PostSignum CA Certificate Policy for Commercial TLS certificates (Algorithm ECC)

Version 1.0.0

TABLE OF CONTENTS

1 INTRODUCTION

This document defines rules and procedures for issuing commercial certificates for TLS. The authorized person of the organization (or the customer in the case of an entrepreneurial natural person) determines which person may apply for the certificate.

1.1 Overview

Česká pošta, s.p. (hereinafter referred to as the Czech Post or ČP) operates a certification authority called PostSignum VCA, which has the following hierarchy:

Root CA name: PostSignum Root QCA ECC R1	SHA-256 fingerprint: 2D41D6D54CF9C81B0725E963C351F192D46581C8989C96C565695F6C8FC6EA67	Valid to: 29. 6. 2038
Root CA name: PostSignum Public ECC R1 CA 2	SHA-256 fingerprint: 55A4BDBECE70E0DD4FCC45436BE1FCFD4A8FED97613E8BE7FA85454F90E58F99	Valid to: 30. 1. 2034

When issuing certificates to end-users, the customer pre-registration model is applied in order to minimize participation of the statutory representative of the particular organization during the entire process, and to require minimum number of documents from person applying for certificates.

A customer who is interested in PostSignum VCA services will conclude an agreement with the Czech Post on the provision of the certification services. The contract specifies the so-called authorized person who, on behalf of the customer, determine which applicants can be issued certificates according to individual certification policies. These applicants are entered into the system of the certification authority and then apply for a certificate at the registration authority of the Czech Post.

The Czech Post may agree with the customer on the special conditions of the registration process or the creation of a new certification policy.

Public key of commercial certificates issued under this certification policy are intended for person who are the customer or in a particular relationship with the customer who concludes a certificate service agreement with the Czech Post. Person who submit for and use certificates issued under this policy will be called the Certificate Applicant. The subscriber of certificate is the customer of the Czech Post.

The customer is responsible for the personal data and the data that is provided in the certificate issued under this certification policy. The certification service provider verifies the compliance between the customer and the public key in the certificate.

Certificates issued under this certification policy can be used for authentication, server authentication, and client authentication.

Fulfilment of requirements specified in this policy are established and enforced by the Certification Practice Statement PostSignum VCA.

1.2 Document Name and Identification

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 apply.

Tab 1. Policy identification

Document name	PostSignum CA Certification Policy for Commercial TLS certificates (ECC)
Document version	1.0.0
Status	draft
OID of the provider of certification services	2.23.134
OID PostSignum Root QCA	2.23.134.1.4.2.1
OID PostSignum Public CA	2.23.134.1.2.2.3
OID of this policy	2.23.134.1.2.1.19.100
Release Date	7. 5. 2024
Effective Date	
Revision Date	
Term of validity	Until further notice or until the date of termination of the services of the PostSignum VCA authorities.

1.2.1 Revise a document

The document is revised at least once a year.

Version	Date of Release	Comments	Author	Approved by
1.0	7. 5. 2024	Draft version	PCA ČP	

1.3 PKI Participants

Subordinate certification authorities may be controlled and operated only by the Czech Post (except for registration authorities – see further below)

Identification and contact data of the provider of certification services are:

Česká pošta, s.p. (Czech Post)

ID reg. No.: 47114983, VAT: CZ47114983

Politických vězňů 909/4, 225 99, Prague 1

Phone: 954 301 111

e-mail: info@cpost.cz

1.3.1 Certification authority (hereinafter referred to as "CA")

The task of CA PostSignum VCA is primarily to issue and manage certificates of PostSignum Public CA and customers of the Czech Post in accordance with defined certification policies.

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

1.3.2 Registration Authorities (hereinafter referred to as "RA")

Registration authority services are provided only by the certification service provider Czech Post.

Registration authorities mostly provide the following services:

- they accept (register) applications for certificate and approve or reject these applications pursuant to valid certification policies,
- they verify identities of applicants for a certificate,
- they make sure that the issued certificate is handed over to the applicant,
- they revoke certificates based on valid certification policies.

Contact information of registration authorities of the Czech Post are available at the webpage of the provider.

1.3.3 Subscribers

Subscriber of commercial certificates who have applied for a commercial certificate (hereinafter referred to as the certificate) and to whom the certificate has been issued

1.3.4 Relying parties

A relying party is any subject relying on the certificate issued by PostSignum VCA. Relying parties do not enter into a contractual relationship with the provider of certification services.

1.3.5 Other participants

The PostSignum VCA certification authority can use external entities to ensure the provision of services.

1.4 Certificate Usage

1.4.1 Appropriate certificate uses

Commercial certificates issued under this certification policy can be used for authentication, server authentication, and client authentication. Prohibited certificate uses.

1.4.2 Certificate usage restrictions

Commercial certificates issued pursuant to this certification policy are not primarily issued for communications or transactions occurring in areas with increased risk of health or property damages, such as chemical operations, air transportation, nuclear facilities etc., or operations related to national security. The Czech Post is ready to discuss with the customer special conditions for providing certification services in the above specified commercial segments.

Commercial certificates issued under this certification policy may only be used for proper and legal purposes and in accordance with applicable law.

1.5 Policy administration

1.5.1 Organization administering the document

The provider of certification services, that is the Czech Post Office, in particular the CA Manager, is responsible for administration of this certification policy.

1.5.2 Contact person

Contact person for certification policy administration is the CA Manager. Additional information may be obtained at the following email address

manager.postsignum@cpost.cz

or at the webpage of the provider.

Report of possible compromise of the private key or other possible misuse of the certificate or other types of fraud can also be reported to the above e-mail address.

1.5.3 Person determining CPS suitability for the policy

The CA Manager is responsible for managing this certification policy, who also decides on the compliance of procedures with the procedures of other certification service providers.

1.5.4 CPS approval procedures referred to in 1.5.3

This document is created by the team for the creation of certification policies of čp, which is established by the Commission for Certification Policies of ČP as necessary, it is managed and controlled by it.

The CA manager submits the developed policy for approval to the Certification Policy Commission, which confirms the OID policy and assigns a version number.

1.6 Definitions and Acronyms

CAA - CAA record indicates the authorization to issue an TLS certificate by a specific certification authority.

CDP (CRL Distribution Point) – URL address specified on the certificate, where the current CRL may be downloaded.

Certificate for electronic seal – certificate for legal person pursuant to [eIDAS].

Coordinated Universal Time (UTC) – Coordinated world time, a time standard based on International atomic time (TAI).

CRL (Certificate Revocation List) – list of revoked certificates. It contains certificates which can no longer be considered valid, for example due to a disclosure of a private key of the relevant subject. CRL is digitally signed by the issuer of certificates – certification authority.

DMZ – demilitarized zone

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

Certificate subscriber – customer since the moment of the certificate issuance.

Policy Approval Authority – PAA – a body authorized to approve, monitor and maintain certification policies and certification Practice Statement, which govern activities of a certification authority.

Public management contact point – Czech Post branch offering selected services to clients.

Qualified certificate – qualified certificate pursuant to [eIDAS].

Qualified electronic time stamp – a qualified electronic time stamp within the meaning of [eIDAS], in the text can also be called as a qualified time stamp or just a time stamp.

CA Manager – a person responsible for operation of PostSignum QCA and PostSignum VCA.

Mobile registration authority – mobile workstation of the Czech Post whose main task is to accept applications for a certificate or to revoke certificates, to inspect identity of applicants and reject or accept applications and to handover the issued certificate to the applicant, or to revoke a certificate.

Subsequent certificate – certificate issued based on a concluded contract as a replacement for already issued PostSignum certificate; the relevant certification policy specifies what data from the original certificate may be changed in the follow-up certificate. To issue a follow-up certificate no physical visit of the registration authority is necessary.

Business point – the central regional branch office providing certification and contract registration services.

Verification registration authority – provides selected registration authority services.

Online Certificate Status Protocol (OCSP) – protocol used to determine online status (revocation) of a certificate.

Imprint – a unique data chain of constant length, which is calculated from any input data; it only represents input data, which means that there are no two identical imprints for two different messages.

Pair data (key pair) – they are the primitive (essential data) of asymmetric cryptography. They are made of a private and public key. In terms of confidentiality the most important requirement is to protect their generation/creation and private key.

PKI – Public Key Infrastructure – infrastructure of public keys

Applicable legislation – 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 the REGULATION of the EUROPEAN PARLIAMENT and of the Council (EU) No 910/2014 from 23 July. July 2014 of electronic identification and services creating trust for electronic transactions in the internal market and on the repeal of Directive 1999/93/EC, including the related legislation.

Signatory – a person defined in [eIDAS].

PostSignum – a hierarchy of certification authorities and timestamp authorities consisting of a root certification authority PostSignum Root QCA, of all subordinate certification authorities for which PostSignum Root QCA issued a certificate, and timestamp authorities, for which any PostSignum certification authority issued a certificate for electronic seal.

PostSignum QCA – a hierarchy of certification authorities, issuing qualified certificates pursuant to [eIDAS].

PostSignum VCA – a hierarchy of certification authorities, issuing commercial certificates.

PostSignum Root QCA – a root certification authority which possesses a self-signed certificate for electronic seal. It issues certificates for electronic seal for subordinate certification authorities and CRL. Within the PostSignum hierarchy there may be other root certification authorities which are marked with a sequence number, for example PostSignum Root QCA 2.

PostSignum Qualified CA – certification authority which possesses certificate for electronic seal signed by root certification authority PostSignum Root QCA. It issues qualified certificates for subject which are not certification authorities. Within the PostSignum QCA hierarchy there may be other subordinate certification authorities which are marked with a sequence number, for example PostSignum Qualified CA 2.

PostSignum Public CA – certification authority which possesses certificate for electronic seal signed by root certification authority PostSignum Root QCA. It issues commercial certificates for subject which are not certification authorities. Within the PostSignum PCA hierarchy there may be other subordinate certification authorities which are marked with a sequence number, for example PostSignum Public CA 2.

PostSignum TSA – authority issuing qualified electronic time stamps pursuant to [eIDAS]. This authority consists of several units (TSU). Each unit has its own key and qualified certificate for electronic seal.

Authorized person – a person who represents a customer before the certification authority. Authorized person must be listed in the contract concluded between the Czech Post and the customer, or the contract may specify that it is a customer itself.

Registration authority – a workstation whose main task is to accept applications for a certificate or to revoke certificates, to inspect identity of applicants and reject or accept applications and to handover the issued certificate to the applicant, or to revoke this certificate.

Distinguishing name – it uniquely identifies the signatory indicating a person according to rules defined in the relevant certification policy.

Secure bug Bugzilla – system for reporting incidents related to the issuance of TLS certificates.

- Serious vulnerabilities include critical software and web application vulnerabilities, faulty APIs that could lead to data breaches, zero-day exploits, and malware infections.

Security Incidents include the following:

Successful unauthorized accesses, acquisitions, disclosures, or thefts of sensitive data or CA equipment involving the CA's systems, infrastructure, networks, applications, or sensitive information (private keys, user credentials, or personally identifiable information).

Ransomware attacks, or other data integrity issues that irrecoverably damage or compromise sensitive CA data.

Confirmed advanced persistent threats that attempt to compromise the CA's infrastructure, systems, or the reliability or validity of certificates.

https://wiki.mozilla.org/CA/Vulnerability_Disclosure#How_to_Disclose_a_Reportable_Vulnerability

Private key – a summary designation of data for creating an electronic signature, data for creating electronic seals, data for encryption and decryption, and data for authentication.

Policy Creation Authority – (PCA) – a team which creates policies and presents them before the Committee for certification policies for approval. PCA is established by the Committee or certification policies which manages and controls its activities.

TXT DNS record - it is used to verify domain ownership when issuing an TLS certificate as one of the verification methods.

Certificate user (relying party) – a person using a certificate issued by PostSignum, for example for verification of electronic signatures, seals or to ensure other security services. Also referred to as a Person relying on a certificate.

Public key – a collective term specifying data which are used to verify an electronic signature, data necessary for verification of electronic seals and data for encryption and authentication.

Provider's website – https://www.postsignum.cz – website of a provider offering PostSignum services.

Customer – a natural person performing business activities, legal person, state or local government body. Concludes a contract with the Czech Post describing provision of certification services.

Employee – a person sharing employment relation or any other relation with the customer for which the customer approved issuance of the relevant certificate pursuant to this certification policy.

Applicant – a person allowed to request PostSignum to issue a certificate according to applicable and valid certification policies. In addition, it also represents a collective term referring to signatory a indicating a natural person.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

Individual document and information storage devices operated by the Czech Post, which is also responsible for the management and operation - as the provider of certification services.

The Czech Post as the provider of certification services is responsible for publishing the relevant information.

This document is available on the provider's website:

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

2.2 Publication of information

Issued certificates are stored in the database of the CA.

Information about issued certificates, about the operation of PostSignum VCA and documentation PostSignum VCA is published in the scope below.

The structure of this certification policy is consistent with the structure specified in RFC 3647.The PostSignum certification authority confirms that this certification policy is in accordance with the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates [CA/B] published on the https://www.cabforum.org. If there is a conflict between this certification policy and [CA/B], the provisions of [CA/B] shall apply.

2.2.1 Certificate and CRL publishing

Certificates of certification authorities are published

- at the website of the provider.

  www.postsignum.cz, or

  www.postsignum.eu

Certificates issued for end-users (and information related to them) which are approved by the customer (certificate subscriber) for publishing, are published

- at the website of the provider.

Information about revoked certificates are published in a form of a list of revoked certificates (CRL)

- at the website of provider, or
- at distribution points/locations in the list of revoked certificates specified on the issued certificate (CDP).

2.2.2 Publishing information about certification authority

Certification policies, Certification Practice Statement, user reports, audit reports and possibly other documents are published on the:

- the Provider's website.

Additional important information, (for example revocation of certificate certification authority) or information about emergency events are published

- at the website of provider,
- at branch offices and registration authorities in a form of a posted text messages,
- in a nationally distributed daily newspaper

2.2.3 Test websites

The following domain certificate statuses are available on this website for testing:

- Valid: https://demo.postsignum.eu:8443/
- Expired: https://demo.postsignum.eu:8444/
- Revoked: https://demo.postsignum.eu:8445/

2.3 Time or frequency of publication

Information is published in the following intervals:

- certification policies, certification Practice Statement and user reports shall be revised at least once a year and published after the approval and release of a new version. The versioning of the document is governed by Chapter 9.12.3.
- certificates, if they have been marked for publication, shall be published electronically no later than 24 hours after receipt of the certificate;
- information on revoked certificates in the form of a list of revoked certificates (CRLs) shall be published immediately after their issuance, but no later than before the expiry of the last published list of revoked certificates.
- relevant information shall be published without delay.

2.4 Access controls on repositories

Certification policies (if intended for publication), CA certificates and certificate revocation lists, and other important information are readable without any restriction.

Pre-certificates are always published, but the applicant can choose whether the certificate will be published on the provider's website.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of name

The name of the subject is created using X.501 standard or rather the follow-up standard X.520.

It must comply with [CA/B] and RFC5280.

Neither the certificate name (CN) nor the Subject Alternative Name entry can contain an IP address or a local domain name (e.g. local).

Domain IDNs are not allowed.

3.1.2 Need for names to be meaningful

Importance of information used in attributes of the subject's certificate and in certificate extensions is described in Chapter 7.

3.1.3 Anonymity or pseudonymity of subscribers

PostSignum Public CA does not support the pseudonym of the certificate requestor or the customer in the Subject item of the certificate.

3.1.4 Rules for interpreting various name forms

The data specified in a certificate application PostSignum Public CA support only the following sets of characters:

- UTF8, Central European set of characters,
- US ASCII.

All data documented by an authorized person or the customer himself during the pre-registration of a certificate application are transferred to the certificates issued by PostSignum Public CA and to the certificate applications in the form in which they are specified in the submitted documents. Transcription, such as the removal of diacritics, is not possible.

3.1.5 Uniqueness of names

Each customer in the certification authority system is assigned a unique identifier, which is stored in the "serialNumber" data in the Subject of the certificate.

The Subject item of the certificate contains a combination of unambiguous customer data (customer ID and customer name) and a unique distinguishing name.

3.1.6 Trademarks

All certificate fields verified by PostSignum VCA must follow the prescribed structure and their correctness and completeness must be demonstrated (see provisions specified in chapter 3.2.3).

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

The applicant for a certificate presents the registration authority with an electronic application in PKCS#10 format, which contains a public key and is signed by a private key corresponding with the public key specified in the application. This guarantees that the applicant for a certificate possessed during the creation of his application a private key corresponding with the public key specified on the application.

3.2.2 Authentication of organization identity

The following provisions also apply to natural person who have been assigned with identification numbers and act as customers.

A customer who is concluding a contract describing provision of certification services demonstrates his identity using a common method accepted in regular trade or business circles. The customer shall use an adequate method to demonstrate its authorization to use the name of the organization which will be specified on certificates.

3.2.2.1 Customer identity verification

The identity of the customer is verified on the basis of the registration number from trusted public registers as Commercial Register or Trade Register by government agency in the jurisdiction of the legal creation known as Reliable Data Source.

3.2.2.2 Business Name Verification

The customer's business name is verified from Reliable Data Source.

3.2.2.3 Verification of the customer's residence

The residence (street address, city, town or locality) of the customer is verified from Reliable Data Source.

3.2.2.4 Customer Domain Name Verification (FQDN)

FQDN verification is performed in accordance with [CA/B] chapters 3.2.2.4.4 (sending a verification e-mail including a Random Value in to the constructed e-mail in the required domain) or 3.2.2.4.7 (verification of DNS TXT record including Random Value during 30 days). Random Value is created by random value generator with following hash SHA256.

Other methods of verifying the domain name are not allowed.

Verification of domain ownership is done by sending a verification email to one of the fixed email addresses selected during the registration process. The e-mail address is always from the domain whose name is to be inserted in the certificate name or in the certificate extension.

In the case of verification using a DNS TXT record, the customer is given a string during the registration process, which must be inserted into the DNS TXT record. This string is verified before the certificate is issued.

FQDN verification method is archived.

RA never delegates FQDN verification to another entity.

All data in the certificate before issuing, both domain and subject data from Reliable Data Source, are verified.

3.2.2.5 IP address verification

Inserting an IP address to the certificate is not allowed..

3.2.2.6 Wildcard domain verification

Wildcard domains are allowed at second and higher levels. Verification be carried out in accordance with Chapter 3.2.2.4. Wildcard certificates are subject to a special check for domains other than .cz. CA check the list of public suffix before issuing.

https://publicsuffix.org/

3.2.2.7 Data source accuracy

Only Reliable Data Source as public registers (www.justice.cz, www.rzp.cz, www.nic.cz) are used for verify the data entered into the certificate. Czech Post has determined that these sources are Reliable Data Sources in accordance with [CA/B].

3.2.2.8 CAA records

During the registration process, the CAA domain record for each dNSName in the subjectAltName extension is verified before the certificate is issued. When processing CAA records, CA process the issue, issuewild as specified in RFC 8659.

If the CAA record for the requested domain is incomplete or contains the domain name postsignum.cz, the request to issue a certificate is accepted. If the CCA record for the requested domain contains a domain name other than postsignum.cz, the request to issue a certificate is rejected.

CAA record is verified after 8 hours when CA get the request for issuing certificate.

The critical flag has default 0, in case of a discrepancy, manual processing takes place. In the case of any trouble CA contact the Applicant of domain certificate. CA is not support iodef record and exceptions are not specified in the CP.

In case of suspicion of mis-use of domain certificate issuance by an unauthorized person, it will be reported to the [CA/B].

3.2.3 Authentication of Individual Identity

3.2.3.1 Verification identity of applicant for issuance of certificate

- The applicant's identity is verified using an e-mail address during the certificate issuance process, see chapter 4.2.

3.2.3.2 Verification identity of applicant in event of revocation certificate

The entrepreneurial person proves his identity when pre-registering the customer's data and when submitting a request for revocation of the certificate. An employee of the organization proves his identity when submitting a request for revocation of the certificate. Presents one valid, undamaged original personal document.

The presented personal document, as specified in the below list, is accepted if the presented document provides information about nationality and identity, and has a photograph of the subscriber, personal ID number (or date of birth if it applies to foreigners), and information demonstrating validity of the document/expiration date. Individual Identity is only verified in case of revocation and the submitted document is checked for alteration or falsification.

- Citizens of the Czech Republic must present original personal ID or passport.
- Foreign citizens must present original travel, diplomatic, company or any other type of passport issued by the foreign state, or a permit issued by Czech authorities and allowing the foreign person to stay in the Czech Republic.

Citizens of EU member states and citizens of Iceland, Liechtenstein, Norway and Switzerland may also submit a original personal document, which was issued to them by the relevant country and which is used to demonstrate their identity in their country.

3.2.4 Non-verified subscriber information

The issued certificate contains only verified information by certification authority.

The Czech Post, as the provider of certification services, does not further verify the correctness of the following: data of the organizational unit subscribe in the list of applicants, which is submitted to the certification service provider by the customer's Authorized person.

3.2.5 Verification of specific rights

The Czech Post, as a provider of certification services, verifies the authorization to apply for a certificate according to this certification policy. Permission to request a certificate is granted by the customer's authorized person.

Creating a certificate request is only possible through the Provider's Customer Portal.

3.2.6 Criteria for Interoperation or Certification

Cooperation with other providers of certification services is not possible.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

In the case of a subsequent certificate request, it is necessary to follow the identification and authentication associated with the issue of the new certificate as in the case of initial identity verification when the first certificate is issued (see section 4.2).Identification and authentication for re-key after revocation

3.3.2 Identification and authentication for re-key after revocation

In case of a revoked certificate and during the identification and authentication process which occurs in connection with the issuance of a new certificate, it is necessary to proceed in the same way as during the first identity verification process done during the issuance of the first certificate (see chapter 4.2).

3.4 Identification and authentication for revocation request

The applicant or authorized person may require certificate revocation. The applicant must demonstrate his identity:

- by providing a password entered during the registration for the issuance of a certificate, or
- by presenting one personal document, if it concerns an employee of an organization or natural person performing business activities (see chapter 3.2.3).

An authorized person shall demonstrate its identity:

- by signing a written application for certificate revocation, or
- by an electronic signature based on the certificate issued by a subordinate certification authority from the PostSignum hierarchy on the application for a certificate revocation sent electronically, or
- by a personal document when application for a certificate revocation is presented in person at a registration authority of the Czech Post; an employee of the registration authority also verifies whether the authorized person is on the updated list of authorized person.

Certificate may also be revoked by the provider of certification services. In this scenario, the authorized applicant for a certificate revocation is the CA Manager.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Subjects/entities authorized to submit an application for a certificate

Application to issue a certificate in line with this certification policy may be submitted by:

- person selected by an authorized person of the customer – organization, or
- natural person performing business activities who concluded a contract describing provision of certification services.

4.1.2 Certificate application processing

4.1.2.1 Contract conclusion

A customer will gain an access to certification services by concluding a written contract describing provision of certification services. This contract is concluded in the following way:

The customer provides the Czech Post with a filled out contract form which is available at the webpage of the provider and the representative of the Czech Post concludes and signs the contract on provision of certification services together with the customer.

Contract forms contain links to the webpage of the provider where you may obtain Certification policies and the current pricelist.

Certification policy and the current pricelist become a part of the contract describing provision of certification services together with [VOP / General Business Terms] on the day when the contract is concluded.

Contract describing provision of certification services contains (besides other information) the following:

- customer identification data (company ID number if applicable),
- scope of provided certification services,
- list of authorized person who will be communicating with the provider of certification services in terms of certificate issuance.

Contract with the customer will be concluded pursuant to generally accepted business rules (statutory representative of the organization, etc.). The Contract can be executed in writing or electronic form.

The Czech Post reserves its right to reject conclusion of any contract describing provision of certification services.

4.1.2.2 Pre-registration of applicants for a certificate

Pre-registration shall be understood as a procedure when the authorized person - a customer, organization or natural person performing business activities approves the list of applicants who may apply for a certificate under this certification policy. This list shall be handed over to the provider of certification services.

The list of applicants contains mandatory and non-mandatory certificate data, which are specified in chapter 7.1. Personal ID number or date of birth of the applicant is not included in the issued certificate.

The authorized person or the customer alone determines whether the issued certificate may be published/made available to the general public without any restrictions.

The Czech Post reserves the right to refuse pre-registration if there are any doubts about the content of the Subject of certificate. A compliance between the applicant and customer (organization) specified on the certificate is guaranteed by an authorized person of the customer (organization) who manages the list of applicants given to the provider of certification services.

4.1.2.3 Customer responsibilities

In particular the customer is obligated:

- to provide true and complete information during the conclusion of a contract describing provision of certification services,
- immediately inform the provider of certification services about any changes in data included in the contract, in particular, changes in information of authorized person,
- immediately inform the provider of certification services about any changes in customer data specified in the certificate. Based on the nature of the change the provider of certification services shall decide whether it is necessary to revoke valid certificates issued on behalf of the customer.

4.1.2.4 Responsibilities of authorized person

In particular, the authorized person is responsible:

- to provide true and complete information about applicants who are authorized to apply for a certificate under this policy,
- immediately inform the provider of certification services about any changes in data included in the list of applicants for a certificate.

Authorized person also determines which customer certificates will be published - through information services of the provider of certification services. These services are available to the general public without any restrictions.

4.1.2.5 Applicant responsibility

In particular, the applicant is obligated:

- to provide true and complete information during the registration of an application for a certificate, and during registration of an application to issue a follow-up certificate,
- to verify whether information on the certificate is correct and correspond with the required data,
- to use and handle private key which correspond with the public key in the certificate issued pursuant to this certification policy with due diligence and to make sure that the key cannot be misused,
- to use private key and the relevant certificate issued pursuant to this certification policy only for purposes specified in this certification policy,
- immediately inform the provider of certification services about any circumstances that may result in certificate revocation, in particular, if there is a suspicion that a private key was misused, to require certificate revocation and stop using the relevant private key,

- to get acquainted with the certification policy based on which the certificate was issued,
- after paired data are generated (private and public key), to make sure that they are stored/backed up properly.

4.1.2.6 Provider responsibilities

Provider of certification services is obligated:

- to verify all data during the customer, or applicant for a certificate registration process, based on presented documents,
- - assess the application for a certificate as soon as possible after the application has been submitted, make a decision on whether to issue a certificate and inform the applicant or customer about this decision, to issue a certificate containing correct data based on information available to the certification authority at the time of the certificate issuance,
- to publish certification policies based on which certificates are being issued at the webpage of the provider, or through other suitable means (see chapter 2.2),
- to publish a qualified certificate for electronic seal of a provider of certification services, in such a way that the identity of the provider may be verified,
- to pay proper attention and care to all activities related to certification services. Proper care includes operations conducted according to:
    - valid legal regulations,
    - this certification policy
    - certification practice statement,
    - system safety policy,
    - operational documentation.

4.2 Certificate application processing

4.2.1 Identification and authentication

The identity of the subscriber is verified based on the e-mail address specified by the authorized person.

4.2.2 Acceptance or rejection of a certificate application

4.2.2.1 Acceptance or rejection of the first application for a certificate

The applicant provides the electronic request in PKCS#10 format to registration authority with containing the public key electronically in the manner specified on the provider's website. A PKCS#10 request cannot be reused after the certificate is issued.

Data will be entered into the certificate according to the valid list of applicants submitted by the authorized person.

The following checks are carried out before issue:

FQDN: If the certificate issuance data contains an incomplete or unauthorized FQDN (IP address, local domain), such a request is rejected. At least one FQDN must be specified in the certificate, which is also specified in the SAN.

Verification of the FQDN according to chapter 3.2.2.4 leads to approval or rejection of the request.

The verified data can not be used to issue another certificate with the same domain name, the FQDN check and verification of the certificate issuance request is performed before each certificate issuance.

Czech Post reserves the right to refuse to issue a certificate to an applicant in accordance with this certification policy.

If an employee of the registration authority has doubts about the submitted application or if other irregularities occur, an employee will refuse to issue a certificate and will inform the certificate applicant of this fact.

If the application is rejected, the application is archived due to suspicion of fraud.

4.2.2.2 Approval or rejection of certificate applications

Subsequent certificates according to this certification policy are not allowed to be issued. When applying for a certificate, proceed according to chapter 4.2.2.1

4.2.3 Time to process certificate applications

The provider of certification services is obligated to evaluate the application for a certificate as soon as possible and to decide whether the certificate will be issued and, a inform the applicant about it. As soon as a positive decision to issue the relevant certificate is issued, the provider is obligated to issue the certificate immediately.

4.3 Certificate issuance

After reviewing and approving the certificate request, the registration authority will enter the request into the certification authority's system for processing. The CA system issues a certificate based on this request and passes it back to the registration authority and publishing services.

The certificate will become valid immediately upon its issuance.

4.3.1 CA actions during certificate issuance

Employees of the registration authority will check the application according to chapter 4.2.2.1 and forward the application to the certification authority.

The certification authority issues a pre-certificate, which it publishes to CT logs in accordance with RFC 6962. The pre-certificate is sent to at least 3 CT logs. The list of CT logs to which pre-certificates are sent is given on the provider's website. In the case of certificate revocation, the pre-certificate is always automatically invalidated as well.The certificate is issued by the system of the certification authority automatically after receiving the record ID from the CT logs.

4.3.2 Notification to subscriber by the CA of issuance of certificate

Information about the location of the issued certificate (URL) is sent to the subscriber's e-mail address, where the issued certificate can be accepted (confirm receipt of the certificate) and the certificate, including the certificate issue protocol, is downloaded.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

After the certificate is issued the applicant for a certificate checks correctness of data on the certificate and confirms acceptance of the certificate.

By accepting certificate the applicant for a certificate confirms on behalf of the customer:

- that he is taking over responsibilities and obligations ensuing from certification policy according to which the certificate was issued,
- that he is not aware of any facts that could demonstrate that the private key corresponding with the public key on the certificate is owned by other person than the authorized person specified in the relevant certification policy,
- that data and information shown on the issued certificate are correct and complete (in particular, that the public key of the certificate corresponds with the public key specified on the provided PKCS#10 application).

By accepting the certificate the customer becomes the subscriber of the certificate.

The issued certificate is given to the subscriber in DER, PEM format.

4.4.2 Publication of the certificate by the CA

Certificates issued by PostSignum Public CA approved for publishing are published electronically no later than within 24 hours after the certificate is received by the applicant.

4.4.3 Notification about the issuance of a certificate sent to other entities

Besides publishing the issued certificate - for which the subscriber provided a consent to publish the certificate, and in addition to sending a note to the applicant or to any other person authorized by the customer, the provider of certification services does not report the issuance of the certificate to any other third party.

4.5 Paired data and certificate usage

Key pairs complianced to certificates have the same validity period as certificates. Key pairs, based on which the certificate was issued by the certification authority PostSignum Public CA, cannot be used in PostSignum Public CA environment again.

4.5.1 Subscriber private key and certificate usage

Subscriber of the certificate:

- uses and handles private key which correspond with the public key on the certificate issued pursuant to this certification policy with due diligence, while making sure that the key cannot be misused,
- in case of a loss or theft, or if there is a suspicion that the private key was compromised, the signatory must inform the provider of certification services about it immediately and stop using the specified private key,

- uses private key and the relevant certificate issued pursuant to this certification policy only for purposes specified in this certification policy under chapter 1.4.1 that is to create electronic signatures, to authentication and encryption.

4.5.2 Relying party public key and certificate usage

The user of the certificate (relying party) issued by PostSignum Public CA:

- obtains PostSignum Public CA a PostSignum Root QCA certificates from a safe source (webpage of the provider, at the branch office) and verifies fingerprints of these certificates.

- before using a certificate issued by PostSignum Public CA, the user of the certificate verifies the validity of PostSignum Public certificate and also the validity of the issued end certificate; the verification process applies to the correctness of the signature of the issuing authority with respect to the current CRL and to the actual/current time, or use OCSP service (this activity is usually handled by the software of the user of the certificate).

- evaluates whether the certificate issued by a subordinate certification authority pursuant to this policy is suitable for the purpose for which the certificate was issued.

4.6 Certificate renewal

Certificate renewal refers to the issuance of a new certificate with the same public key but with a new validity term. PostSignum VCA does not provide this service.

4.6.1 Circumstance for certificate renewal

PostSignum VCA does not provide this service.

4.6.2 Who may request renewal

PostSignum VCA does not provide this service.

4.6.3 Renewal certificate request processing

PostSignum VCA does not provide this service.

4.6.4 Notification of new certificate issuance to subscriber

PostSignum VCA does not provide this service.

4.6.5 Conduct constituting acceptance of a renewal certificate

PostSignum VCA does not provide this service.

4.6.6 Publication of the renewal certificate by the CA

PostSignum VCA does not provide this service.

4.6.7 Notification of certificate issuance by the CA to other entities

PostSignum VCA does not provide this service.

4.7 Certificate re-key

PostSignum VCA does not provide this service.

4.8 Certificate modification

Certificate with modified data may be issued only as

- a new certificate, while following procedure specified in chapters 4.1 through 4.4, or
- Data change must be reported by the customer to the provider using suitable notification method, before a new application for a new or follow-up certificate is submitted.
- If any data shown on the current certificate are no longer valid, it is necessary to request a revocation of such certificate through suitable and accepted means.

4.8.1 Circumstance for certificate modification

All changes of data on the relevant certificate must be reported to the provider of certification services by submitting a modified list of applicants.

Should the provider of certification services find out that data about a customer or applicant for a certificate available in the system of the certification authority do not match the reality, the provider is allowed to modify these data.

4.8.2 Who may request certificate modification

Change list of applicants is submitted by the authorized person of the customer (organization, a natural person performing business activities).

4.8.3 Processing certificate modification requests

An employee, or possibly the system of the registration authority shall verify the following:

- if it concerns an authorized person, the system shall verify whether this person is listed on the current list of authorized person of the customer; if such person is physically present (a visit) then the identity of such person is checked based on presented personal ID/documents,
- if it concerns the customer itself, whether the customer has concluded a valid contract describing provision of certification services, and the identity of the customer according to presented personal ID/documents.

Then the employee, or possibly the system of the registration authority, updates the data about the applicant for a certificate in the system of the certification authority.

4.8.4 Notification of new certificate issuance

Identical procedures as in the case of the issuance of the first certificate shall apply. See provisions specified in chapter 4.3.2.

4.8.5 Conduct constituting acceptance of modified certificate

Identical procedures as in the case of the issuance of the first certificate shall apply. See provisions specified in chapter 4.4.1).

4.8.6 Publication of the modified certificate by the CA

Identical procedures as in the case of the issuance of the first certificate. See provisions specified in chapter 4.4.2.

4.8.7 Notification of certificate issuance by the CA to other entities

Identical procedures as in the case of the issuance of the first certificate shall apply. See provisions specified in chapter 4.4.3.

4.9 Certificate revocation and suspension

A request to revoke a certificate may be submitted through methods specified below:

- a personal visit at the registration authority (only during regular business hours of the relevant contact office)

List of contact offices/branches of the registration authority is specified at the webpage of the provider.

- Telephone

Telephone: 954 303 303

- E-mail (nonstop)

E-mail: postsignum@cpost.cz

- Web application (nonstop)

Website: www.postsignum.cz/zneplatneni_certifikatu.html

Validity of a certificate ends when it is revoked and when published on the list of revoked certificates.

If the certificate does not need to be revoked during its validity, the certificate shall end on the day specified as the end of the certificate validity. After the certificate expires, it is stored in the database of the issuing certification authority and archived according to valid legislature and archiving requirements of the Czech Post.

4.9.1 Circumstances for revocation

4.9.1.1 Reasons for End User Certificate Revocation

- any suspicion that a certificate private key may have been compromised,
- failure of a customer to comply with requirements specified in the contract describing provision of certification services,
- request of the certificate subscriber,
- other reasons (death, termination, restriction or deprivation of legal rights of the subscriber; loss of information accuracy based on which the certificate was issued).
- In all cases, the certificate is revoked within 24 hours of receiving the request for revocation.

- CA Postsignum allows you to choose one of the following revocation reasons:

- unspecified 0 - Represented by the omission of a reasonCode must be omitted if the CRL entry is for a Certificate not technically capable of causing issuance unless the CRL entry is for a Subscriber Certificate subject to these Requirements revoked prior to July 15, 2023.

- keyCompromise 1 - Indicates that it is known or suspected that the Subscriber's Private Key has been compromised. CA Postsignum do not expect to receive proofs of key compromise.

- affiliationChanged 3 - Indicates that the Subject's name or other Subject Identity Information in the Certificate has changed, but there is no cause to suspect that the Certificate's Private Key has been compromised.

- superseded 4 - Indicates that the Certificate is being replaced because: the Subscriber has requested a new Certificate, the CA has reasonable evidence that the validation of domain authorization or control for any fully-qualified domain name or IP address in the Certificate should not be relied upon, or the CA has revoked the Certificate for compliance reasons such as the Certificate does not comply with these Baseline Requirements or the CA's CP or CPS.

- cessationOfOperation 5 - Indicates that the website with the Certificate is shut down prior to the expiration of the Certificate, or if the Subscriber no longer owns or controls the Domain Name in the Certificate prior to the expiration of the Certificate.

- certificateHold 6 – must not be included if the CRL entry is for 1) a Certificate subject to these Requirements, or 2) a Certificate not subject to these Requirements and was either A) issued on-or-after 2020-09-30 or B) has a notBefore on-or-after 2020-09-30.

- privilegeWithdrawn 9 - Indicates that there has been a subscriber-side infraction that has not resulted in keyCompromise, such as the Certificate Subscriber provided misleading information in their Certificate Request or has not upheld their material obligations under the Subscriber Agreement or Terms of Use.

In the case of report can be send to the e-mail Incident.postsignum@cpost.cz

4.9.1.2 Reasons for invalidating the certificate of the subordinate CA

See chapter 5.7.3.1.

4.9.2 Who can request revocation

Certificate revocation may be requested by:

- customer (certificate subscriber) through the use of an authorized person or statutory representative,

- applicant to the certificate,

- CA Manager

4.9.3 Procedure for revocation request

4.9.3.1 Personal revocation request made by the subscriber to the registration authority

An applicant may request a certificate revocation in person at the office of the registration authority where the applicant must demonstrate his identity (see chapter 3.2.3). He will sign a written application for a

certificate revocation printed out by the registration authority. This application contains certificate serial number, the name of the issuing certification authority and the reason for the revocation (optional).

The employee of the registration authority will search for the certificate and begins with the revocation process. He will verify whether the applicant has the right to request revocation of the relevant certificate. If the verification is successful, the employee of the registration authority will send the revocation request to the system of the certification authority for processing. When the system of the certification authority completes the process, the employee will verify the status of the certificate and will hand the certificate revocation protocol over to the applicant.

4.9.3.2 Certificate revocation application submitted via fax or by phone or through other remote channels

The applicant may submit a request for certificate revocation over the phone by calling the phone number specified in chapter 4.9, or through the use of other remote channels specified at the webpage of the provider. Revocation service by the phone is available 24 hours a day. Each submitted application must contain the certificate serial number, the name of the issuing certification authority, certificate revocation password and the reason for the revocation (optional).

The employee authorized to carry out the revocation will check the revocation password on the application in relation to the password entered during the certificate application registration process. If both passwords match the certificate is revoked. If they do not match the employee will not revoke the certificate and will inform the applicant.

If the revocation is successful, a revocation protocol is created and emailed to the applicant to the email address specified on the revoked certificate (if the certificate contains an e-mail address) and to the contact e-mail address of the applicant specified in the system of the certification authority.

4.9.3.3 A request for a certificate revocation submitted by authorized person

If the customer requires certificate revocation, he shall do so in written form. The authorized person shall come in person to the registration authority of the Czech Post, where a written application for a certificate revocation will be produced.

If the authorized person owns a certificate designed for signing and issued by subordinate certification authority within the PostSignum hierarchy, the person may send the certificate revocation request via email message fitted with electronic signature to the email address specified in chapter 4.9.

If the revocation is successful, a revocation protocol is created and emailed to the authorized person. The applicant is informed about the certificate revocation by email sent to address and to the address specified in the revoked certificate (if the certificate contains an e-mail address) and to the contact e-mail address of the applicant specified in the system of the certification authority.

4.9.3.4 Certificate revocation required by the certification authority

Also the provider of certification services may decide to revoke the certificate, providing that certificate subscriber or the customer violated certification policy rules or contractual requirements. In such scenario, PostSignum VCA will inform the customer about the certificate revocation and will specify the reason why the certificate was revoked. CA Manager submits the signed application for a certificate revocation electronically to any employee authorized to perform certificate revocations.

If the revocation is successful, a revocation protocol is created and emailed immediately to the applicant together with explanation of reasons why the certificate was revoked, to the address and to the address

specified on the revoked certificate (if the certificate contains an e-mail address) and to the contact e-mail address of the applicant specified in the system of the certification authority.

4.9.3.5 Certificate Problem Report

Subscribers, Relying Parties, Application Software Suppliers, and other third parties can report suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. of possible compromise of the private key or other possible misuse of the certificate or other types of fraud can also be reported to the e-mail address:

Incident.postsignum@cpost.cz

4.9.4 Revocation request grace period

As soon as a person authorized to request a certificate revocation learns about the reason for the certificate revocation, it must require revocation of the relevant certificate immediately.

4.9.5 Time within which CA must process the revocation request

The time when the application to revoke the relevant certificate is received until the CRL containing the revoked certificate is published cannot exceed 24 hours.

4.9.6 Responsibilities of relying parties verifying the certificate revocation

The user of the certificate issued by PostSignum Public CA (relying party) is obligated to proceed in line with provisions specified in chapter 4.5.

4.9.7 Frequency of the issuance of revoked certificates

A list of revoked certificates (CRL) is issued immediately after the request to revoke a certificate is processed. If the certificate is not revoked, new CRL is issued at least every 24 hours. The list of revoked certificates is published:

- at distribution locations CRL (CDP) specified on the certificate
- on the webpage of the provider,
- at the independent provider of web services.

The frequency of issuing CRLs for subordinate CAs is once every 12 months from the last issue.

Primary source of the current CRL are CRL distribution locations.

4.9.8 Maximum allowed delay when issuing a list of revoked certificates

The list of revoked certificates is published immediately after its issuance; provisions specified under chapter 4.9.5 must be observed.

4.9.9 Option to verify certificate status online (hereinafter "OCSP")

The following apply for communicating the status of Certificates which include an Authority Information Access extension with an id-ad-ocsp accessMethod. OCSP responses conform to RFC6960 and/or RFC5019. OCSP responses is:

Signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked.

The following applies to communicating the status of certificates that include extending access to authority information with the id-ad-ocsp access method. OCSP responses conform to RFC6960 and/or RFC5019. The OCSP responses are:

- Signed by an OCSP responder whose certificate is signed by the CA that issued the certificate whose revocation status is being checked.
- Checking certificate status online using the OCSP protocol by PostSignum VCA is a service available to the general public.

Every certificate issued under this CP includes a link to the pertinent OCSP responder, refer to certificate profile in chapter 7.1.2.

4.9.10 On-line revocation checking requirements

The following SHALL apply for communicating the status of Certificates which include an Authority Information Access extension with an id-ad-ocsp accessMethod. OCSP responders operated by the CA SHALL support the HTTP GET method, as described in RFC 6960 and/or RFC 5019.

The CA MAY process the Nonce extension (1.3.6.1.5.5.7.48.1.2) in accordance with RFC 8954. The validity interval of an OCSP response is the difference in time between the thisUpdate field, inclusive. For purposes of computing differences, a difference of 3,600 seconds shall be equal to one hour, and a difference of 86,400 seconds shall be equal to one day, ignoring leap-seconds. This is also valid for sub certificate.

The CA SHALL update information provided via an Online Certificate Status Protocol

i. at least every twelve months; and
ii. within 24 hours after revoking a Subordinate CA Certificate. If the OCSP responder receives a request for the status of a certificate serial number that is “unused”, then the responder SHOULD NOT respond with a “good” status.

It is possible to use the general public available OCSP service to verify the certificate issued under this CP. The OCSP service is provided according to the standard RFC 6960. The format of the OCSP request and response is given in chapter 7.3.

4.9.11 Other forms of revocation advertisements available

In addition to the above-specified certificate status verification, the provider of certification services does not provide additional options to report a revoked certificate.

4.9.12 Special requirements re-key compromise

4.9.13 Circumstances for suspension

The Certificate revocation procedure in the event of private key compromise is not different from theCertificate revocation procedure described above, see section 4.9.1.

PostSignum VCA does not provide this service. The validity of the certificate can not be suspended.

4.9.14 Who can request suspension

PostSignum VCA does not provide this service.

4.9.15 Procedure for suspension request

PostSignum VCA does not provide this service.

4.9.16 Limits on suspension period

PostSignum VCA does not provide this service.

4.10 Certificate status services

Certificate status may be verified:

- on the list of revoked certificates (CRL) using a service allowing public access to PostSignum VCA information via HTTP protocol, or
- using a service allowing search for issued certificates available at the webpage of the provider, or
- using OCSP service.

4.10.1 Operational characteristics

List of revoked certificates and information about certificate status is considered public information. The list of revoked certificates (CRL) is published at locations specified under chapter 4.9.7. Information about certificate revocation is included in the CRL at least until its validity period.

Under the service allowing search for issued certificates available at the webpage of the provider, also information about the searched certificate status is published. However, this information is for informative purposes only and shall be treated as additional information to the current CRL, which is the trusted source for certificate status information.

The OCSP service returns the status of the certificate in real time (on-line) based on the sent request, which must comply the requirements specified in the Certification Practice Statement. The OCSP server's response is signed by the OCSP server's certificate and has a prescribed format, specified in the Certification Practice Statement. Certificate status information obtained using the OCSP service is the binding source of certificate status information.

4.10.2 Service availability

The list of revoked certificates is available through the service allowing access to public information 7 days a week 24 hours a day. Solution architecture and emergency plans are designed in a certain way in order to make sure that there is always one location available where the current information about the list of revoked

certificates may be obtained. Under normal operating conditions, the response time for obtaining this information is 10 seconds or less.

Certificate search service is available 7 days a week 24 hours a day.

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

In the case of non-availability can be send to the e-mail incident.postsignum@cpost.cz

4.10.3 Other characteristics of certificate status service

Other characteristics of certificate status services have not been established.

4.11 Termination of services used by the subscriber of the certificate

Services provided to the certificate subscriber shall end on the day when the contract between the customer and provider of certification services expires. This does not apply to certificate revocation services which are provided throughout the entire validity of the relevant certificate.

Termination of a contract describing provision of certification services or withdrawal from this contract is subject to general business terms and conditions [VOP].

4.12 Public key escrow and recovery

PostSignum VCA does not provide this service.

4.12.1 Public key escrow and recovery policy and practices

PostSignum VCA does not provide this service.

4.12.2 Session public key encapsulation and recovery policy and practices

PostSignum VCA does not provide this service.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

The following documents were processed on behalf of PostSignum VCA:

- System safety policy describing safety principles applicable to physical, procedural and personal segments;
- Emergency plan describing emergency situation handling procedures and procedures guaranteeing service level maintenance in case of emergency situation,
- Operational and safety procedures logically describing procedures observed by PostSignum VCA, and
- Organizational activities ensuring fulfilment of a task called Public Certification Authority of the Czech Post, which (besides other tasks) assigns PostSignum VCA roles.

The above-mentioned documents were produced based on risk analysis results. The CA's security program include an annual Risk Assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;

2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and

3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

The risk analysis is carried out and evaluated in accordance with the internal regulations of the Czech Post.

These documents are also available to person who inspect adherence to PostSignum VCA safety principles. This chapter is based on the above specified document and provide a brief overview of basic safety principles utilized by PostSignum VCA.

5.1 Physical security controls

5.1.1 Site location and construction

PostSignum VCA uses the following types of permanent workplaces located in spaces of the Czech Post, or at facilities of contractual partners of the Czech Post:

- central workplace/office (main and backup location),
- operator center workstation (in particular, for supporting information system management),
- registration authority workplace and
- business locations.

The used structure is based on safety requirements specified in a document called System safety policy. In general, all the above specified workplaces adhere to clearly defined perimeter and are protected against unauthorized entry with mechanical components/systems. Central workstations are protected similarly as "Confidential" areas.

In addition there is also a mobile workstation of the registration authority where the lack of physical safety elements is compensated with organizational safety rules.

5.1.2 Physical access

Each type of workplace has an operational code, which defines what employees have physical access to that particular workplace. Spaces are protected against unauthorized entry with mechanical components (safety locks and bars), and the central workplace is protected with an independent electronic security system loop. Regime measures defined by the System safety policy apply to mobile registration authority.

5.1.3 Power and air-conditioning

Central workplaces are connected to uninterrupted power supply unit (UPS) and are equipped with air-conditioning systems which maintain optimum humidity and temperature in the room.

5.1.4 Water exposures

Central workplaces are located outside of flood areas.

Central workplaces areas are equipped with flood warning system.

5.1.5 Fire prevention and protection

Central workplace areas are equipped with electric fire warning system (EPS).

5.1.6 Media storage

Safety boxes are used to store PostSignum VCA data, at least one of them is located outside the premises of the central workplaces.

5.1.7 Waste management

Paper documents and media used by PostSignum VCA are disposed safely:

- storage media are physically destroyed or a suitable software is used ensuring complete deletion of data stored on the media,
- paper documents are disposed of in a facility designated for that purpose..

5.1.8 Off-site backup

A backup location for PostSignum VCA was built where operations are transferred in emergency situations when proper VCA operations in the main location cannot be ensured. Also regular PostSignum VCA system backups are sent to this backup location on regular basis.

5.2 Procedural Controls

5.2.1 Trusted roles

PostSignum VCA has defined goals which are handled by operators of PostSignum VCA. There are rules based on which individual goals are assigned. That means who will assign the employee with the relevant role and who will recall it and what roles may not be handled by one person simultaneously. All access rights (at the level of physical access, at the level of access to operating system and at the level of application access) belong to these roles.

A special attention is paid to assignment of roles allowing access to central PostSignum VCA.

5.2.2 Number of person required per task

PostSignum VCA has defined activities which require the presence of more than one person. These include mainly activities when a private key of certification authority is handled and when cryptographic module is used to generate and store private key of the certification authority (secure cryptographic module).

5.2.3 Identification and authentication for each role

The subscriber of each role must identify and authenticate personal data when accessing VCA sources. Each user is assigned with a unique identification valid for all systems where the user have access. PostSignum VCA systems use identification by name or rather by a certificate and authentication through the use of a password or private key.

5.2.4 Roles requiring division of responsibilities

PostSignum VCA has established rules based on which individual roles are assigned and also rules which are used for role separation. These rules are specified in a document called Organizational activities ensuring fulfilment of a task called Public certification authority of Czech Post.

5.3 Personnel security controls

5.3.1 Requirements on qualification, experience and clearances

Roles ensuring operation, management and maintenance and development of PostSignum VCA systems are assigned based on procedures (for example based on references, trial periods etc.), which ensure that these functions will be assigned to trusted and highly qualified employees. Similar procedures apply to conclusion of contracts with external employees or contractual partners.

If the person is not an employee of the Czech Post, but an employee of its contractual partner, then requirements and regulations valid at the relevant partner shall apply.

5.3.2 Assessment of personal reliability

PostSignum VCA operating roles are assigned exclusively to person who have been employed by the Czech Post for long time and have provided good personal and work in references.

If the person is not an employee of the Czech Post, but an employee of its contractual partner, then requirements and regulations valid at the relevant partner shall apply.

5.3.3 Requirements for the preparation for role performance

All employees involved in the operation, management, maintenance and development of PostSignum VCA systems are properly trained, primarily RA operators performing the role of Validation Specialist. RA operators are trained once a year and a record must be made of the completion of the training. The training also includes a course focusing on system safety and behaviour of the system during emergency situations.

A written training report must be produced from each training course, which must contain (in addition to other information) the training date, contents, name of the instructor and list of attendees. This report must be signed by all participants and by the instructor.

As far as roles assigned by the CA manager are concerned, this training may be replaced with an introductory session where the employee is introduced to all documents describing operation of VCA and applicable to the relevant role.

If the person is not an employee of the Czech Post, but an employee of its contractual partner, then requirements and regulations valid at the relevant partner shall apply.

5.3.4 Training frequency and training requirements

PostSignum VCA offers a programme focusing on the creation, maintenance and strengthening of safety awareness based on individual roles.

CA Manager organizes regular operator training (in particular when PostSignum VCA procedures are changed).

5.3.5 Job rotation frequency and sequence

Requirements on employee rotation frequency have not been defined.

5.3.6 Sanctions for unauthorized actions

Penalties focusing on discipline violations are subject to applicable regulations of the Czech Post, or to applicable provisions specified in a contract concluded between the Czech Post and its contractual partner.

5.3.7 Independent contractor requirements

Contractual (external) workers are subject to similar criteria as employees of the Czech Post.

5.3.8 Documentation supplied to personnel

PostSignum VCA staff may use documentation applicable to their roles, in particular

- safety policy,
- certification policy,
- certification practice statement,

operational documentation – manuals and work procedures designed for operators.

5.4 Audit Logging Procedures

Auditing and archiving policy (attached to a document called System safety policy) has been created for PostSignum VCA and describes basic inspection principles and PostSignum VCA auditing and archiving regulations. This document is also available to person who inspect adherence to PostSignum VCA safety principles. This chapter is based on the Auditing and archiving policy document and provides a brief overview of basic inspection principles utilized by PostSignum VCA.

5.4.1 Types of recorded events

In order to check, analyse or investigate emergency events (in general, to be able to demonstrate the sequence of PostSignum VCA operations and their assignment to a particular person who called them), records describing issuance of certificates, termination of certificates, the use of keys and PostSignum VCA

certificates, as well as other important records are stored (for example termination of activities of a certification authority).

Written audit records must be signed and must contain the name of the employee who created the record.

Log records include the following elements:

1. Date and time of record;

2. Identity of the person making the journal record; and

3. Description of the record.

None of these operations are allowed to a third party.

5.4.2 Record processing frequency

Auditing reports are inspected by person who were assigned the relevant role and task, during intervals defined in the System safety policy. These reports are also subject to internal and external inspections.

5.4.3 Auditing report storage time

Auditing reports are stored for 10 years, unless other applicable regulation require longer time.

5.4.4 Protection of auditing logs

Auditing reports are stored in a certain way in order to protect them from theft, modifications or destruction - either deliberate or intentional (fire, water).

Auditing reports stored as data files are archived on non-rewritable (permanent) storage media.

5.4.5 Auditing log back up procedures

Auditing reports (except for auditing reports in electronic form describing activity of central components of the certification authority) are usually not backed up; there are only archived. Important auditing reports related to certificate issuance are stored in two copies, whereas each copy is stored at a different location.

5.4.6 Auditing log collection system (internal or external)

PostSignum VCA environment is not equipped with any auditing report central collection system. Auditing reports are collected under individual PostSignum VCA.

5.4.7 Event notification process used to notify the subject which caused the event

A subject which caused an event recorded in auditing logs is not notified about this event.

5.4.8 Evaluation of vulnerability

Auditing reports are regularly inspected and analyzed for the existence of reports describing nonstandard events, which may point out to an attempt to compromise security. Also procedures defining how to proceed in these cases are established.

Reports describing nonstandard events are also handed over (besides others) to the CA Auditor.

Vulnerability checks of the certification authority's systems are performed at least once a year.

5.5 Records Archival

Auditing and archiving policy has been created for PostSignum VCA which describes basic inspection principles and PostSignum VCA auditing and archiving regulations. This document is also available to person who inspect PostSignum VCA.

5.5.1 Types of records archived

In PostSignum VCA the following records are being archived:

- software and data including issued certificates and CRL,
- all documents relevant to registration of applications for a certificate, including contracts,
- reports describing assignment of PostSignum VCA roles and operator training records,
- logs automatically created by components of PostSignum VCA information system.

5.5.2 Retention period for archive

Software, data and auditing reports are archived for 10 years.

5.5.3 Protection of archive

Archive is protected through technical and object safety measures. Archive is also protected against environmental impacts such as temperature, humidity etc.

5.5.4 Archive backup procedures

Backup procedures of archived information are specified in a separate document called Auditing and archiving policy, which is accessible to person who inspect PostSignum VCA (in addition to other person).

5.5.5 Requirements for time-stamping of records

If PostSignum VCA uses time stamp it refers to qualified electronic time stamps PostSignum QCA.

5.5.6 Archive collection system (internal or external)

Within the PostSignum VCA environment reports are collected or moved to CA archive according to procedures specified in the Auditing and archiving policy document.

5.5.7 Procedures to obtain and verify archive information

Data archive and software equipment are locked in specific safety boxes.

Each location which has a safety box must maintain a protocol describing stored archiving media and where all handling procedures and use of stored media are recorded.

Access to archives is limited to person who have been assigned with the applicable roles.

5.6 Key changeover

Validity of keys of certification authorities in the PostSignum VCA hierarchy is limited.

Sufficiently in advance, but no less than one year before the validity of PostSignum Root QCA certificate expires, a new ceremonial issuance of the new certificate must take place. The result of the ceremony is the actual creation of a new self-signed certificate of root certification authority, which shall be published while following procedures specified in chapter 1.5.

At least one year before the validity of the certificate expires the operator of certification authority PostSignum Public CA is obligated to apply at PostSignum Root QCA for the issuance of another certificate.

The planned exchange of certification authority keys must be notified to customers no later than 3 months before the issuance of a new PostSignum Root QCA certificate, one month before the exchange of the PostSignum Public CA certificate. This notice (including the reason for the expiry of the certificate) will be published on the provider's website and at all PostSignum VCA registration offices.

When there is no longer need to use original data necessary to create electronic seal, the Czech Post must demonstrate destruction of these data, - which were used to sign commercial certificates and list of revoked certificates. The Czech Post must create a report describing destruction of such data.

This procedure shall also apply to a situation when there is a need to exchange data due to insufficient guarantees provided by the used algorithm or by its parameters (for example the module size).

5.7 Compromise and disaster recovery

Documents describing management of emergency situations as well as restoration procedures have been created for PostSignum VCA.

These documents are available (in addition to other person) to person inspecting PostSignum VCA.

PostSignum VCA staff is properly trained in emergency situation handling procedures. Emergency plan is tested at least once a year.

5.7.1 Incident and compromise handling procedures

The security of the means of the certification authority after a natural disaster or other extraordinary event is elaborated in the documents Crisis plan for the protection of the object and Plan for managing crisis situations and recovery plan. Emergency plan tests are verified at least once a year by an external auditor.

5.7.2 Computing resources, software, and/or data are corrupted

In case of a security incident of compromise of the keys of certification authorities described in chapters 5.7.3, these incidents are reported to the Secure bug Bugzilla.

The security of the means of the certification authority after a natural disaster or other extraordinary event is elaborated in the documents Crisis plan for the protection of the object and Plan for managing crisis situations and recovery plan.

5.7.3 Procedure applicable to situations when data used for the creation electronic seal have been compromised

5.7.3.1 Subordinate certification authority key disclosure

If there is a suspicion that private key PostSignum Public CA has been compromised, all certificate subscribers, and the supervisory body and to subjects which have concluded contract directly related to the provision of certification services will be informed electronically about the fact that this authority will no

longer provide its activities. This notification will also be published at the webpage of the provider and at all registration offices/workplaces of PostSignum VCA and in one nationally published newspaper. This notification shall also specify the reason for the termination of the certificate belonging to this particular certification authority.

PostSignum Root QCA will immediately revoke the PostSignum Public CA certificate and PostSignum Public CA will revoke all valid certificates issued to end customers. Invalidated/revoked certificates will be immediately published on the relevant CRL.

After the information about emergency termination of activities is published, also validity of all certificates issued by PostSignum Public CA will be terminated.

The Czech Post shall destroy data used to create electronic seal for PostSignum Public CA, which were used to signing commercial certificates, as well as the list of revoked certificates providing that there is a suspicion that these certificates were compromised. The Czech Post must create a report describing destruction of such data.

This procedures shall also apply to situations when the algorithm used to create electronic seal is suddenly weakened and indisputably discredits the credibility of the issued certificates and the list of issued certificates.

5.7.3.2 Disclosure of PostSignum Root QCA key

If there is a suspicion that PostSignum Root QCA key has been compromised, the provider of certification services shall revoke the PostSignum Root QCA certificate and all certificates of subordinate certification authorities and all valid certificates issued by these authorities; revoked certificates will be published immediately on the relevant CRL. All certificate subscribers, and the supervisory body and to subjects which have concluded contracts directly related to the provision of certification services will be notified electronically or in writing about certificate revocations (or possibly about the fact that the relevant authority will no longer provide its activities). This notification will also be published at the webpage of the provider and at all registration offices/workplaces of PostSignum VCA and in one nationally published newspaper. This notification shall also specify the reason for the termination of the certificate belonging to this particular certification authority.

After the information about emergency termination of activities is published, also validity of all certificates issued by PostSignum Root QCA, as well as by subordinate certification authorities will be terminated.

The Czech Post shall destroy data used to create electronic seal PostSignum Root QCA, which were used to signing qualified certificates and the list of revoked certificates, providing that there is a suspicion that these certificates were compromised. The Czech Post must create a report describing destruction of such data.

This procedures shall also apply to situations when the algorithm used to create electronic seal is suddenly weakened and indisputably discredits the credibility of the issued certificates and the list of issued certificates.

5.7.4 Business continuity capabilities after a disaster

Restoration of activities after a breakdown is subject to a valid internal document called Emergency situation procedure plan and Restoration plan.

5.8 CA or RA Termination

5.8.1 Termination of Root CA

Termination of PostSignum Root QCA must be notified in writing to all subscribers of valid certificates, the supervisory authority and entities that have concluded a contract directly related to the provision of certification services and also published on the Provider's website and at all workplaces of the PostSignum VCA registration authority. In the event that the termination of the authority's activities includes the termination of the validity of its certificate, this information, including the relevant reason for the termination, must also be included in the notification. As long as at least one certificate issued by PostSignum Root QCA is valid, PostSignum Root QCA must provide at least the function of revoking the certificate and issuing a CRL.

If PostSignum Root QCA is not able to ensure this function while the issued certificates remain valid, PostSignum Root QCA must inform subscribers of valid certificates about this fact and specify until what date this function will be provided/available. This date cannot come earlier than 6 months after this notification is sent out. As of this date PostSignum Root QCA will invalidate/revoke all issued and valid certificates and will issue last CRL. Only after that activities of PostSignum Root QCA may be terminated.

In such scenario, contracts describing provision of certification services will be terminated by the Czech Post through a withdrawal or resignation.

Following the termination of contracts, the Czech Post shall destroy data used to create electronic seal PostSignum Root QCA, which were used to sealing qualified certificates as well as the list of revoked certificates. The Czech Post must produce a report clearly demonstrating that these data were destroyed. These reports/records must be stored in accordance with provisions specified in this certification policy and as described in chapter 5.4.

5.8.2 Termination of a subordinate CA

Written notification of termination of activities of PostSignum Public CA must be delivered to all subscribers possessing valid certificates and to subjects which have concluded contracts directly related to the provision of certification services. This notification must also be published at the webpage of the provider and at all registration offices/workplaces of PostSignum VCA. This notification must also provide information about certificate termination including explanation of reasons for the termination. If at least one certificate issued by PostSignum Public CA remains valid, PostSignum Public CA must provide (at least) certificate revocation function and CRL issuance function.

If PostSignum Public CA is not able to ensure this function while the issued certificates remain valid, PostSignum Root CA must inform subscribers of valid certificates about this fact and specify until what date this function will be provided/available. This date cannot come earlier than 3 months after this notification is sent out. As of this date PostSignum Public CA will invalidate/revoke all issued and valid certificates and will issue last CRL. Only after that activities of this authority may be terminated.

Revoked qualified certificate for electronic seal PostSignum Public CA will be published at CRL PostSignum Root QCA at the time specified in the certification policy of PostSignum Root QCA.

In such scenario, contracts describing provision of certification services will be terminated by the Czech Post through a withdrawal or resignation.

Following the termination of contracts the Czech Post shall destroy data used to create electronic seal PostSignum Public CA which were used to sealing qualified certificates and the list of revoked certificates. The Czech Post must produce a report clearly demonstrating that these data were destroyed. These

reports/records must be stored in accordance with provisions specified in this certification policy and as described in chapter 5.4.

5.8.3 Termination of RA

Information about the termination of activities provided by a registration authority workplace/office is provided to customers through notes placed on notification boards at the relevant workplace or building and at the webpage of the provider. The notification about termination of activities of the relevant workplace must also specify the address and contact information of the replacement workplace/office.

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

PostSignum does not provide a key generation (paired data) service for certificate applicant. PostSignum VCA does not come into contact with the applicants' private keys, is not responsible for their protection or backup.

6.1.1 Key pair generation

Key pairs of certification authorities - under the PostSignum VCA hierarchy, are generated and stored in hardware cryptographic module. Generation of these key pairs is done under a controlled process supervised by the CA Manager and CA Auditor.

Key pairs of individual components or PostSignum VCA systems (infrastructure keys) are generated under controlled PostSignum VCA system environment. These key pairs are stored in cryptographic module; in order to access these key pairs the operating staff must insert a chip card and enter PIN.

Key pairs of PostSignum VCA operators (including RA operators; inspection keys) are generated in dedicated chip cards, which do not allow (due to their structure) private key exporting. In order to use private keys, PIN must always be entered. Chip cards are then handed over to operators in personally or via traceable parcel separately from the access PIN code.

Applicant private keys are generated and stored by the applicant for a certificate. Keys may be generated and then stored both in software and hardware storage units. PostSignum VCA does not prescribe specific storage requirements (not prescribed for the use of a means for the safe creation of electronic signatures).

The quality control of public keys is performed in accordance with paragraph 6.1.6.

6.1.2 Private key delivery to subscriber

PostSignum VCA does not provide key's pair generation service on request of the applicant.

6.1.3 Public key delivery to certificate issuer

A public key of the applicant is delivered to the provider of certification services in electronic form in the application for a certificate in PKCS#10 format.

6.1.4 CA public key delivery to relying parties

Certificates of certification authorities and also certificates, which have been approved for publishing, are published through a procedure specified in Chapter 2.

6.1.5 Key sizes

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

Certificate subscriber keys have a module length a pLen and qLen min. 256 bit for the ECDSA algorithm, specifically the P-256, P-384 and P-521 curve (secp256r1, secp384r1, secp521r1).

An algorithm other than ECDSA is not allowed for certificate subscribers.

6.1.6 Public key parameters generation and quality checking

The parameters used in the creation of public keys of PostSignum VCA components are generated by the corresponding software and hardware equipment. The algorithms used and their parameters comply with the requirements of technical standards.

The parameters used to create the certificate requestor's public keys are generated by the requestor's software or hardware and are not the responsibility of the certificate service provider.

Public key quality control is set at the CA level, which checks the uniqueness and allowed length of the public key. In the event that an algorithm that has been broken is used to generate the private key, the CA reserves the right to reject the request.

The CA reserves the right to reject a certificate request if it does not contain the following requirements:

- corresponding algorithm must be used

- key size

- compromised algorithm

- unique key (unused)

6.1.7 Key usage purposes

End-user keys may only be used in accordance with the rules described in Section 1.4.

PostSignum Root CA keys must not be used to issue end-user certificates.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The CA implement physical and logical safeguards to prevent unauthorized certificate issuance.

6.2.1 Cryptographic module standards and controls

During operation, the private key of the CA is stored in an unencrypted form in an activated and configured cryptographic module (secure cryptographic module), which only one person needs to turn on and off.

To activate a cryptographic module (a secure cryptographic module) and to recover the private key after a disaster (or in another cryptographic module), the cooperation of several, but at least three people is required.

6.2.2 Sharing secrets

The private key of the CA is stored in an activated and configured cryptographic module (secure cryptographic module) during operation, which only one person needs to turn on and off.

To activate a cryptographic module (a secure cryptographic module) and to recover the private key after a disaster (or in another cryptographic module), the cooperation of several, but at least three people is required.

6.2.3 Private key storage

PostSignum VCA does not provide a service which would require a private key storage.

6.2.4 Private key backup

A private key of a certification authority is backed up in encoded form. When keys need to be restored in a new or in initialized module, cooperation of at least three person is required.

6.2.5 Private key archival

The private keys of the CAs in the PostSignum VCA hierarchy are not archived. After the ca's operation is terminated, the keys, including backups, are destroyed, of which a record is made.

6.2.6 Private key transfer into or from a cryptographic module

The CA private key is generated in a cryptographic module (a secure cryptographic module), and all unencrypted key operations are performed only in that module. The key leaves the cryptographic module only in encrypted form on backups created and protected in accordance with the provisions of the internal documents System Security Policy, Operational and Security Procedures and Audit and Archiving Policy (part of [SBP]).

The key is inserted into the original cryptographic module after the authentication of one worker with access to key backups and the cryptographic module.

The key is inserted into the new or initialized cryptographic module with backups after the authentication of two workers who do not have access to the private key backup and who do not have the right to activate the private key (start the CA process).

6.2.7 Private key storage on cryptographic module

Cryptographic module used to generate and store private keys of certification authorities (a tool used to create electronic signature) is active within the PostSignum VCA hierarchy, and complies with FIPS 140-2 Level 3 standards.

6.2.8 Method of activating private key

The private key of a certification authority is activated by an authorized operating staff in accordance with internal documents called System safety policy, and Operational and Security Procedures.

6.2.9 Method of deactivating private key

The private key of the certification authority is deactivated by the authorized operator in accordance with the internal documents System Security Policy and Operational and Security Procedures.

6.2.10 Method of destroying private key

The private key of a CA stored in a cryptographic module is destroyed by the means provided by the cryptographic module if the cryptographic module is to be temporarily used for other purposes, if the cryptographic module ceases to operate, or if the CA whose keys are stored in the cryptographic module ceases to operate. This destruction of the private key is carried out by an authorized operator in accordance with the provisions of the internal documents System Security Policy and Operational and Security Procedures or at the request of the CA Manager.

The destruction of the private key is carried out by putting the cryptographic module in an initialized state, when all cryptographic material (including the private key of the CA) is securely erased using the

mechanisms of the cryptographic module. destroying the private key includes deleting all backed up copies of the keys and disabling the cards used to access the keys.

6.2.11 Cryptographic module rating

Due to the fact that the cryptographic module used to store the CA's private key has successfully passed the FIPS 140-2 level 3 rating, it is not expected to contain material errors at the device design level. Nevertheless, it is continuously monitored whether an attack on this device has been discovered in order to respond to such a threat in a timely manner.

6.3 Other aspects of key pair management

6.3.1 Public key archival

Public keys in the form of end-user certificates are archived in accordance with an internal document called Auditing and archiving policy.

6.3.2 Certificate operational periods and key pair usage periods

The validity period of the certificate issued under this certification policy is specified in the certificate. The validity of the certificate must not exceed 385 days.

6.4 Activation data

The PostSignum VCA system uses activation data of various nature, such as access passwords, PINs and others. All aspects related to activation data, their generation, installation and use are described in the internal documents System Security Policy, Operational and Security Procedures and in internal operating documentation.

6.4.1 Activation data generation and installation

Activation data is usually created or entered by a worker who will continue to use it. Otherwise, when it is generated by another entity, random data meeting the general requirements for this data is used and an obligation is defined to change this randomly generated data immediately.

All activation data created must meet the requirements for its length or composition.

6.4.2 Activation data protection

All activation data must be protected from disclosure to an unauthorized person. All employees of the PostSignum VCA have the relevant obligations in this sense and are listed in the internal document System Security Policy.

6.4.3 Other activation data aspects

Other aspects related to activation data, their generation, installation and use are described in the internal documents System Security Policy, Operational and Security Procedures and in internal operational documentation.

6.5 Computer security Controls

6.5.1 Specific computer security technical requirements

For each component in the PostSignum VCA hierarchy, settings are defined to ensure the safety of the component at the technological level, which are based on the standards [ETSI EN 319 401], [ETSI EN 319 411] and [CA/B].

All RA operators issuing certificates to end users have access to the RA system provided only through multi-factor authentication.

6.5.2 Computer security rating

After construction, the PostSignum VCA system underwent an external security compliance check aimed at meeting the requirements specified in [CA/B].

6.6 Life cycle technical controls

6.6.1 System development controls

The implementation of the system was carried out according to the KeyStep methodology, which was created specifically for the design and implementation of large-scale PKI projects. The development of partial applications was carried out in accordance with the internal methodology of the development of the Czech Post.

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

6.6.2 Security management controls

The security of PostSignum VCA systems is verified by operational controls implemented within the established information security management system according to [ISO 27001], security compliance checks performed by ČP inspection staff and external audits carried out by an external entity.

6.6.3 Life cycle security controls

Part of the change management is also the evaluation of the impact of the changes on the security of the solution. In the case of large changes or after a series of smaller changes, a differential or repeated risk analysis is carried out.

6.7 Network security controls

Local networks of central workplaces (main and backup locations) containing central PostSignum VCA systems are separated from the internal network of ČP by a firewall. This firewall does not allow any communication from the internal network of ČP directly to the local network containing PostSignum VCA systems. All communication towards the local network of the central workplace is terminated at the dedicated DMZ.

In addition, the internal network of ČP is separated from all external networks, including the Internet , by its own firewall.

All communication outside the dedicated local network of central workplaces is encrypted.

Network security checks are performed continuously using security threat assessment tools. Once a year, a network security check is carried out.

In the event of a network security breach, the operation of all components of the certification authority is immediately stopped.

The network security of the certification authority's systems is in accordance with [CA/B].

6.8 Time-stamps

See chapter 5.5.5.

7 PROFILES OF CERTIFICATES, REVOKED CERTIFICATES AND OCSP

7.1 Certificate profile

PostSignum VCA issues certificates conforming to the X.509 standard. Certificate serial numbers are generated sequentially. The certificate profiles of the Root, subordinate authority, and the requester certificate profile are listed in the following subsections.Commercial domain certificate profile.

7.1.1 Version Number

PostSignum Public CA issues certificates compliant with the X.509 version 3 standard.

7.1.2 Content and extension items in the certificate

The items in the certificate correspond to RFC 5280.

7.1.2.1 Root CA Certificate

Name of the item	**Value/use flag**
Version	3 (0x2)
Serial Number	17:fd:91:4b:88:02:6b:6c:33:fa:fa:d1:ba:ad:86:cd:5e:79:5f:a9
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	29. 6. 2023 08:11:35 UTC
Not After	29. 6. 2038 08:11:35 UTC
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 extension see the table below*
Signature	*electronic seal provider of certification services*

Extensions in the 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	

7.1.2.2 Subordinate CA Certificate

Name of the item	**Value/use flag**
Version	3 (0x2)
Serial Number	60:68:1a:67:1b:68:f4:40:ed:c7:34:be:fe:c0:05:0d:7b:33:a9:49
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	30. 1. 2024 11:25:29 UTC
Not After	30. 1. 2034 11:25:29 UTC
Subject	
(C) countryname	CZ
organizationIdentifier	NTRCZ-47114983
About organisationName	Česká pošta, s.p.
CN commonName	PostSignum Public ECC R1 CA 2
Subject Public Key Info	
Algorithm	ECDSA
SubjectPublicKey	*The public key*
Extensions	*certificate extension see the table below*
Signature	*electronic seal provider of certification services*

Extensions in the 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	
Extended Key Usage	id-kp clientAuth id-kp-serverAuth	No
CertificatePolicies		No
Policy Identifier	2.5.29.32.0 (Any)	
User Notice	Tento certifikat pro elektronickou pecet byl vydan v souladu s narizenim EU c. 910/2014.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/	

7.1.2.3 Certificate of Subscriber

Entry	Value	Note	
Version	3 (0x2)	Items are mandatory in all issued certificates and cannot be changed.	
Serial number	certificate serial number assigned by the certification authority		
SignatureAlgorithm	ECDSA With SHA384		
Issuer			
C countryName	CZ	Items are mandatory in all issued certificates and cannot be changed.	
OID 2.5.4.97 organizationIdentifier	NTRCZ-47114983		
O organisationName	Česká pošta, s.p.		
CN commonName	PostSignum Public ECC R1 CA 2		
Validity			
Not Before	Start of validity of issued certificate (UTCTime)	Items are mandatory in all issued certificates and cannot be changed.	
Not After	End of validity of issued certificate (UTCTime)		
Subject			
C countryName	Country code from the customer's registered office address	mandatory	The data is supplemented on the basis of data in public registers

ST stateOrProvinceName	The name of the country from the address of the customer's registered office	optional	The data is supplemented on the basis of data in public registers
L localityName	The name of the municipality from the address of the customer's seat	mandatory	The data is supplemented on the basis of data in public registers
STREET streetAddress	The street name from the customer's address	optional	The data is supplemented on the basis of data in public registers
OID 2.5.4.97 organizationIdentifier	Contains the organization's ID number according to international standards in the form: NTRxx-IČO of the organization	mandatory	The data is supplemented on the basis of data in public registers xx is the country code, corresponds to item C (countryName)
O organisationName	The name of a legal entity or a natural person doing business	mandatory	The data is supplemented on the basis of data in public registers
serialNumber	Unique customer identifier assigned by the certification service provider in the form: Dnumber	mandatory	
Subject Public Key Info			
Algorithm	ECDSA (P-256, P-384, P-521)	Items are mandatory in all issued certificates and cannot be changed.	
SubjectPublicKey	Public key with ECDSA Algorithm (P-256, P-384, P-521)		
Extensions	Certificate extension according to the table below		
Signature	Electronic seal of the certification service provider		

Extensions in the certificate:

Entry	Value	Note	
Authority Key Identifier			
Key Identifier		Items are mandatory in all issued certificates and cannot be changed.	
Subject Key Identifier			
Subject Alternative Name			
dNSName	DNS name Up to 20 DNS names can be entered in the certificate.	mandatory	The certificate must contain at least one dNSName record
Key Usage (critical extension)			
DigitalSignature		Items are mandatory in all issued certificates and cannot be changed.	
Extended Key Usage			
KeyPurposeID	id-kp-serverAuth	Items are mandatory in all issued certificates and cannot be changed.	
KeyPurposeID	id-kp-clientAuth		
Certificate Policies			
Policy Information [1]			

Policy Identifier	The OID of this certification policy	Items are mandatory in all issued certificates and cannot be changed.
Policy Information [2]		
Policy Identifier	2.23.140.1.2.2 organization-validated	Items are mandatory in all issued certificates and cannot be changed. The exception is certificates issued to a natural person doing business, which do not contain this identifier.
CRL Distribution Points		
URI	http://crl.postsignum.cz/crl/pspubliceccr1ca2.crl	Items are mandatory in all issued certificates and cannot be changed.
URI	http://crl2.postsignum.cz/crl/pspubliceccr1ca2.crl	
URI	http://crl.postsignum.eu/crl/pspubliceccr1ca2.crl	
AuthorityInfoAccess		
accessMethod URI	id-ad-caIssuers (1.3.6.1.5.5.7.48.2) http://crt.postsignum.cz/crt/pspubliceccr1ca2.crt	Items are mandatory in all issued certificates and cannot be changed.
accessMethod URI	OCSP (1.3.6.1.5.5.7.48.1) http://ocsp.postsignum.cz/OCSP/ECCVCA2/	
Signed Certificate Timestamp		
The entry conforms to RFC 6962 and contains the timestamp and ID of Certificate Transparency logs (CT logs) that contain the issued precertificate that corresponds to the issued domain certificate. The pre-certificate is sent to at least 3 CT logos. The list of CT logs to which precertificates are sent is given on the provider's website.		

7.1.2.4 OCSP Responder Certificate Profile

Entry name	Value / index
Version	3 (0x2)
Serial Number	60:68:1a:67:1b:68:f4:40:ed:c7:34:be:fe:c0:05:0d:7b:33:a9:49
SignatureAlgorithm	ECDSA With SHA384
Issuer	
C countryName	CZ
organizationIdentifier OID 2.5.4.97	NTRCZ-47114983
O organisationName	Česká pošta, s.p.
CN commonName	PostSignum Public ECC R1 CA 2
Validity	
Not Before	30. 1. 2024 11:25:29 UTC
Not After	30. 1. 2034 11:25:29 UTC
Subject	
C countryName	CZ
organizationIdentifier OID 2.5.4.97	NTRCZ-47114983
O organisationName	Česká pošta, s.p.
OU organizationalUnitName	PostSignum Services
CN commonName	PostSignum ECC VCA 2 - OCSP Responder X *(X is a number indicating a specific OCSP responder)*
Subject Public Key Info	
Algorithm	ECDSA (P-384)
SubjectPublicKey	Public key with ECDSA Algorithm (P-384)
Extensions	*certificate extension according to the table below*
Signature	*electronic seal of the certification service provider*

Extensions in the certificate:

Entry name	Value / index	Critical yes/no
Authority Key Identifier		no
Key Identifier	*used*	
Subject Key Identifier	*used*	no
Key Usage		yes
DigitalSignature	yes	
NonRepudiation	no	
KeyEncipherment	no	
DataEncipherment	no	
KeyAgreement	no	
KeyCertSign	no	
CRLSign	no	
Extended Key usage		no
KeyPurposeID	id-kp-OCSPSigning	
CertificatePolicies		no
Policy Information		
Policy Identifier	OID of this certification policy	
AuthorityInfoAccess		no
accessMethod URI	id-ad-caIssuers (1.3.6.1.5.5.7.48.2) http://crt.postsignum.cz/crt/pspubliceccr1ca2.crt	
OCSP No Check	id-pkix-*ocsp-nocheck*	no

7.1.2.5 All Certificates

PostSignum VCA will not issue a certificate that contains a different keyUsage flag, extKeyUsage value, certificate extension, or other data not specified in sections 7.1.2.1, 7.1.2.2, or 7.1.2.3. PostSignum VCA reserves the right to insert items into the certificate on the basis of the specified profiles in the event of a change in technical standards.

7.1.3 Cryptographic algorithm object identifiers (hereinafter "OID")

PostSignum VCA uses the following algorithms:
ecdsa-with-SHA384 (OID 1.2.840.10045.4.3.3) for applicant certificates
ecdsa-with-SHA512 (OID 1.2.840.10045.4.3.4) for root and subordinate authority certificates

7.1.4 Name forms

The rules for writing names and titles are given in chapters 3.1.1 to 3.1.4. Entries in the certificate must not separately contain the following characters: ',' (comma), '-' (dash) and ' ' (space).

The FQDN in the CN or SAN entry must not contain the '_' (underscore) character.

7.1.5 Name constraints

No "Name Constraints" are applied in PostSignum VCA.

7.1.6 Certificate policy OID

Each end requester certificate contains a reference to the policy under which the certificate was issued (policy OID). The OID of this policy is given in chapter 1.2.

The certificate also contains the OID 2.23.140.1.2.2 (organization-validated) according to the [CA/B] specification for certificates with verified organization identity.

The Root and subordinate CA certificates is listed OID 2.5.29.32.0 (Any Policy).

7.1.7 An extending item "Policy Constraints"

An extending item "Policy Constraints" is not used in PostSignum VCA.

7.1.8 Syntax and semantics of the extending item called "Policy Qualifiers"

The extending item "Policy Qualifier" contains a link to a webpage of the provider where the relevant certification policy may be obtained - based on which the certificate was issued.

7.1.9 Writing method of a critical extending item called "Certificate Policies"

Writing method of "Certificate Policies" is specified in Chapter 7.1.2.3. This item is not marked as critical.

7.2 A profile of a list of revoked certificates

CRL profile

Item name	**Value/Usage index**
Version	2 (0x1)
Issuer Distinguished Name	
C countryName	CZ
Related to OID 2.5.4.97: organizationIdentifier	NRTRCZ-47114983
O organisationName	Česká pošta, s.p.
CN commonName	PostSignum Public ECC R1 CA 2
Validity	
This Update	Validity date of issued CRL (UTCTime)
Next Update	CRL (UTCTime) issued expiration
RevokedCertificates	repeating entry for each invalidated certificate
UserCertificate	serial number of the revoked certificate
RevocationDate	date and time of invalidation
CrlEntryExtensions	extension of the CRL entry according to the table below
CrlExtensions	CRL extension according to the table on Chapter 7.2.2.
SignatureAlgorithm	ECDSA With SHA512
Signature	electronic seal of the provider of certification services

7.2.1 Version number

PostSignum Public CA issues lists of revoked certificates complying with X.509, version 2 standard.

7.2.2 CRL and CRL entry extensions

Extension in CRL

Extension item name	Value/Usage index	Critical yes/no
CrlEntryExtensions Item Extension		
DisabilityDate	The date and time of the event leading to the revocation of the certificate; optional extension	no
ReasonCode	the reason for the certificate revocation	no
CRL (CrlExtensions) extensions		
Authority Key Identifier		no
Key Identifier	used	
AuthorityCertIssuer	used	
AuthorityCertSerialNumber	used	
CRL Number	the CRL serial number assigned by the CA	no

7.3 OCSP Profile

OCSP conforms to RFC 6960.

OCSP request structure – OCSP Request Data

Item name	Description	Value/Usage Flag
Version	OCSP version (required)	1
Requestor List		
Certificate ID	data about the queried certificate – the item can be repeated	
Hash Algorithm	request hash	SHA-1
Issuer Name Hash	hash calculated from the name of the certificate issuer	
Issuer Key Hash	hash calculated from the public key fingerprint of the certificate issuer	
Serial Number	serial number of the requested certificate	
Request Extensions		
OCSP Nonce	Random, once generated number (64 bits). If it is contained in the request, then the reply also contains it. (optional)	

The OCSP request may not be sign.

OCSP response structure – OCSP Response Data

Item Name	Description	Value/index
OCSP Response Status	Natural number indicating the status of the response	0 – successful 1 – malformedRequest 2 – internalError 3 – tryLater 6 – unauthorized
Response Type	Basic OCSP Response	
Version	OCSP protocol version	1
Responder Id	OCSP server signing certificate DN	
Produced At	OCSP server response signature time	

Responses:		
Certificate ID	The data correspond to the data in the application	
Cert Status	The status of the certificate: good – certificate is valid revoked – certificate is invalidated unknown – the status of the certificate is unknown (e.g. such a certificate is does not exist)	0 – good 1 – revoked 2 – unknown
Revocation Time	The time of certificate revocation. The item is listed only if the Cert Status=revoked	
Revocation Reason	The reason of certificate revocation. The item is listed only if the Cert Status=revoked	The CRLReason contain a value permitted for CRLs, as specified in Section 4.9.1.1.
This Update	.The time when the response status is indicated	
Response Extensions		
OCSP Nonce	Random, once generated number (64 bits). If it is included in the application, then it contains a reply. (optional item)	

7.3.1 Version number

The OCSP protocol version is 1.

7.3.2 Extension items OCSP

The extension in the OCSP request and response is listed in the tables in Chapter 7.3.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

In the PostSignum VCA environment, inspections are regularly carried out at least 1 time per year. The audited periods always follow each other. These regular checks may be supplemented by additional checks as necessary, inter alia on the basis of a decision of the CA Manager, the management of the Czech Post or the internal audit of the Czech Post.

Part of the inspection is a check of security compliance.

8.2 Identity/qualifications of auditor

Internal control is carried out by employees familiar with PKI issues and training for the task. The personnel performing the inspection are referred to as CA Auditors in the VCA documentation.

The CA's audit is performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural person or Legal Entities that collectively possess the following qualifications and skills:

1. Independence from the subject of the audit;

2. The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme (see Section 8.4);

3. Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;

4. For audits conducted in accordance with any one of the ETSI standards accredited in accordance with ISO 17065 applying the requirements specified in ETSI EN 319 403;

5. Bound by law, government regulation, or professional code of ethics

8.3 Assessor's relationship to assessed entity

Internal control is carried out by employees of the Czech Post who do not participate in the operation of the PostSignum VCA certification authority.

External control may only be carried out by a person or company independent of the Czech Post.

8.4 Topics covered by assessment

The audit is carried out in accordance with the standards [ETSI EN 319 401], [ETSI EN 319 411] (the latest version of the referenced ETSI documents should be applied) Part 1 – 3 in accordance with Mozilla and CCADB requirements.

8.5 Communication of results

The results of the inspections are handed over to the CA Manager, who will ensure the correction of the identified deficiencies.

If an incident is detected (e.g., a mis-issued certificate, in general states that conflict with any applicable standards governing this certification policy), the requirements set forth at wiki.mozilla (CA/Responding To Incident) are followed.

8.6 Communication of evaluation results

A signed written report is prepared on the performance of each audit in accordance with [CA/B] according to the provisions provided on this website https://www.ccadb.org/policy#51-audit-statement-content. The report is forwarded to the Manager of the CA. He will ensure its distribution and discussion.

In the event that a separate audit opinion is included in the report, the CA Manager may decide to publish it.

The audit report is published on its website by the audit company.

8.7 Self-audits

In the PostSignum VCA environment, internal checks are regularly carried out on a random sample (min. 3% of issued certificates) at least 1 time in 3 months.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

The price for provided certification services is specified in the contract concluded between the customer and provider of certification services and it is based on the currently valid pricelist. The price for issued certificates may also be included in the price of other service provided by the Czech Post.

9.1.2 Certificate access fees

The service of accessing the certificate on the list of issued certificates is provided free of charge.

9.1.3 Revocation or status information access fees

Certificate revocation service and information about certificate status is provided free of charge.

9.1.4 Fees for additional services

Prices for other PostSignum VCA services are specified in the pricelist of the Czech Post.

9.1.5 Refund policy

No provisions in this chapter.

9.2 Financial responsibility

9.2.1 Insurance coverage

The Czech Post carries a damage liability insurance to cover possible damages.

9.2.2 Other assets and guarantees

The assets of the Czech Post are listed in the Annual Report. The annual report is filed in the Commercial Register at the Municipal Court in Prague under file number A7565.

The annual report can also be viewed on the website of the Czech Post (www.ceskaposta.cz).

9.2.3 Insurance policy or guarantees for end-entities

PostSignum VCA does not provide this service.

9.3 Confidentiality of business information

Based on applicable legal regulations and within maximum possible scope, each involved party is obligated to protect from unauthorized disclosure information, circumstances and facts learned in connection with the fulfilment of the contract describing provision of certification services, including information and facts which were not exclusively marked in written form as shareable.

9.3.1 Scope of confidential information

Confidential and sensitive information and facts are regarded all information, except for those contained in documents marked as "Public".

9.3.2 Information not within the scope of confidential information

The following information:

- have become public knowledge without the fault of the receiving Party, either intentionally or through omission,
- the receiving party is legally at its disposal prior to the conclusion of the contract for the provision of certification services, unless such information has been the subject of another previously concluded information protection agreement between the parties involved, or unless such information is in itself a trade secret,
- they are the result of a procedure in which the receiving party reaches them independently and is able to substantiate this with its records or with the confidential information of a third party,
- after the conclusion of a contract for the provision of certification services, a third party shall provide the receiving party which does not obtain such information directly or indirectly from the party that owns it or does not obtain it in an unlawful manner as the receiving party would know or should have known,
- are listed in the commercial certificate if the subscriber has given his consent to its publication.

9.3.3 Responsibility to protect confidential information

Responsibility for the processing of confidential information in PostSignum VCA lies with the Czech Post, as a provider of certification services, all its employees and contractual partners.

9.3.4 Providing sensitive information for judicial or administrative purposes

All information processed in PostSignum VCA is made available to authorities authorized by law in cases where required by law and to the extent required by law. Disclosure of the information shall be ensured by the CA Manager after the authorities authorised by law have demonstrated their authority in the manner customary in such cases.

9.4 Privacy Policy

The Czech Post ensures the protection of personal data of person to whom it gains access when providing certification services. The privacy policy is contained in the General Terms and Conditions of Certification Services and is based on the [GDPR].

9.4.1 Personal data

Personal data is the identified information or identifiable natural person. Identifiable natural person is natural person whom can be identified directly or indirectly.

9.4.2 Responsibility to protect personal data

The Czech Post - as the provider of certification services and all its employees and contractual partners are liable for protection of personal data processed in PostSignum VCA systems and within the applicable scope specified in [GDPR].

9.4.3 Information not deemed private

In this area, the relevant provisions of the [GDPR], generally binding legal regulations and internal regulations of the Czech Post regulating the issue of personal data protection are followed.

9.5 Intellectual property rights

This certification policy and all other related documents are protected under copyrights owned by the Czech Post and represent an important know-how of the Czech Post. Further, the Czech Post is also the owner of exclusive rights regarding the information system necessary to operate PostSignum VCA, and relevant to the structure, organization, screen appearance and to the provider webpage contents.

PostSignum grants permission to reproduce and distribute this document, provided that they are reproduced and distributed in full.

9.6 Representations and warranties

9.6.1 Representation and Warranties of CA

The Czech Post guarantees that it will fulfill all obligations imposed by this certification policy and the provisions of relevant legal regulations and standards, especially [CA/B].

The Czech Post provides the above guarantees for the entire duration of the contract for the provision of certification services.

9.6.2 Representation and Warranties of RA

In the provision of registration authority services, the Czech Post as a provider of certification services cannot be represented by a third party.

9.6.3 Subscriber representations and warranties

The customer (certificate subscriber) or applicant is responsible for fulfilling all the obligations of customers and applicants for the certificate specified in this certification policy.

9.6.4 Relying party representations and warranties

The related party guarantees that all obligations of the related party existing prior to the use of the qualified certificate will be properly fulfilled. These obligations and responsibilities are specified in this certification policy, in particular in chapter 4.5.

9.6.5 Representations and warranties of other participants

Entities that are directly involved in the operation of the PostSignum VCA on the basis of a contractual relationship with a certification service provider are obliged to comply with the provisions of the certification policy, certification practice statement, system security policy and other internal documents.

9.7 Disclaimer of guaranties/warranties

Guaranties specified in chapter 9.6 above are exclusive guaranties/warranties offered by the Czech Post and no other warranties are provided.

The Czech Post is not liable for defects in provided services occurred due to incorrect or unauthorized use of services provided under a contract for provision of certification services caused by the provider, in particular, for defects occurred due to operations conducted contrary to requirements specified in this certification policy or for defects occurred due to force majeure events including temporary interruptions of telecommunication services etc.

9.8 Limitation of liability

Czech Post is not liable for damage resulting from the use of a commercial certificate if the subscriber or the relying person fails to comply with the restrictions on its use specified in this certification policy and published on the Provider's website .

Czech Post is not liable for damage resulting from the use of a commercial certificate in the period after receipt of the request for its revocation if the Czech Post meets the deadline for publication of the invalidated commercial certificate on the list of invalidated certificates (CRL), specified in Chapter 2 of 1.5.

Czech Post will continuously verify, with increasing operational experience in the provision of certification services, whether the conditions for limiting The liability of Czech Post set out in this provision correspond to the usual market conditions and the reasonable commercial risk of Czech Post.

The provisions of this Article shall survive termination of this certification policy.

9.9 Indemnities

Unless specified otherwise in valid legal regulations, the Czech Post is responsible and answers to the subscriber of the certificate for damages caused by a failure of the Czech Post to observe its obligations specified in the contract for provision of certification services.

9.10 Term and Termination

9.10.1 Term

The period of validity of this certification policy is from the date of issue specified in Section 1.2.

9.10.2 Termination

The validity of this document shall be terminated if

- replaced with a newer version, or
- the Czech Post stops providing services as the provider of certification services.

9.10.3 Effect of termination and survival

Should this document be terminated due to termination of services, then restrictions and provisions specified in Chapter 9. related to commercial and legal issues shall remain valid.

9.11 Individual notices and communications with participants

9.11.1 Communication with the provider of certification services

All information the provider of certification services wishes to share with customers shall be published at the webpage of the provider or posted on bulletin boards at individual workplaces of registration authorities. Important information, such as a suspicion that a key of certain certification authority in the PostSignum hierarchy has been compromised, shall be posted by the provider of certification services at his webpage and at the same time, a written or electronic notification shall be sent to relevant customers.

Customer – organization or a natural person performing business activities communicate with the provider certification services through an authorized person. Authorized person deals with the workplace of the registration authority or communicates with CA business locations.

Communication between the customer and provider certification services may also be done electronically. If there is a legal requirement to prove a certain electronic communication, it must be related to certificates issued by PostSignum VCA, or by other authority which the Czech Post selects as credible. Czech Post and the customer shall be agreed in writing in advance about accept of the certificate in form of amendment to the contract.

9.11.2 Communication within PostSignum VCA system

Communication in the PostSignum VCA system is governed by the valid regulations of the Czech Post and internal documents of the PostSignum VCA task.

9.11.3 Communication language

All communication in the PostSignum VCA system must take place in the Czech language, unless both parties agree otherwise.

9.12 Amendments

9.12.1 Procedure for amendment

Change management procedures are specified in the Chapter 1.5.

9.12.2 Notification mechanism and period

The issuance of a new certification policy with changed OID (see the following chapter), will be announced under the News column at the webpage of the provider.

Should guarantees provided by used cryptographic algorithms be weakened and require imminent intervention, all certificate subscribers] and subjects which have concluded contracts directly related to provision of certification services will be informed about it in written form or electronically. This notification will be published at the webpage of the provider and at all offices/workplaces of PostSignum VCA registration authority. Other necessary actions described in the certification policy will follow this announcement.

If there is no imminent danger of delay this announcement shall be done at least 10 business days before the new certification policy becomes valid.

9.12.3 Circumstances under which OID must be changed

The Czech Post has assigned object identifiers (OID) used by PostSignum VCA environment based on its internal regulations.

OID are assigned:

- to PostSignum Root QCA,
- to each certification authority to which PostSignum Root QCA issued a certificate, in particular, to PostSignum Public(V) CA,
- to each certification policy based on which certificates are issued under PostSignum VCA.
- OID are not assigned to registration authorities or to the Certification Practice Statement.
- Any change in the certification policy requires a change in the document version and change of OID.

9.13 Dispute resolution provisions

In case of any dispute between PostSignum VCA and customer, the customer may turn to

- CA Manager, or
- to a registration authority (in the form of a complaint request).

If none of the above specified instances solves the dispute, the dispute between the customer and PostSignum VCA will be solved locally by the relevant court of law which has the applicable jurisdiction.

9.14 Governing Law

Activities of PostSignum VCA are governed by the laws of the Czech Republic.

9.15 Compliance with Applicable Law

The activities of PostSignum VCA are in accordance with the legal order of the Czech Republic.

The relationship between the Czech Post and the customer is regulated by a written contract on the provision of certification services.

9.16 Miscellaneous provisions

9.16.1 Entire Agreement

No provisions available in this Chapter.

9.16.2 Assignment

The Czech Post may transfer a part or all responsibilities of the provider of certification services over to another legal entity which guarantees the same level of security and provided services. Relations between the Czech Post and this entity shall be specified in a separate contract. Responsibilities and obligations of the Czech Post, as the provider of certification services, shall remain unaffected by this contract.

Partial acceptance or acceptance of all obligations of the provider of certification services by a third party does not limit services or guaranties provided by the Czech Post in terms of customers and relying parties.

9.16.3 Severability

The Contract for the Provision of Certification Services concluded between the Customer and the Czech Post remains valid even if any part thereof ceases to be valid, unless both parties agree otherwise.

If there is a conflict between this certification policy and [CA/B], the provisions of [CA/B] shall apply.

9.16.4 Disclaimer

No provisions available in this chapter.

9.16.5 Force Majeure

Czech Post is not responsible for breaches of its obligations caused by force majeure, such as large-scale natural disasters, strikes, civil unrest or a state of war.

9.16.6 Accessibility for the people with disabilities

The trust services provided and the end-user products used in providing those services are accessible to person with disabilities. More detailed information regarding the provision of services to these person 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 provisions

9.17.1 Outline of a Set of Provisions

When creating Certification policies and Certification Practice Statement the following documents were taken into consideration:

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

[eIDAS] REGULATION (EU) No. 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/ES

[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 at 27 of April 2016 on the protection of natural person 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] CSN ISO/IEC 27001:2014 Information Technologies – Security Techniques - Information Security Management Systems - Requirements

[RFC 6960] Internet X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP

[RFC 6962] Certificate Transparency

[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 No. 297/2016 Coll., trust services for electronic transactions as amended

9.17.2 References and literature

[VOP] General Terms and Conditions of Certification services.