal checking services, such as the OCSP service and issuance of the withdrawn registration certificate lists;
- withdrawal of the current subscribers' registration certificates which have not been withdrawn earlier, when appropriate;
- issuance of the replacement registration certificates by certification authority-successor;
- further location of the RK NCA private keys and cryptographic modules, containing these private keys;
- provisions necessary for the services transmission by the RK NCA to its successor.

6. MONITORING OF THE RK NCA TECHNICAL SAFETY

6.1. ISSUANCE AND INSTALLATION OF THE RK NCA KEY PAIRS AND RK NCA SUBSCRIBERS

6.1.1. Generation of the RK NCA key pair

The RK NCA generates all key pairs used in the RK NCA PKI. Generation of key pairs is carried out by means of encryption protection modules certified in accordance with applicable standards of the Republic of Kazakhstan RK ST 1073-2007 at the level not lower than the second one.

Generation of the RK NCA key pairs is carried out exclusively in accordance with the approved internal regulations with the participation of authorized responsible officials and under the supervision of an independent party. Ceremony of generation of the RK NCA key pairs is activated in accordance with 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.

6.1.2. Delivery of the Private key to the RK NCA Subscriber

Currently, the RK NCA issuances key pairs to the RK NCA subscribers only with use of the following media types:

1) on the ID (for individuals, citizens of the Republic of Kazakhstan);

2) directly on the certified secured media that excludes possibility of keying material compromise (disclosure or modification), such as KazToken, JaCarta, eToken;

3) on the file system of a subscriber.

Key pairs of the RK NCA subscribers are password protected in accordance with Clause 6.4.1 hereof.

Record of key pairs on the ID is carried out by one of the following methods:

1) in the case of online filling an application on a stand-alone basis for registration certificate issuance, record is provided independently by the certified service receiver by means of smart card reader;

2) in the case of a personal filling an application by service receiver or his representative to the RA, record is provided by the CA operator by means of smart card reader.

Key pairs on a certified secured media shall be registered as follows:

1) in the case of online filling an application on a stand-alone basis for registration certificate issuance, record is provided independently by the certified service receiver on a certified secured media.

The RK NCA maintains internal monitoring through the organizational and technical measures to avoid storing of subscribers' private keys in the RK NCA in any form.

6.1.3. Public Key Delivery to the RK NCA Subscriber of the RK NCA IS

The public key of a RK NCA subscriber is generated as a part of key pairs, and thus does not require delivery to the RK NCA IS.

6.1.4. Delivery of the RK NCA Public Key to the Relying Party

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

6.1.5. Keys Sizes

Key pairs of the RK NCA subscribers are released in accordance with RSA (PKCS No.1) algorithm and have the following length:

- private key - 2048 bit;
- public key- 2048 bit.

The RK NCA also releases subscribers' key pairs for legal entities in accordance with GOST algorithm and have the following length:

- private key – 256 bit;
- public key- 512 bit.

6.1.6. Parameters of Public Key Generation

Parameters of public key generation are defined in Clause 6.1.1.

6.1.7. Purposes of Key Use

In accordance with above mentioned Clause **Ошибка! Источник ссылки не найден.**.

6.2. PROTECTION CONTROLS OF THE NCA RK PRIVATE KEYS AND RK NCA SUBSCRIBERS, AND LIFE-CYCLE MANAGEMENT FOR THE NCA RK CRYPTOGRAPHIC HARDWARE

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

6.2.1. Standards and Control of Cryptographic Hardware

The RK NCA allows only cryptographic hardware certified for compliance with the applicable standards in the Republic of Kazakhstan that determine general technical requirements to the means of cryptographic information protection for compliance not lower than the second level of security.

The RK NCA implements a number of technical and organizational measures to ensure the confidentiality and integrity of the cryptographic hardware during transportation, commissioning and operation in the main and backup RK NCA sites. RK NCA also implements a number of technical and organizational measures to ensure the operation and maintenance of cryptographic hardware in strict correspondence with its technical and operational documentation, as well as the internal regulations of physical security in accordance with Clause 5.1 hereof and Rules of procedure in accordance with the Clause 5.2 hereof.

The RK NCA cryptographic hardware shall be stored and used only in the dedicated protected RK NCA objects. Decommissioning of the RK NCA cryptographic hardware for repair shall be accompanied by a guaranteed cleaning and, if possible, physical destruction of the memory storage devices. The final decommissioning of the RK NCA cryptographic hardware shall be accompanied by physical destruction of cryptographic hardware in a secure environment.

Arrangements for reception, maintenance and decommissioning of the RK NCA cryptographic hardware shall be carried out in the presence of authorized responsible officials included in a list of trusted roles in accordance with Clause 5.2 hereof.

6.2.2. Sharing of the RK NCA Private Key between Responsible Parties under the Scheme of m from n

Cryptographic operations are carried out manually and require the use of the RK NCA private keys made with the use of a backup copy of the RK NCA private key, secured by means of the shared secret. In this regard, the information necessary to restore the backup copy of the RK NCA private key ("secret") are shared into n parts. The successful restore of the backup copy of the RK NCA private key requires at least m secret parts. In generating the m and n secret is defined by the formula: $n > m + 1$.

Secret parts are stored by the responsible participants of the RK NCA key pairs generation in accordance with the requirements of the Republic of Kazakhstan legislation and the RK NCA internal regulatory documentation in accordance with Clause6.4.1 hereof.

6.2.3. Private Key Deposition of the RK NCA Subscribers

Private keys of the RK NCA subscribers are not deposited.

6.2.4. Backup Copy of the RK NCA Private Key

In the event of the RK NCA private keys damage or inaccessibility, there are available its backup copies in the RK NCA key pairs generation. Backup RK NCA key pairs are protected by the secret in accordance with Clause 6.2.2 hereof.

The backup procedure is regulated and documented to ensure the RK NCA control environment functioning and possibility for private keys recovery.

6.2.5. RK NCA Private Key Archiving

Archiving of expired RK NCA private keys is not allowed.

6.2.6. Import and Export of the RK NCA Private Keys Stored in Cryptographic Modules

The RK NCA key material outside the cryptographic module exists solely in encrypted form to ensure the integrity and confidentiality of the RK NCA key material.

Cryptographic key material export from RK NCA cryptographic modules is possible only as a backup of the private key, according to Clause 6.2.4 hereof.

6.2.7. Storage of the RK NCA Private Key in the Cryptographic Module and Subscriber's Private keys on the Secured Media

Cryptographic modules that store the RK NCA private keys, does not allow storage of key material in an unencrypted form in the hardware, including RAM.

Private keys of the RK NCA subscribers that stored in certified secured media are stored in accordance with the requirements of the standard PKCS No. 11.

6.2.8. Activation Methods for the RK NCA Private key and Subscribers

Prior to use, the RK NCA private keys are activated manually in accordance with Clause 6.2.1 hereof.

Prior to use, private keys of the RK NCA subscribers are activated by setting a password. Further use of the private keys is possible just after password entering.

6.2.9. Deactivation Methods for Personal Key

The RK NCA private key deactivation is not provided due to its safe storage on the RK NCA hardware and cryptographic module.

6.2.10. Destruction Methods for RK NCA Private key and the RK NCA Subscribers

All decommissioned parts of the RK NCA private keys shall be destructed with guaranteed recovery impossibility. Destruction of the RK NCA private key is carried out by authorized officials in the presence of a monitoring person.

Private keys destruction of the RK NCA subscribers is the responsibility of the RK NCA subscribers.

6.2.11. RK NCA Cryptographic Modules Analysis

All cryptographic modules used by the RK NCA are certified in accordance with the requirements of applicable standard of the Republic of Kazakhstan RK ST 1073-2007 and are not lower than the second level. The use of non-certified cryptographic modules is not allowed in accordance with the internal regulations of the RK NCA, this Statement and Policy for use of the registration certificates.

6.3. OTHER ASPECTS OF MANAGEMENT FOR RK NCA KEY PAIRS

6.3.1. RK NCA Public Keys Archiving

All RK NCA public keys and the RK NCA subscribers which ever have the registration certificates are archived in the composition of the relevant registration certificates in accordance with Clause 5.5 hereof.

6.3.2. Validity of Registration Certificates and Key pairs Use

The validity of the RK NCA registration certificates is 5 years. The validity of the RK NCA registration certificates is 1 year. The validity of the RK NCA registration certificates of TSP and OSCP services is 1 year. In case of withdrawal of the RK NCA registration certificates or RK NCA subscribers the validity period ends at the time of the withdrawal. The use of key pairs of withdrawn RK NCA registration certificates or the RK NCA subscribers is not allowed.

6.4. ACTIVATION DATA

6.4.1. Generation and Installation of Activation Data for Private keys

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

The RK NCA private keys generation is accompanied with creation of the “secret” on the secured media of key information in accordance with the procedure in accordance with Clause 6.2.2 hereof. The use of ‘secret’ requires two-factor authentication, that is use of the media of the secret party and the corresponding unique PIN-code.

Responsible participants of the RK NCA private keys generation are selected on the basis of compliance with the separation principle for powers and independence. Activation data of each secret part entrusted to the responsible participant are entered directly by the responsible participant and not disclosed by the other responsible participants.

The RK NCA private keys have password protection, password is defined by the subscriber in key pairs generation on the ID or secured media. Subscriber private keys generated on the file system are protected by a standard password "123456" which shall be changed immediately by the subscriber after key generation.

6.4.2. Activation Data Protection

Participants of the RK NCA PKI shall provide activation data protection for their private keys or for secret trusted part of the RK NCA private key against disclosure and change and also ensure the availability of their activation data.

Responsible participants of the RK NCA key pairs generation accept responsibility for storage of the entrusted secret and activation data in a written form.

The RK NCA Subscribers are responsible for password protection of their private key against disclosure in accordance with the requirements of the Republic of Kazakhstan legislation, the requirements hereof and the RK NCA PKI User Agreement for state service.

6.4.3. Other Aspects of Data Activation

Activation data of the RK NCA private keys are derived from the use with the help of procedures to protect against loss, theft, modification, disclosure or unauthorized use of private keys activated by these data. Activation data that are not a subject to further storage are derived from the use by means physical destruction.

6.5. COMPUTER SECURITY CONTROLS

6.5.1. Special Technical Requirements to Computer Security

The RK NCA hardware and software is protected by means of:

- organizational and technical security arrangement (including access control, software update control, virus protection and so on);
- event recording.

6.5.2. Computer Security Evaluation

The RK NCA uses certified computer security tools, this is evidenced by the successful evaluation of high level security.

The RK NCA provides periodic evaluation of the infrastructure vulnerabilities with risk evaluation and subsequent risk handling.

6.6. CONTROLS FOR SECURITY LIFE-CYCLE

6.6.1. System Development Control

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

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

6.6.2. Security management control

The RK NCA maintains a security management control in accordance with the requirements of RK ST ISO/IEC 27001 standard and internal documents of the STS RSE.

6.6.3. Management of security life-cycle

The RK NCA maintains a security management control in accordance with the requirements of the RK ST ISO/IEC 27001 Standard.

6.7. NETWORK SECURITY CONTROL

The RK NCA provides security of its internal networks, as well as the security of data transmitted over the external networks. The RK NCA provides organizational and technical measures against unauthorized access and attacks on their networks. Policies and procedures on network security control are documented and approved, but not published because they contain confidential information of the RK NCA.

6.8. TIME STAMP MAKING

By means of a special registration certificate, the RK NCA signs information on date and exact time of the events recorded, including:

- Date and exact time of life-cycle events of registration certificates;
- Date and exact time of issuance and validity of withdrawal lists of registration certificates;
- Date and exact time of responses from the services on registration certificates status verification.

7. STRUCTURE OF THE NCA RK SUBSCRIBER'S REGISTRATION CERTIFICATE AND RCRL

7.1. STRUCTURE OF NCA RF SUBSCRBER'S REGISTRATION CERTIFICATE

7.1.1. Structure of the Reassigned Registration Certificate of the National Certification Authority of the Republic of Kazakhstan (under the RSA Algorithm)

Field	Description	OID, criticality	Content
Base fields of the registration certificate in X.509 v3 format			
Version	Version of X.509 standard	–	V3
SerialNumber	Registration certificate serial number	–	Positive integer (up to 20 byte)
Signature Algorithm	Signature algorithm	1.2.840.113549.1.1.11	sha256WithRSAEncryption
Issuer	Data on the registration certificate issuer	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
Validity from	Validity from	UTC TIME	Valid from: YYMMDDHHMMSSZ UTC
Validity to	Validity to	UTC TIME	Valid to: YYMMDDHHMMSSZ UTC
Subject	Data on registration certificate owner	C=2.5.4.6 L= 2.5.4.7 S=2.5.4.8 O=2.5.4.1 0 CN =2.5.4.3	C = KZ (required field) L = ASTANA (required field) S = ASTANA (required field) O = РМК «МЕМЛЕКЕТТІКТЕХНИКАЛЫҚҚЫЗМЕТ» (required field) CN = ҰЛТТЫҚҚУӘЛАНДЫРУШЫОРТАЛЫҚ (RSA) (required field)
PublicKey	Public key	1.2.840.113549.1.1.1	Value
Additional fields of the registration certificate in X.509 v3 format			
Subject Key Identifier	Subject key identifier	2.5.29.14	Value of subject key identifier in hexadecimal format
Authority Key Identifier	Authority key identifier	2.5.29.35	Value of authority key identifier in hexadecimal format
Basic Constraints	Basic constraints	2.5.29.19, critical	Subject type = Certification authority Constraints for path length = Not available
Key Usage	Key usage	2.5.29.15, critical	Registration certificate signing, Withdrawal list autonomous signing (CRL), Withdrawal list signing (CRL) (06)
Ceritifcate Policy	Registration certificate policy	2.5.29.32	[1] Registration certificate policy: Policy identifier = 1.2.398.3.3.1.1 [1,1] Data on policy qualifier: Identifier of policy qualifier = CPS Qualifier: http://pki.gov.kz/cps
Ceritifcate Authority Information Access	Certificate authority information access	1.3.6.1.5.5.7.1.1	[1]Certificate Authority Information Access Access method = Certificate authority vendor (1.3.6.1.5.5.7.48.2)

			Additional name: URL=http://root.gov.kz/cert/root_rsa.cer
Crl Distribution Points	Withdrawal lists distribution points	2.5.29.31	[1] Withdrawal list distribution point (CRL) Distribution point name: Full name: URL=http://crl.root.gov.kz/rsa.crl URL=http://crl1.root.gov.kz/rsa.crl
Digital Signature	Certificate authority digital signature (2048 bit)	1.2.840.113549.1.1.11	Value

7.1.2. Structure of the Reassigned Registration Certificate of the National Certification Authority of the Republic of Kazakhstan (under the GOST Algorithm).

Field	Description	OID, criticality	Content
Base fields of the registration certificate in X.509 v3 format			
Version	Version of X.509 standard	–	V3
Serial Number	Registration certificate serial number	–	Positive integer (up to 20 byte)
Signature Algorithm	Signature algorithm	1.2.398.3.10.1.1.1.2	GOST 34.310-2004
Issuer	Data on registration certificate issuer	CN=2.5.4.3 O=2.5.4.10 C=2.5.4.6	CN = НЕГІЗГІ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST) O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» C = KZ
Validity from	Validity from	UTC TIME	Valid from: YYMMDDHHMMSSZ UTC
Validity to	Validity to	UTC TIME	Valid to: YYMMDDHHMMSSZ UTC
Subject	Data on registration certificate owner	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	C = KZ (required field) L = ASTANA (required field) S = ASTANA (required field) O = РМК «МЕМЛЕКЕТТІКТЕХНИКАЛЫҚҚЫЗМЕТ» (required field) CN = ҰЛТТЫҚҚУӘЛАНДЫРУШЫОРТАЛЫҚ (GOST) (required field)
Public Key	Public key (512 bit)	1.2.398.3.10.1.1.1.1 with characteristics 1.2.398.3.10.1.1.1.1.1 1.2.398.3.10.1.3.1.1.0	Value
Additional fields of the registration certificate in X.509 v3 format			
Subject Key Identifier	Subject key identifier	2.5.29.14	Value of subject key identifier in hexadecimal format
Authority Key Identifier	Authority key identifier	2.5.29.35	| Value of authority key identifier in hexadecimal format
Basic Constraints	Basic constraints	2.5.29.19, critical	Subject type = Certification authority Constraints for path length = Not available
Key Usage	Key usage	2.5.29.15, critical	Registration certificate signing, Withdrawal list autonomous signing (CRL), Withdrawal list signing (CRL) (06)
Ceritifcate Policy	Registration certificate policy	2.5.29.32	[1] Registration certificate policy: Policy identifier =1.2.398.3.3.1.1 [1,1] Data on policy qualifier: Identifier of policy qualifier = CPS Qualifier: http://pki.gov.kz/cps
Ceritifcate Authority	Certificate authority information access	1.3.6.1.5.5.7.1.1	[1] Certificate Authority Information Access Access method = Certificate authority vendor

Information Access			(1.3.6.1.5.5.7.48.2) Additional name: URL=http://root.gov.kz/cert/root_gost.cer
Crl Distribution Points	Withdrawal lists distribution points	2.5.29.31	[1] Withdrawal list distribution point (CRL) Distribution point name: Full name: URL=http://crl.root.gov.kz/gost.crl URL=http://crl1.root.gov.kz/gost.crl
Digital Signature	Certificate authority digital signature (512 bit)	1.2.398.3.10.1.1.1.2	Value

7.1.3. Structure of User's Registration Certificate (individual person) of the National Certification Authority of the Republic of Kazakhstan (for signature)

Field	Description	OID, criticality	Content
Base fields of the registration certificate in X.509 format			
Version	Version of X.509 standard	–	V3
Serial Number	Registration certificate serial number	–	Positive integer (up to 20 byte)
Signature Algorithm	Signature algorithm	1.2.840.113549.1.1.11	sha256WithRSAEncryption
Issuer	Data on registration certificate issuer	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	C = KZ (required field) L = ASTANA (required field) S = ASTANA (required field) O = РМК «МЕМЛЕКЕТТІКТЕХНИКАЛЫҚҚЫЗМЕ» (required field) CN = ҰЛТТЫҚҚУӘЛАНДЫРУШЫОРТАЛЫҚ (RSA) (required field)
Validity from	Validity from	UTC TIME	Valid from: YYMMDDHHMMSSZ UTC
Validity to	Validity to	UTC TIME	Valid to: YYMMDDHHMMSSZ UTC
Subject	Data on registration certificate owner	E =1.2.840.113549.1.9.1 SERIALNUMBER = 2.5.4.5 SN=2.5.4.5 G=2.5.4.42 CN =2.5.4.3 L=2.5.4.7 S=2.5.4.8 C=2.5.4.6	E = E-mail address (not required field) SERIALNUMBER = IIN012345678910 (required field) SN = Surname (not required field) G = Patronymic (not required field) CN = Surname Name (required field) L = City (required field) S = Region (required field) C = KZ (required field)
PublicKey	Public key value (2048 bit)	1.2.840.113549.1.1.1	Value
Additional fields of the registration certificate in X.509 format			
Subject Key Identifier	Subject key identifier	2.5.29.14	Value of subject key identifier in hexadecimal format
Authority Key Identifier	Authority key identifier	2.5.29.35	Value of authority key identifier in hexadecimal format
Key Usage	Key usage	2.5.29.15, critical	Digital signature, Imputability
Extended Key Usage	Extended key usage	2.5.29.37	Protected e-mail -1.3.6.1.5.5.7.3.4 Individual person - 1.2.398.3.3.4.1.1
Ceritifcate Policy	Registration certificate policy	2.5.29.32	[1] Registration certificate policy: Policy identifier =1.2.398.3.3.2.3 [1,1] Data on policy qualifier: Identifier of policy qualifier = CPS Qualifier: http://pki.gov.kz/cps

			[1,2] Data on policy qualifier: Identifier of policy qualifier = Text of the notification Qualifier: http://pki.gov.kz/cps
Ceritifcate Authority Information Access	Certificate authority information access	1.3.6.1.5.5.7.1.1	[1] Certificate Authority Information Access Access method = Certificate authority vendor (1.3.6.1.5.5.7.48.2) Additional name: URL=http://pki.gov.kz/cert/pki_rsa.cer [2] Certificate Authority Information Access Access method= Protocol determining the registration certificate status through network (1.3.6.1.5.5.7.48.1) Additional name: URL=http://ocsp.pki.gov.kz
Crl Distribution Points	Withdrawal lists distribution points	2.5.29.31	[1] Withdrawal list distribution point (CRL) Distribution point name: Full name: URL= http://crl.pki.gov.kz/rsa.crl URL= http://crl1.pki.gov.kz/rsa.crl
Freshest Crl Distribution Points	Freshest CRL	2.5.29.46	[1] Freshest CRL Distribution point name: Full name: URL= http://crl.pki.gov.kz/d_rsa.crl URL= http://crl1.pki.gov.kz/d_rsa.crl
Digital Signature	Certificate authority digital signature (4096 bit)	1.2.840.113549.1.1.11	sha256WithRSAEncryption

7.1.4. Registration Certificate Structure for the User (Individual) of the National Certification Authority of the Republic of Kazakhstan (for Authentication)

Field	Description	OID, criticality	Content
Base fields of the registration certificate in X.509 format			
Version	Version of X.509 standard	–	V3
Serial Number	Registration certificate serial number	–	Positive integer (up to 20 byte)
Signature Algorithm	Signature algorithm	1.2.840.113549.1.1.11	sha256WithRSAEncryption
Issuer	Data on registration certificate issuer	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	C = KZ (required field) L = ASTANA (required field) S = ASTANA (required field) O = РМК «МЕМЛЕКЕТТІКТЕХНИКАЛЫҚҚЫЗМЕТ» (required field) CN = ҰЛТТЫҚҚУӘЛАНДЫРУШЫОРТАЛЫҚ (RSA) (required field)
Validity from	Validity from	UTC TIME	Valid from: YYMMDDHHMMSSZ UTC
Validity to	Validity to	UTC TIME	Valid to: YYMMDDHHMMSSZ UTC
Subject	Data on registration certificate owner	E =1.2.840.113549.1.9.1 SERIALNUMBER = 2.5.4.5 SN=2.5.4.5 G=2.5.4.42 CN =2.5.4.3 L=2.5.4.7 S=2.5.4.8 C=2.5.4.6	E = E-mail address of the individual person (not required field) SERIALNUMBER = IIN012345678910 (required field) SN = Surname (not required field) G = Patronymic (not required field) CN = Surname Name (required field) L = City (required field) S = Region (required field) C = KZ (required field)
PublicKey	Public key value (2048	1.2.840.113549.1.1.1	Value

	bit)		
Additional fields of the registration certificate in X.509 format			
Subject Key Identifier	Subject key identifier	2.5.29.14	Value of subject key identifier in hexadecimal format
Authority Key Identifier	Authority key identifier	2.5.29.35	Value of authority key identifier in hexadecimal format
Key Usage	Key usage	2.5.29.15, critical	Digital signature, key encryption
Extended Key Usage	Extended key usage	2.5.29.37	Client authentication -1.3.6.1.5.5.7.3.2 Individual person- 1.2.398.3.3.4.1.1
Ceritifcate Policy	Registration certificate policy	2.5.29.32	[1]Registration certificate policy: Policy identifier =1.2.398.3.3.2.4 [1,1] Data on policy qualifier: Identifier of policy qualifier= CPS Qualifier: http://pki.gov.kz/cps [1,2] Data on policy qualifier: Identifier of policy qualifier = Text of the notification Qualifier: http://pki.gov.kz/cps
Ceritifcate Authority Information Access	Certificate authority information access	1.3.6.1.5.5.7.1.1	[1] Certificate Authority Information Access Access method = Certificate authority vendor(1.3.6.1.5.5.7.48.2) Additional name: URL=http://pki.gov.kz/cert/pki_rsa.cer [2] Certificate Authority Information Access Access method = Protocol determining the registration certificate status through network (1.3.6.1.5.5.7.48.1) Additional name: URL=http://ocsp.pki.gov.kz
Crl Distribution Points	Withdrawal lists distribution points	2.5.29.31	[1] Withdrawal list distribution point (CRL) Distribution point name: Full name: URL=http://crl.pki.gov.kz/rsa.crl URL=http://crl1.pki.gov.kz/rsa.crl
Freshest Crl Distribution Points	Freshest CRL	2.5.29.46	[1] Freshest CRL Distribution point name: Full name: URL=http://crl.pki.gov.kz/d_rsa.crl URL=http://crl1.pki.gov.kz/d_rsa.crl
Digital Signature	Certificate authority digital signature (4096 bit)	1.2.840.113549.1.1.11	sha256WithRSAEncryption

7.1.5. Registration Certificate Structure for the User (Legal Entity) of the National Certification Authority of the Republic of Kazakhstan (for Signature)

Field	Description	OID, criticality	Content
Base fields of the registration certificate in X.509 format			
Version	Version of X.509 standard	–	V3
Serial Number	Registration certificate serial number	–	Positive integer (up to 20 byte)
Signature Algorithm	Signature algorithm	1.2.398.3.10.1.1.1.2	GOST 34.310-2004
Issuer	Data on registration certificate issuer	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	C = KZ (required field) L = ASTANA (required field) S = ASTANA(required field) O = РМК «МЕМЛЕКЕТТІКТЕХНИКАЛЫҚҚЫЗМЕТ» (required field)

			CN = ҰЛТТЫҚҚУӘЛАНДЫРУШЫОРТАЛЫҚ (GOST) (required field)
Validity from	Validity from	UTC TIME	Valid from: YYMMDDHHMMSSZ UTC
Validity to	Validity to	UTC TIME	Valid to: YYMMDDHHMMSSZ UTC
Subject	Data on registration certificate owner	E =1.2.840.113549.1.9.1 SERIALNUMBER = 2.5.4.5 SN=2.5.4.4 G=2.5.4.42 CN =2.5.4.3 OU=2.5.4.11 O=2.5.4.10 L=2.5.4.7 S=2.5.4.8 C=2.5.4.6	E = E-mail address (not required field) SERIALNUMBER = IIN012345678910 (required field) SN = Surname (not required field) G = Patronymic (not required field) CN = Surname Name (required field) OU = BIN012345678910 (required field) O = Company name (required field) L = City (required field) S = Region (required field) C = KZ (required field)
Public Key	Public key value (512 bit)	1.2.398.3.10.1.1.1.1 with characteristics 1.2.398.3.10.1.1.1.1.1 1.2.398.3.10.1.3.1.1.0	GOST 34.310-2004
Additional fields of the registration certificate in X.509 format			
Subject Key Identifier	Subject key identifier	2.5.29.14	Value of subject key identifier in hexadecimal format
Authority Key Identifier	Authority key identifier	2.5.29.35	Value of authority key identifier in hexadecimal format
Key Usage	Key usage	2.5.29.15, critical	Digital signature, Imputability
Extended Key Usage	Extended key usage	2.5.29.37	Secured e-mail -1.3.6.1.5.5.7.3.4 Legal entity - 1.2.398.3.3.4.1.2 Unknown key usage (OID), where OID is defined as a set of available identifiers. Available identifiers: 1.2.398.3.3.4.1.2.1 – The first head of the legal entity entitled to sign 1.2.398.3.3.4.1.2.2 – Person entitled to sign 1.2.398.3.3.4.1.2.3 - Person entitled to sign the financial documents 1.2.398.3.3.4.1.2.4 – Personnel officer with the power to approve applications to issuance registration certificates submitted by the legal entity employees 1.2.398.3.3.4.1.2.5 – Company employee
Ceritifcate Policy	Registration certificate policy	2.5.29.32	[1]Registration certificate policy: Policy identifier =1.2.398.3.3.2.1 [1,1]Data on policy qualifier: Identifier of policy qualifier=CPS Qualifier: http://pki.gov.kz/cps [1,2]Data on policy qualifier: Identifier of policy qualifier = Text of the notification Qualifier: http://pki.gov.kz/cps
Certificate Authority Information Access	Certificate authority information access	1.3.6.1.5.5.7.1.1	[1]Certificate Authority Information Access Access method = Certificate authority vendor(1.3.6.1.5.5.7.48.2) Additional name: URL=http://pki.gov.kz/cert/pki_gost.cer [2]Certificate Authority Information Access Access method = Protocol determining the

			registration certificate status through network (1.3.6.1.5.5.7.48.1) Additional name: URL= URL=http://ocsp.pki.gov.kz
Crl Distribution Points	Withdrawal lists distribution points	2.5.29.31	[1]Withdrawal list distribution point (CRL) Distribution point name: Full name: URL= http://crl.pki.gov.kz/gost.crl URL=http://crl1.pki.gov.kz/gost.crl
Freshest Crl Distribution Points	Freshest CRL	2.5.29.46	[1]Freshest CRL Distribution point name: Full name: URL=http://crl.pki.gov.kz/d_gost.crl URL=http://crl1.pki.gov.kz/d_gost.crl
Digital Signature	Certificate authority digital signature (512 bit)	1.2.398.3.10.1.1.1.2	GOST 34.310-2004

7.1.6. Registration Certificate Structure for the User (Legal Entity) of the National Certification Authority of the Republic of Kazakhstan (For Authentication)

Field	Description	OID, criticality	Content
Base fields of the registration certificate in X.509 format			
Version	Version of X.509 standard	–	V3
Serial Number	Registration certificate serial number	–	Positive integer (up to 20 byte)
Signature Algorithm	Signature algorithm	1.2.840.113549.1.1.11	sha256WithRSAEncryption
Issuer	Data on registration certificate issuer	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	C = KZ (required field) L = ASTANA(required field) S = ASTANA(required field) O = РМК «МЕМЛЕКЕТТІКТЕХНИКАЛЫҚҚЫЗМЕТ» (required field) CN = ҰЛТТЫҚҚУӘЛАНДЫРУШЫОРТАЛЫҚ (RSA) (required field)
Validity from	Validity from	UTC TIME	Valid from: YYMMDDHHMMSSZ UTC
Validity to	Validity to	UTC TIME	Valid to: YYMMDDHHMMSSZ UTC
Subject	Data on registration certificate owner	E =1.2.840.113549.1.9.1 SERIALNUMBER =2.5.4.5 SN=2.5.4.5 G=2.5.4.42 CN =2.5.4.3 OU=2.5.4.11 O=2.5.4.10 L=2.5.4.7 S=2.5.4.8 C=2.5.4.6	E = E-mail address (not required field) SERIALNUMBER = IIN012345678910 (required field) SN = Surname (not required field) G = Patronymic (not required field) CN = Surname Name (required field) OU = BIN012345678910 (required field) O = Company name (required field) L = City (required field) S = Region (required field) C = KZ (required field)
Public Key	Public key value (2048 bit)	1.2.840.113549.1.1.1	Value
Additional fields of the registration certificate in X.509 format			
Subject Key Identifier	Subject key identifier	2.5.29.14	Value of subject key identifier in hexadecimal format
Authority Key Identifier	Authority key identifier	2.5.29.35	Value of authority key identifier in hexadecimal format
Key Usage	Key usage	2.5.29.15, critical	Digital signature, key encryption

Extended Key Usage	Extended key usage	2.5.29.37	Client authentication (1.3.6.1.5.5.7.3.2) Legal entity (1.2.398.3.3.4.1.2) Unknown key usage (OID), where OID is defined as a set of available identifiers. Available identifiers: 1.2.398.3.3.4.1.2.1 – The first head of the legal entity entitled to sign 1.2.398.3.3.4.1.2.2 – Person entitled to sign 1.2.398.3.3.4.1.2.3 - Person entitled to sign the financial documents 1.2.398.3.3.4.1.2.4 – Personnel officer with the power to approve applications to issuance registration certificates submitted by the legal entity employees 1.2.398.3.3.4.1.2.5 – Company employee
Ceritifcate Policy	Registration certificate policy	2.5.29.32	[1]Registration certificate policy: Policy identifier =1.2.398.3.3.2.2 [1,1]Data on policy qualifier: Identifier of policy qualifier= CPS Qualifier: http://pki.gov.kz/cps [1,2]Data on policy qualifier: Identifier of policy qualifier = Text of the notification Qualifier: http://pki.gov.kz/cps
Ceritifcate Authority Information Access	Certificate authority information access	1.3.6.1.5.5.7.1.1	[1]Certificate Authority Information Access Access method = Certificate authority vendor(1.3.6.1.5.5.7.48.2) Additional name: URL=http://pki.gov.kz/cert/pki_rsa.cer [2]Certificate Authority Information Access Access method = Protocol determining the registration certificate status through network (1.3.6.1.5.5.7.48.1) Additional name: URL=http://ocsp.pki.gov.kz
Crl Distribution Points	Withdrawal lists distribution points	2.5.29.31	[1]Withdrawal list distribution point (CRL) Distribution point name: Full name: URL=http://crl.pki.gov.kz/rsa.crl URL=http://crl1.pki.gov.kz/rsa.crl
Freshest Crl Distribution Points	Freshest CRL	2.5.29.46	[1]Freshest CRL Distribution point name: Full name: URL=http://crl.pki.gov.kz/d_rsa.crl URL=http://crl1.pki.gov.kz/d_rsa.crl
Digital Signature	Certificate authority digital signature(4096 bit)	1.2.840.113549.1.1.11	sha256WithRSAEncryption

7.1.7. Registration Certificate Structure for the User (Treasury - Client IS) of the National Certification Authority of the Republic of Kazakhstan (for Signature)

Field	Description	OID, criticality	Content
Base fields of the registration certificate in X.509 format			
Version	Version of X.509 standard	–	V3
Serial Number	Registration certificate serial number	–	Positive integer (up to 20 byte)
Signature Algorithm	Signature algorithm	1.2.398.3.10.1.1.1.2	GOST 34.310-2004

Issuer	Data on registration certificate issuer	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	C = KZ (required field) L = ASTANA (required field) S = ASTANA (required field) O = РМК «МЕМЛЕКЕТТІКТЕХНИКАЛЫҚҚЫЗМЕТ» (required field) CN = ҰЛТТЫҚҚУӘЛАНДЫРУШЫОРТАЛЫҚ (GOST) (required field)
Validity from	Validity from	UTC TIME	Valid from: YYMMDDHHMMSSZ UTC
Validity to	Validity to	UTC TIME	Valid to: YYMMDDHHMMSSZ UTC
Subject	Data on registration certificate owner	E =1.2.840.113549.1.9.1 SERIALNUMBER =2.5.4.5 SN=2.5.4.5 G=2.5.4.42 CN =2.5.4.3 BUSINESSCATEGORY = 2.5.4.15 DC=0.9.2342.19200300.100.1.25 OU=2.5.4.11 O=2.5.4.10 L=2.5.4.7 S=2.5.4.8 C=2.5.4.6	E = E-mail address (not required field) SERIALNUMBER = IIN012345678910 (required field) SN = Surname (not required field) G = Patronymic (not required field) CN = Surname Name (required field) BUSINESSCATEGORY = KS01234 (required field) DC = ROLE01 (required field) OU = BIN012345678910 (required field) O = Company name (required field) L = City (required field) S = Region (required field) C = KZ (required field)
PublicKey	Public key value(512 bit)	1.2.398.3.10.1.1.1.1 with characteristics 1.2.398.3.10.1.1.1.1.1 1.2.398.3.10.1.3.1.1.0	GOST 34.310-2004
Additional fields of the registration certificate in X.509 format			
Subject Key Identifier	Subject key identifier	2.5.29.14	Value of subject key identifier in hexadecimal format
Authority Key Identifier	Authority key identifier	2.5.29.35	Value of authority key identifier in hexadecimal format
Key Usage	Key usage	2.5.29.15, critical	Digital Signature, Imputability
Extended Key Usage	Extended key usage	2.5.29.37	Unknown key usage (OID), where OID is defined as a set of available identifiers. Available identifiers: Legal entity -1.2.398.3.3.4.1.2; Information system K2 -1.2.398.5.19.1.2.2.1
Ceritifcate Policy	Registration certificate policy	2.5.29.32	[1] Registration certificate policy: Policy identifier =1.2.398.5.19.1.2.2.1.2 [1,1]Data on policy qualifier: Identifier of policy qualifier= CPS Qualifier: http://pki.gov.kz/cps
Certificate Authority Information Access	Certificate authority information access	1.3.6.1.5.5.7.1.1	[1] Certificate Authority Information Access Access method = Certificate authority vendor (1.3.6.1.5.5.7.48.2) Additional name: URL = http://pki.gov.kz/cert/pki_gost.cer [2] Certificate Authority Information Access Access method = Protocol determining the registration certificate status through network (1.3.6.1.5.5.7.48.1) Additional name: URL=http://ocsp.pki.gov.kz
Crl	Withdrawal lists	2.5.29.31	[1] Withdrawal list distribution point (CRL)

Distribution Points	distribution points		Distribution point name: Full name: URL=http://crl.pki.gov.kz/gost.crl URL=http://crl1.pki.gov.kz/gost.crl
Freshest Crl Distribution Points	Freshest CRL	2.5.29.46	[1] Freshest CRL Distribution point name: Full name: URL=http://crl.pki.gov.kz/d_gost.crl URL=http://crl1.pki.gov.kz/d_gost.crl
Digital Signature	Certificate authority digital signature (512 bit)	1.2.398.3.10.1.1.1.2	GOST 34.310-2004

7.1.8. Registration Certificate Structure for the User (Treasury - Client IS) of the National Certification Authority of the Republic of Kazakhstan (For Authentication)

Field	Description	OID, criticality	Content
Base fields of the registration certificate inX.509 format			
Version	Version of X.509 standard	–	V3
Serial Number	Registration certificate serial number	–	Positive integer (up to 20 byte)
Signature Algorithm	Signature algorithm	1.2.840.113549.1.1.11	sha256WithRSAEncryption
Issuer	Data on registration certificate issuer	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	C = KZ (required field) L = ASTANA(required field) S = ASTANA(required field) O = РМК «МЕМЛЕКЕТТІКТЕХНИКАЛЫҚҚЫЗМЕТ» (required field) CN = ҰЛТТЫҚҚУӘЛІАНДЫРУШЫОРТАЛЫҚ (RSA) (required field)
Validity from	Validity from	UTC TIME	Valid from: YYMMDDHHMMSSZ UTC
Validity to	Validity to	UTC TIME	Valid to: YYMMDDHHMMSSZ UTC
Subject	Data on registration certificate owner	E =1.2.840.113549.1.9.1 SERIALNUMBER =2.5.4.5 SN=2.5.4.5 G=2.5.4.42 CN =2.5.4.3 BUSINESSCATEGORY= 2.5.4.15 DC=0.9.2342.1920030 0.100.1.25 OU=2.5.4.11 O=2.5.4.10 L=2.5.4.7 S=2.5.4.8 C=2.5.4.6	E = E-mail address (not required field) SERIALNUMBER = IIN012345678910 (required field) SN = Surname (not required field) G = Patronymic (not required field) CN = Surname Name (required field) BUSINESSCATEGORY= KS01234 (required field) DC = ROLE01 (required field) OU = BIN012345678910 (required field) O = Company name (required field) L = City (required field) S = Region (required field) C = KZ (required field)
Public Key	Public key value (2048 bit)	1.2.840.113549.1.1.1	Value
Additional fields of the registration certificate in X.509 format			
Subject Key Identifier	Subject key identifier	2.5.29.14	Value of subject key identifier in hexadecimal format
Authority Key Identifier	Authority key identifier	2.5.29.35	Value of authority key identifier in hexadecimal format

Key Usage	Key usage	2.5.29.15, critical	Digital signature, key encryption
Extended Key Usage	Extended key usage	2.5.29.37	Client authentication(1.3.6.1.5.5.7.3.2) Unknown key usage (OID), where OID is defined as a set of available identifiers. Available identifiers: 1.2.398.3.3.4.1.2 – Legal entity; 1.2.398.5.19.1.2.2.1 – Information system K2
Ceritifcate Policy	Registration certificate policy	2.5.29.32	[1]Registration certificate policy: Policy identifier =1.2.398.5.19.1.2.2.1.3 [1,1]Data on policy qualifier: Identifier of policy qualifier= CPS Qualifier: http://pki.gov.kz/cps
Authority Info Access	Certificate authority information access	1.3.6.1.5.5.7.1.1	[1] Certificate Authority Information Access Access method = Certificate authority vendor (1.3.6.1.5.5.7.48.2) Additional name: URL=http://pki.gov.kz/cert/pki_rsa.cer [2] Certificate Authority Information Access Access method= Protocol determining the registration certificate status through network (1.3.6.1.5.5.7.48.1) Additional name: URL=http://ocsp.pki.gov.kz
Crl Distribution Points	Withdrawal lists distribution points	2.5.29.31	[1]Withdrawal list distribution point (CRL) Distribution point name: Full name: URL=http://crl.pki.gov.kz/rsa.crl URL=http://crl1.pki.gov/kz/rsa.crl
Freshest Crl Distribution Points	Freshest CRL	2.5.29.46	[1]Freshest CRL Distribution point name: Full name: URL=http://crl.pki.gov.kz/crl/d_rsa.crl URL=http://crl1.pki.gov.kz/crl/d_rsa.crl
Digital Signature	Certificate authority digital signature (4096 bit)	1.2.840.113549.1.1.11	sha256WithRSAEncryption

7.1.9. Structure of the SSL Individual's Registration Certificate of the National Certification Authority of the Republic of Kazakhstan

Field	Description	OID, criticality	Contente
Registration Certificate Basic fields in X.509 format			
Version	X.509 Version Standard	–	V3
Serial Number	Registration Certificate Serial Number	–	Positive integer (not more than 20 byte)
Signature Algorithm	Signature Algorithm	1.2.840.113549.1.1.11	sha256WithRSAEncryption
Issuer	Registration Certificate Issuer Data	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	C = KZ (mandatory field) L = АСТАНА (mandatory field) S = АСТАНА (mandatory field) O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (mandatory field) CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA) (mandatory field)
Validity from	Validity from	UTC TIME	Valid from: YYMMDDHHMMSSZ UTC
Validity to	Validity to	UTC TIME	Valid to : YYMMDDHHMMSSZ UTC
Subject	Registration Certificate Holder Data	E =1.2.840.113549.1.9.1	E = E-mail (optional) SERIALNUMBER = IIN012345678910

		SERIALNUMBER = 2.5.4.5 CN =2.5.4.3 L=2.5.4.7 S=2.5.4.8 C=2.5.4.6	(mandatory field) CN = Domain name (mandatory field) L = City (mandatory field) S = Region (mandatory field) C = KZ (mandatory field)
Public Key	EDS public key value (2048 Bits)	1.2.840.113549.1.1.1	Value
Additional fields of the Registration Certificate in the X.509 format			
Subject Key Identifier	Subject Key Identifier	2.5.29.14	Subject Key Identifier value in hexadecimal format
Authority Key Identifier	Certification Authority Key Identifier	2.5.29.35	Certification Authority Key Identifier value in hexadecimal format
Extended Key Usage	Extended Key Usage	2.5.29.37	Checking identity of the server (1.3.6.1.5.5.7.3.1) Individual - 1.2.398.3.3.4.1.1
Key Usage	Key Usage	2.5.29.15, criticality	A digital signature, keys encryption
Subject Alternative Name	Subject Alternative Name		DNS-= Domain name -1 DNS-name= Domain name -2 DNS-name= N (mandatory field)
Authority Info Access	Certification Authority Info Access	1.3.6.1.5.5.7.1.1	[1] Certification Authority Info Access Access Method = (Certification Authority Provider (1.3.6.1.5.5.7.48.2) Alternative name: URL = http://pki.gov.kz/cert/pki_rsa.cer [2] Certification Authority Info Access Access Method = Protocol determining the registration certificate state through the network (1.3.6.1.5.5.7.48.1) Alternative name: URL=http://ocsp.pki.gov.kz
Ceritifcate Policy	Registration Certificate Policy	2.5.29.32	1] Certificate Policy: Policy Identifier = 1.2.398.3.3.2.5 [1,1] Policy Qualifier Information: Qualifier Identifier Policy Qualifier Identifier =CPS Qualifier: http://pki.gov.kz/cps
Crl Distribution Points	CRL Distribution Points	2.5.29.31	[1]Distribution Point (CRL) Distribution Point Name: Full Name: URL=http://crl.pki.gov.kz/rsa.crl URL=http://crl1.pki.gov.kz/rsa.crl
Freshest Crl Distribution Points	Freshest CRL	2.5.29.46	[1]Freshest CRL Distribution Point Name: Full Name: URL=http://crl.pki.gov.kz/d_rsa.crl URL=http://crl1.pki.gov.kz/d_rsa.crl
Digital Signature	Digital Signature DS (4096 Bits)	1.2.840.113549.1.1.1.1	Value

7.1.10. Structure of the SSL Legal Entity's Registration Certificate of the National Certification Authority of the Republic of Kazakhstan

Field	Description	OID, criticality	Content
Basic fields of the registration certificate in the X.509 format			

Version	Version Standard X.509	–	V3
Serial Number	Registration Certificate Serial Number	–	Positive integer (not more than 20 byte)
Signature Algorithm	Signature Algorithm	1.2.840.113549.1.1.11	sha256WithRSAEncryption
Issuer	Registration Certificate Issuer Info	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	C = KZ (mandatory field) L = ASTANA (mandatory field) S = ASTANA (mandatory field) O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (mandatory field) CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA) (mandatory field)
Validity from	The start time for period	UTC TIME	Valid from: YYMMDDHHMMSSZ UTC
Validity to	Expiration Time	UTC TIME	Valid for: YYMMDDHHMMSSZ UTC
Subject	Registration Certificate Holder Data	E =1.2.840.113549.1.9.1 SERIALNUMBER =2.5.4.5 SN=2.5.4.4 CN =2.5.4.3 OU=2.5.4.11 O=2.5.4.10 L=2.5.4.7 S=2.5.4.8 C=2.5.4.6	E = E-mail (optional) SERIALNUMBER = IIN012345678910 (mandatory field) CN = Domain name (mandatory field) OU = BIN012345678910 (mandatory field) O = Name of the Company (mandatory field) L = City (mandatory field) S = Region (mandatory field) C = KZ (mandatory field)
Public Key	Public Key Value (2048 Bit)	1.2.840.113549.1.1.1	Value
Additional fields of the Registration Certificate in the X.509 format			
Subject Key Identifier	Subject Key Identifier	2.5.29.14	Subject Key Identifier value in hexadecimal format
Authority Key Identifier	Certification Authority Key Identifier	2.5.29.35	Authority Key Identifier value in hexadecimal format
Extended Key Usage	Extended Key Usage	2.5.29.37	Checking identity of the server (1.3.6.1.5.5.7.3.1) Legal Entity - 1.2.398.3.3.4.1.2
Key Usage	Key Usage	2.5.29.15, criticality	A digital signature, keys encryption
Subject Alternative Name	Subject Alternative Name		DNS-name= Domain name-1 DNS-name= Domain name-2 DNS-name= N (mandatory field)
Authority Info Access	Certification Authority Info Access	1.3.6.1.5.5.7.1.1	[1] Certification Authority Info Access Access Method = Certification Authority Provider (1.3.6.1.5.5.7.48.2) Alternative Name: URL = http://pki.gov.kz/cert/pki_rsa.cer [2] Certification Authority Info Access Access Method = Protocol determining the registration certificate state through the network (1.3.6.1.5.5.7.48.1)

			Alternative Name: URL=http://ocsp.pki.gov.kz
Ceritifcate Policy	Registration Certificate Policy	2.5.29.32	1]Certificate policy: Policy Identifier = 1.2.398.3.3.2.5 [1,1] Policy Qualifier Information: Qualifier Identifier Policy Qualifier Identifier =CPS Qualifier: http://pki.gov.kz/cps
Crl Distribution Points	CRL Distribution Points	2.5.29.31	[1]Distribution Point (CRL) Distribution Point Name: Full Name: URL=http://crl.pki.gov.kz/rsa.crl URL=http://crl1.pki.gov.kz/rsa.crl
Freshest Crl Distribution Points	Freshest CRL	2.5.29.46	[1]Freshest CRL Distribution Point Name: Full Name: URL=http://crl.pki.gov.kz/d_rsa.crl URL=http://crl1.pki.gov.kz/d_rsa.crl
Digital Signature	Digital Signature DS (4096 Bits)	1.2.840.113549.1.1.1.1	Value

7.1.11. Information about Registration Certificate Withdrawal List of the National Certification Authority of the Republic of Kazakhstan

Field	Description	OID, criticality	Content
Basic Fields RCRL in X.509 format			
Version	Standard Version X.509	–	V2
Issuer	Issuer RCRL data	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	C = KZ (mandatory field) L = АСТАНА (mandatory field) S = АСТАНА (mandatory field) O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (mandatory field) CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA) (mandatory field)
This Update	RCRL Time Issue	UTC TIME	Valid from: YYMMDDHHMMSSZ UTC
Next Update	RCRL Next Update	UTC TIME	Valid for: YYMMDDHHMMSSZ UTC
Signature Algorithm	Signature Algorithm	1.2.840.113549.1.1.11	sha256WithRSAEncryption
RCRL Additional fields in the X.509 format			
Number CRL	RCRL Number	2.5.29.20	In series increasing number
Authority Key Identifier	Certificate Authority Key Identifier	2.5.29.35	Certificate Authority Key Identifier value in hexadecimal format
Digital Signature	Digital Signature DS (4096 бит)	1.2.840.113549.1.1.11	sha256WithRSAEncryption

7.1.12. Information about GOST Registration Certificate Withdrawal List of the National Certification Authority of the Republic of Kazakhstan

Field	Description	OID, criticality	Content
RCRL Basic Fields in the X.509 format			
Version	Standard Version X.509	–	V2
Issuer	Issuer RCRL Data	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	C = KZ (mandatory field) L = АСТАНА (mandatory field) S = АСТАНА (mandatory field) O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (mandatory field) CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ

			ОРТАЛЫҚ (GOST) (mandatory field)
This Update	RCRL Time Issue	UTC TIME	Valid from: YYMMDDHHMMSSZ UTC
Next Update	RCRL Next Update	UTC TIME	Valid for: YYMMDDHHMMSSZ UTC
Signature Algorithm	Signature Algorithm	1.2.398.3.10.1.1.1.2	GOST 34.310-2004
RCRL Additional fields in the X.509 format			
Number CRL	RCRL Number	2.5.29.20	In series increasing number
Authority Key Identifier	Certificate Authority Key Identifier	2.5.29.35	Certificate Authority Key Identifier value in hexadecimal format
Digital Signature	Certificate Authority Digital Signature (512 Bit)	1.2.398.3.10.1.1.1.2	GOST 34.310-2004

7.1.13. Information about RSA (Delta CRL) Registration Certificate Withdrawal List of the National Certification Authority of the Republic of Kazakhstan

Поле	Описание	OID, критичность	Содержание
RCRL Basic Fields in the X.509 format			
Version	Standard Version X.509	–	V2
Issuer	Issuer RCRL Data	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	C = KZ (mandatory field) L = ACTAHA (mandatory field) S = ACTAHA (mandatory field) O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (mandatory field) CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA) (mandatory field)
This Update	RCRL Time Issue	UTC TIME	Valid from: YYMMDDHHMMSSZ UTC
Next Update	RCRL Next Update	UTC TIME	Valid for: YYMMDDHHMMSSZ UTC
Signature Algorithm	Signature Algorithm	1.2.840.113549.1.1.11	sha256WithRSAEncryption
RCRL Additional fields in the X.509 format			
Number CRL	RCRL Number	2.5.29.20	In series increasing number
Authority Key Identifier	Certificate Authority Key Identifier	2.5.29.35	Certificate Authority Key Identifier value in hexadecimal format
Freshest CRL	Difference RCRL Identifier	2.5.29.46, critical	–
Digital Signature	Digital Signature DS (4096 Bit)	1.2.840.113549.1.1.11	sha256WithRSAEncryption

7.1.14. Process of the Policy Semantics Critical Expand

Not applied.

7.1.15. Information about GOST Registration Certificate Withdrawal List (Delta CRL) of the National Certification Authority of the Republic of Kazakhstan

Field	Description	OID, critically	Content
Basic Fields RCRL in X.509 format			
Version	Standard Version X.509	–	V2

Issuer	RCRL Issue Data	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	C = KZ (mandatory field) L = АСТАНА (mandatory field) S = АСТАНА (mandatory field) O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (mandatory field) CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST) (mandatory field)
This Update	RCRL Time Issue	UTC TIME	Valid from: YYMMDDHHMMSSZ UTC
Next Update	RCRL Next Update	UTC TIME	Valid for: YYMMDDHHMMSSZ UTC
Signature Algorithm	Signature Algorithm	1.2.398.3.10.1.1.1.2	GOST 34.310-2004
RCRL Additional fields in the X.509 format			
Number CRL	RCRL Number	2.5.29.20	In series increasing number
Authority Key Identifier	Certificate Authority Key Identifier	2.5.29.35	Certificate Authority Key Identifier value in hexadecimal format
Freshest CRL	Difference RCRL Identifier	2.5.29.46, critical	–
Digital Signature	Digital Signature DS (512 Bit)	1.2.398.3.10.1.1.1.2	GOST 34.310-2004

7.1.16. OCSP RSA Registration Certificate of the National Certification Authority of the Republic of Kazakhstan Structure

Field	Description	OID, critically	Content
Registration Certificate Basic fields in the X.509 format			
Version	X.509 Standard Version	–	V3
Serial Number	Registration Certificate Serial Number	–	Positive integer (not more than 20 byte)
Signature Algorithm	Signature Algorithm	1.2.840.113549.1.1.11	sha256WithRSAEncryption
Issuer	Registration Certificate Issuer Data	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	C = KZ (mandatory field) L = АСТАНА (mandatory field) S = АСТАНА (mandatory field) O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (mandatory field) CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA) (mandatory field)
Validity from	Validity from	UTC TIME	Valid from: YYMMDDHHMMSSZ GMT
Validity to	Validity to	UTC TIME	Valid to: YYMMDDHHMMSSZ GMT
Subject	Registration Certificate Holder Data	CN =2.5.4.3 OU=2.5.4.11 O=2.5.4.10 L=2.5.4.7 S=2.5.4.8 C=2.5.4.6 SERIALNUMBER = 2.5.4.5	CN = Tools name (mandatory field) OU = Subdivision (mandatory field) O = Company Name (mandatory field) L = City (mandatory field) S = Region (mandatory field) C = KZ (mandatory field) SERIALNUMBER = IIN012345678910 (mandatory field)
Public Key	EDS public key value (2048 Bit)	1.2.840.113549.1.1.1	Value
Registration Certificate Additional fields in the X.509 format			
Subject Key Identifier	Subject Key Identifier	2.5.29.14	Subject Key Identifier value in hexadecimal format

Authority Key Identifier	Certification Authority Key Identifier	2.5.29.35	Certification Authority Key Identifier value in hexadecimal format
Extended Key Usage	Extended Key Usage	2.5.29.37	Online Certificate Status Protocol (1.3.6.1.5.5.7.3.9)
Ceritifcate Authority Information Access	Ceritifcation Authority Information Access	1.3.6.1.5.5.7.1.1	[1] Ceritifcation Authority Information Access Access Method = Certification Authority Provider (1.3.6.1.5.5.7.48.2) Alternative name: URL=http://pki.gov.kz/cert/pki_rsa.cer
Crl Distribution Points	Crl Distribution Points	2.5.29.31	[1]Crl Distribution Point (CRL) Distribution Point Name: Full name: URL=http://crl.pki.gov.kz/rsa.crl URL=http://crl1.pki.gov.kz/rsa.crl
Freshest Crl Distribution Points	Freshest Crl	2.5.29.46	[1]Freshest CRL Distribution Point Crl Name: Full Name: URL=http://crl.pki.gov.kz/d_rsa.crl URL=http://crl1.pki.gov.kz/d_rsa.crl
OCSP No Withdrawal Checking	OCSP No Withdrawal Checking	1.3.6.1.5.5.7.48.1.5	Empty value
Digital Signature	Certification Authority Digital Signature (4096 Bit)	1.2.840.113549.1.1.11	sha256WithRSAEncryption

7.1.17. Structure of the OCSP GOST Registration Certificate of the National Certification Authority of the Republic of Kazakhstan

Field	Description	OID, critically	Content
Registration Certificate Basic fields in the X.509 format			
Version	Standard Version X.509	–	V3
Serial Number	Registration Certificate Serial Number	–	Positive integer (not more than 20 byte)
Signature Algorithm	Signature Algorithm	1.2.398.3.10.1.1.1.2	GOST 34.310-2004
Issuer	Registration Certificate Issuer Data	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	C = KZ (mandatory field) L = АСТАНА (mandatory field) S = АСТАНА (mandatory field) O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (mandatory field) CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST) (mandatory field)
Validity from	Validity from	UTC TIME	Valid from: YYMMDDHHMMSSZ GMT
Validity to	Validity to	UTC TIME	Valid to: YYMMDDHHMMSSZ GMT
Subject	Registration Certificate Holder Data	CN =2.5.4.3 OU=2.5.4.11 O=2.5.4.10 L=2.5.4.7 S=2.5.4.8 C=2.5.4.6	CN = Service name (mandatory field) OU = Subdivision (mandatory field) O = Company Name (mandatory field) L = City (mandatory field) S = Region (mandatory field) C = KZ (mandatory field)
Public Key	EDS public key value (512 Bit)	1.2.398.3.10.1.1.1.1 With parameters 1.2.398.3.10.1.1.1.1.1 1.2.398.3.10.1.3.1.1.0	GOST 34.310-2004
Registration Certificate Additional fields in the X.509 format			

Subject Key Identifier	Subject Key Identifier	2.5.29.14	Subject Key Identifier value in hexadecimal format
Authority Key Identifier	Certification Authority Key Identifier	2.5.29.35	Certification Authority Key Identifier value in hexadecimal format
Extended Key Usage	Extended Key Usage	2.5.29.37	Online Certificate Status Protocol (1.3.6.1.5.5.7.3.9)
Crl Distribution Points	Crl Distribution Points	2.5.29.31	[1]Crl Distribution Point (CRL) Distribution Point Name: Full name: URL=http://crl.pki.gov.kz/gost.crl URL=http://crl1.pki.gov.kz/gost.crl
Freshest Crl Distribution Points	Freshest Crl	2.5.29.46	[1]Freshest CRL Distribution Point Name: Full Name: URL=http://crl.pki.gov.kz/d_gost.crl URL=http://crl1.pki.gov.kz/d_gost.crl
OCSP No Withdrawal Checking	OCSP No Withdrawal Checking	1.3.6.1.5.5.7.48.1.5	Empty Value
Digital Signature	Certification Authority Digital Signature (512 Bit)	1.2.398.3.10.1.1.1.2	GOST 34.310-2004

7.1.18. Structure of the TSP RSA Registration Certificate of the National Certification Authority of the Republic of Kazakhstan

Field	Description	OID, critically	Content
Registration Certificate Basic Fields in the X.509 format			
Version	Standard Version X.509	–	V3
Serial Number	Certificate Serial Number	–	Positive integer (not more than 20 byte)
Signature Algorithm	Signature Algorithm	1.2.840.113549.1.1.11	sha256WithRSAEncryption
Issuer	Registration Certificate Issuer Data	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	C = KZ (mandatory field) L = АСТАНА (mandatory field) S = АСТАНА (mandatory field) O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (mandatory field) CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA) (mandatory field)
Validity from	Validity from	UTC TIME	Valid from: YYMMDDHHMMSSZ GMT
Validity to	Validity to	UTC TIME	Valid to: YYMMDDHHMMSSZ GMT
Subject	Registration Certificate Holder Data	CN =2.5.4.3 OU=2.5.4.11 O=2.5.4.10 L=2.5.4.7 S=2.5.4.8 C=2.5.4.6 SERIALNUMBER = 2.5.4.5	CN = Tools Name (mandatory field) OU = Subdivision (mandatory field) O = Company Name (mandatory field) L = City (mandatory field) S = region (mandatory field) C = KZ (mandatory field) SERIALNUMBER = IIN012345678910 (mandatory field)
Public Key	EDS public key value (2048 Bit)	1.2.840.113549.1.1.1	Value
Registration Certificate Additional fields in the X.509 format			
Subject Key	Subject Key Identifier	2.5.29.14	Subject Key Identifier value in hexadecimal

Identifier			format
Authority Key Identifier	Certification Authority Key Identifier	2.5.29.35	Certification Authority Key Identifier value in hexadecimal format
Extended Key Usage	Extended Key Usage	2.5.29.37, critical	Time Stamping setting (1.3.6.1.5.5.7.3.8)
Ceritifcate Authority Information Access	Ceritifcation Authority Information Access	1.3.6.1.5.5.7.1.1	[1] Ceritifcation Authority Information Access Access Method = Certification Authority Provider (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://pki.gov.kz/cert/pki_rsa.cer [2] Ceritifcation Authority Information Access Access Method = Protocol determining the registration certificate state through the network (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.pki.gov.kz
Crl Distribution Points	Withdrawal List Distribution Points	2.5.29.31	[1] Withdrawal List Distribution Point (CRL) Distribution Point Name: Full Name: URL=http://crl.pki.gov.kz/rsa.crl URL=http://crl1.pki.gov.kz/rsa.crl
Freshest Crl Distribution Points	Freshest CRL	2.5.29.46	[1] Freshest CRL Distribution Point Name: Full Name: URL=http://crl.pki.gov.kz/d_rsa.crl URL=http://crl1.pki.gov.kz/d_rsa.crl
Digital Signature	Certification Authority Digital Signature (4096 Bit)	1.2.840.113549.1.1.11	sha256WithRSAEncryption

7.1.19. Structure of the TSP GOST Registration Certificate of the National Certification Authority of the Republic of Kazakhstan

Field	Description	OID, critically	Content
Registration Certificate Basic Fields in X.509 format			
Version	Standard Version X.509	–	V3
Serial Number	Registration Certificate Serial Number	–	Positive integer (not more than 20 byte)
Signature Algorithm	Signature Algorithm	1.2.398.3.10.1.1.1.2	GOST 34.310-2004
Issuer	Registration Certificate Issuer Data	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	C = KZ (mandatory field) L = АСТАНА (mandatory field) S = АСТАНА (mandatory field) O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (mandatory field) CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST) (mandatory field)
Validity from	Validity from	UTC TIME	Valid from: YYMMDDHHMMSSZ GMT
Validity to	Validity to	UTC TIME	Valid to: YYMMDDHHMMSSZ GMT
Subject	Registration Certificate Holder Data	CN =2.5.4.3 OU=2.5.4.11 O=2.5.4.10 L=2.5.4.7 S=2.5.4.8 C=2.5.4.6	CN = Tools Name (mandatory field) OU = Subdivision (mandatory field) O = Company Name (mandatory field) L = Город (mandatory field) S = Область (mandatory field) C = KZ (mandatory field)
Public Key	EDS public	1.2.398.3.10.1.1.1.1 With parameters	GOST 34.310-2004

	key value (512 Bit)	1.2.398.3.10.1.1.1.1.1 1.2.398.3.10.1.3.1.1.0	
Additional Fields in the Registration Certificates in the X.509 Format			
Subject Key Identifier	Subject Key Identifier	2.5.29.14	Subject Key Identifier value in hexadecimal format
Authority Key Identifier	Certification Authority Key Identifier	2.5.29.35	Certification Authority Key Identifier value in hexadecimal format
Extended Key Usage	Extended Key Usage	2.5.29.37, critical	Time Stamping setting (1.3.6.1.5.5.7.3.8)
Certificate Authority Information Access	Certification Authority Information Access	1.3.6.1.5.5.7.1.1	[1] Certification Authority Information Access Access Method = Certification Authority Provider (1.3.6.1.5.5.7.48.2) Alternative Name: URL = http://pki.gov.kz/cert/pki_gost.cer [2] Certification Authority Information Access Access Method = Protocol determining the registration certificate state through the network (1.3.6.1.5.5.7.48.1) Alternative Name имя: URL=http://ocsp.pki.gov.kz
Crl Distribution Points	Withdrawal List Distribution Points	2.5.29.31	[1] Withdrawal List Distribution Point (CRL) Distribution Point Name: Full Name: URL=http://crl.pki.gov.kz/gost.crl URL=http://crl1.pki.gov.kz/gost.crl
Freshest Crl Distribution Points	Fresh CRL	2.5.29.46	[1]Fresh CRL Distribution Point Name: Full Name: URL=http://crl.pki.gov.kz/d_gost.crl URL=http://crl1.pki.gov.kz/d_gost.crl
Digital Signature	Digital Signature Cetification Authority (512 Bit)	1.2.398.3.10.1.1.1.2	GOST 34.310-2004

7.1.20. Syntax and Semantics of the Policy Qualifiers

Not applied.

7.2. OCSP PROFILE

The OCSP service version used by the RK NCA for registration certificate status checking, complies with RFC 6960 recommendations.

Extensions processed by the OCSP service, as well as the criticality, complies with RFC 6960 recommendations.

7.2.1. Version Number

The RK NCA uses 1 OCSP version to check the status of the registration certificates

7.2.2. OCSP Extensions

Extensions processed by OCSP tools, as well as their criticality conform the RFC 6960 recommendations.

8. COMPLIANCE AUDIT

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

8.1. PERIOTICITY AND CAUSES FOR INSPECTIONS

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

In accordance with the WebTrus International Standard requirements, the STS RSE plans to purchase external audit services that comply with the requirements specified in Clause 8.2 hereof from independent auditing organizations.

The owner carries out state procurement of services for the certification audit for compliance with the WebTrust International Standard.

8.2. AUDITORS AND THEIR QUALIFICATIONS

The RK NCA internal control environment audit for compliance with the WebTrust International Standard 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 WebTrust International Standard. License from WebTrust Standard owner shall be issued after qualification verification of the audit organization.

8.3. RELATIONS BETWEEN RK NCA AND AUDIT ORGANIZATIONS

Audit organizations carrying out the audit of the RK NCA internal control environment for compliance with the WebTrust International Standard are independent of the STS RSE and Owner.

8.4. AUDIT OBJECTIVES

The NCA internal control environment audit is carried out in accordance with WebTrust International Standard for Certification Authorities. The scope of inspection includes the following WebTrust international standard sections:

1) disclosure of the RK NCA business practices:
   - management of the policy on use of the RK NCA registration certificates;
   - application registration certificates of the RK NCA instruction;
2) RK NCA environment controls:
   - information security management;
   - assets classification and management;
   - personnel safety;
   - physical security management;
   - RK NCA activities management;
   - access control;
   - development and support systems management;
- business continuity management;
- monitoring and compliance management;
- documentation.

3) lifecycle keys controls of the RK NCA:
   - RK NCA keys generation;
   - RK NCA keys storage, backup and recovery;
   - distribution of public keys of the RK NCA;
   - RK NCA keys usage;
   - RK NCA keys archiving and destruction;
   - RK NCA compromise keys controls;
   - CIPF RK NCA lifecycle management.

4) lifecycle subscribers RK NCA keys controls:
- RK NCA services on generating subscribers' keys RK NCA;
- RK NCA subscribers' keys management requirements.

5) RK NCA registration certificates lifecycle management controls:
- subscribers' registration;
- RK NCA registration certificates issuance;
- RK NCA registration certificates withdrawal;
- RK NCA registration certificates check.

8.5. MEASURES TO BE TAKEN WHEN SHORTCOMINGS AND IRREGULARITIES HAVE BEEN IDENTIFIED

As a result of the RK NCA internal control environment audits for compliance with the WebTrust International Standard, licensed audit organizations shall provide to Owner the final report containing a list of identified shortcomings or irregularities, as well as description of the risks related with shortcomings or irregularities and recommendations for their elimination. On the basis of the final report of the audit, officials of STS RSE make up plans to eliminate shortcomings and irregularities, indicating deadlines, responsible persons and the results of the plan implementation. The plan approved by the Owner's responsible persons. Control over the execution of the shortcomings and irregularities elimination plan is carried out by the Owner.

The RK NCA provides the Owner with information on the identified shortcomings elimination in accordance with the plan to eliminate shortcomings and irregularities. The RK NCA provides independent licensed auditors with information about elimination of the previously identified shortcomings at the next annual audit of the RK NCA internal control environment.

8.6. ANNOUNCEMENT CONCERNING RESULTS

Announcement on the results of the audit is described in Section 8.5.

9. LEGAL AND BUSINESS ISSUES

9.1. PAYMENT FOR SERVICES

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

9.1.1. Payment for the Registration Certificate Issuance or Renewal

Issuance of registration certificates is free of charge.

9.1.2. Payment for the Registration Certificate Access

The RK NCA does not charge fee for access to the registration certificate.

9.1.3. Payment for the Registration Certificate Status Information Access

RCRL information access is free of charge.

9.1.4. Payment for Other Services

Not applicable.

9.1.5. Reimbursement Policy

Not applicable.

9.2. FINANCIAL LIABILITY

9.2.1. Insurance

Not provided.

9.2.2. Other Financial Liability

Not provided.

9.2.3. The Scope of the Insurance and Guarantees for End Entities

Not applicable.

9.3. CONFIDENTIALITY OF THE NCA RK INFORMATION

9.3.1. Confidential information of the RK NCA

In the course of business processes RK NCA receives, uses and stores confidential information, 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 is not considered as confidential one.

9.3.2. Information Outside of Confidential Information

The RK NCA participants recognize that the registration certificate, information on their withdrawal or other information about the registration certificate status, the public part of the Registration Certificates Register and the information contained therein is not considered as confidential information.

9.3.3. Responsibility to Protect the RK NCA Confidential Information

The RK NCA 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 THE NCA RK SUBSCRIBERS' PERSONAL DATA

9.4.1. Provision of confidentiality of the RK NCA subscribers' personal data

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

In the event of termination of the activities the RK NCA has to inform all participants of the RK NCA PKI and authorized body thirty days before the termination thereof.

When the RK NCA terminates its activities, the registration certificates issued to them and the corresponding keys of the Electronic Digital Signature, data of the registration certificates of the RK NCA

subscribers shall be transferred to other certification centers in coordination with the subscribers of the RK NCA registration certificate.

At the expiration of the term the RK NCA subscribers' registration certificates and the corresponding EDS keys not transferred to other certification authorities, will terminate and shall be kept in accordance with the legislation of the Republic of Kazakhstan.

9.4.2. Information considered as the RK NCA Subscribers' Personal Data

The RK NCA considers the RK NCA subscribers' information specified in the registration certificates as subscriber's personal data.

9.4.3. Information not Considered as the RK NCA Subscribers' Personal Data

The RK NCA does not consider as personal data any information contained in the RK NCA registration certificates of the subscribers, as well as other information that shall be mandatory publicized in accordance with the current legislation of the Republic of Kazakhstan.

9.4.4. Responsibility for protection of the RK NCA subscribers' personal data

The RK NCA is responsible for the protection of the processed, received, used and stored RK NCA subscribers' personal data in accordance with the current legislation of the Republic of Kazakhstan.

9.4.5. Consent to Use of the RK NCA Subscribers' Personal Data

When applying for the issuance of the RK NCA registration certificates a service recipient confirms its consent to the collection, processing, use and storage of personal data in accordance with the user agreement.

9.4.6. Disclosure of the RK NCA subscribers' personal data to law enforcement and judicial authorities

The RK NCA provides confidential personal information about the RK NCA subscriber data to law enforcement and judicial authorities in accordance with applicable legislation of the Republic of Kazakhstan.

9.4.7. Other Grounds for Disclosure of the RK NCA Subscribers' Personal Data

Not applicable.

9.5. INTELLECTUAL PROPERTY RIGHTS

The RK NCA reserves the intellectual property rights to the registration certificate which it issues, and on its status information. At the same time the RK NCA does not prohibit copy and distribution of registration certificates on a nonexclusive free of charge basis subject to the conditions of use and completeness of the copy of the registration certificates in accordance with the terms of the concluded user Agreement. The RK NCA also does not prohibit the usage of information on the status of the registration certificates for the implementation of the relying party functions.

IS participants served by the RK NCA, recognize the intellectual property rights of the RK NCA to these Rules and other documents RK NCA, regulating the CA activities.

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

Complimentary keys that correspond to the registration certificate issued by the RK NCA, make proprietary (including intellectual) of the relevant actors of PKI RK NCA, regardless of the physical media in which these complimentary keys are stored and by which they are protected. In particular, public keys, registration certificates and part of the RK NCA private keys secret are the property (including intellectual property) of the RK NCA.

9.6. OBLIGATIONS

9.6.1. RK NCA Obligations

The RK NCA has the following obligations:

1) creation of Electronic Digital Signature keys on the applications of participants of electronic document management system with taking measures to protect the private key of Electronic Digital Signature from unauthorized access;

2) registration certificates issuance, registration, withdrawal, storage, maintaining of the registration certificates register issued in the established order;
2-1) approval of the application rules of the registration certificate for each type of registration certificate;
3) accounting of valid and withdrawal registration certificates;
4) proof of affiliation and the validity of the Electronic Digital Signature public key, registered by certification authority in accordance with the legislation of the Republic of Kazakhstan;

The RK NCA is obliged to take all necessary measures to prevent the loss, modification, and counterfeiting of stored public Electronic Digital Signature keys.
For failure to fulfill obligations provided for in Clause above, the RK NCA is responsible in accordance with the current legislation of the Republic of Kazakhstan.

9.6.2. CR Obligations
In accordance with Clause 1.4.2 above.

9.6.3. Obligations of a Subscriber
The owner of the registration certificate has the right to require Certification Authority to revoke a registration certificate in cases if it involves violation of the access to the Electronic Digital Signature private key corresponding public key specified in the registration certificate.
The owner of the registration certificate has obligations:
1) to provide Certification Authority with reliable information;
2) to use the private key corresponding to the public key listed in the registration certificate;
3) to take measures to protect the Electronic Digital Signature private key owned by him 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. Obligations of Relying Parties
Not applicable.

9.6.5. Obligations of the Other Participants
Not applicable.

9.7. GUARANTEE WITHDRAWAL

Not applicable.

9.8. LIMITATION OF LIABILITY

Not applicable.

9.9. GUARANTEES

9.9.1. RK NCA's Guarantees
The RK NCA guarantees the provision of public services, with exception of objective reasons, false positives and business need.

9.9.2. State Corporation's Guarantees
The State Corporation guarantees:

- lack of intentional distortion of the facts, made by CR operators or known to them in applications for the issuance of the RK NCA registration certificates;
- lack of random mistakes made by RA operators due to negligence when considering applications for issuance in applications for issuance registration certificate;
- timely information for service recipients of the issuance of registration certificates on the conditions, obligations and responsibilities that obtaining the registration certificate of the RK NCA entails.

9.9.3. Guarantees and obligations of the RK NCA subscribers
The RK NCA Subscriber guarantees to use the RK NCA registration certificate in accordance with these

Rules and the current legislation of the Republic of Kazakhstan

9.9.4. Relying Parties' Guarantees

Relying parties ensure that they:

have sufficient information to make reasonable decisions on the extent to which they want to rely on information from the registration certificate;

are solely responsible for making decisions, rely or not rely on this information;

accept the legal consequences of breaches of obligations of relying party under the conditions of this Rules.

9.10. DURATION AND TERMINATION OF THE ORDER

9.10.1. Entry into force

This Rules enter into force immediately since it was signed and published in the RK NCA online resource.

9.10.2. Termination

These Rules remain in force until the new version replacement during RK NCA functioning. Replacement of a new version is made in accordance with Clause 1.6 of these Rules.

9.10.3. Legal consequences of termination

Since termination of these Rules participants of PKI RK NCA remain bound by the terms of the latest version of the Rules in all registration certificates before the expiration period of validity of each registration certificate.

9.11. INDIVIDUAL NOTIFICATION AND INTERACTION WITH PARTICIPANTS

The RK NCA use any of the available methods for the official notification of PKI RK NCA participants.

9.12. AMENDMENTS

9.12.1. Amendments

Amendments and supplements hereof are prepared by the Public Key Infrastructure (PKI) service and are documented in the form of a separate document containing the current text of the Rules or the notification date amendments and supplements to its current text.

Publication of the current edition of the Rules or the notification about amendments and supplements to it is made on the official web-site of the RK NCA at the following address: pki.gov.kz.

9.12.2. Notification mechanism and period

The RK NCA reserves the right without prior notice to make minor amendments and supplements to these Rules, including, but not limited with misprints corrections, change of addresses, links and contact information. Decisions on significance of these amendments and supplements are made at the sole discretion of the RK NCA.

9.12.3. Reasons for the Object Identifiers to be Changed

If in connection with the amendments and supplements to these Rules the RK NCA identified the need to change the object identifier in the relevant Policy of registration certificates application, new object identifiers for each type of registration certificate shall be specified in current text of these Rules that must be set to be operation at the same time with amendments and supplements to these Rules.

9.13. DISPUTE SETTLEMENT PROCEDURE

The STS RSE Financial responsibility for non-performance or improper performance of the RK NCA obligations to subscribers cannot exceed 50 (fifty) monthly calculation indices (2,121 tenge). At the same time the STS RSE is not liable for indirect, special, incidental, consequential damages and lost profits.

9.14. CURRENT LEGISLATION

The legal validity, interpretation of these Rules shall be governed in accordance with the current legislation of the Republic of Kazakhstan.

9.15. COMPLIANCE WITH THE APPLICABLE LAW

The legal validity, interpretation of these Rules shall be governed in accordance with the current legislation of the Republic of Kazakhstan.

9.16. OTHER REGULATIONS

9.16.1. Agreement Entirety

Not specified.

9.16.2. Rights Transfer

Not provided.

9.16.3. Severability

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

9.16.4. Enforcement (attorneys' compensation and waiver)

Not specified.

9.16.5. Force Majeure

Not specified.

9.17. OTHER PROVISIONS

Not provided.