# Certificate Policy of PostSignum Root QCA for the certificates of subordinate CA (Algorithm ECC)

Version 1.0.2

**Table of contents**

# 1 INTRODUCTION

This document sets out the rules and procedures by which the root certification authority PostSignum Root QCA self-signed certificate and certificates issued to subordinate CAs that are operated within the hierarchy of PostSignum Czech post.

## 1.1 Overview

Česká pošta, s.p. (hereinafter referred to as well as ČP or the Czech post) established a two-level named hierarchy of certification authorities PostSignum. This certification policy describes the rules by which the root CA issues certificates of PostSignum Root QCA.

Certificates issued under this policy are certificates for electronic seal within the meaning of [eIDAS] hereinafter referred to as the certificate. Are issued to root and subordinate CAs, which are operated within the hierarchy of PostSignum Czech post.

CA, which has been issued with the certificate referred to in this certificate policy, it must be operated by Czech post, s.p.

Subscribers of certificates issued by PostSignum Root QCA are therefore a certification authority operated by the Czech post that issue certificates to other entities, but which are no longer certifying authorities.

The private key corresponding to the public key in the certificate issued by the authority PostSignum Root QCA is designed for:

- sealing certificates of entities that are not CAs,
- sealing of the certificate revocation list (CRL – Certificate Revocation List).

The rules for issuing and managing certificates according to this policy are further described in the practice statement, current certification of PostSignum QCA.

## 1.2 Document Name and Identification

Table 1 policy Identification

| | |
|---|---|
| The name of the document | Certification policy of PostSignum Root QCA (ECC) |
| Version of the document | 1.0.2 |
| The status of the | the final version |
| The OID of the provider of certification services | 2.23.134 |
| PostSignum Root QCA OID | 2.23.134.1.4.2.1 |
| The OID of this policy | 2.23.134.1.4.1.24.100 |
| Release date | 29. 5. 2023 |
| Effective date | 1. 6. 2023 |
| Revision date | 7. 5. 2025 |
| The period of validity | Until further notice or until the date of termination of service authorities PostSignum QCA. |

### 1.2.1 Document revision

| Version | Revision date | The reason and a description of the changes | The author of the | Approved by the |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| 0.9 | 1. 3. 2022 | Draft | PCA ČP | |
| 0.91 | 1. 4. 2023 | Changes to the nomenclature of certificates | PCA ČP | |
| 1.0.0 | 24. 5. 2023 | The comments of the commission for CP have been incorporated | PCA ČP | PAA ČP |
| 1.0.1 | 7. 5. 2024 | Revision without changes | PCA ČP | |
| 1.0.2 | 7. 5. 2025 | Revision without changes | PCA ČP | |

1.3 PKI Participants

Česká pošta, s. p., as a provider of certification services, set up the hierarchy of certification authorities PostSignum named, which is operated by a root certification authority PostSignum Root QCA and the subordinate certification authority that provides different certification services. Subordinate CAs can be controlled and operated only by the Czech post, s.p. (with the exception of the registration authorities).

The identity and contact details of the provider of certification services are:

Česká pošta, s. p.

COMPANY REGISTRATION NO. 47114983, VAT REGISTRATION NUMBER CZ47114983

Politických vězňů 909/4, 225 99 Praha 1

Tel: 800 104 410, e-mail: info@cpost.cz

Česká pošta, s. p. became an accredited certification service provider on the basis of 3.8.2005 accreditation granted by the Ministry of Informatics of the CZECH REPUBLIC.

Czech post in 1.7.2016 become a qualified service provider trust in accordance with [eIDAS].

1.3.1 Certification authority ("CA")

Postsignum Root QCA forms the root of the hierarchy of certification authorities operating within PostSignum. Its job is to primarily issue and manage certificates of certification authorities operating within PostSignum. Security measures, which are Root QCA PostSignum protected, are proportionate to the importance of this certification authority.

Detailed information about CA can be found on the provider's website www.postsignum.cz/.

1.3.2 registration authorities (“RA”)

Application for issue of a certificate under this certificate policy is communicated to the Manager of CA, along with attached documents (see paragraph 4.1.2) passes to the Commission for certification policy (see paragraph 1.3.5.1).

CA Manager contact details are listed in the paragraph. 1.5.2.

1.3.3. Subscribers applied for issue of the certificate, and that certificate was issued

Certificates are issued for Cas, whose operator is the Czech post. Authorized by the certificate of the subordinate CA is a CA Manager.

1.3.4 Relying parties

The relying party (the user certificate) is any natural or legal person relying on a certificate issued by PostSignum QCA. Relying parties do not enter into a contractual relationship with the provider of certification services.

1.3.5. Other participating entities

1.3.5.1 External participating entities

Certification authority PostSignum QCA may use to ensure the provision of services to external bodies.

1.3.5.2 Internal participating entities

The Commission for certification policy ČP

The Commission for the ČP certification policies (Policy Approval Authority PAA ČP) is a body that establishes, monitors and maintains the policy governing the activity of the CAs in the hierarchy of PostSignum. This is how the policy for the root CA (PostSignum Root QCA), so on the policy for subordinate CA certificate (PostSignum Qualified CA).

The Commission for certification policy ČP

- establish team for certification policies ČP, directs and controls his activity,
- approve new certification policies,
- maintains and checks for an existing policy,
- responsibility for policy consistency and integrity,
- approve any changes to the certification policies
- responsibility for publishing the current version of certification policies.

The Commission for certification policy ČP can be contacted at

paa.postsignum@cpost.cz

Certification policies team ČP

Team for the creation of the Czech post certification policies (Policy Creation Authority – PCA CP) is responsible for policy making, be submitted for approval to the Commission for policy. PCA ČP is established by the Commission as necessary for the certification policy of the ČP, it is managed and controlled.

1.4 Certificate usage

1.4.1 Use of certificate admissible

Certificates issued under this certificate policy may only be used for the verification of the electronic seal a subordinate CA in the hierarchy of PostSignum on it issued certificates or certificate revocation lists.

1.4.2 Certificate use restrictions

Certificates issued under this certificate policy is to be used only in connection with the ordinary and legal purposes and in accordance with applicable law.

1.5 Policy administration

For initiating changes in the certification policy or by initiating a new certification policies is the responsibility of the Manager of CA. The forwards the request to the team for creating the certification policies (PCA ČP).

Any changes to this certificate policy are subject to the approval of the Commission for certification policy of the ČP (PAA ČP). PAA ČP assigns a new version number, which allows you to identify the version of the.

PAA ČP decides whether a new version of certification policies will be published on the website of the provider or other means, or both.

In the case of upcoming major changes, i.e. the certification policies. changes that have an impact on the applicability of a certificate, warranty, liability or processes (and which throws a change OID) will be prepared to change the published way referred to in paragraph 9.12.2.

1.5.1 Organization administering the certificate policy or certification practice statement

The management of this certification policy is the responsibility of the provider of certification services, i.e. the Czech post, s.p., specifically, the Manager of the CA.

1.5.2 Contact person organization that manages the certification policy or certification practice statement

The contact person in case management of this certificate policy is the Manager of CA. More information can be obtained at the email address

manager.postsignum@cpost.cz

or on the website of the provider.

1.5.3. The body responsible for deciding on the compliance procedures of the provider with the procedures of other certification service providers

The management of this certification corresponds to the policy CA Manager, which also decides on the conformity of the procedures with the practices of other providers of certification services.

1.5.4. The procedures for the approval of compliance under 1.5.3

This document is produced by the team for creating the certification policies ČP (Policy Creation Authority – PCA ČP). PCA ČP is established by the Commission as necessary for the certification policy of the ČP, it is managed and controlled. PCA ČP passes the document to the Commission for approval to the certification policy.

The new version of certificate policies and certificate are created as needed, practice statement, in particular:

- When such a change of PostSignum QCA (e.g. changing procedures) which will affect the contents of those documents,

- If you are a regular inspection of the surrounding environment of PostSignum QCA have been identified changes to the requirements of these documents.

For initiating changes in certificate policy or CPS or initialize a new certificate policy or CPS is the responsibility of the Manager of CA. In the preparation of changes in certificate policy or CPS will decide in CA Manager based on the list of identified changes, how the planned changes will be published. The Commission for certification policies as needed appoint PCA ČP, whom the Manager then passes the list of CA required changes to incorporate. Drawn up by policy or CPS shall provide the Manager of CA for approval to the Commission for certification policy, which then confirms the OID (only policy) and assigns the version number.

1.6 Definitions and Acronyms

**Accreditation-** The term of accreditation is meant to obtain the status of a qualified trust service provider according to [eIDAS].

**CDP (CRL Distribution Point)** -URL address in the certificate, from which you can download the current CRL.

**Certificate for electronic seal-** certificate for legal persons within the meaning of [eIDAS].

**Coordinated Universal Time (UTC)** – Coordinated universal time, the time standard based on International Atomic time (TAI).

**CRL (Certificate Revocation List)** – certificate revocation list. Contains certificates that are still cannot be considered valid, for example, disclosure of the corresponding private key of the subject. CRL issuer certificate is digitally signed – CA.

**Subscriber of the certificate -** the customer from the moment of issue of the certificate.

ECC – (Elliptic Curve Cryptography) is a cryptographic algorithm based on elliptic curves.

HSM – (Hardware security module) is a cryptographic module that is used to securely store private keys.

**Commission for the certification policies of ČP (Policy Approval Authority-PAA)** -the authority in whose jurisdiction is to approve, monitor and maintain certification policies and certification practice statement, which governs the activities of certificate authority.

**Qualified electronic time stamp** – qualified timestamp as defined in [eIDAS].

**CA Manager** -a person in a management role, responsible for the operation of PostSignum QCA and PostSignum VCA.

**Business place** --Central regional offices that provide certification services and providing for the registration of contracts.

**Online Certificate Status Protocol (OCSP)** – Protocol for the online determine the status (revocation) of the certificate.

**Supervisory body –** Supervisory authority over the qualified trust service providers according to the [eIDAS] that is determined on the basis of existing legislation.

**Imprint** - a unique data string constant length, which is calculated from any input data clearly represents the input data;, i.e. There is no the same fingerprint for two different messages.

**Paired data (key pair)** – Are the basic primitive, asymmetric cryptography. It is composed of private and public key. In terms of confidentiality, it is necessary to protect their generation and the private key.

**Sealing person -** person as defined in [eIDAS].

**PKI** - Public Key Infrastructure

**Applicable legal regulations** – We refer to the legislation on electronic signature, in particular the area then the law on trust services for electronic transactions 297/2016 Coll. and REGULATION of the EUROPEAN PARLIAMENT and of the Council (EU) No. 910/2014 dated July 23, 2014 about electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC including the downstream legislation.

**PostSignum** - CA hierarchy and authority of time stamp consisting of root CA PostSignum Root QCA, all subordinate certification authorities for which PostSignum Root QCA has issued a certificate,, and the authorities of the time stamp, for which one of the certification authorities PostSignum qualified certificate issued.

**PostSignum QCA** - hierarchy of certification authorities issuing qualified certificates within the meaning of [eIDAS].

**PostSignum VCA** - hierarchy of certification authorities, issuing commercial certificates.

**PostSignum Root QCA** - root CA that has a self-signed certificate. Issues certificates to subordinate CAs and CRL. In the hierarchy of PostSignum can be other root CAs that are additionally identified by a serial number, for example. Postsignum Root QCA 2.

**PostSignum Qualified CA** - CA that has a certificate signed by a root CA PostSignum Root QCA. Issuing qualified certificates for entities that are not CAs. In the hierarchy of PostSignum QCA there may be other subordinate CAs that are additionally identified by a serial number, for example. Postsignum Qualified CA 2.

**PostSignum Public CA** -CA that has a certificate signed by a root CA PostSignum Root QCA. Issuing commercial certificates for entities that are not CAs. In the hierarchy of PostSignum VCA

there may be other subordinate CAs that are additionally identified by a serial number, for example. Postsignum Public CA 2.

**PostSignum TSA** – the authority of issuing qualified electronic time stamp within the meaning of [eIDAS]. The authority is composed of multiple units (TSU). Each unit has a private key and certificate for qualified electronic seal.

**QCA ČP** – see PostSignum QCA.

**Registration authority** – the workplace, whose basic task is to take the certificate request or its revocation, check the identity of applicants, then accept or reject the request and pass it to the certificate issued to the applicant or this certificate void.

**Distinguished name** -uniquely identifies the signer according to the rules defined by the certification policy.

**Private key** – combined term electronic signature creation data or data to create an electronic seal, for encrypting and decrypting data and data for authentication.

**Certification policy development team (Policy Creation Authority - PCA)** – the team that produces the policies, be submitted for approval to the Commission for certification policy. PCA is set up by the Commission for certification policy that directs and controls its operation.

**Certificate user (relying party)** – a person who uses a certificate issued by PostSignum, for example, for the verification of the electronic signature or seal or to provide other security services. Also referred to as the Person relying on the certificate.

**VCA ČP-** see PostSignum VCA.

**Public key** – summary data for verifying an electronic signature or electronic authentication seal data and data for encryption.

**Provider websit** - https://www.postsignum.cz – service provider website of PostSignum.

**Customer -** natural person not performing any business activities, natural person performing business activities, legal person, state or local government body. Concluded with the Czech post contract for the provision of certification services.

**Employee -** a person in an employment or other relationship to the customer for which the customer has approved the issue of a certificate under this certificate policy.

**Applicant** – a person who has the right to apply for the certificate by some of PostSignum from valid certification policies.

## 2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

### 2.1 Repositories

Each of the storage of information and documentation and for their operation corresponds to the Česká pošta, s. p. as a provider of certification services.

For the publication of information corresponds to the Česká pošta, s. p. as a provider of certification services.

This document is available on the provider's website:

https://www.postsignum.cz/certifikacni_politiky_root_qca.html

2.2 Publication of certification information

Issued certificates are stored in the CA database.

Information on issued certificates, on the operation of PostSignum QCA and PostSignum QCA documentation are published in the following range.

The structure of this certification policy is consistent with the structure specified in RFC 3647.

The PostSignum certification authority confirms that this certification policy complies with the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates [CA/B] document published at http://www.cabforum.org. In the event of a conflict between this Certification Policy and [CA/B], the provisions of [CA/B] shall prevail.

2.2.1. Publication of certificates and CRLs

Certificates issued by CA and the certificates are published

- on the website of the provider

https://www.postsignum.cz

Certificate status information are published in the form of the certificate revocation list (CRL)

- on the website of the provider

http://crl.postsignum.cz

http://crl2.postsignum.cz

http://crl.postsignum.eu

2.2.2. Disclosure of information about certification authority

Message to the user and, where appropriate, certification policies or other documents are published on the

- website of the provider

For more important information, in particular information required by applicable laws and regulations (such as the withdrawal of accreditation, the revocation of the certificate of the CA), or information about the incident are published

- on the website of the provider,
- on business sites, and RAS in the form that is posted the text of the notification,
- in a nationally distributed journal.

2.3 Time or frequency of publication

Information shall be published in the following intervals:

- certification policies, certification practice statement and the report are published to the user (if they are intended for publication) after the approval and release of a new version, but always before the beginning of the document (and in the case of certification policies before issuance of the first certificate);
- certificates, if they have been marked for publication are published electronically at the latest within 24 hours from the receipt of the certificate subscriber;
- certificate status information in the form of the certificate revocation list (CRL) are published immediately after they are issued, at the latest before the end of the last published certificate revocation list (i.e., at least once every 12 months), and
- important information, in particular the information required by the applicable legislation shall be published without delay.

2.4 Access controls on repositories

Certification policies (if they are intended for publication), the CA certificates and certificate revocation lists and other important information are accessible for reading without any restrictions.

Modification of published data is enabled, only the authorized operation and processes of the CA.

## 3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

Name of the body is designed according to the standard X.501 or connecting standard X 520.

3.1.2 Requirement for meaningfulness of names

The importance of the data used in attributes of the certificate subject and certificate extensions is described in Chapter 7.

3.1.3 Anonymity and using of the pseudonym

The Czech post does not support a pseudonym in the Subject subordinate CA certificate.

3.1.4 Rules for interpreting various name forms

In certificates issued by PostSignum Root QCA are supported only by the following character sets:

- UTF8, the characters of the Central European character sets
- US ASCII.

All information documented during the registration application for a subordinate CA in the certificate requests and certificates issued by PostSignum Root QCA, are transmitted in the form in which they are listed in the submitted documents. Transcription, such as removing the diacritics, is not possible.

3.1.5 Uniqueness of names

Postsignum Root QCA reserves the right to modify the designation of the certificate subscriber (the Subject entry in the certificate), so as to guarantee the uniqueness of names, so that the same distinguished name was not assigned to two different entities.

3.1.6 Trade marks

All the fields in a certificate issued under this policy shall include the information relating to the subordinate certification authority. A certificate may contain only brand names or registered trademarks that are owned by the Czech post, s. p., or to which it has the consent of the owner.

3.2 Initial identity validation

3.2.1 Data Consistency Verification, i.e. the process of verifying that a person has a private key that matches the public key

The applicant shall submit an electronic request for a certificate in PKCS # 10 format containing a public key that is signed by the private key corresponding to the public key specified in the request. It is shown that the applicant for the certificate at the time of creating the application owned the private key corresponding to the public key specified in the request.

3.2.2 Verification of the identity of a legal entity or an organizational component of the state

Certificates are issued for CAs, whose operator is the Czech post. Authorized by the certificate of the subordinate CA is a CA. Manager, your identity and your privileges in accordance with the internal rules is illustrated by the Czech post.

3.2.3 Verifying identity of the natural person

See the provisions of paragraph 1. 3.2.2.

3.2.4 Unverified information that applies to the subscriber of the certificate

All the information listed in the certificate issued by the subordinate CA certificate are properly authenticated.

3.2.5 Authentication of specific rights

No provisions in this paragraph.

3.2.6 Criteria for interoperability

Cooperation with other providers of certification services is possible only after approval by the Commission for certification policy of the ČP, on the basis of the concluded contract and under the conditions defined by the Commission.

3.3 Identification and authentication for re-key request

3.2 Identification and authentication when processing requests to the public key in the certificate exchange

3.3.1 Identification and authentication during a routine exchange private key and its corresponding public key ("data matching")

The provisions applying to the initial identity verification referred to in paragraph 1. 3.2.

3.3.2 Identification and authentication when replacing a pair of data after the revocation of the certificate

The provisions applying to the initial identity verification referred to in paragraph 1. 3.2.

3.4 Identification and authentication for revocation request

An eligible applicant for revocation of the certificate of the subordinate CA is manager of CA. The CA manager documents his identity and his authorization according to the internal regulations of the Czech Post.

Invalidation of a subordinate CA certificate can also occur at the will of the certification service provider. In this case, the authorized applicant for certificate revocation is the CA Manager. As a preliminary measure, the supervisory body defined by applicable legal regulations may request the invalidation of the certificate. In this case, the authorized applicant for certificate invalidation is the representative of this authority.

## 4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

4.1.1 Entities authorized to apply for a certificate

Certificates are issued for CAs, whose operator is the Czech post. Authorized by the certificate of the subordinate CA is a CA Manager.

4.1.2 Registration process and responsibilities of provider and applicant

Written request to issue the subordinate CA certificate is presented to the Commission for certification policies. The request must contain the following identifying information certification authority for which the certificate is to be issued:

- name of the CA,
- CA operator – advanced operators in the context of the Czech post.

The application must be signed by the Manager of CA.

Written applications and all attached documents are archived in accordance with [ZoSVD].

4.1.2.1. The responsibility of the applicant

The applicant shall, in particular:

- to provide truthful and complete information when registering a certificate request
- check whether the data referred to in the certificate are correct and correspond to the relevant data,
- dispose of the private key that matches the public key in a certificate issued under this certificate policy, with due diligence, so as to prevent its unauthorized use,
- use a private key and corresponding certificate issued under this certificate policy only for the purposes set out in this certificate policy,
- immediately inform the provider of certification services of the facts which lead to the revocation of the certificate, in particular on the suspicion that a private key has been compromised, the certificate revocation request, and stop using the corresponding private key,
- become familiar with the certification policy, according to which the certificate was issued.

4.1.2.2. Liability of the provider

The provider of certification services is in particular required to:

- in the process of registration of the certificate requester to verify all of the information referred to in the documents submitted,
- issue a certificate containing the factually correct information based on the information that is available to the certification authority at the time of issue of the certificate,
- publish the certificate policies under which certificates are issued by, prescribed ways (see paragraph 2.2),
- publish the certificate of the certification services provider so that they can make sure of his identity,
- pay due attention to all the activities associated with the provision of certification services; proper care includes operations in accordance
- with valid legal regulations,
- with this certification policy,
- with the certification practice statement,
- with the system security policies,
- with the operational documentation.

4.2 Certificate application processing

4.2.1. Identification and authentication

The provisions of paragraph 3.2.2.

4.2.2. Acceptance or rejection of the application for a certificate

The Commission for certification policy of the ČP on the basis of the submitted request, decide whether it will be for a given certification authority issued the certificate.

4.2.3 Certificate request processing time

Decision on the acceptance or rejection of the request of the applicant for the certificate is communicated within 30 working days of the request.

4.3 Certificate issuance

4.3.1 Actions of the CA during certificate issuance

After the approval of a written request from Manager CA issuing a certificate to a worker having an electronic certificate request in PKCS # 10 format, containing the relevant data with the same values, which are listed in the transmitted documents. Together with the electronic certificate request passes a second written request of the Manager of a CA that contains the following information:

- name of the CA,
- CA operator – advanced operators in the context of the Czech post
- copy of the public key of the CA.

All provided information must correspond with the information given in the written request for a certificate. If the data is within 10 working days from the moment of the submission of this request, the certificate is issued.

The certificate becomes valid at the moment of issue.

4.3.2 Notification of certificate issuance to the certificate subscriber

The provider of certification services shall inform the applicant for the certificate of issue of the certificate no later than one working day from the issue of the certificate.

4.4 Certificate acceptance

4.4.1 Actions associated with receiving the certificate

A subordinate CA is an applicant for a certificate in DER format passed along with the certificate of PostSignum Root QCA. An applicant for a certificate, or his authorized representative personally takes the certificate and checks that the data referred to in the certificate is in order. If the applicant agrees, takes the certificate, and this Act shall certify by signing under the Protocol on acceptance of the certificate. If the details are not correct, the provider of certification services shall within 10 working days to issue certificate with corrected data.

By signing the Protocol, the subscriber of the certificate confirms:

- that takes the obligations arising out of the certification policy according to which the certificate was issued,

- that he is not aware of any facts that would indicate that the private key corresponding to the public key in the certificate is owned by a person other than what is allowed in the applicable certificate policy,

- that the information on the certificate are correct and complete.

4.4.2 Publication of certificates issued by the provider

Certificates issued by PostSignum Root QCA and intended for publication shall be published electronically.

4.4.3 Notification of certificate issuance to other entities

In addition to the publication of the certificate issued by the certification services provider shall not issue a certificate to any third party.

4.5 Paired data and certificate usage

Key pairs bound with certificates have the same duration as the certificates. Key pairs on the basis of which a certificate has already been issued by the PostSignum Root QCA CA cannot be reused in the PostSignum Root QCA again.

4.5.1 Using the private key and the certificate subscriber of certificate

The certificate subscriber is obliged in particular:

- dispose of the private key that matches the public key in a certificate issued under this certificate policy, with due diligence, so as to prevent its unauthorized use,

- in the case of loss, theft or suspected private key being compromised and shall immediately inform the provider of certification services and at the same time to end the use of the private key,

- enjoy a private key and corresponding certificate issued under this certificate policy only for the purposes set out in this certificate policy, referred to in paragraph 1. 1.4.

4.5.2 Public key and certificate the relying party

The user certificate issued by PostSignum Root QCA (the relying party) must in particular:

- PostSignum Root QCA to obtain a certificate from a safe source (Web page of the provider, the Web page of a supervisory authority, the registration authority in the workplace) and verify the fingerprint ("fingerprint") of this certificate.

- Before using a certificate issued by PostSignum Root QCA PostSignum Root certificate to validate the QCA and the validity of the issued certificate; a check is performed on the correct signature of the issuing authority and the current CRL and the current time.

4.6 Certificate renewal

Renewal of a certificate issued under this certificate policy is not possible. At the appropriate time before the expiry of the existing certificate, the applicant shall request for the issue of a new certificate (para. 4.1); It is not necessary to change the Subject of the certificate requestor.

4.6.1 Conditions for renewing a certificate

See the provisions of paragraph 4.6.

4.6.2 Bodies eligible for certificate renewal

See the provisions of paragraph 4.6.

4.6.3 Certificate renewal request processing

See the provisions of paragraph 4.6.

4.6.4 Notice of issue of the certificate of the renewed certificate subscriber

See the provisions of paragraph 4.6.

4.6.5 Tasks connected with takeover of the renewed certificate

See the provisions of paragraph 4.6.

4.6.6 Publication issued by the renewed certificates provider

See the provisions of paragraph 4.6.

4.6.7 Notice of issue of the renewed certificate to other entities

See the provisions of paragraph 4.6.

4.7 Exchange of data for authentication of electronic signatures certificate

When exchanging the public key in the certificate is required to apply for a new certificate (para. 4.1); It is not necessary to change the subject the subordinate CA certificate.

4.8 Certificate modification

The certificate with the changed data can be issued only as a new certificate in accordance with the procedures referred to in paragraphs 4.1-4.4.

4.9 Certificate revocation and suspension

The validity of the certificate is suspended at the time of the revocation and publication of the certificate revocation list.

If there is no certificate for its validity must be revoked, expires in the time period stated in the certificate. Each certificate issued after the end of its validity remains continue to be stored in the database of the issuing CA and archived in accordance with the applicable legislation and regulations archive of the Czech post.

4.9.1 Conditions for revocation of certificate

The certificate may be invalidated by the will of the subscriber of the certificate, the will of the provider of certification services or at the base of a supervisory authority for an interim measure.

4.9.2 Bodies competent to apply for revocation of the certificate

On the revocation of the certificate may apply to the subscriber of the certificate by the CA Manager or a representative of the supervisory authority.

4.9.3 Certificate revocation request

4.9.3.1 Revocation of the certificate at the request of the certificate subscriber

CA Manager asks for revocation of the certificate in writing. In the application for revocation must be given the reason for the revocation.

4.9.3.2 Revocation of the certificate of PostSignum Root QCA

The provider of certification services might invalidate a certificate subscriber who runs a subordinate CA in contradiction with documents that have been attached to the application for a certificate. The reason for revocation may also be non-compliance with the rules of this certification policy or suspected compromised keys subordinate CA.

CA Manager serves a written request for revocation of the certificate of the subordinate CA, which passes one of operators authorized to revocation of the certificate. After the successful revocation of the certificate of the child CA is created, the certificate revocation Protocol, which is immediately sent to the Manager of CA. CA is the Manager of the subordinate CA certificate revocation also is informed by telephone or through electronic the post office.

4.9.3.3 Revocation of the certificate of the supervisory body

For the revocation of a certificate may, as a precautionary measure, asked a supervisory body. A representative of the supervisory authority is asking for the revocation of a certificate in writing, the request must include the reason for the certificate revocation.

After the successful revocation of the certificate of the child CA is created, the certificate revocation Protocol, which is immediately sent to the Manager of CA. CA is the Manager of the subordinate CA certificate revocation also is informed by telephone or through electronic the post office.

4.9.4 Postponement time for a certificate invalidation

In the moment when the person entitled to apply for revocation of the certificate becomes aware of the fact, that is the reason for the revocation of the certificate, shall promptly request revocation of the certificate.

4.9.5 Maximum time for  provider must implement the certificate revocation request

A certificate issued under this certificate policy will be invalidated immediately after authorizing the request for invalidation.

CRL containing a invalided certificate issued according to this certification policy is published immediately after the certificate has not been invalidated.

4.9.6 Obligations of relying party to verify that the certificate has not been invalidated

The user certificate issued by PostSignum Root QCA (the relying party) is obliged to act in accordance with the provisions of paragraph 1. 4.5.2.

4.9.7. Periodicity of the issuance of the certificate revocation list

Certificate revocation list (CRL) of PostSignum Root QCA is issued and published at least once every 12 months:

- CRL distribution points (CDP) listed in the certificate,
- on the website of the provider.

The primary source of the current CRL is a website www.postsignum.cz.

4.9.8 Maximum delay in issuing the certificate revocation list

Certificate revocation list is published as soon as possible after publication; It is always complied with the provisions of paragraph 1. 4.9.5.

4.9.9. Authentication option status of certificate online ("OCSP")

Certificates issued according to this certification policy can be verified using a publicly available OCSP service operated by PostSignum QCA.

The URL address of the Services is listed in the issued certificate according to this certification policy, see the certificate profile in chapter 7.1.2

4.9.10 Requirements when verifying the status of the certificate online

A publicly available OCSP service can be used to verify the certificate issued according to this certification policy. The OCSP service is operated in 24/7 mode and provided according to the RFC 6960 standard. The application format and OCSP responses are listed in chapter 7.3.

4.9.11 Other forms of revocation notification

The certification services provider does not provide any additional options, in addition to the above, for the verification of the certificate status.

4.9.12 Any differences the procedure in case of invalidation of compromise of the private key

Procedure for revocation of the certificate in the case of a compromise of the private key is the same as the General procedure for revocation of the certificate.

4.9.13 Conditions for the suspension of the certificate

Postsignum QCA this service does not provide. The validity of the certificate cannot be suspended.

4.9.14 Bodies competent to request suspension of the certificate

Postsignum QCA this service does not provide.

4.9.15 Requests for suspension of the certificate

Postsignum QCA this service does not provide.

4.9.16 Limitation on the suspension of the certificate

Postsignum QCA this service does not provide.

4.10 Certificate status services

You can verify the certificate status

- on the certificate revocation list (CRL) in the framework of services to enable the access to public information of PostSignum QCA HTTP
- using OCSP.

4.10.1 Operational characteristics

A list of certificate revocation and certificate status information are considered to be publicly available information. Certificate revocation list (CRL) is published in the places listed in section 4.9.7. The certificate invalidation information is at least provided by the CRL until its validity.

The OCSP service returns the status of the certificate in real time (on-line) on the basis of the submitted application. Which must meet the particulars specified in the certification implementing directive. The OCSP server response is signed by the OCSP server certificate and has the prescribed format listed in the certification implementation directive .. Information on the status of the certificate obtained using the OCS is a binding source of certificate information.

4.10.2 Service availability

Certificate revocation list is through the service that allows access to public information is available 7 days a week 24 hours a day. The architecture of the solution, and emergency plans are designed so that there was always at least one place where you can get the current certificate revocation list. Under normal operating conditions the response to obtaining this information is 10 seconds or less.

The OCSP service is available 7 days a week 24 hours a day.

4.10.3 Other characteristics status of certificate services

Other characteristics status of the certificate services are not provided.

4.11 End of subscription

The provision of services for the subscriber of the certificate (due to the fact that the certificate is issued to a subordinate CA in the management of the ČP) is closed at the moment of termination of the provision of services subordinate CA.

4.12 Private key storage at a trusted third party and their renewal

Postsignum QCA this service does not provide.

4.12.1 Policy and procedures in storage and renewing a private key

Postsignum QCA this service does not provide.

4.12.2 Policy and procedures for encapsulation and restoring the encryption key for the session

Postsignum QCA this service does not provide.

## 5 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

For the PostSignum QCA documents have been processed:

- System security policy, describing the principles of safety in the field of physical, procedural and personnel;
- Plan for crisis management and recovery plan, describing the procedures for maintaining guaranteed service levels in the event of an emergency,
- Operating and safety procedures, describing procedures to be followed logically in PostSignum QCA, and directive
- Organizing tasks Qualified certification authority of Česká Pošta, s. p., besides regulates the area of filling the roles of PostSignum QCA.

These documents have been drawn up on the basis of the results of the risk analysis carried out.

These documents are. accessible to the persons that perform safety checking of conformity of PostSignum QCA. This chapter is based on the above document and provides a brief overview of the basic safety principles applicable to PostSignum QCA.

5.1 Physical security controls

Activities associated with the management and operation of PostSignum Root QCA are carried out exclusively on the central sites.

5.1.1 Location and construction

In PostSignum QCA there are the following types of stable operations located in the premises of Česká Pošta, s. p. or its contractual partners:

- the central site (main and backup site)
- operator workplace centres (in particular for supporting management information system),
- workplace registration authorities and
- business place.

Used construction of the safety requirements outlined in the System security policy; in General, all of the above types of workplaces have a clearly defined perimeter and are protected against unauthorized intrusion by mechanical means.

5.1.2 Procedural Controls

For each type of workplace is in its operating regulations defined who workers have physical access to the workplace. Areas are protected against unauthorized intrusion, by mechanical means, on a central place of work is also a separate loop electronic signalling equipment.

5.1.3 Power and air conditioning

The central site are connected to an uninterruptible power supply (UPS) and have installed air conditioning, which maintains temperature and humidity the optimal for operating the device.

5.1.4. Effects of water

Central departments are located outside of the flood plains.

The central areas workplaces are equipped with alarm flooding. This alarm is output at the workplace occupied 24 hours a day, 7 days a week.

5.1.5 Firefighting measures and protection

Areas of central departments are equipped with electronic fire signalling (EPS). This alarm is output at the workplace occupied 24 hours a day, 7 days a week.

5.1.6 Media storage

For the purposes of storing the data of PostSignum QCA are safes, at least one of them is outside areas of buildings of central departments.

5.1.7 Waste disposal

Paper documents and media that are used in PostSignum QCA, are after are not necessary, disposed of in a safe manner:

- media are physically destroyed or program is sufficient to ensure a full erase media
- paper documents are disposed of in a dedicated device.

5.1.8 Backups outside of the building

For the PostSignum QCA was built on the location where the backup operation in emergency situations, when it is not possible to secure the proper operation of the QCA in the main site, and where they are also regularly sent backup systems of PostSignum QCA.

5.2 Process safety

5.2.1 Trusted roles

In PostSignum QCA have been defined roles that takes the operation of PostSignum QCA. The rules are established, according to which the roles are obsazovány, that is, a worker in the role, who appoints and dismisses that role may not act at the same time by one person. All of the access rights (at the level of physical access, on the access level for the operating system on the access level to the application) are bound to these roles.

Special attention is given, in particular, when filling the roles have access to the central systems of PostSignum QCA, thus all systems dedicated to the operation of PostSignum Root QCA.

5.2.2 Number of persons required to ensure the individual activities

In PostSignum QCA are defined in activities requiring the presence of more than one person. In particular, activities in which are handled with the private key of the CA and s from the

cryptographic module used to generate and store the private key (tool for creating electronic seal) certificate authority.

5.2.3 Identification and authentication for each role

A representative of each role must be used when access to the resources of PostSignum QCA to identify and authenticate. Each user is assigned a unique identification in all systems, to which it has access. In the systems of PostSignum QCA is used on behalf of the identification and authentication of certificate or password or private key.

5.2.4 Roles requiring separation of duties

In QCA Postsignum the rules according to which individual roles are occupied as well as the rules for separation of roles. These rules are stated in the document of organizational provision of a qualified certification authority of Česká Pošta, s. p..5.3 Personnel security controls.

The roles associated with operation of PostSignum Root QCA (the role of ensuring the operation and administration that have direct access to the system of PostSignum Root QCA) only employees may be appointed.

5.3.1 Requirements on qualifications, experience and integrity

The roles of the operation, management, maintenance and development of Postsignum QCA systems are occupied on the basis of procedures (eg. requiring references, testing periods, etc.), which ensure that these functions are occupied by credible and qualified employees. Similar procedures apply to concluding contracts with external co-workers or contractual partners.In the event that the person is not an employee of Česká Pošta, s. p., but its contractual partner, the requirements listed in the proper range with the partner.

5.3.2. Assessment of the reliability of the persons

In the roles of operation of PostSignum QCA are designated solely to persons who are employed in the longer period of Czech post, s. p., and have a good working and personal references.

In the event that the person is not an employee of Česká Pošta, s. p., but its contractual partner, the requirements listed in the proper range with the partner.

5.3.3. Requirements for the preparation for the role performance, initial training

All staff involved in the operation, management, maintenance and development of systems of PostSignum QCA, are trained. Part of the training is the training of the security of the system and about the behavior in emergency situations.

The role of the designated Manager of the CA can be replaced by a proven worker training to familiarize yourself with all of the documents governing the operation of the QCA is related to the role.

In the event that the person is not an employee of Česká Pošta, s. p., but its contractual partner, the requirements listed in the proper range with the partner.

5.3.4 Requirements and frequency of training

In PostSignum QCA is there a program creating, maintaining and enhancing safety consciousness, differentiated according to the roles.

The Manager of the CA on a regular basis (in particular changes in the procedures of PostSignum QCA) organised training of the operator.

5.3.5 Periodicity and sequence of rotation of staff between the different roles

Requirements for the rotation of staff and its frequency is not defined.

5.3.6 Sanctions for unauthorized actions of employees

Penalties for violation of work discipline is governed by the rules of Česká Pošta, s.p., or the provisions of the agreement between the Czech post and the contract partner.

5.3.7 Independent contractor requirements (vendor)

The contract (external) workers are applied similar criteria as to the staff of Česká Pošta, s.p.

5.3.8 Documentation provided to employees

Staff of PostSignum QCA has available documentation related occupied the role, especially

- security policy,
- certification policy,
- certification practice statement,
- operations documentation--manuals and working procedures for the operator.

5.4 Audit logging procedures

For the PostSignum QCA was prepared by the Audit and archival policy document (annexed to document the system security policy), which describes the policy of control, auditing and archiving of PostSignum QCA. This document is available to persons who carry out a check of the safety compliance of PostSignum QCA. This chapter is based on document and archive the audit policy and provides a brief overview of the basic principles applied in the control of PostSignum QCA.

5.4.1 Types of event recorded

For inspection and any analysis and examination of incidents (in General, in order to ensure the possibility to demonstrate the sequence of operation of PostSignum QCA and their assignment to the person who causes it) records are kept of the events at issue, their the validity of certificates, keys, and certificates of PostSignum QCA and other significant events (e.g., termination of the activities of the CA).

The audit records in written form must be signed and must indicate the name of the worker, which issued the alert.

5.4.2 Frequency of processing records

Audit records are checked by the persons in charge of this task, the corresponding role in the intervals defined System security policies. Furthermore, they are subject to internal and external review.

5.4.3 Retention period of audit records

Audit records are kept for a period of ten years, unless another regulation does not provide for a longer period.

5.4.4 Protection of audit records

Audit records are stored so that they are protected against theft, modification and destruction of intentional and unintentional (fire, water).

Audit records in the form of data files are archived on the media protected against transcripts.5.4.5 Backup procedures for the audit of records

The audit records in written form are generally not backed up; are only archived. Important audit records in written form associated with the issuance of certificates are also stored in electronic form.

The audit records in electronic form are backed up in the form of backup archives created after each change in the systems of PostSignum Root QCA.

5.4.6 Audit collection system records (internal or external)

Audit records are collected internally within each system of PostSignum QCA.

5.4.7 Notification of event procedure to the body that caused it

The entity that caused the event recorded in the audit log, this fact is not in any way be communicated.

5.4.8 Vulnerability Assessments

Audit records are searched at regular intervals, controlled and analysed for the presence of records of non-standard events that may indicate an attempt to breach security. The following are the procedures to follow in such cases.

Reports on non-standard events are. transmitted and the auditor of CA.

At least once a year, the certification authority systems are checked for vulnerability.

5.5 Records archival

For the PostSignum QCA was prepared by the Audit and archival policy document that describes the policy control, audit and archiving in PostSignum QCA. This document besides, is the accessible to persons who carry out a check of PostSignum QCA.

5.5.1 Types of information and documentationthat are kept

In PostSignum QCA are archived these records:

- software and data, including the issued certificates and CRLs,
- all documentation related to the registration of the certificate request, including contracts,
- a record of capturing the role of PostSignum QCA and operator training records,

- the logs are automatically generated by the components of the information system of PostSignum QCA.

5.5.2 retain stored information and documentation

Program equipment, data and audit records are archived for ten years, unless another regulation provides longer.

5.5.3 storage security of stored information and documentation

The archive is secured by measures of a technical and object security. It is also protected against environmental influences, such as temperature, humidity, etc.

5.5.4 Procedures to back up stored information and documentation

The archive backup procedures are regulated by separate document the audit and archive policy, that is. be accessible to persons carrying out control of PostSignum QCA.

5.5.5 Requirements for using the time stamps in the storage of information and documentation

If you are in PostSignum QCA utilized the time stamps, it is a qualified electronic time stamp of PostSignum QCA.

5.5.6 Collection system of stored information and documentation (internal or external)

In an environment of PostSignum QCA audit records are collected and moved to the archives in accordance with the procedures set out in the audit document and archive policy.

5.5.7 Procedures to obtain and verify the stored information and documentation

Data and software archives are located in the designated vaults.

At each site, where it is located, must be kept safe protocol for the stored archive media, in which are recorded all the manipulation of stored media.

Access to the archives is limited to persons in their respective roles.

5.6 Replacement of a public key in a superior provider certificate

Keys in the hierarchy of certification authorities PostSignum QCA is limited.

Well in advance, but not less than 1 year before the certificate expires PostSignum Root QCA must take place the ceremony of issuing the new certificate. The result of the ceremony will be created a new self-signed root CA certificate, which will be published in the manner described in Chapter 2.

The planned CA key exchange must be notified to the customer not later than 6 months before the release of the new certificate of PostSignum Root QCA. This notification shall be (including the reason for the termination of validity of the certificate), published on the website of the provider and the registration authority at all workplaces of PostSignum QCA.

After their needs using the original private key which was used for the sealing of qualified certificates and certificate revocation lists, this key Czech post demonstrably destroy and this destruction makes a record.

This procedure will also be used in the case where you will need to perform key exchange because of the inadequacy of the guarantees provided by the used algorithm or its parameters (e.g. the size of the module).

5.7 Compromise and disaster recovery

For the PostSignum QCA documents were drawn up describing the crisis management and the procedures for the subsequent reconstruction.

This documentation is. accessible for persons carrying out control of PostSignum QCA.

Staff of PostSignum QCA is properly trained in what to do in case of an accident. Test the emergency plan shall be carried out at least once a year.

5.7.1 Procedure in case of an incident and compromise

The CA resource security after the natural disaster, or other extraordinary event is fleshed out in the document of crisis management Plan and a recovery plan.

5.7.2 Damage to computing resources, software or data

The CA resource security after the natural disaster, or other extraordinary event is fleshed out in the document of crisis management Plan and a recovery plan.

5.7.3 Procedure for compromising a private key of the provider

In the case of a suspected compromise of the private key of PostSignum Root QCA will be informed in writing or electronically all the subscribers of the certificates, the supervisory authority and the entities that have concluded a contract directly relating to the provision of certification services of the extraordinary termination of the activities of the authority; the notice will also be published on the website of the provider, in all workplaces registration authority PostSignum QCA and one nationally published journal. Included in the notification will be the reason for the termination of the CA certificate.

As a technical measure of the certification services provider performs the PostSignum Root QCA revocation of the certificate, valid certificates of all subordinate CAs and all valid certificates issued by them; the certificates will be voided immediately published on the relevant CRL.

After the publication of the information about the extraordinary termination of activity is terminated, all certificates issued by PostSignum Root QCA and subordinate CAs.

The Czech post demonstrably destroys private key of PostSignum Root QCA, which served for the sealing of certificates and certificate revocation lists, where there is a suspicion of compromise, and this destruction makes a record.

This procedure will also be used if the algorithm used for the creation of electronic seals, which undoubtedly question the credibility of the issued certificates and lists of issued certificates.

5.7.4 Ability to recover after a disaster

Continuation of the processes of disaster CA depends on the type of disaster and its consequences, and it is for the management decisions of the Czech post. About management decisions with a minimum of delay must be notified to all customers of PostSignum QCA.

If the management of the Czech post decides to terminate the operation of PostSignum QCA does not exceed the downtime of the services of PostSignum QCA 20 working days.

5.8 CA or RA termination

5.8.1 Cessation of activities of a root certification authority

PostSignum Root QCA termination must be notified in writing to all the subscribers of valid certificates, the supervisory authority and the entities that have concluded a contract directly relating to the provision of certification services and also published on the website the provider and all workplaces registration authority PostSignum QCA. In the event that part of their activities is the termination of the authority of the certificate, must be part of this announcement, including the relevant reason for termination of validity. As long as at least one valid certificate issued by PostSignum Root QCA PostSignum Root QCA must provide at least the function of revocation of the certificate and CRL issuance.

PostSignum Root QCA, if this function is not able to ensure throughout the period of validity of the issued certificates, shall inform the subscriber of the relevant certificates, together with an indication of the date by when it will be delivered. This date can be the first 6 months of the date of sending the notification. To this date the PostSignum Root QCA invalidates all previously issued certificates are valid and will issue the last CRL. Only then can the activity of PostSignum Root QCA terminated.

In this case, the contract for the provision of certification services terminated by the ČP agreement or notice.

Subsequently, ČP demonstrably destroys private key of PostSignum Root QCA, which served for the sealing of certificates and certificate revocation lists, and about the destruction of records. Records shall be stored in accordance with the provisions of this certification policy described in Chapter 5.4.

5.8.2 Cessation of activities of a provider of certification services

The activities of a provider of certification services will be terminated in accordance with the applicable legislation. If after the termination of the activities of a provider of certification services will no longer be possible to provide access to the data that have been recorded due to the provision of certification services, and that could serve for the purposes of providing evidence in judicial and administrative proceedings and for the purpose of ensuring the continuity of services, so these data to the Manager of the CA of a supervisory authority.

5.8.3 Withdrawal of accreditation

In the event of the withdrawal of accreditation must be information on the withdrawal of the accreditation in writing or electronically communicated to all the subscribers of the relevant certificates and entities that have concluded a contract directly relating to the provision of certification services and published on website of the provider, in all workplaces registration authority PostSignum QCA and other ways listed in the current legislation. Part of the

information and the communication that will be qualified certificates issued by that provider cannot continue to use under the applicable legislation. In this case, management ČP will be decided on the basis of the relevant decision of the supervisory authority.

# 6 TECHNICAL SECURITY CONTROLS

## 6.1 Data generation and installation

Key pairs in the hierarchy of certification authorities PostSignum QCA are generated in the corresponding hardware module; the key pairs are generated in dedicated hardware resources, which its design does not permit the export of private keys.

### 6.1.1. Pair of generating data

Key pairs in the hierarchy of certification authorities PostSignum QCA are generated and stored in a hardware cryptographic module. To generate those key pairs is performed in a controlled process, in which progress is supervised by the Manager of the CA and CA Auditor.

Key pairs of individual components or systems of PostSignum QCA (infrastructure) are generated in a controlled environment systems of PostSignum QCA. These key pairs are stored in the cryptographic module; for access to these key pairs you must insert your smart card and type the PIN.

Key pairs of operators of PostSignum QCA (including RA; the control key) are generated in dedicated hardware resources, which its design does not permit the export of private keys. For the use of the private key is always necessary to enter the PIN.

### 6.1.2 Private key transfer applicant

Postsignum QCA does not provide service to generate the key pair for the certificate requester.

### 6.1.3 Public key Transmission providers of certification services

The public key of the certification services provider to requestor is delivered in electronic form, in a certificate request in PKCS#10 format.

### 6.1.4 CA public key Provision embraces the parties

CA certificates are published in the manner described in Chapter 2.

### 6.1.5. Length of the pair data

Certification authorities' keys in the PostSignum hierarchy have a pLen and qLen 512 bit for the ECDSA algorithm, specifically the P-521 curve (secp521r1).

### 6.1.6 Public key parameters generation and quality checking

Parameters used when creating the public key component of PostSignum QCA are generated by software and hardware equipment. The used algorithms and their parameters correspond to the requirements of applicable legal regulations or technical standards, which regulate the activities of certification service providers.

Quality parameters keys generated within PostSignum QCA is automatically tested used softwares.

6.1.7. Restrictions on the use of public keys

Public key subordinate CAs may be used only in accordance with the rules described in Chapter 1.4

6.2 Private key data protection and security of cryptographic modules

6.2.1 Standards for cryptographic modules, and terms of use

Cryptographic module used to generate and store the private key of certificate authorities (a tool for creating electronic seal) operating in the hierarchy of PostSignum meets the requirements of FIPS 140-2 Level 3 and Comon Criteria EAL 4+.

6.2.2 Sharing Secrets

The CA's private key is stored in the activated during operation and the configured cryptographic module (tool for creating electronic seals), which turn on and off, it is sufficient for one person.

To activate the cryptographic module (tools for creating electronic seals) and recover the private key after a crash (possibly in another cryptographic module) is needed for interoperability of several, at least three people. In the case of the solution to critical state, who does not tolerate delay, it is possible to recover the private key with the concurrence of two people.

6.2.3 Private key storage

The service require the storage of private keys PostSignum QCA does not provide.

6.2.4 Private key backup

The CA private key is backed up in encrypted form; to encrypt the symmetric AES algorithm is used. The encrypted keys are stored on the hard disk of the device that contains the cryptographic module. Backup these keys can one person; restored to the activated module from which the backup originated, also.

When you restore the backup of the keys to a new or initiated the need for interoperability of at least three people.

6.2.5 Storage of private keys

The private keys of certification authorities PostSignum hierarchy are not archived. After the closure of the CA are formally received destroyed.

6.2.6 Private key transfer into or from a cryptographic module a cryptographic module

The CA private key is generated in the cryptographic module (secure cryptographic module) and all clear key operations shall be carried out only in the module. Key leaves the cryptographic module in encrypted form only on the backups created and protected in accordance with the provisions of the documents the system security policy, operational and security procedures and Audit and archive policy (part of [SBP]).

The key is a cryptographic module is inserted into the original from backups after the authentication of a single worker with access to the advances and key to the cryptographic module.

The key is to a new or initiated by the cryptographic module is inserted from backups after the authentication of the two workers, in normal operation also in the presence of CA and CA Auditor Manager.

6.2.7 Private key storage on cryptographic module

The private key of the CA is stored during operation in plaintext form in activated and configured cryptographic module (secure cryptographic module), which turn on and off, it is sufficient for one person.

To activate the cryptographic module (secure cryptographic module) and recover the private key after a crash (possibly in another cryptographic module) is needed for interoperability of several, at least three people. In the case of the solution to critical state, who does not tolerate delay, it is possible to recover the private key with the concurrence of two people.

6.2.8. Procedure to activate a private key

The CA private key is activated by an authorized operator in accordance with a system security policy and the operational and security procedures. The PostSignum Root QCA activation is performed (except in the cases described in the plan of crisis management and recovery plan) solely in the context of the planned execution in the presence of CA and CA Auditor Manager who oversees the cryptographic module containing the the private key is activated until the time of deactivation.

6.2.9 Procedure to deactivate a private key

The private key of the CA is deactivated by an authorized operator in accordance with a system security policy and the operational and security procedures.

6.2.10 Repeat the procedure for the destruction of the private key

The CA's private key stored in the HSM module is destroyed the resources provided by the HSM module in the event of termination of the activities of CAs whose keys are stored in the HSM module. This private key destruction is carried out by an authorized service in accordance with the provisions of the system security policy document and document operational and safety procedures, or at the request of the Manager of CA.

The destruction of the private key is made indicating the HSM in the initialized state, when the use of the mechanisms of HSM securely erases all cryptographic material (including the private key of the CA). The destruction of the private key also includes deleting the backed-up copies of the keys and the deactivation of the cards to be used for access to the keys.

6.2.11 Cryptographic module rating

Due to the fact that the cryptographic module used for the custody of the CA's private key has passed evaluation by FIPS 140-2 level 3 and Common Criteria EAL 4+, it contains serious errors at the level of the design of the device. Nevertheless, continuously monitors whether the attack was discovered on this device, in order to respond to such threats in a timely manner.

6.3 Other aspects of pair data management

6.3.1 Public key storage

The public key in the form of certificates issued by PostSignum Root QCA authority are archived in accordance with the audit and archive policy.

6.3.2. Maximum validity time of the certificate issued to the applicant and paired data

The validity of the certificate issumed by the Postsignum Root QCA is given in the certificate and it is 15 years. The validity of the certificate issuined by the subordinate certification authority is staved in the certificate and is 10 years. Key pairs tied to certificates have the same validity time as certificates.

6.4 Activation data

In the system of PostSignum QCA are used the activation data of different nature, such as passwords, PIN and other. All aspects related to the activation data, generate, install and use, are described in the system security policy, operational and safety procedures and operational documentation.

6.4.1 Generating and installing activation data

Activation data are going mostly under construction or awarded by a worker who is going to be used. In the opposite case, when it generates the other body, they are used in the random data that meets the general conditions for this data and is defined by these randomly generated data can immediately change.

All generated by the activation data must complied with the requirements for their length or composition.

6.4.2 Activation data Protection

All activation data must be protected from disclosure to any unauthorised person. The relevant obligations in this sense, all the staff of PostSignum QCA and are listed in the system security policy.

6.4.3 Other aspects of activation data

Other aspects of activation data, their generation, installation and use are described in the system security policy, operational and safety procedures and operational documentation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

For each component in the hierarchy of PostSignum QCA are defined by setting the component's safe on the technological level, which are based on the requirements of the applicable legislation and related documents, and in particular of the standards [ETSI EN 319 401], [ETSI EN 319 411] and [CA/B].

6.5.2 Computer security rating

The system of PostSignum QCA passed after the construction of the external control of the conformity of safety-oriented to meet the requirements imposed by legislation on the qualified trust service providers, and in particular the requirements set out in [eIDAS].

6.6 Life-cycle safety

6.6.1 System development management

Implementation of the system was carried out according to the methodology of KeyStep that was created specially for the design and implementation of a large scale PKI projects. Development of partial applications took place in accordance with the internal development of the methodology of the Czech post.

Subsequent changes are implemented in accordance with a defined change management.

6.6.2 Security management controls

The safety systems of PostSignum QCA is validated operational controls were introduced in the framework of the established management system of information security in accordance with [ISO 27001], security compliance checks carried out by the staff of the Česká pošta, s.p. checks and external audits carried out by the external body.

6.6.3 Life cycle security management

Part of the change management is assessing the impact of changes on the safety solution. In the case of major changes or after a series of minor amendments to the differential is performed or repeated risk analysis.

6.7 Network security

Central systems of PostSignum Root QCA certification authorities that provide certificate issuance, not connected to any network.

6.8 Time-stamps

See section 5.5.5.

## 7 PROFILES OF CERTIFICATES, CERTIFICATE REVOCATION LIST AND OCSP

7.1 Certificate profile

Postsignum Root QCA issues certificates to x.509-compliant. Profiles of the certificate root and subordinate CAs are listed in the following tables.

Table 2 profile of the Root CA certificate

| Name of the item | Value/use flag |
|---|---|
| Version | 3 (0x2) |
| Serial Number | *Postsignum Root QCA assigns each a unique number issued by the certificate.* |
| The SignatureAlgorithm | ECDSA With SHA512 |
| The issuer | |
| (C) countryname | CZ |
| organizationIdentifier | NTRCZ-47114983 |
| About organisationName | Česká pošta, s.p. |
| CN commonName | Postsignum Root QCA ECC R1 |
| The validity of the | |
| Not Before | *The origin of the certificate's validity-UTCTime* |
| Not After | *The end of the certificate's validity-UTCTime* |
| Subject | |
| (C) countryname | CZ |
| organizationIdentifier | NTRCZ-47114983 |
| About organisationName | Česká pošta, s.p. |
| CN commonName | Postsignum Root QCA ECC R1 |
| Subject Public Key Info | |
| Algorithm | ECDSA |
| SubjectPublicKey | *The public key* |
| Extensions | *certificate extensions in accordance with table 4* |
| Signature | *electronic seal provider of certification services* |

Table 3 Subordinate CA certificate profile

| Name of the item | Value/use flag |
|---|---|
| Version | 3 (0x2) |
| Serial Number | *Postsignum Root QCA assigns each a unique number issued by the certificate.* |
| The SignatureAlgorithm | ECDSA With SHA512 |
| The issuer | |
| (C) countryname | CZ |
| organizationIdentifier | NTRCZ-47114983 |
| About organisationName | Česká pošta, s.p. |
| CN commonName | Postsignum Root QCA ECC R1 |
| The validity of the | |
| Not Before | *The origin of the certificate's validity-UTCTime* |
| Not After | *The end of the certificate's validity-UTCTime* |
| Subject | |
| (C) | CZ |

| | |
|---|---|
| countryname | |
| organizationIdentifier | NTRCZ-47114983 |
| About organisationName | Česká pošta, s.p. |
| CN commonName | *The name of the certification authority* |
| Subject Public Key Info | |
| Algorithm | ECDSA |
| SubjectPublicKey | *The public key* |
| Extensions | *certificate extensions from table 5* |
| Signature | *electronic seal provider of certification services* |

### 7.1.1 Version number

Postsignum Root QCA issues certificates to compliant x.509 version 3.

### 7.1.2 Extension items in a certificate

Expansion items used in the certificate of the root and subordinate CAs are listed in the following tables.

Table 4 Extensions in the Root CA certificate

| **The name of the expanding items** | **Value/use flag** | **Critical yes/no** |
|---|---|---|
| Authority Key Identifier | | No |
| Key Identifier | *It is used* | |
| Subject Key Identifier | *It is used* | No |
| Key Usage | | Yes |
| DigitalSignature | No | |
| NonRepudiation | No | |
| Keyencipherment | No | |
| Dataencipherment | No | |
| KeyAgreement | No | |
| KeyCertSign | Yes | |
| CRLSign | Yes | |
| Basic Constraints | | Yes |
| CA | TRUE | |

Table 5 Extensions in the certificate of the subordinate certification authority

| **The name of the expanding items** | **Value/use flag** | **Critical yes/no** |
|---|---|---|
| Authority Key Identifier | | No |
| Key Identifier | *It is used* | |
| Subject Key Identifier | *It is used* | No |
| Key Usage | | Yes |
| DigitalSignature | No | |
| NonRepudiation | No | |
| Keyencipherment | No | |

| | | |
|---|---|---|
| Dataencipherment | No | |
| KeyAgreement | No | |
| KeyCertSign | Yes | |
| CRLSign | Yes | |
| Extended Key Usage | *The subordinate CA certificate shows the following purposes always depending on what types of certificates a particular subordinate CA issues.*id-ms-kp-document-signing, id-kp-emailProtection, id-kp clientAuth id-kp-serverAuth, id-kp-timeStamping | No |
| CertificatePolicies | | No |
| Policy Identifier | 2.5.29.32.0 (Any) | |
| User Notice | This is a certificate for electronic seal according to Regulation (EU) No 910/2014. | |
| CRL Distribution Points | | No |
| The URI of the | http://crl.postsignum.cz/crl/psrooteccr1.crl | |
| The URI of the | http://crl2.postsignum.cz/crl/psrooteccr1.crl | |
| The URI of the | http://crl.postsignum.eu/crl/psrooteccr1.crl | |
| Basic Constraints | | Yes |
| CA | TRUE | |
| PathLenConstraint | 0 | |
| AuthorityInfoAccess | | |
| AccessMethod | id-ad-caIssuers (1.3.6.1.5.5.7.48.2) | |
| The URI of the | http://crt.postsignum.cz/crt/psrooteccr1.crt | |
| AccessMethod | id-ad-caIssuers (1.3.6.1.5.5.7.48.1) | |
| The URI of the | http://ocsp.postsignum.cz/OCSP/RQCAECCR1/ | |

Notes:

- Some of the items of the certificate does not contain diacritics because of better legibility of particulars in the certificate in the different systems.

7.1.3 Object identifiers ("OID") algorithms

Algorithms used in PostSignum QCA are not assigned an OID. In the hierarchy of PostSignum QCA is not using specific algorithms that would be developed by the operator of PostSignum QCA or his supplier, but only the algorithms conforming to the requirements of applicable legal regulations and technical standards, which regulate the activity of certification service providers.

7.1.4 Methods of registration of names and names

The rules for the registration of names, and the names are listed in paragraphs 3.1.1 to 3.1.4.

7.1.5 Name constraints

No "Name Constraints" restrictions are applied.

7.1.6 Certificate policy OID

In the issued certificate for the subordinate certification authority is in accordance with [RFC5280] set out a special policy anyPolicy with the markings OIDS 2.5.29.32.0

The OID of this policy (of the document) provided in paragraph 1.2 (Tab. 1)

7.1.7 Expansion entry "Policy Constraints"

Expanding the entry "Policy Constraints" in PostSignum QCA does not use.

7.1.8 Syntax and semantics policy qualifiers expansion items "Policy Qualifiers"

Expanding the entry "Policy Qualifier" contains in the form of User Notice that the certificate was issued as a certificate for electronic seal referred to in [eIDAS].

7.1.9 Method of enrollment critical expansion "Certificate Policies"

How to write an extension item "Certificate Policies" is shown in table 4 and 5. This item is not marked as critical.

7.2 Profile of Certificate revocation list

Table 6 CRL Profile

| **Name of the item** | **Value/use flag** |
|---|---|
| Version | 2 (0x1) |
| The Issuer Distinguished Name | |
| (C)<br>countryname | CZ |
| organizationIdentifier | NTRCZ-47114983 |
| About<br>organisationName | Česká pošta, s.p. |
| CN<br>commonName | Postsignum Root QCA ECC R1 |
| The validity of the | |
| This Update | *Release date* |
| Next Update | *Release date + 12 months* |
| RevokedCertificates | *repeating entry for each revoked certificate* |
| UserCertificate | *the serial number of the revoked certificate* |
| RevocationDate | *date and time of revocation* |
| CrlEntryExtensions | *CRL entry extensions according to table 7* |
| CrlExtensions | *CRL extensions according to table 7* |
| The SignatureAlgorithm | ECDSA With SHA512 |
| Signature | *electronic seal provider of certification services* |

7.2.1 Version number

Postsignum Root QCA publishes certificate revocation lists in accordance with the x.509 standard, version 2.

7.2.2. Expansion of the certificate revocation list items and records in a certificate revocation list

Table 7 extensions in CRLS

| **The name of the expanding items** | **Value/use flag** | **Critical yes/no** |
|---|---|---|
| Item extension (CrlEntryExtensions) | | |
| InvalidityDate | *date and time of occurrence of the event leading to the revocation of the certificate; Optional extensions* | No |

| | | |
|---|---|---|
| ReasonCode | *the reason for the revocation of the certificate* | No |
| Extensions for CRLS (CrlExtensions) | | |
| Authority Key Identifier | | No |
| Key Identifier | *It is used* | |
| CRL Number | *Postsignum Root QCA assigns a unique number to each CRL* | No |

## 7.3 OCSP Profile

The OCSP is in line with RFC 6960.

Structure of OCSP request - OCSP Request Data

| Item name | Description | Value/use flag |
|---|---|---|
| Version | OCSP version (required item) | 1 |
| Requestor List | | |
| Certificate ID | Certificate data - Item may be repeated | |
| Hash Algorithm | hash of the request | SHA-1 |
| Issuer Name Hash | hash calculated from the name of the issuer of the certificate | |
| Issuer Key Hash | hash calculated from the print of the issuer of the certificate | |
| Serial Number | serial number of the certificate | |
| Request Extensions | | |
| OCSP Nonce | Random once generated number (64 bits). If it is included in the application, it also contains an answer. (optional item) | |

OCSP request may not be signed.

Structure of OCSP response - OCSP Response data

| Item name | Description | Value/use flag |
|---|---|---|
| OCSP Response Status | Number indicating the state of response | 0 – successful<br>1 – malformedRequest<br>2 – internalError<br>3 – tryLater<br>6 – unauthorized |
| Response Type | Basic OCSP Response | |
| Version | Protocol OCSP version | 1 |
| Responder Id | DN Signature Certificate OCSP Server | |
| Produced At | Signature time OCSP server response | |
| Responses: | | |
| Certificate ID | Data correspond to the data in the application | |
| Cert Status | Certificate status<br>good – certificate is valid<br>revoked – certificate is revoked<br>unknown - certificate is unknown (eg. Certificate do not exist) | 0 – good<br>1 – revoked<br>2 – unknown |

| | | |
|---|---|---|
| Revocation Time | Certificate revocation time. The item is listed only in the case of Cert Status = Revoked | |
| Revocation Reason | Reason for revocation of the certificate. The item is listed only in the case of Cert Status = Revoked | |
| This Update | The time from which the state of response is indicated. | |
| Response Extensions | | |
| OCSP Nonce | Random once generated number (64 bits). If it is included in the application, it also contains an answer. (optional item) | |

7.3.1 Version number

The OCSP version number is 1.

7.3.2 OCSP expansion items

The extension in the request and OCSP response is shown in the tables in chapter 7.3.

## 8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Periodicity of evaluation or circumstances for evaluating

In PostSignum QCA, checks are regularly carried out at least once a year. Controlled periods always follow themselves. In addition to these internal controls are performed by the external audit according to the legislation in force. These regular checks can be added as needed by reviewing, inter alia, on the basis of the decision of the Manager of the CA, the Czech post management or internal audit of the Czech post.

8.2 Evaluator identity and qualifications

The internal inspection is carried out by the knowledgeable employees of the PKI and training for the task. The inspection workers are referred to as CA auditors in QCA documentation.

Only an accredited person or a company knowing the issue of PKI implementation with sufficient qualifications in this area may be an external auditor.

8.3 Relation of the evaluator to the evaluated entity

Internal control is carried out by employees of Česká Pošta, s. p.

External control may be performed only by a person or a company independent of the Česká Pošta, s. p.

8.4 Evaluated areas

The area-rated within the regular checks are specified in the current legislation and the relevant standards.

8.5 Procedures applied to discovered defects

The results of the checks are passed, the Manager for the CA to ensure remedy any identified deficiencies.

In case of detection of deficiencies, which seriously affect the PostSignum QCA's ability to meet its obligations and requirements specified in the current legislation, it aborts the PostSignum QCA issue certificates until they are remedied.

8.6 Sharing evaluation result

For the execution of each control is drawn up, signed the written report, which is forwarded to the Manager of CA. The ensure its distribution and consultation. If necessary, the manager shall ensure that the CA message is passed to the supervisory authority the term determined in the applicable legislation.

In the case where the message is included in the separate opinion of the Auditor, the Manager can decide on its publication of CA.

The audit company publishes the inspection report on its website.

## 9 OTHER BUSINESS AND LEGAL ISSUES

9.1 Fees

9.1.1 Fees for the issue or renewal of the certificate

The operator of all CAs in the hierarchy of PostSignum QCA is the Czech post, fees for issuing certificates to subordinate CAs.

9.1.2 Fees for access to the certificate to the list of issued certificates

Service access to the certificate to the list of issued certificates is provided free of charge.

9.1.3 Fees for information about the status of the certificate or the certificate revocation

Service of certificate revocation and certificate status information are provided free of charge.

9.1.4 Fees for other services

The operator of all CAs in the hierarchy of PostSignum QCA is the Czech post, charges for other services billed.

9.1.5 Any other provisions relating to fees (including reimbursements)

See paragraph 9.1.1.

9.2 Financial responsibility

9.2.1 Cover insurance

The Czech post has concluded liability insurance in such a way to cover any possible damage.

9.2.2 Other assets and guarantees

The assets of the Czech post are listed in the annual report. The annual report is stored in the commercial register at the municipal court in Prague under the brand A7565.

The annual report is also available for viewing on the website of the Czech post (www.ceskaposta.cz).

9.2.3 Insurance or warranty coverage for end users

Postsignum QCA this service does not provide.

9.3 Confidentiality of business information

The operator of all CAs in the hierarchy of PostSignum QCA is the Czech post. In the field of the protection of business information to apply the provisions of the General internal regulations the ČP relating to the classification and protection of information.

9.3.1. List of sensitive information

Are considered as confidential all information, except for information contained in documents marked with "information intended for the general public".

9.3.2 Information outside of sensitive information

Confidential information shall not be considered classified and labelled as "information intended for the general public".

9.3.3 Responsibility for protection of sensitive information

Responsibility for handling confidential information in PostSignum QCA carries the Czech post, as a provider of certification services, all its employees and contractors.

9.4 Privacy of personal information

Česká pošta ensures the protection of personal data of persons to whom it obtains access during the provision of certification services. The principles of personal data protection are contained in the General Terms and Conditions of Certification Services and are based on the GDPR.

9.4.1 Personal data

Personal data are treated as information that fall under the protection of [Z110]. In particular all the information relating to identified or identifiable natural person (an employee of ČP).

9.4.2 Responsibility for the protection of personal data

Responsibility for the protection of personal data processed in systems of PostSignum QCA carries the Czech post, as a provider of certification services, all its employees and contractors are in the range of [GDPR].

9.4.3 Provision of personal data

In this area it is proceeded according to the respective establishment of [GDPR], generally binding legal regulations and the internal regulations of Česká Pošta, governing the protection of personal data.

9.5 Intellectual property rights

This certification policy and all related documents are protected by copyright of the Czech post and presenting a significant know-how of the Czech post. Czech post is also the subscriber of the exclusive rights to the information system for the operation of PostSignum QCA and the structure, organization, looks to screens and Web content providers.

Distribution and reproduction of this document only in its entirety is permitted.

9.6 Representation and warranties of the participants

Česká pošta guarantees that it will fulfill all obligations imposed by this certification policy and the mandatory provisions of the relevant legal regulations and standards.The Czech post provides the above warranty throughout the period of validity of the contract for the provision of certification services.

9.6.1 Representation and CA warranties

See the provisions of paragraph 9.6.

9.6.2 Representation and RA warranties

See the provisions of paragraph 9.6.

9.6.3 Representation and warranties of the certificate subscriber, signing or indicating person

See the provisions of paragraph 9.6.

9.6.4 Representation and relying party guarantee

The relying party shall be liable for the fulfillment of all the obligations that are imposed on the relying party prior to use of a certificate. These obligations are listed in this certificate policy, especially in paragraph 4.5.2.

9.6.5 Representation and warranties of other participating entities

See the provisions of paragraph 9.6.

9.7 Disclaimers of gauranties/warranties

The guarantee referred to in article 9.6 above are exclusive guarantees the Czech post and the Czech Post Office does not provide other guarantees.

Czech post is not liable for defects resulting from the services provided due to improper or unauthorized use of the services, in particular for the operation in accordance with the conditions

set out in this certificate policy, as well as for defects arising due to force majeure, including temporary failure of telecommunications links, etc.

9.8 Limitations of liability

Czech post is not liable for damage resulting from the use of a certificate, if there is on the part of the person relying to comply with restrictions on its use, referred to in this certificate policy, and published on the website of the provider.

Czech post will be kept as operating experience with the provision of certification services to verify whether the conditions of the limitation of liability of the Czech post referred to in that provision correspond to normal market conditions and reasonable business risk of the Czech the post office.

The provisions of this article shall remain in force even after the termination of this certificate policy.

9.9 Indemnities

If it is not apparent from the mandatory provisions of applicable law otherwise, corresponds to the Czech post the relying party for harm caused by the violation of the obligations of the Czech post in connection with the provision of certification services.

9.10 Term and termination

9.10.1 Validity period

The period of validity of this certificate policy is from the issue date referred to in paragraph 1.2 until further notice.

9.10.2 Termination

The validity of the document is terminated in case of

- replacing it with a newer version, or
- the termination of the provision of services the Czech post, s. p. as a provider of certification services.

9.10.3. Consequences of termination and continuation of the obligations

In the event of termination of this document as a result of the termination of the provision of services shall remain in force limitations and provisions set out in Chapter 9, which relate to the business and Legal Affairs.

9.11 Individual notices and communications with participants

9.11.1 Communication with the provider of certification services

All the information which it wishes to communicate to the provider of certification services embraces the Parties shall publish on its website and on message boards in workplaces RA. Relevant information, such as a suspected key being compromised some of the hierarchy of

certification authorities PostSignum certification services provider, says again on the website and the ways described in paragraph 2.2.

9.11.2 Communications within the system of PostSignum QCA

Communication in the system of PostSignum QCA is governed by applicable provisions of the Czech post and the internal documents of the task of PostSignum QCA.

9.11.3 Communication language

All communication in the system of PostSignum QCA must be in Czech language, unless both parties agree otherwise.

9.12 Amendments

9.12.1 Procedure for amendments

Procedures for the incorporation of the changes are listed in the paragraph. 1.5.

9.12.2. Procedure for notification of changes

Issue of a new certificate policy OID is changed (see following chapter) will be announced in the news on the website of the provider.

In the case of identification of a weakening of guarantees provided by the used cryptographic algorithms that require urgent intervention in writing or electronically will be notified to all the

subscribers of the certificates, the supervisory authority and the entities that have concluded a contract directly related to the provision of certification services. The notice will also be published on the website of the provider, in all workplaces by the registration authority of PostSignum QCA. On this announcement may establish additional actions that are described in this certificate policy.

9.12.3 Circumstances in which OID must be changed

Česká pošta, s.p. has assigned according to their internal rules, object identifiers (OIDs) used in the environment of PostSignum QCA.

OIDS are assigned:

- Postsignum Root QCA,
- each certification authority PostSignum Root QCA, which issued the certificate, in particular certification authority PostSignum Qualified CA,
- each certification policy, under which are issued certificates within PostSignum QCA.

OIDS are not assigned registration or certification authorities (CAs) practice statement.

Only a major change in the certification policy will trigger a document version change at the x.X level as well as an OID change. Minor changes, possibly revisions without changes cause the document to be versioned at the x.x.X level, leaving the OID unchanged.

9.13 Dispute resolution provisions

In the event of a dispute between the operator of PostSignum Root QCA and the subordinate CA (by the applicant) it is possible to contact the parent CA personnel Manager.

9.14 Governing law

Operation of PostSignum QCA is governed by the laws of the Czech Republic.

9.15 Compliance with applicable law

Operation of PostSignum QCA is in accordance with the applicable legislation of the Czech Republic.

The structure of this certificate policy is in accordance with the structure set out in RFC 3647.

9.16 Other provisions

9.16.1 Framework agreement

No provisions in this paragraph.

9.16.2 Cession of rights

Czech Post Office may delegate part or all of the obligations of the certification services provider to another legal entity, which is to ensure the same level of safety as well as of the services provided. Relations between the Czech post and the body will be regulated by a special agreement.

In the case of termination of the activities of a qualified certification services provider will use the Czech post reasonable efforts for taking over the management of existing qualified certificates and related agenda by another qualified provider of certification services. In this case, the relations between the certification services provider and qualified the Czech post also adjusted the special agreement.

Takeover of part or all of the obligations of the provider of certification services by a third party does not restrict services or guarantees given by the Czech post due to customers and embraces the parties.

9.16.3 Severability of provisions

Contract for the provision of certification services concluded between the customer and the Czech post remains valid even in the event that any part of the void, unless both parties agree otherwise.

9.16.4 Disclaimer

No provisions in this paragraph.

9.16.5 Majeure

The Czech post shall not be liable for breach of its obligations due to force majeure, interventions such as a natural disaster of great magnitude, strikes, civil unrest, or a State of war.

9.16.6 Accessibility for people with disabilities

The trust services provided and the end-user products used in providing those services are accessible to persons with disabilities. More detailed information regarding the provision of services to these persons will be provided by the registration authorities or Customer Support. Contact details are listed on the provider's website www.postsignum.cz.9.17 Other measures

9.17.1 Management documents

When creating certificate policies and certification practice statement was taken into account, in particular, the following documents:

[CA/B] CA/Browser Forum - Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates

[eIDAS] REGULATION of the EUROPEAN PARLIAMENT and of the Council (EU) No. 910/2014 of 23 December 2003. July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

[ETSI EN 319 401] Electronic Signatures and Infrastructures ' (ESI); General Policy Requirements for Trust Service Providers

[ETSI EN 319 411] Electronic Signatures and Infrastructures ' (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1-3

[ETSI EN 319 412] Electronic Signatures and Infrastructures ' (ESI); Certificate Profiles; Part 1-5

[ETSI EN 119 312] Electronic Signatures and Infrastructures ' (ESI); Cryptographic Suites

[GDPR] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[ISO 27001] ISO/IEC 27001:2006 information technology-security techniques-Information Security Management Systems — requirements

[RFC 6960] Internet x.509 Internet Public Key Infrastructure Online Certificate Status Protocol-OCSP

[RFC 5280] Internet x.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[RFC 3647] Internet x.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

[ZoSVD] Act 297/2016 Coll., on trust services for electronic transactions, as amended

9.17.2 Links and literature

[VOP] General terms and conditions of certification services.