|  |
| --- |
| APPROVEDMinutes of the Board Meeting of JSC 'Belarusian Universal Commodity Exchange' dated 31.10.2019 No. 219 (as amended by Minutes of the Board Meeting dated 26.08.2021 No. 158) |

**Certificate Policy**

for Certification Authority Certificates for Participation in Exchange Trading

Minsk

Table of Contents

[1. REQUIREMENTS APPLICABLE TO PUBLIC KEY INFRASTRUCTURE PARTICIPANTS 9](#_Toc256000001)

[1.1. Requirements Applicable to the EEAS CA 9](#_Toc256000002)

[1.2. Requirements Applicable to EEAS CA Subscribers 9](#_Toc256000003)

[1.3. Requirements Applicable to the Relying Party 9](#_Toc256000004)

[2. REQUIREMENTS APPLICABLE TO THE EEAS CA 10](#_Toc256000006)

[2.1. Keys Management Requirements 10](#_Toc256000007)

[2.1.1. Generation of the EEAS CA Signature Private Key 10](#_Toc256000008)

[2.1.2. Storage, Backup and Recovery of the Certification Authority Signature Private Key 10](#_Toc256000009)

[2.1.3. Distribution of EEAS CA Public Keys 10](#_Toc256000010)

[2.1.4. Depositing of the EEAS CA Private Key 10](#_Toc256000011)

[2.1.5. Use of the EEAS CA Private Key 10](#_Toc256000012)

[2.1.6. Expiry of the Validity Period of the EEAS CA Private Key 11](#_Toc256000013)

[2.1.7. Management of the EDS Device Used to Generate the PKC 11](#_Toc256000014)

[2.2. PKC Management Requirements 11](#_Toc256000015)

[2.2.1. Registration of the Subscriber 11](#_Toc256000016)

[2.2.2. PKC Issue 12](#_Toc256000017)

[2.2.3. PKC Distribution 13](#_Toc256000018)

[2.2.4. PKC Revocation and Suspension 13](#_Toc256000019)

[2.2.5. PKC Reactivation and Data Update 13](#_Toc256000020)

[2.3. Management of EEAS CA Operations 14](#_Toc256000021)

[2.3.1. Security Management 14](#_Toc256000022)

[2.3.2. Distribution of regulatory and organizational documents 14](#_Toc256000023)

[2.3.3. Assets Classification and Management 14](#_Toc256000024)

[2.3.4. Personnel-Related Security Issues 15](#_Toc256000025)

[2.3.5. Physical Protection and Protection from Adverse Environmental Impact 15](#_Toc256000026)

[2.3.6. Operating Activity Management 15](#_Toc256000027)

[2.3.7. System Access Management 16](#_Toc256000028)

[2.3.8. Implementation and Maintenance of Information Systems 16](#_Toc256000029)

[2.3.9. Post-Failure Recovery and Business Continuity 16](#_Toc256000030)

[2.3.10. Termination of EEAS CA Operations 17](#_Toc256000031)

[2.3.11. Retention of PKC-Related Information 17](#_Toc256000032)

[2.4. Administrative Provisions 18](#_Toc256000033)

REGULATORY REFERENCES

1. Law of the Republic of Belarus No. 455-Z dated 10.11.2008 'On Information, Informatization and Protection of Information'.
2. Law of the Republic of Belarus No. 113-Z dated 28.12.2009 'On Electronic Documents and Electronic Digital Signatures'.
3. Order of the Operations and Analysis Center under the President of the Republic of Belarus No. 62 dated 30.08.2013 'On Certain Matters Related to Technical and Cryptographic Protection of Information'.
4. GOST 21.101-93 ‘Main Requirements to Work Documents’.
5. STB ISO/IEC 27001-2011 ‘Information Technologies. Security Methods. Information Security Management Systems. Requirements.’
6. STB 34.101.1-2014 (ISO/IEC 15408-1:2009) ‘Information Technologies and Security. Criteria for the Assessment of Security of Information Technologies. Part 1. Introduction and General Model’. (ISO/IEC 15408-1:2009, MOD).
7. STB 34.101.2-2014 (ISO/IEC 15408-2:2008) ‘Information Technologies and Security. Criteria for the Assessment of Security of Information Technologies. Part 2. Functional Security Requirements’. (ISO/IEC 15408-2:2008, MOD).
8. STB 34.101.3-2014 (ISO/IEC 15408-3:2008) ‘Information Technologies and Security. Criteria for the Assessment of Security of Information Technologies. Part 3. Security Guarantee Requirements’. (ISO/IEC 15408-3:2008, MOD).
9. STB 34.101.17-2012 ‘Information Technologies. Certificate Request Syntax’.
10. STB 34.101.19-2012 ‘Information Technologies and Security. Formats of Certificates and Lists of Revoked Applicable to Certificates in the Public Key Infrastructure’.
11. STB 34.101.48-2012 ‘Information Technologies and Security. Requirements to Certificate Policies Applicable to Certificates Issued by Certification Authorities’.

LIST OF ABBREVIATIONS

|  |  |
| --- | --- |
| CKD | cryptographic key device |
| CP | Certificate Policy |
| ISS | information security system |
| PKC | public key certificate  |
| LRC | list of revoked certificates  |
| TR | technical regulations |
| CA | certification authority  |
| EDS | electronic digital signature |

TERMS AND DEFINITIONS

Subscriber shall mean any legal entity or individual, including any individual entrepreneur, with which/whom a services contract is executed.

Generation of private and public keys shall mean the process that involves implementation of the algorithm used to generate the private key and the corresponding public key.

Relying party shall mean any legal entity or individual that relies on the authenticity of the information contained in the public key certificate, and/or on the electronic digital signature authenticated with such certificate.

Private key compromise shall mean loss of trust in the private key.

Cryptographic key device shall mean any special detachable software/hardware data storage device which is connected to a USB port of the computer, and is used for the storage of private keys of the subscribers in an encrypted form.

Revocation of a public key certificate shall mean the process that involves early termination of a public key certificate.

Certificate policy shall mean a named set of rules that indicate the applicability of a certificate to a particular community and/or class of applications with common security requirements.

Suspension of a certificate shall mean the process that involves modification of the public key certificate status to exclude the possibility of its use during the suspension period.

EEAS CA Regulations shall mean the document entitled 'Regulations of JSC ‘Belarusian Universal Commodity Exchange’ on Distribution of Public Keys for Authentication of Digital Signatures for Participation in Exchange Trading'.

Public key certificate shall mean an electronic document issued by the service provider and containing information certifying that the public key specified in such certificate is owned by a certain entity or individual, or other information stipulated by Law of the Republic of Belarus No. 113-Z dated 28.12.2009 'On Electronic Documents and Electronic Digital Signatures' and other legislative acts of the Republic of Belarus.

Information security system (ISS) shall mean the totality of organizational and technical measures aimed at ensuring security of information assets, including development and implementation of appropriate policies and procedures, creation of technological infrastructure, and deployment of software- and hardware-based security features.

List of revoked certificates shall mean an electronic document created by the Exchange and containing information on public key certificates which are terminated or suspended prior to expiry of the validity period of the public keys specified in such certificates.

Certificate validity period shall mean the period of time during which the Enterprise guarantees that the relevant PKC is valid and current.

Certification authority (CA) shall mean the provider of services related to the issue, distribution, and storage of public key certificates and lists of revoked public key certificates.

Authorized representative shall mean the individual authorized to represent any legal entity or individual, including any individual entrepreneur, in its/his/her relations with the Exchange.

INTRODUCTION

The certificate policy ('CP') shall be defined as a named set of rules that indicate the applicability of a certificate to a particular community and/or class of applications with common security requirements. The Certification Authority of the Electronic Exchange Auctions System ('EEAS CA') shall be the main body in the CP responsible for the enforcement of requirements applicable to the management of the life cycle of public key certificates ('PKCs').

This document is developed in accordance with the existing legislation of the Republic of Belarus governing operations in the area of protection of information, informatization and electronic documents management (Law of the Republic of Belarus No. 455-Z dated 10.11.2008 'On Information, Informatization and Protection of Information'), including subject to the applicable requirements of STB 34.101.48-2012 'Information Technologies and Security. Requirements to Certificate Policies Applicable to Certificates Issued by Certification Authorities' and STB ISO/IEC 27001-2011 'Information Technologies. Security Methods. Information Security Management Systems. Requirements'.

This CP is developed in accordance with the document entitled 'Regulations of JSC ‘Belarusian Universal Commodity Exchange’ on Distribution of Public Keys for Authentication of Digital Signatures for Participation in Exchange Trading' ('EEAS CA Regulations').

The Exchange shall have all subscribers review this CP.

The Exchange shall notify the subscribers and other stakeholders of any amendments and additions to this CP.

This CP shall provide the methodology to be used by the Exchange in the course of conduct by the EEAS CA of the following operations:

* issue and life cycle support (storage, suspension, reactivation, revocation) of PKCs used for authentication of electronic digital signatures for participation in exchange trading;
* issue and distribution of subscriber PKCs;
* issue and storage of lists of revoked subscriber PKCs;
* registration of the owners of private keys;
* registration of PKC issue and revocation requests;
* maintenance of the database of issued subscriber PKCs;
* termination, suspension, and reactivation of PKCs;
* verification of the information stored in PKCs;
* registration and storage of subscriber public key cards;
* reliable verification of ownership of a public key by a certain entity or individual;
* certification of the form of external presentation of hard copies of electronic documents.

The requirements stipulated by this CP shall be implemented by the EEAS CA in accordance with the EEAS CA Regulations.

1. REQUIREMENTS APPLICABLE TO PUBLIC KEY INFRASTRUCTURE PARTICIPANTS

1.1. Requirements Applicable to the EEAS CA

The EEAS CA shall comply with all requirements stipulated by this CP.

The EEAS CA shall be responsible, in accordance with the existing legislation, for ensuring compliance with the procedures stipulated by this CP, even if it delegates the public keys distribution function to its subcontractors.

This CP shall not contain any provisions that are contrary to the EEAS CA Regulations.

1.2. Requirements Applicable to EEAS CA Subscribers

Each EEAS CA subscriber shall:

* guarantee that all information provided for the issue and use of its public key and PKC is complete and accurate;
* use its private and public keys only to generate and verify its electronic digital signature ('EDS'), always subject to any other restrictions as are stipulated by the EEAS CA Regulations and published on the Exchange website www.butb.by;
* generate the signature private key using only a certified EDS device;
* generate the public key on the basis of the private keys using only a certified EDS device;
* keep its private key secret;
* protect its private key from accidental destruction or modification (alteration);
* revoke its public key if the corresponding private key is compromised;
* refrain from using its private key if the corresponding public key is revoked, or its validity period has expired.

If an authorized representative is acting for the subscriber, such authorized representative shall notify the subscriber of the above requirements.

1.3. Requirements Applicable to the Relying Party

Prior to establishing trust in any electronic document (in particular, any PKC), the relying party shall:

* ensure that the PKC is valid (including by checking whether it has been revoked or suspended, or its validity period has expired);
* ensure that the intended use of the PKC is consistent with the intended area of its application, and complies with any other restrictions related to its use as are specified in such PKC or in this CP.

2. REQUIREMENTS APPLICABLE TO THE EEAS CA

2.1. Keys Management Requirements

2.1.1. Generation of the EEAS CA Signature Private Key

The EEAS CA signature private key shall be generated under the supervision of at least two employees of the Exchange in a structurally protected environment.

The signature private key and the EEAS CA signature authentication public key shall be generated using only a certified EDS software/hardware device.

The EEAS CA and the employees of the Exchange shall generate a new key pair for the signing of newly issued PKCs prior to the expiry of the validity period of the signature private key, and take all steps to prevent disruption of operations of any participant relying on an EEAS CA PKC. New EEAS CA keys shall also be created and distributed in accordance with this CP.

2.1.2. Storage, Backup and Recovery of the Certification Authority Signature Private Key

The EEAS CA signature private key shall be stored in a cryptographically protected file container on the EEAS CA server.

The EEAS CA shall back up its private keys.

The backup copies of private keys shall be stored in a protected form on cryptographic key devices ('CKDs').

EEAS CA private keys shall be copied and recovered in the presence of at least two employees of the Exchange.

Access controls for the CKDs storing backup copies of CA private keys shall completely prevent unauthorized access to them.

2.1.3. Distribution of EEAS CA Public Keys

The EEAS CA shall distribute its signature authentication public key in the form of a PKC.

The relying party shall verify the authenticity and integrity of the EEAS CA EDS public key at the time of its receipt.

2.1.4. Depositing of the EEAS CA Private Key

The EEAS CA shall not deposit its private keys.

2.1.5. Use of the EEAS CA Private Key

The EEAS CA shall use its private keys only to issue PKCs and lists of revoked certificates ('LRCs'), and to provide PKC status information.

2.1.6. Expiry of the Validity Period of the EEAS CA Private Key

EEAS CA signature private keys shall not be used upon expiry of their validity periods, and shall be destroyed in a way that precludes their recovery.

2.1.7. Management of the EDS Device Used to Generate the PKC

The EEAS CA shall ensure security of the EDS device for the entire period of its use for the generation of PKCs.

The EEAS CA shall guarantee that:

* the EDS device used to issue PKCs and LRCs was not damaged in the course of its delivery;
* the EDS device used to issue PKCs and LRCs was not compromised in the course of its storage;
* installation, activation, backup, and reactivation of EEAS CA EDS keys with the EDS device are performed under the supervision of at least two authorized employees of the Exchange;
* the EDS device used to issue PKCs or LRCs operates properly.

2.2. PKC Management Requirements

2.2.1. Registration of the Subscriber

The EEAS CA shall, at the time of registration of the subscriber for receipt of the PKC, establish and verify that all provided information is reliable, complete, and accurate.

Prior to entering into the contract, the subscriber shall review the norms and rules related to the use of the PKC. The EEAS CA shall use durable data storage devices to provide such information, including electronic information, in the official language of the Republic of Belarus.

The EEAS CA shall, acting in accordance with the existing legislation, verify authenticity of the subscriber and completeness and accuracy of the provided information.

The identify of an individual shall be verified using an identification document permitted by the existing legislation, such document confirming the surname, name, patronymic, date of birth, and identification number of such individual.

If the subscriber is a legal entity, the following information shall be furnished and confirmed to verify its authenticity:

* surname, name, patronymic, date of birth, and identification number of the authorized person;
* full name and legal status of the legal entity;
* any appropriate current registration information on the legal entity;
* information proving that the subscriber is an authorized representative of the legal entity.

The EEAS CA shall register all information used to verify the identity of the subscriber, including the number of the identification document permitted by the existing legislation, the date of issue of such document, and the name (code) of the body which issued such document, as well as other information.

If the registration documents are submitted by an authorized representative acting for the subscriber, it shall be necessary to furnish the EEAS CA with a document confirming that such authorized representative is entitled to engage in such activities (i.e., that the PKC issue request shall be drawn by the authorized representative for all members of such entity).

The EEAS CA shall register the contract with the authorized representative, such contract to contain:

* a description of the rights and obligations of the subscriber;
* the following provisions (or references to the documents governing such provisions):

о consent authorizing the EEAS CA to store the information provided at the time of registration, and perform any subsequent revocation or transfer of such information to third parties, on the same terms as are prescribed by this CP for the situations where the EEAS CA terminates its operations;

о consent of the subscriber to the publication of the PKC, and the terms of such publication;

о confirmation that the information contained in the PKC is true and accurate.

The aforementioned registration information shall be retained so as to enable its provision as evidence in legal proceedings for a period of time stipulated by the existing legislation of the Republic of Belarus.

The subscriber shall submit to the EEAS CA, together with the PKC issue request, the public key card with the handwritten signature of the representative of the subscriber and an impression of the seal of the private key owner which is a legal entity, or with the handwritten signature of the private key owner which is an individual, including the personal signature of the individual entrepreneur.

2.2.2. PKC Issue

The PKCs issued by the EEAS CA shall contain the following:

* EEAS CA identifier;
* information uniquely identifying the entity or individual which is the owner of the public key;
* intended use of the PKC;
* value of the public key;
* start and end dates of the validity period of the PKC;
* identification number of the PKC;
* EEAS CA EDS.

The EEAS CA shall guarantee that the PKC identification number is

unique.

The EEAS CA shall ensure confidentiality and integrity of the registration data transmitted at the time of exchange with the subscriber.

2.2.3. PKC Distribution

The public key certificate of the EEAS CA subscriber shall become valid upon its issue. The EEAS CA shall notify the subscriber of the issue of its PKC. The EEAS CA shall place the issued PKC on the server hosting the register of certificates of the Exchange.

The EEAS CA may revoke an active PKC and issue a new PKC in accordance with the provisions of paragraphs 2.2.4 and 2.2.2.

The information on the intended use of the PKC shall be available to the relying parties.

Such information shall be available 24 hours a day 365 days a year. In the event of any system/service failure or operation of other factors beyond the control of the EEAS CA, the EEAS CA shall do everything reasonably possible to guarantee that such information service remains unavailable only for the shortest possible period of time.

2.2.4. PKC Revocation and Suspension

The EEAS CA shall revoke any PKC on the basis of the relevant request within the period of time stipulated by the EEAS CA Regulations.

PKC revocation requests shall be processed by the EEAS CA as soon as they are received.

Revocation requests shall be identified and verified by the EEAS CA to ensure that they are received from reliable sources.

The subscriber of the revoked or suspended PKC shall be notified by the EEAS CA of the change in the status of its PKC.

If any PKC is revoked, it shall not be used again.

PKC status information shall be disseminated by the EEAS CA through the LRC which shall be issued and published during the same day.

The PKC revocation and status notification services offered by the EEAS CA shall be available 24 hours a day 365 days a year. In the event of any system/service failure or operation of other factors beyond the control of the EEAS CA, the EEAS CA shall guarantee that such information service remains unavailable only for the shortest possible period of time.

2.2.5. PKC Reactivation and Data Update

PKC reactivation shall be performed by the EEAS CA on the basis of the request filed by the subscriber.

The PKC shall be reactivated without changing the public key of the subscriber, or any other registration information contained in such PKC.

Prior to reactivating the PKC, the EEAS CA shall ensure that the information used to confirm the identity and authority of the subscriber remains true and accurate at the time of filing of the reactivation request.

2.3. Management of EEAS CA Operations

2.3.1. Security Management

The EEAS CA management shall be responsible for taking steps to protect information, define the EEAS CA information security policy, and ensure that such policy is reviewed by all relevant EEAS CA personnel.

EEAS CA information security requirements shall be

defined based on the findings of systematic risk assessments. Such risk assessments shall be conducted periodically and methodically so as to cover any changes in protection requirements and risks affecting assets, threats, vulnerabilities, adverse consequences, significance of individual risks, and possible major changes.

The EEAS CA shall be responsible for all aspects of provision of the public key distribution services, even if some of those services are provided by its subcontractors. Liability of all third parties

shall be determined on the basis of appropriate contracts with such third parties.

The EEAS CA shall develop documents governing physical security of EEAS CA premises, as well as operating procedures for the information systems and assets engaged in the provision of public keys distribution services.

2.3.2. Distribution of regulatory and organizational documents

The EEAS CA shall guarantee that all its required regulatory and

organizational documents are available to the subscribers and relying parties.

The EEAS CA shall provide the subscribers with access

to the following EEAS CA regulatory and organizational documents:

* this CP;
* EEAS CA Regulations;
* documents on restrictions on the use of issued PKCs;
* documents on the duties of the subscribers.

2.3.3. Assets Classification and Management

All EEAS CA assets shall be clearly defined, and an inventory of all critical assets shall be created and periodically updated. In addition, information ownership and classification shall be coordinated and documented for each asset. The value of each asset to the EEAS CA shall be measured subject to the level of its criticality, and protection categories and levels commensurate with its criticality shall be selected. It shall be necessary to identify the owners of all key assets, and define their responsibility for the completion of the relevant information security management steps.

2.3.4. Personnel-Related Security Issues

The EEAS CA shall engage for the provision of its public keys distribution services only employees who are properly qualified, have the requisite experience, and have passed the test for compliance with the EEAS CA HR policy requirements.

The job descriptions of EEAS CA employees shall define their roles, rights, obligations, and responsibility for the protection of information. They shall also define their access rights and procedures governing access to protected information, and the penalties that shall be imposed for the commission of unauthorized actions and breach of information security policies or EEAS CA procedures.

2.3.5. Physical Protection and Protection from Adverse Environmental Impact

The EEAS CA shall provide physical access to the hardware used for the generation and revocation of PKCs only to duly authorized persons.

The EEAS CA shall exercise proper control to prevent emergence of any situations where critical information is lost, damaged, or compromised, which may results in suspension of its operations.

The EEAS CA shall exercise proper control to prevent emergence of any situations where any information or hardware used for the processing of such information is compromised or stolen.

An EEAS CA server center shall be created to provide a physically protected environment which shall ensure prompt detection and prevention of unauthorized use, access, or disclosure of any information processed by the EEAS CA.

The EEAS CA shall provide physical protection and protection from adverse environmental impact for all premises hosting system resources, as well as for such system resources and all hardware used to support EEAS CA operations.

2.3.6. Operating Activity Management

The EEAS CA information system and the information processed by the EEAS CA shall be protected from viruses and untrusted software.

The EEAS CA shall record, and ensure prompt response to, all ISS failures and incidents.

The EEAS CA shall define and implement procedures affecting provision of public keys distribution services.

The EEAS CA shall plan steps to ensure that its system resources and disc space are sufficient for proper information processing and storage.

The EEAS CA shall promptly take coordinated steps to provide rapid response to any security incidents, and limit the impact of security breaches.

The EEAS CA shall regularly check its audit logs for traces of malicious activities.

2.3.7. System Access Management

When connecting its information system to the internet, the EEAS CA shall use information protection devices which have compliance certificates issued by the National Compliance Certification System of the Republic of Belarus.

The EEAS CA ISS may employ cryptographic protection devices to ensure confidentiality, integrity (absence of alterations) and validity of information.

The EEAS CA shall restrict access to EEAS CA information and system functions in accordance with the Information Security Policy, and ensure that the existing computer security controls are sufficient to segregate security administrators from all other EEAS CA employees. Access shall be granted only to those resources that are required for the users to continue their operations in that capacity.

EEAS CA employees shall successfully pass the identification and authentication procedure before they may use critical hardware employed in PKC management.

EEAS CA employees shall be held responsible for all their activities, e.g., on the basis of saved event logs.

The EEAS CA shall guarantee that local network components are maintained in a physically secure environment, and that their configuration is periodically tested for compliance with the requirements stipulated by the Information Security Policy.

The EEAS CA server center shall engage in continuous monitoring, and have proper alarm systems to efficiently detect, record, and respond to unauthorized and erroneous attempts to access its resources.

The application used to determine the revocation status shall monitor access with a view to detect attempts to modify revocation status information.

2.3.8. Implementation and Maintenance of Information Systems

The EEAS CA shall use safe and trusted information systems and products protected from modification.

Security requirements shall be reviewed at all stages of development of information systems for the EEAS CA with a level of detail sufficient to properly ensure that security mechanisms are reliably embedded in such systems.

2.3.9. Post-Failure Recovery and Business Continuity

The EEAS CA shall guarantee that its operations are renewed as fast as possible after any failure, including situations where any EEAS CA signature private key is compromised.

The EEAS CA shall have a post-failure recovery and business continuity plan describing all reasonably predictable types of failures and compromises affecting provision of its public keys distribution services.

The data contained in EEAS CA information systems and required to ensure continued operation of the EEAS CA shall be backed up and stored in safe location suitable for prompt recovery of EEAS CA operations after any incident of failure.

The EEAS CA post-failure recovery and business continuity plan shall treat any compromise or suspected compromise of any EEAS CA signature private key as a failure.

If any EEAS CA signature private key is compromised, it shall:

* notify all subscribers, relying parties, and other CAs with which it has executed contracts or other agreements on compromise response measures;
* announce that all PKCs and LRCs issued with the use of such EEAS CA key are no longer valid.

2.3.10. Termination of EEAS CA Operations

In the event of termination of EEAS CA operations, it shall guarantee that potential threats to the subscribers and relying parties are reduced to a minimum, and that all PKC information shall be preserved for submission as evidence in legal proceedings, if necessary.

In the event of termination of its operations, the EEAS CA shall:

* notify the subscribers, relying parties, and other CAs with which it has executed contracts or other agreements;
* limit all authorities previously granted to the subcontractors providing public keys distribution services for the benefit of the EEAS CA;
* take all steps required for the transfer of its duties related to the storage of registration information and archive records, including all revocation status information, for an appropriate period of time agreed with the subscribers and relying parties;
* destroy its signature private keys.

2.3.11. Retention of PKC-Related Information

The EEAS CA shall guarantee that all relevant PKC-related information shall be retained for an approved period of time, in particular, to enable its submission as evidence in legal proceedings that involve electronic documents.

The EEAS CA shall maintain confidentiality and integrity of all current and archived PKC-related records.

The EEAS CA shall provide access to PKC-related records for the purpose of their submission as evidence in legal proceedings.

All documentable events and data shall be properly documented by the EEAS CA.

The EEAS CA shall guarantee that all events related to the registration of subscribers and issue of PKCs are properly recorded.

The EEAS CA shall retain all registration information, including the following:

* the number of the identification document of the applicant permitted by the existing legislation, the date of issue of such document, the name (code) of the body which issued such document, and the identification number;
* copies of requests and identification documents, including the signed contract;
* all supplementary materials to the subscriber contract;
* identifier of the entity accepting requests.

2.4. Administrative Provisions

The EEAS CA norms and rules shall ensure independent operation of the EEAS CA and objectivity of its decisions.

The Exchange is registered as a legal entity in accordance with the existing legislation.

The Exchange shall ensure provision of services to all individuals and entities seeking EEAS CA services and approaching the Exchange for such services.

The liability of the Exchange shall be stipulated by the contract executed by the Exchange with the individual or entity to which the relevant services are provided.

The Exchange shall approve procedures governing review of requests and complaints received from EEAS CA service consumers, and resolution of disputes arising in connection with the provision of EEAS CA services.

The operations of the Exchange may not depend in any way on the actions or decisions of any third parties, including as regards approval of any decisions on provision and termination of services.

ATTACHMENT

to EEAS CA ISS Certificate Policy

|  |  |
| --- | --- |
| **PUBLIC KEY CARD**for EDS Verification (on two sheets)   |  |

**Name of the Entity – Public Key Owner:**

Healthcare Institution 'Brest Dental Clinic'

**Payer Identification Number (UNP):** 290293301

**Full Name:** Darya Vasilyevna Domracheva

**Cell Phone Number:**

**Legal Address:**

**Country:** BY

**Region:**

**District:**

**City:** Brest

**ZIP Code:** 223316

**Street, House, Block, Office:** Kuybyshev Street 402

**Identity document:**

Passport 123333, issued by Oktyabrsky Regional Division of Internal Affairs for the City of Minsk

**Identification Number:** 2342322151515

**Authorities:**

**Document Title:** Charter

**Document Number:**

**Document Type:**

**Authority Start Date:** 02.06.2015

**Authority End Date:** 01.01.2222

***Signature and certification of the first sheet of the public key card***

**Signature of Public Key Owner**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** Darya Vasilyevna Domracheva

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 20\_\_

L.S.

**Public Key Validity Period:**

Start: 2017-09-13T09:43:04Z

End: as per certificate validity period

**Signature Private Key Use Period:**

Start: 2017-09-13T09:43:04Z

End: as per certificate validity period

**Algorithm:** STB 34.101.45

**Public Key Value:**

252E89F1 DBEC2917 2611A3F3 87AD330F 18303E3D 2488FE62 A6194F78 695766C7 3EEEAC8F 46C21BF5 70602BE1 A3DD78F9 3C934AAD 33EB368E C670AAD4 511B8E84

**Algorithm Parameters:**

Object identifier of the set of long-term parameters (according to STB 34.101.45):

1.2.112.0.2.0.34.101.45.3.1

**Signature of Public Key Owner**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** Darya Vasilyevna Domracheva

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 20\_\_

L.S.

**Card Certified by:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 20\_\_

L.S.