Certification practice statement for the commercial certificate authority Česká Pošta, s.p. PostSignum VCA

Version 4.1.0

Evidence of revisions and changes

Version	Revison date	The reason and a description of the changes	The author of the	Approved by the
1.0	31.12.2004	The first version	PCA ČP	PAA ČP
1.3	7.11.2005	Document updates	PCA ČP	PAA ČP
1.4	1.9.2006	Document updates	PCA ČP	PAA ČP
1.5	1.6.2010	Document updates	PCA ČP	PAA ČP
2.0	1.7.2012	Document updates	PCA ČP	PAA ČP
3.0	10.1.2014	Add OCSP	PCA ČP	PAA ČP
3.1	10.2.2016	Completion of the registration process	PCA ČP	PAA ČP
3.1	1.9.2020	Document revision without version change - minor changes in references to documents and legislation	PCA ČP	
4.0.0	1.9.2021	Add a new way of authentication through remote identification and minor changes.	PCA ČP	PAA ČP
4.0.1	15.8.2022	Document revision without changes	PCA ČP	
4.0.2	15.8.2023	Document revision without changes	PCA ČP	
4.1.0	7. 5. 2024	Added ECC algorithm	PCA ČP	PAA ČP

Table of Content

1 INTRODUCTION

This certification practice statement activities in the hierarchy of certification authorities PostSignum VCA relate to the issuance of commercial certificates in accordance with all applicable certification policies.

1.1 Overview

Česká pošta, s. p. (even the Czech post or ČP) as a provider of certification services established a two-level hierarchy of certification authorities PostSignum VCA, which are operated by the CA issuing commercial certificates. The root of this hierarchy is the PostSignum Root QCA, issuing qualified certificates for electronic seal to subordinate CAs. The hierarchy of certification authorities PostSignum Root QCA formed, the subordinate CA PostSignum Public CA and perhaps other subordinate CAs, which so explicitly specifies the Czech post is called the PostSignum VCA (VCA for short) and is used to issue commercial certificates to end users.

This certification practice statement (CPS only) the following or elaborates on selected topics of individual certification policies (and CP) and adjusts so the issue of commercial certificates in the hierarchy of PostSignum VCA. In the event of a conflict between the CPS and the certification policy that refers to this CPS, certificate policy applies.

Certification authority PostSignum CA was built and is operated in accordance with the generally accepted standards in the field of PKI.

The CPS provides factual information that describes the

- the procedures to be used in the provision of certification services (or links to documents describing these procedures),

the technologies, processes and operational conditions that enable the provision of certification services.

The procedures outlined in this CPS, along with the technologies and processes described in other documents set forth the procedures and rules leading to ensure the credibility and integrity of the certification authorities PostSignum VCA in the provision of certification services, as well as trust certificates that are issued by PostSignum VCA, and from the time of issue of the certificate until it expires.

1.1.1 Certification services provided by PostSignum VCA

Certification services offered by certification authority PostSignum VCA are stated in the relevant certification policies.

For issuing certificates to subordinate CAs in the hierarchy of PostSignum is created a special policy of PostSignum Root QCA.

1.2 Document Name and Identification

The name of the document	Certification practice statement for PostSignum VCA
Version of the document	4.1.0
The status of the	final
PostSignum Root QCA OID	2.23.134.1.4.2.1
The OID of this CPS	It is not allocated
Release date	7. 5. 2024
Effective date	17. 5. 2024
Revision date	
The period of validity	Until further notice or until the date of termination of service authorities PostSignum VCA.

1.3 PKI Participants

This certification practice statement applies to

- all certification services that are provided by the subordinate CA from the hierarchy of PostSignum VCA,
- all certificates issued by any subordinate CAs in the hierarchy.

1.3.1 Certification authority ("CA")

PostSignum VCA is made up of a hierarchy of CAs. Is an umbrella institution within which operates other certification authorities.

Services are provided by the CAs provider of certification services.

Contact details of the certification services provider are listed and published in every certificate policy, according to which the CA issues certificates, and on the website of the provider.

1.3.1.1 PostSignum Root QCA

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

Postsignum Root QCA provides the following services (in accordance with documented operating procedures):

- generate your own keys,
- release of self-signed certificate for an electronic seal,
- publication of the self-certificate for an electronic seal on the website of the provider and other appropriate means,
- providing information on issued certificates,

- determination of the naming conventions for the subordinate certification authority, in accordance with the standard X 501 or traceable standard X 520,
- paperwork associated with the registration of applicants for a certificate
- release certificates for the electronic seal for subordinate CAs,
- revocation of certificates according to the rules laid down in the certification policies,
- publication of the certificate revocation lists on the website of the provider

1.3.1.2 Subordinate certification authority

The main task of subordinate CAs in the hierarchy of PostSignum is to issue and manage certificates for customers of the Czech post in accordance with defined certification policies.

Certification authority PostSignum included in the hierarchy, i.e. PostSignum Public CA and any other subordinate CAs, which the Czech post explicitly specifies, in particular, provide these services (in accordance with documented operating procedures):

- generate your own key pair,
- request a certificate for the PostSignum Root QCA,
- publication of all certification policies under which the certificates are issued on its Web site,
- paperwork associated with the registration of applicants for a certificate
- release of qualified certificates or commercial certificates to end entities (entities that are not CAs), registration authority and technological components that are part of the CA,
- revocation of certificates according to the rules laid down in the certification policies,
- publication of issued certificates, with the consent of the subscriber of the publication gave the provider's website,
- publication of the certificate revocation lists on the website of the provider.

1.3.2 Registration authorities ("RA")

Services are provided by RA certification services provider or an external entity pursuant to a contract with the provider of certification services.

Registration authority provide the services referred to in the relevant certificate policy.

1.3.2.1 Stationary registration authority

Stationary registration authority is operated by the provider of certification services to business offices and focal points of the public administration of the Czech post or an external entity in a defined site.

1.3.2.2 Mobile registration authority

The mobile registration authority is mobile workplace, operated by the Czech post or external body.

1.3.2.3 Workplace for the receipt of applications for the issue of a subsequent certificate

Electronic applications for subsequent certificate (data exchange for authentication of electronic seals, or tags) are accepted at address

E-mail: podatelna.postsignum@cpost.cz

1.3.2.4 Nonstop revocation service

The service is operated 24 hours a day, is intended solely for the reception of applications for revocation of the certificate mainly outside the working hours of registration authorities of the Czech post. The contact details are

Phone: 954 303 303

E-mail: postsignum@cpost.cz

Web site: https://www.postsignum.cz/

1.3.2.5 Central registration authority

It is a system that ensures the issuance of a certificate to applicants who have proven their identity through remote identification.

1.3.3 Subscriber

Subscriber of certificates and signing or sealing person who applied for the issue of the certificate and that the certificate was issued.

1.3.3.1 Customers

The PostSignum VCA customer is a natural or legal person who enters into a written contract for the provision of certification services with the Czech Post. Certificates are issued:

- organizations that concluded with the Czech post contract for the provision of certification services,
- natural persons (individuals), which concluded with the Czech post contract for the provision of certification services.

The Czech post, the customer at the moment of issue of the certificate the applicant becomes the subscriber of the certificate.

1.3.3.2 Authorized person

The authorized person is the person defined by the customer – the organization when concluding the contract on the provision of certification services. This person acts towards certification services provider as a customer's representative, determines in particular, employees who have the right to apply for a certificate with PostSignum VCA and which certificate they have the right to apply for (including the type of certificate - policy according to which the certificate will be issued).

In the case of non-business natural person (citizens), the customer automatically becomes the authorized person.

1.3.3.3 Applicant

The applicant for the certificate is an employee of the customer – the organization or individual who has the right to apply for a certificate under any of the applicable certificate policies.

1.3.4 Relying parties

The relying party is any natural or legal person relying on a 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

1.3.5.1 External participating entities

In the operation of the CA is also particularly involved the hardware, software and data connection suppliers:

1.3.5.2 Internal participating entities

The Commission for certification policy CP:

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

The Commission for certification policy CP provides:

- establishes the Team for creating the certification policies ČP, directs and controls his activity,
- approve the new certification policies, and in the case of politician Root QCA decides on their publication,
- maintains and checks for an existing policy,
- is responsible for the consistency and integrity of the policies,
- approve any changes to the CPS,
- is responsible for publishing the current version of CPS,
- is responsible for the consistency and integrity of the CPS.

The Commission for certification policy CP can be contacted at:

paa.postsignum@cpost.cz

Certification policies team CP:

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

1.4 Certificate usage

1.4.1 Appropriate Certificate Uses

Certificates issued by PostSignum VCA can be used:

- to validation the electronic signature
- to encryption
- to server identification
- to client identification

1.4.2 Prohibited Certificate Uses

Restrictions on use of the certificate is set out in the relevant certificate policy. In General, however, that the certificate issued by PostSignum VCA certification policies are not primarily intended for communication or transactions in areas with an increased risk of damage to persons or property, such as chemical plants, air traffic, traffic nuclear facilities, etc. or in connection with security and System State.

1.5 Policy Administration

For initiating changes in the certification detailed directive or initialize a new certification practice statement is the responsibility of the Manager of CA. The forwards the request to the team for creating the certification policies (PCA CP).

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

The new version of the certification practice statement will be published in the form of an internal directive of the Czech post. PAA ČP decides whether it is necessary to publish information about new version of certification practice statement also another form, or both.

In the case of upcoming major changes, i.e. the certification policies. changes that have an impact on the applicability of a certificate, warranty, liability or processes (and which throws a change OID), the upcoming amendment is published in the manner specified in the applicable certificate policy.

1.5.1 Organization Administering the Document

The management of this certification carrying out the directive is the responsibility of the provider of certification services, i.e. the Czech post, represented for this purpose by the Manager of the CA.

1.5.2 Contact person

The contact person in case management of this certification practice statement is Manager of the CA. More information can be obtained at the email address:

manager.postsignum@cpost.cz , or

on the website of the provider:

www.postsignum.cz

1.5.3 Person Determining CPS Suitability for the Policy

The management of this certification practice statement for compliance with the certification for compliance with the policies or practices of other certification service providers corresponds to the Manager of the CA.

1.5.4 CPS Approval Procedures

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

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

- When the appearance of a new type of certificate
- change of PostSignum VCA (e.g. changing procedures) which will affect the contents of those documents,
- if during the inspection of the surrounding environment of PostSignum VCA have been identified changes to the requirements of these documents.

For initiating changes in certificate policy or CPS or initialize a new certificate policy or CPS is the responsibility of the Manager of CA. In the preparation of changes in certificate policy or CPS will decide in CA Manager based on the list of identified changes, how the planned changes will be published. The Commission for certification policies as needed appoint PCA ČP, whom the Manager then passes the list of CA required changes to incorporate.

Drawn up by policy or CPS shall provide the Manager of CA for approval to the Commission for certification policy, which then confirms the OID (only policy) and assigns the version number.

1.6 Definitions and Acronyms

Certificate Online - The application used to issue a certificate through remote identification

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

The certificate for electronic seal- certificate for legal persons within the meaning of [eIDAS]

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

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

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

DMZ - demilitarized zone

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

The Commission for the CP certification policies (Policy Approval Authority - PAA) -the authority in whose jurisdiction is to approve, monitor and maintain policy and CPS, which governs the activities of certificate authority.

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

Qualified certificate for electronic signature – a qualified certificate as defined in [eIDAS].

Qualified certificate for the electronic seal – qualified certificate, as defined in [eIDAS].

Qualified certificate for the authentication of websites - the qualified certificate as defined in [eIDAS]

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

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

Mobile registration authority - mobile workplaces of Czech post, whose basic task is to take applications for issue of the certificate or its revocation, check the identity of applicants, then accept or reject the request and pass it to the certificate issued to the applicant or the certificate void.

Subsequent certificate – a certificate issued on the basis of the concluded contract as a replacement for already issued certificate of PostSignum certification policy provides for appropriate; that details of the original certificate may be in a subsequent certificate changed. For the release of the subsequent certificate is not required by a physical visit to the registration authority.

NIA - The national point for identification and authentication is the public administration information system. The system is designed for secure and guaranteed remote user authentication.

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

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

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

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

Validation the registration authority – provides registration authority services.

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

Creator of a seal - person as defined in [eIDAS]

PKI - Public Key Infrastructure

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 REGULATION of the EUROPEAN PARLIAMENT and of the Council (EU) No. 910/2014 dated July 23, 2014 about electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC including the downstream legislation.

Signatory – a person as defined in [eIDAS].

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

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

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

PostSignum Root QCA - root CA that has a self-signed certificate or a qualified certificate for electronic seal. Certificates for the electronic seal for the subordinate CA certificate and CRL. In the hierarchy of PostSignum can be other root CAs that are additionally identified by a serial number, for example. Postsignum Root QCA 2.

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

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

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

Authorized person – one who against the certification authority acts as the representative of the customer. The authorised person must be listed in the contract between the customer and the Czech post, where appropriate, the Treaty stipulates that it is a customer.

Electronic identification device - this is a device that is used to remotely prove the applicant's identity when using the Certificate Online application. The device must have a "high" guarantee level and must be issued within a qualified electronic identification system in accordance with [ZoEI] and [eIDAS].

QESCD – (Qualified Electronic Signature Creation Device) qualified means of creating the electronic signature in accordance with [eIDAS]

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

Distinguished name -uniquely identifies the signer person according to the rules defined by the applicable certificate policy.

Private key – combined term electronic signature creation data, the data for creation of electronic seals, for encrypting and decrypting data and data for authentication.

Managing applicants – application to ensure information support the registration process and registration (SŽ).

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

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

VCA ČP - see PostSignum VCA.

Public key – summary data for verifying an electronic signature, the data for electronic authentication seal and data for encryption.

Provider's website – https://www.postsignum.cz – service provider Web pages of PostSignum.

Customer - natural person, entrepreneurial natural person, legal person, State authority or local government authority. Concluded with the Czech post contract for the provision of certification services.

Customer - organization – the body that requires the indication of the name of the Organization and of the identification number certificate.

Customer - entrepreneurial natural person – doing business person with an assigned identification number.

Customer – natural person – a person or business-non-entrepreneur a person without an assigned identification number.

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

Applicant – a person who has the right to apply for the certificate by some of PostSignum from valid certification policies; it is besides collectively to the signer the natural person.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

Each of the storage of information and documentation and for their operation corresponds to the Czech post as a provider of certification services.

For the publication of information corresponds to the Czech post as a provider of certification services.

2.2 Publication of certification information

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

2.2.1 Publication of certificates and CRLs

CA certificates are published

- on the website of the provider

http://www.postsignum.cz,

http://www.postsignum.eu

- in issued certificates is placed a link on the issuing CA in the form of certificate extensions (AuthorityInfoAccess).

Issued certificates of end users (and related information), for which the customer (the certificate subscriber) has agreed to the publication are published

- on the website of the provider

The certificates are published in the formats DER, PEM, and TXT.

Information about invalid certificates are published in the form of the certificate revocation list (CRL)

- on the website of the provider

Certificate revocation list is published in the formats DER, PEM, and TXT. Enabled protocol is HTTP or HTTPS.

- on the certificate revocation list distribution points set out in the certificate (issued by the CRL Distribution Points)

2.2.2 Disclosure of information about the certification authority

Certification policies, the message to the user and, where appropriate, and other documents are published on the

- website of the provider, or
- trading places (only for reference).

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

- on the website of the provider,
- the registration authorities in the form of the text that is posted the notice, or
- in a nationally distributed journal.

2.3 Time or frequency of publication

Information on the periodicity of the publication is listed in each certification policy, in General, however, that:

- certificate policy, certification practice statement, and the message for the user are published after approval and release of a new version, but always before the beginning of the document (and in the case of certification policies before issuing the first certificate);

- certificates, if they have been marked for publication are published after their release to the time specified in the certificate policy;

- information about invalid certificates in the form of the certificate revocation list (CRL) are published immediately after they are released, however, at the latest, before the end of the last published certificate revocation list. No later than once every 24 hours, and usually every 4 hours or after every revocation of the certificate.

- important information shall be published without delay.

2.4 Access controls on repositories

For more information about access to information provided by PostSignum VCA are listed in each certification policy, in General, however, that

- certification policy, the message for the user, the CA certificates and certificate status information are accessible for reading without any restrictions;

- the certificates of end users that were intended for publication, are available for reading without any restrictions.

Certification services provider does not allow unauthorized access to the issued certificates, which have not held to be spoken consent to the disclosure. Access the issued certificates, which was ratified by the subscriber of the publication, it is limited to searching for these certificates according to the specified criteria.

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

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

Due to the fact that certificates issued by PostSignum VCA for the various entities by different certification policies, and generally cannot be collectively define details about the types of names listed on the certificate. These data are defined in each certification policy.

3.1.2 Need for Names to Be Meaningful

Due to the fact that certificates issued by PostSignum VCA for the various entities by different certification policies, and generally cannot be collectively define the requirements on significance names. These data are listed in each certification policy.

3.1.3 Anonymity or Pseudonymity of Subscribers

In General, the of PostSignum VCA does not support the issuance of the certificate or certificates containing the anonymous pseudonym. More detailed information is given in each certification policy.

3.1.4 Rules for interpreting various name forms

Due to the fact that certificates issued by PostSignum VCA for the various entities by different certification policies, and generally cannot be collectively define rules for interpreting various name forms. These data are listed in each certification policy.

3.1.5 Uniqueness of names

Due to the fact that certificates issued by PostSignum VCA for the various entities by different certification policies, and generally cannot be collectively define the way in which the uniqueness of names is to be secured. These data are listed in each certification policy.

In General, however, that the same distinctive PostSignum VCA does not assign the name of two different entities. However, it can issue two or more certificates with the same name in the Subject field, distinguishing, but always it is a certificate for the same entity, which is guaranteed in accordance with the certification policy, according to which the certificate is issued.

In the case where the measures despite all the colliding of names, this will be forwarded to the Manager for the CA, which, in cooperation with the participating customers shall negotiate without delay.

3.1.6 Recognition, Authentication, and Role of Trademarks

Due to the fact that certificates issued by PostSignum VCA for the various entities by different certification policies, and generally cannot be collectively define the way it is treated the case insert a trademarks or registered trademarks in the certificate.

In General, however, that all the fields of the certificate, which verifies the PostSignum VCA, prescribed structure and must be accompanied by their accuracy and completeness.

3.2 Initial identity validation

3.2.1 Verification of compliance data to verify whether a person has the private key of the corresponding to the public key

The applicant shall submit a registration authority an electronic certificate request in PKCS # 10, where the information about the entity to which the certificate is to be issued, including the subject's public key. These data, together with the public key are digitally signed with the private key. The registration authority verifies the digital signature of the application. If the signature is verified as valid, it shall be deemed that the applicant owns the private key corresponding to the public key that will be listed in the certificate.

3.2.2 Authentication of Organization Identity

The identity of the Organization shall be demonstrated when concluding the contract on the provision of certification services in a manner customary in the trade.

3.2.2.1 Conclusion of the contract with the customer – organizations

Authorization to sign for the Organization shall be demonstrated when concluding the contract on the provision of certification services in a manner customary in the course of trade (specific procedures are listed on the website of the provider).

The Czech post concludes with the customer for the provision of certification services under the conditions defined by the commercial code.

Contract for the provision of certification services includes among others. the list of the authorized persons who will be with the supplier of certification services to communicate regarding the issuing of the certificates. The contract is concluded, as is usual in trade (representative of the Organization, etc.).

3.2.2.2 Pre-registration of applicants for the certificate at the customer-organization

The registration authority PostSignum VCA verifies the physical identity of the requester using standard personal documents. Because in the certificate are placed also data about the Organization to which the applicant belongs, the registration authority PostSignum VCA operator must also verify this binding.

Therefore, they are in the contract on the provision of certification services defined by authorized persons, whom to PostSignum VCA guarantee the link between the applicant and the organization. The assignee must perform pre-register of applicants who can apply for a certificate of PostSignum VCA. If on the contrary, ceases to be in the interest of the customer, so that the applicant could apply for the certificate, the designated officer shall notify the CA to this change, it may request for the revocation of certificates that have been issued to the applicant.

The authorized person sends or transmits to the provider of certification services for a list of applicants who can apply for a certificate based on a certificate policy. The list is signed by an authorized person, the statutory representative or agent. Validation of the signatory shall be carried out by checking the identity of those persons in the case of physical transmission of the

list of applicants or by checking the electronic signature of the person using the personal certificate issued by PostSignum in case of electronic transmission of the list of the applicants.

The first pre-registration may also be

- in the preparation of the contract and the annexes on a commercial site, in this case, the registration becomes valid only after the signing of the contract, or
- when signing the contract on the registration authority.

3.2.2.3 Change assignee

At the time of the contract with the customer – organizations may experience a change in designation of the authorized persons. The change must be captured in the appendix to the contract, where there will be a new person in charge and the specimen signature.

3.2.3 Authentication of Individual Identity (natural person)

3.2.3.1 The authentication of entrepreneurial natural persons or employees of an organization

Individual entrepreneur proves your identity when you pre-registration and customer data when applying for the issue and revocation of the certificate. An employee of the Organization demonstrates its identity when applying for the issue and revocation of the certificate. Submit one valid, undamaged personal document.

Types of documents that may be filed when the identity verification are listed in a particular certificate policy.

The employee of the registration authority will check:

- whether the document is valid,
- whether the photos on the document corresponds to the applicant for the certificate.

An individual entrepreneur or employee of an organization can prove his / her identity even remotely using the Electronic Identification Document. The Certificate Online application located on the provider's website, is used for this method of proving identity.

An individual entrepreneur or employee organizations can prove your identity in other ways as described in the applicable certificate policy.

3.2.3.2 The authentication of nonentrepreneurial natural person

Nonentrepreneurial natural person, as an individual, proving their identity one personal document and one complementary document.

Enumeration of personal and additional documents accepted the registration authority is listed in the certification policy, according to which the certificate is issued to a natural person.

The registration authority checks:

- whether the documents are valid,
- whether the photos on the documents corresponds to the natural person.

A non-business natural person can prove his / her identity even remotely using the Means of Electronic Identification. The Certificate Online application, which is located on the provider's website, is used for this method of proving identity.

In the certification policy, additional requirements may be laid down on the control, such as proof of identity in a different way, the existence of the record to the applicant in the register of eligible applicants, etc.

Conclusion of the contract with the customer – a natural person

The customer will come to the registration authority and asks for the issue of a certificate for a physical person. Furthermore, manual registration authority shall transmit its identifying information, including the address of residence, necessary for the conclusion of the contract. These data demonstrate a manner specified by the certificate policy.

The contract can also be concluded electronically in the Certificate Online application.

The Czech post concludes with the customer for the provision of certification services under the conditions defined by the commercial code. (specific procedures are listed on the website of the provider).

3.2.4 Non-verified Subscriber Information

A detailed list of information about the customer or applicant, including the information, whether the information is validated and how, is listed in the certification policy. In General, the Czech post as a provider of certification services requires the support of most of the identifying information referred to in the contract or in the certificate.

3.2.5 Validation of Authority

See the relevant certificate policy.

3.2.6 Criteria for interoperability

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

Cooperation with other certification authorities operated by the same provider of certification services is possible in particular at the level of the subordinate certification authority issuing the certificate authority PostSignum Root QCA, and under the conditions defined in the relevant certification policy.

3.3 Identification and authentication for re-key request in the certificate

3.3.1 Identification and authentication in the routine exchange of private key and their corresponding public key (hereinafter "pair data")

During a routine exchange of paired data (the successor of the certificate) is required the physical presence of the applicant the registration authority in the workplace. On the issue of subsequent certificate is requested electronically. The claimant authenticates using the electronic signature certificate issued by PostSignum-based defined in the applicable certificate policy.

3.3.2 Identification and authentication for Re-key after Revocation

In the case of revocation of the certificate is required when identification and authentication associated with the issuance of a new certificate to proceed as in the case of the initial verification of identity when issuing the first certificate (see Chapter 3.2.3).

When processing an application for a subsequent certificate, which the applicant has authenticated using revoked -based electronic signature certificate, in this case, the request will be rejected by the registration authority.

3.4 Identification and authentication for revocation request

The applicant or the subscriber of the certificate, when the certificate revocation request authenticates

- knowledge of the password for the tombstone, which entered (or was generated) when you register for the certificate request,
- personal document similar to the registration of the certificate request, or

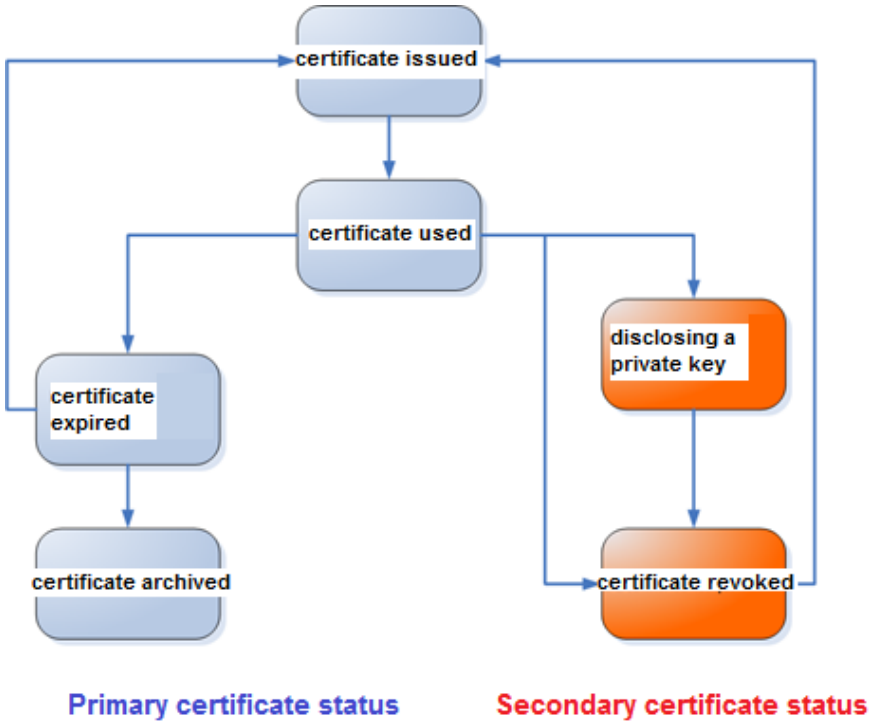
- by electronic signature, based on a certificate issued by a subordinate certification authority from the PostSignum hierarchy, on electronically sent requests for certificate revocation, or

- remotely using a devices of electronic identification.

In the certification policy can be defined that have a right to request revocation of the certificate and any other person. In this case, is provided also in politics the way that person when requesting the revocation of the certificate identifies and authenticates.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIRMENTS

The life cycle of certificates issued by PostSignum VCA is illustrated in the following figure:



The figure represents the highest level of the administration of certificates within PostSignum VCA. The certificate may be in any of the primary or secondary conditions. These certificates have the primary status:

- certificate issued,
- certificate used,
- certificate expired,
- certificate archived.

All certificates issued by PostSignum VCA are going through those primary status.

Secondary certificate statuses are:

- disclosing a private key,
- certificate revoked.

The secondary status represent an exceptional situation, therefore, it is assumed that

- most of the certificates issued by PostSignum VCA comes through in its life cycle, only the primary States,

PostSignum VCA supports all referred to the States, but the certificate does not support any temporary conditions, such as the suspension of the certificate.

4.1 Certificate application

How to register a certificate request are defined in the applicable certificate policy.

4.1.1 Who Can Submit a Certificate Application

PostSignum VCA is oriented to:

- Customers - organizations that want to issue certificates for employees, who have a particular relationship to the organization. Process a certificate request is, and in the final phase comes the certificate requester (employee organization or person defined by the Organization) to a registration authority with the electronic certificate request and with the relevant papers.

- Customers - natural persons who want to leave the issue certificates for yourself. Process a certificate request is a single stage, during a single visit customer registration authority will establish a contractual relationship and will even issue a certificate based on the delivered electronic certificate request.

4.1.2 Enrollment Process and Responsibilities

Custom registration process, the requirements for this process, and the provider's liability and the applicant are described in the relevant certificate policy.

4.2 Certificate Application Processing

Certificate request handling procedures are defined in the applicable certificate policy.

4.2.1 Performing Identification and Authentication Functions

Before processing the request, the applicant must be identified by a certificate and the authentication must be performed. The specific requirements for the process of identification and authentication are defined in the applicable certificate policy.

4.2.2 Approval or Rejection of Certificate Applications

Procedure and requirements for the control of eligibility application are defined in the applicable certificate policy.

4.2.3 Time to Process Certificate Applications

Certificate request processing time is defined in the applicable certificate policy. In General, however, that the certificate is issued, usually on the day of submission of the application.

4.3 Certificate issuance

The procedures of issuing the certificate are defined in the relevant certificate policy.

4.3.1 CA Actions during Certificate Issuance

Procedure and requirements for the issuing of the certificate are described in the applicable certificate policy.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

List of bodies informed about the issue of the certificate is listed in the applicable certificate policy. In general, however, that the issue of the certificate shall inform the certification services provider of the certificate requester.

4.4 Certificate Acceptance

Procedure and requirements for acceptance of a certificate are described in the applicable certificate policy.

4.4.1 Conduct Constituting Certificate Acceptance

A certificate is usually issued shortly after the approval of the application to the applicant and its insertion into the system of the CA. The applicant to take over the issued certificate by using the URL sent to the applicant. The applicant shall proceed to the Web page located at the URL that will be sent to contain

- details of the certificate issued,
- the certificate policy under which the certificate was issued, and
- Select accept/not accept the issued certificate.

In the event that the applicant has agreed with the content of the certificate and the certification provisions of the relevant policy, chooses the option to accept. If the applicant does not agree with the content of the certificate has the option not to accept.

The certificate issued to the applicant is offered for download in the PEM and DER format. the applicant has the option to download an electronic version of the Protocol on the issue of the certificate.

4.4.2 Publication of the Certificate by the CA

The certificate for which was ratified with the publication of the subscriber is within 24 hours of receipt published on the website of the provider.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

In addition to the publication of the issued certificate for which was ratified by the subscriber of the publication, the provider of certification services shall not issue a certificate to any third party.

4.5 Paired data and certificate usage

Key pairs bound with certificates have the same duration as the certificates. Key pairs are expired, they cannot be reused within a single CA in the hierarchy of PostSignum VCA.

4.5.1 Subscriber Private Key and Certificate Usage

The applicant for a certificate issued by PostSignum VCA is entitled to use the private key and the corresponding certificate only for the purposes specified in the certification policy according to which the certificate was issued.

4.5.2 Relying Party Public Key and Certificate Usage

The relying party is authorized to use a certificate issued by PostSignum VCA only for the purposes and under the conditions specified in the relevant certificate policy under which the certificate was issued.

4.6 Certificate renewal

PostSignum VCA this service does not provide.

4.6.1 Circumstance for Certificate Renewal

PostSignum VCA this service does not provide.

4.6.2 Who May Request Renewal

PostSignum VCA this service does not provide.

4.6.3 Processing Certificate Renewal Request

PostSignum VCA this service does not provide.

4.6.4 Notification of New Certificate Issuance to Subscriber

PostSignum VCA this service does not provide.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

PostSignum VCA this service does not provide.

4.6.6 Publication of the Renewal Certificate by the CA

PostSignum VCA this service does not provide.

4.6.7 Notification of issue of the renewed certificate to other entities

PostSignum VCA this service does not provide.

4.7 Certificate Re-key

Data exchange public key service in the certificate is referred to as the successor of the certificate. This designation will be used later in the text.

The successor of the certificate is conducted in a manner defined certification policy. In General, an application for a subsequent certificate is signed by an advanced electronic signature and is sent on a dedicated central registration authority. The issued certificate is then available on the website of the provider, where it is carried out by its acceptance and withdrawal.

4.7.1 Circumstance for Certificate Re-key

Conditions for the issuance of a subsequent certificate are listed in the certification policy.

4.7.2 Who May Request Certification of a New Public Key

List of entities that can request the release of subsequent certificate is listed in the applicable certificate policy.

4.7.3 Processing the request on the exchange of public key

Procedures of registration of the request for renewal of the certificate are defined in the applicable certificate policy.

4.7.4 Notification of the issuance of a certificate with exchanged public key

List of bodies informed about the issue of the certificate is listed in the applicable certificate policy. In General, however, that the issue of the certificate shall inform the certification services provider of the certificate requester.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

Procedure and requirements for acceptance of a certificate are described in the applicable certificate policy.

4.7.6 Publication of the Re-keyed Certificate by the CA

Subsequent to the publication of certificates, the same rules apply as for the publication of the initial certificate issued in the usual way (see section 4.4.2).

4.7.7 Notification of issue of the certificate with the exchanged public key to other entities

For notification of the release of the subsequent certificates the same rules apply as for notification about the release of the initial certificate issued in the usual way (see section 4.4.3).

4.8 Certificate Modification

The conditions for the amendment of the particulars in the certificate are defined in the applicable certificate policy. In General, the revocation of an existing certificate and to issue an initial certificate with new data in the usual way (see Chapter 4.3).

4.8.1 Circumstance for Certificate Modification

The conditions for the amendment of the particulars in the certificate are defined in the applicable certificate policy. In General, if there is a change in the particulars in the certificate issued by PostSignum VCA, the certificate subscriber must immediately notify this change to the provider of certification services.

4.8.2 Who May Request Certificate Modification

If there is a change in the particulars in the certificate issued by PostSignum VCA, the certificate subscriber must immediately notify this change to the provider of certification services. For the customer's organization announces changes in employees ' certificates, the designated person, either electronically or in writing. To change notification will use the contact

details listed in the contract for the provision of certification services. Natural person announces changes of data in certificates in person registration authority in the workplace, electronically or in writing.

4.8.3 Processing Certificate Modification Requests

Processing of the request for the change of the data in the certificate is defined in the applicable certificate policy.

4.8.4 Notification of issue of the certificate with the changed data

Issuing of the certificate with the changed data is identical with the release of the initial certificate in the usual manner and for notifying the relevant provisions are applied (see section 4.3.2).

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Issuing of the certificate with the changed data is identical with the release of the initial certificate, as usual, and for the transposition of the relevant provisions are applied (see section 4.4.1).

4.8.6 Publication of the Modified Certificate by the CA

Issuing of the certificate with the changed data is identical with the release of the initial certificate, as usual, and for the publication of the relevant provisions are applied (see section 4.4.2).

4.8.7 Notification of issue of the certificate with the changed data to other entities

Issuing of the certificate with the changed data is identical with the release of the initial certificate, as usual, and for the notification to other entities, the relevant provisions are applied (see section 4.4.3).

4.9 Certificate revocation and suspension

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

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

4.9.1 Conditions for revocation of the certificate

Generally these are cases where there is a risk of abuse and issued a valid certificate. The most common reasons for revocation of the certificate are provided in the relevant certificate policy.

4.9.2 Who Can Request Revocation

On the revocation of the certificate may request the applicant and the customer (the certificate subscriber).

Revocation of the Certificate Manager can initiate a CA as a representative of the certification authority that issued the certificate.

4.9.3 Certificate revocation request

The procedure and method of the request for revocation of the certificate are described in the applicable certificate policy.

4.9.4 Revocation Request Grace Period

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

4.9.5 Time within Which CA Must Process the Revocation Request

The time from the receipt of the request for revocation of the certificate service to the publication of PostSignum VCA CRL containing the appropriate certificate shall not exceed 24 hours.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying party obligations are listed in the certification policy. In General, however, that relying parties must verify its status using the certificate to the current CRL is published on the website of the provider.

4.9.7 CRL Issuance Frequency

Certificate revocation list (CRL) root certification authority PostSignum Root QCA is published at least once a year.

Certificate revocation list (CRL) subordinate CAs in the hierarchy of PostSignum is published after each revocation of the certificate or once every 24 hours, usually every 4 hours.

4.9.8 Maximum Latency for CRLs

All of the procedures, processes and emergency plans are set up so that the issue of the certificate revocation list was kept and referred to in chapters 4.9.4, 4.9.5 and 4.9.7 has been observed.

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

PostSignum VCA to provide this service as a publicly accessible free service, which is provided by the RFC 6960. A certificate profile is specified in the policy for issuing certificates, OCSP and OCSP profile requests and responses are listed in section 7 of this document.

4.9.10 Certificate while validating the Statute Requirements online

See the provisions in Chapter 4.9.9.

4.9.11 Other forms of revocation notification

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

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

Procedure for revocation of the certificate in the case of compromise of private key is consistent with the General procedure for revocation of the certificate.

4.9.13 Conditions for the suspension of the certificate

PostSignum VCA this service does not provide.

4.9.14 Bodies competent to request suspension of the certificate

PostSignum VCA this service does not provide.

4.9.15 Requests for suspension of the certificate

PostSignum VCA this service does not provide.

4.9.16 Limitation on the suspension of the certificate

PostSignum VCA this service does not provide.

4.10 Certificate status services

You can verify the status of the certificate

- the certificate revocation list (CRL) in the service of exposing public information of PostSignum VCA HTTP
- within the issued certificate lookup service available on the website of the provider (does not apply to certificates issued by PostSignum Root QCA), or
- using OCSP.

4.10.1 Operational characteristics

A list of certificate revocation and certificate status information are considered to be publicly available information. Certificate revocation list (CRL) is published in three places:

- on the website of the provider,
- an independent provider of Web services.

The primary source of the current CRL is the Web page of the provider.

In the context of a search service issued certificates available on the website of the provider is also published giving information about the State of the search certificate. This certificate status information is not binding, it is merely a complementary information to the current CRL, that is always the only authentic source of information about the status of the certificate.

4.10.2 Service availability

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

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

OCSP service availability is 7 days a week 24 hours a day.

4.10.3 Other characteristics status of certificate services

Other characteristics status of the certificate services are not provided.

4.11 Termination of services used by the applicant of the certificate

Possible cases of the expiry of the certificate are listed in the relevant certificate policy.

4.12 Storage of private key for a trusted third party and their recovery

The private key of the certificate subscribers are generated and administered by the applicant for the certificate. This is the key for the RSA and ECDSA algorithm, key length allowed is defined in the applicable certificate policy. PostSignum VCA with these key does not come into contact with, is not responsible for their protection or backup.

4.12.1 Policy and procedures for safekeeping and restoring private key

PostSignum VCA this service does not provide.

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

PostSignum VCA this service does not provide.

5 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

For the PostSignum VCA documents have been processed:

- System security policy, describing the principles of safety in the field of physical, procedural and personnel;
- Plan for crisis management and recovery plan, describing the procedures for maintaining guaranteed service levels in the event of an emergency,
- Operating and safety procedures, describing procedures to be followed logically in PostSignum VCA, and directive
- Organizing job Public certification authority of Česká Pošta, s. p., besides in particular, the role the occupation area governs the PostSignum VCA.

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

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

5.1 Physical Controls

A detailed description of the requirements and measures from the field of physical safety, it is mentioned in a document the system security policy [SBP].

5.1.1 Site Location and Construction

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

- Central workplace (main and backup site)
- operator's workplace Centre (in particular for supporting management information system),
- site registration authority (typically a merchant site certification authority) and
- workplace verification registration authorities (typically the focal points of the public administration).

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

In addition, there is the workplace of the mobile registration authority, where there is the absence of physical security measures is offset by measures from the organizational security.

5.1.2 Physical access

For each type of workplace is in its operating regulations defined who workers have physical access to the workplace. Areas are protected against unauthorized intrusion by mechanical means (safety locks and bars), a central place of work is also a separate loop electronic signalling equipment. On site verification registration authority and the mobile registration authority are subject to the regime measures defined in System security policy [SBP].

5.1.3 Power and air conditioning

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

5.1.4 Water Exposures

Central departments are located outside of the flood plains.

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

5.1.5 Fire Prevention and Protection

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

5.1.6 Media storage

For the purposes of storing the data of PostSignum VCA safes, at least one of them is outside the premises of the central workplace buildings.

5.1.7 Waste disposal

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

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

5.1.8 Off-Site Backup

For the PostSignum VCA was built on the location where the backup operation in emergency situations, when it is not possible to secure the proper operation of the VCA in the main site, and where they are also periodically saved backups of the system of PostSignum VCA.

5.2 Procedural Controls

A detailed description of the requirements and process safety measures and the allocation of roles is set out in document organizing tasks VCA [OZU], in a document, the system security policy [SBP] and internal documentation of PostSignum VCA.

5.2.1 Trusted roles

See the relevant certificate policy.

5.2.2 Number of Persons Required per Task

See the relevant certificate policy.

5.2.3 Identification and Authentication for Each Role

See the relevant certificate policy.

5.2.4 Roles requiring separation of duties

See the relevant certificate policy.

5.3 Personnel Controls

A detailed description of the requirements and measures from the area of staff security and the allocation of roles is set out in document organizing tasks VCA [OZU] and in document System security policy [SBP].

5.3.1 Qualifications, Experience, and Clearance Requirements

See the relevant certificate policy.

5.3.2 Background Check Procedures

See the relevant certificate policy.

5.3.3 Training Requirements

See the relevant certificate policy.

5.3.4 Retraining Frequency and Requirements

See the relevant certificate policy.

5.3.5 Job Rotation Frequency and Sequence

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

5.3.6 Sanctions for Unauthorized Actions

See the relevant certificate policy.

5.3.7 Independent Contractor Requirements

See the relevant certificate policy.

5.3.8 Documentation Supplied to Personnel

See the relevant certificate policy.

5.4 Audit logging procedures

See the relevant certificate policy.

5.4.1 Types of event recorded

See the relevant certificate policy.

5.4.2 Frequency of processing records

See the relevant certificate policy.

5.4.3 Retention period of audit records

See the relevant certificate policy.

5.4.4 Protection of audit records

See the relevant certificate policy.

5.4.5 Audit Log Backup Procedures

See the relevant certificate policy.

5.4.6 Audit collection system records (internal or external)

See the relevant certificate policy.

5.4.7 Notification to Event-Causing Subject

See the relevant certificate policy.

5.4.8 Vulnerability Assessments

See the relevant certificate policy.

5.5 Records archival

See the relevant certificate policy.

5.5.1 Types of information and documentation

See the relevant certificate policy.

5.5.2 Retain stored information and documentation

See the relevant certificate policy.

5.5.3 Storage security of stored information and documentation

See the relevant certificate policy.

5.5.4 Procedures to back up stored information and documentation

See the relevant certificate policy.

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

See the relevant certificate policy.

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

See the relevant certificate policy.

5.5.7 Procedures to obtain and verify the stored information and documentation

See the relevant certificate policy.

5.6 Key Changeover

See the relevant certificate policy.

5.7 Compromise and disaster recovery

See the relevant certificate policy.

5.7.1 Procedure in case of an incident and compromise

See the relevant certificate policy.

5.7.2 Corruption of computing resources, software and/or data

See the relevant certificate policy.

5.7.3 Data being compromised and procedure for creating electronic seal

5.7.3.1 Compromise of the private key the subordinate certification authority

See the relevant certificate policy.

5.7.3.2 Compromise of the private key of PostSignum Root QCA

See the relevant certificate policy.

5.7.4 Ability to recover after a disaster

Continuation of the processes of disaster CA depends on the type of disaster and its consequences.

In the event of an accident of the small and medium-scale operation of PostSignum VCA passes into the backup site. CA is run in restricted mode, which only provides for invalidating certificates and publishing CRLs.

In the event of a disaster of great magnitude (natural disaster, a State of war), the restoration is the activity of PostSignum VCA things management decision of the Czech post. About management decisions with a minimum of delay must be notified to all customers of PostSignum VCA.

If the management of the Czech post decides to terminate the operation of PostSignum VCA, downtime of certification services shall not exceed 20 working days.

5.8 CA or RA Termination

5.8.1 Termination of activities of a root certification authority

See the relevant certificate policy.

5.8.2 Termination of activities of the subordinate certification authority

See the relevant certificate policy.

5.8.3 Termination of registration authority

See the relevant certificate policy.

5.8.4 Termination of activities of a provider of certification services

See the relevant certificate policy.

5.8.5 Withdrawal of accreditation

See the relevant certificate policy.

6 TECHNICAL SECURITY CONTROLS

A detailed description of the requirements and technical safety measures is set out in a document the system security policy [SBP]; PostSignum VCA system settings and measures in the form of procedures are described in the internal documentation of PostSignum VCA.

6.1 Data generation and installation

6.1.1 Key Pair Generation

How do I generate a pair of data is described in the applicable certificate policy.

6.1.2 Private Key Delivery to Subscriber

PostSignum VCA does not provide service to generate the key pair for the certificate requester.

6.1.3 Public Key Delivery to Certificate Issuer

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

6.1.4 CA Public Key Delivery to Relying Parties

Certificates of certification authorities, as well as certificates for whom publication has been approved, are published in the manner described in Chapter 2.

6.1.5 Key Sizes

The length of the used keys/modules are laid down in the relevant certification policies.

The keys of the CAs in the hierarchy of PostSignum have for the RSA algorithm, the length of the module at least 4096 bits and for the ECDSA algorithm keys have a pLen and qLen 512 bit, specifically the P-521 curve (secp521r1).. Key certificate subscribers have for the RSA and ECDSA algorithm, the length of the module defined in the applicable certificate policy.

6.1.6 Public Key Parameter Generation and Quality

The procedure for generating public key and checking their quality is described in the relevant certification policy.

6.1.7 Key Usage Purposes

End users ' public keys can only be used in accordance with the rules described in Chapter 1.4

6.2 Protection of private key and security of cryptographic modules

6.2.1 Cryptographic Module Standards and Controls

Standards and conditions for the use of cryptographic modules are described in the applicable certificate policy.

6.2.2 Private Key (n out of m) Multi-Person Control

Sharing the secret as described in the applicable certificate policy.

6.2.3 Storage of private key

The service, which would require the storage of private keys, PostSignum VCA does not provide.

6.2.4 Private Key Backup

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

6.2.5 Private Key Archival

Data retention for electronic signature creation data to create an electronic seal, or data for creating electronic seals described in the certification policy.

6.2.6 Private Key Transfer into or from a Cryptographic Module

Data transfer for creating electronic seal to the cryptographic module or of cryptographic module is described in the applicable certificate policy.

6.2.7 Private Key Storage on Cryptographic Module

Save data for creating electronic seal in the cryptographic module is described in the applicable certificate policy.

6.2.8 Method of Activating Private Key

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

6.2.9 Method of Deactivating Private Key

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

6.2.10 Method of Destroying Private Key

The procedure for the destruction of the electronic signature creation data or electronic seals creation data is described in the applicable certificate policy.

6.2.11 Cryptographic module Rating

The evaluation of cryptographic modules is described in the applicable certificate policy.

6.3 Other aspects of paired data management

6.3.1 Public Key Archival

The public key in the form of end-user certificates are archived in accordance with the audit and archive policy.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The period for which shall be issued public key certificates to end users, which is laid down in the relevant certification policies.

6.4 Activation data

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

6.4.1 Activation data generation and installation

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

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

6.4.2 Activation data Protection

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

6.4.3 Other aspects of activation data

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

6.5 Computer security control

6.5.1 Specific computer security technical requirements

Specific computer security technical requirements are described in the applicable certificate policy.

6.5.2 Computer security Rating

Evaluation of computer security is described in the applicable certificate policy.

6.6 Life-cycle Technical Controls

6.6.1 System development controls

Management of the development of the system is described in the applicable certificate policy.

6.6.2 Security management controls

Safety management controls are described in the applicable certificate policy.

6.6.3 Life-cycle security controls

The safety management of the life cycle is described in the applicable certificate policy.

6.7 Network security

Network security is described in the applicable certificate policy.

6.8 Time-stamping

See section 5.5.5.

7 CERTIFICATE AND CRL PROFILES

7.1 Certificate profile

PostSignum VCA can issue certificates based on the x.509 standard, version 3, in which they are defined, inter alia, an expansion of the items of the certificate, which can limit the use of the certificate, where appropriate, provide additional information about the certificate or the subscriber. PostSignum VCA supports expansion of the items described in the corresponding certification policies. CA reserves the right to insert additional items in the certificate, if it will require a change in legislation or standards that govern the activities of certification service providers.

7.1.1 Version number

Certificates issued by PostSignum VCA - compliant x.509 version 3.

7.1.2 Certificate Extension items in the

Certificates are used is specified in the extension of the individual certification policies.

7.1.3 Object identifiers ("OID") algorithms

Algorithms used in PostSignum VCA are not assigned an OID. In the hierarchy of PostSignum VCA is not using specific algorithms that would be developed by the operator of PostSignum VCA or his supplier, but only the algorithms conform to the requirements applicable standards.

7.1.4 Type of names

Certificates issued by PostSignum VCA contain business name and business ID number of the certificate issuer, and the business name, or the name or the name and surname of the subscriber of the certificate.

In certificates issued by PostSignum VCA the following character sets are supported:

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

7.1.5 Name Constraints and names

Used the names must be exact transcriptions of data provider of certification services or the customer applying for the issue of a certificate, i.e. must be identical to the master or reportable.

Additional rules for creating names and any other restrictions are set out in the applicable certificate policy.

7.1.6 Certificate policy OID

In every end user's certificate is a link to a policy under which the certificate was issued (OID policies).

7.1.7 Expansion entry "Policy Constraints"

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

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

Expanding the entry "Policy Qualifier" contains a link to the provider's website where you can obtain the certificate policy under which the certificate was issued, and text information about the fact that the certificate was issued.

7.1.9 How to write a critical expansion of the item "Certificate Policies"

How to write an extension item "Certificate Policies" is listed in the applicable certificate policy. This item is not marked as critical.

7.2 The certificate revocation list profile

7.2.1 Version number

In PostSignum VCA are issued certificate revocation lists in accordance with the x.509 standard, version 2.

7.2.2 The expansion of the certificate revocation list items and records in a certificate revocation list

A detailed profile of the CRL is listed in the certification policy. In General, the certificate revocation lists are used the following expansion:

- The Authority Key Identifier (KeyIdentifier AuthorityCertIssuer +, AuthorityCertSerialNumber)
- CRL Number,
- Revocation Reason (for the individual record of the certificate),
- Invalidity Date (for an individual certificate record; optional).

7.3 OCSP Profile

OCSP certificate profile is listed in the certification policy for issue of the certificate OCSP, which is published on the website of the provider.

The structure of the OCSP request OCSP Request-Data

Name of the item	Description	Value/use index
Version	OCSP version (required entry)	1
Requestor Sheet		
Certificate ID	information about the queried certificate – an item may be repeated	
Hash Algorithm	the hash of the request	SHA-1
The Issuer Name Hash	the hash computed from the name of the publisher certificate	
Issuer Key Hash	the computed hash from the fingerprint of the public key of the certificate issuer	

Serial Number	the serial number of the certificate subject	
Request Extensions		
OCSP Nonce	Random, once generated number (64-bit). If it is contained in the request, then it contains the answer. (optional item)	

OCSP request not need be signed.

The structure of the OCSP response OCSP Response Data

Name of the item	Description	Value/use 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	The OCSP protocol version	1
Responder Id	Responder OCSP signing certificate DN	
Produced At	Responder OCSP response signing time in UTC	
Responses:		
Certificate ID	The data conform to the application	
Cert Status	Status of the certificate. good – the certificate is valid revoked - certificate is revoked unknown-the certificate status is unknown (for example, such a certificate does not exist)	0 – good 1 — revoked 2-unknown
Revocation Time	Time of revocation of a certificate. The item is listed only in the case of Cert Status = revoked	
Revocation Reason	The reason for the certificate revocation. The item is listed only in the case of Cert Status = revoked	
This Update	The time in UTC, which is indicated by the status of the response.	
Response Extensions		
OCSP Nonce	Random, once generated number (64-bit). If it is contained in the request, then it contains the answer. (optional item)	

7.3.1 Version number

See section 7.3

7.3.2 OCSP Extension items

See section 7.3

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The evaluation of conformity is further dealt with in the document and archive the audit policy, which is annexed to the system security policy [SBP].

8.1 Frequency or circumstances of assessment

8.1.1 Internal control

At least once every 12 months, staff of the Department of internal audit and risk management

- validated compliance with generally binding legal regulations, internal rules, of the measures adopted and established procedures,
- verified the appropriateness, functionality, efficiency and effectiveness of risk management, internal management and control systems and mechanisms.

On the implementation of each internal controls must be drawn up, signed the written report. The message is archived in the same way as the other records on the operation of PostSignum VCA and retained for at least 10 years.

8.1.2 External control

The safety and integrity of the systems and processes of PostSignum VCA is verified by an external control carried out by the auditor independent of the Czech post checks the extent of the total set by applicable laws and regulations.

For the execution of each control must be drawn up, signed the written report. The message is archived in the same way as the other records on the operation of PostSignum VCA and retained for at least 10 years.

8.2 Evaluator identity and qualifications

See the relevant certificate policy.

8.3 Assessor's relationship to the rated entity

See the relevant certificate policy.

8.4 Evaluated areas

In the context of the checks shall be verified by compliance with the generally binding and internal regulations, security and integrity of systems.

In the framework of the regular internal controls is evaluated compliance with generally binding legal regulations, internal rules, of the measures adopted and established procedures, and appropriateness, functionality, efficiency and effectiveness of risk management, internal management and control systems and mechanisms.

In the framework of the external audit shall be assessed in particular the fact that the

- provider of trusted systems operates in accordance with the applicable law and relevant standards,

- the provider makes changes to the trusted systems in accordance with the safety documentation provider with its components governing the management of change.

8.5 Procedures applied to discovered defects

See the relevant certificate policy.

8.6 Sharing evaluation result

See the relevant certificate policy.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

The valid price list is published on the website of the provider.

9.1.2 Certificate Access Fees

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

9.1.3 Revocation or Status Information Access Fees

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

9.1.4 Fees for Other Services

The valid price list is published on the website of the provider.

9.1.5 Refund Policy

No provisions in this chapter.

9.2 Financial responsibility

9.2.1 Insurance Coverage

See the relevant certificate policy.

9.2.2 Other Assets

See the relevant certificate policy.

9.2.3 Insurance or Warranty Coverage for End-Entities

PostSignum VCA this service does not provide.

9.3 Confidentiality of business information

9.3.1 Scope of Confidential Information

For sensitive information, are considered in the course of trade any confidential information, the circumstances and the information, which is one of the interested parties in connection with the performance of contract for the provision of certification services and which has not been agreed in writing between the Contracting Parties, that may be published.

Sensitive information is always treated as information marked as:

- internal
- trade secrets
- confidential information

- other proprietary information

9.3.2 Information outside of sensitive information

See the relevant certificate policy.

9.3.3 Responsibility for protection of sensitive information

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

9.4 Privacy of Personal Information

The Czech post ensures the protection of personal data of people gets access in the provision of certification services. Privacy policies are contained in the certification policies, general terms and conditions of the CP [VOP] and based on the relevant provisions of Act No. 101/2000 Coll., on the protection of personal data, as amended.

The Czech post provides information to the extent modified by the certificate policy subscribers, persons or persons which draws, as well as auditors for the purposes of representation of the match, and also provides information to the extent necessary on the basis of mandatory provisions of applicable law (e.g., law enforcement authorities in the cases required in criminal legislation).

ČP has carried out an analysis of the security risks and on the basis of established measures for the protection of personal data processed. Detailed specification adopted safety measures is contained in internal documents. These documents are regularly subject to inspection of the safety match. In the relevant certificate policy and partly in this document describes the basic security measures. ČP continuously monitors the security environment in similar companies in Europe to respond to potential security risks.

9.5 Intellectual property rights

Certificate policy, certification practice statement, and all related documents are protected by copyright of the Czech post and presenting a significant know-how of the Czech post. Czech post is also the subscriber of the rights to the information system for the operation of the CA and the structure, organization, looks to screens and Web content providers. The CP is the bearer of the following registrations of domain names, in connection with the provision of certification authority: postsignum.cz.

9.6 Representation and warranties

The Czech post as a provider of certification services guarantees that will fulfill any obligations imposed by the contract with the customer, the certification policy, internal regulations and mandatory provisions of the relevant legislation.

The Czech post provides the above warranty throughout the period of validity of the contract for the provision of certification services.

9.6.1 CA Representations and Warranties

9.6.1.1 PostSignum Root QCA Guarantees

Certification authority PostSignum Root QCA guarantees that

- will pay due attention to all the activities associated with the provision of certification services; proper care includes operations in accordance
- with internal operational documentation
- the certification policy
- this certification practice statement,
- system security policies,
- the applicable law,
- will maintain this certification practice statement,
- will be in the realm of its competence to enforce compliance with the rules described in this certification practice statement,
- publish the certification policy, according to which issues certificates and which is intended for publication, on the website of the provider, or by other appropriate means,
  - publish the self-signed certificate and the imprint of the self-signed certificate in at least two independent ways,
- without undue delay shall examine the certificate request, shall issue a decision, whether the certificate will be issued, and this decision will inform the applicant, the
- issue the certificate x.509 compliant and meeting the requirements of the applicant,
- issue a certificate containing the factually correct information based on the information that is available to the certification authority at the time of issue of the certificate, without the errors caused by operation of the CA when entering data
- will inform the applicant that the certificate was issued, and shall forward the certificate issued to the applicant,
- publish the certificate, which was accepted by the applicant, without undue delay on the provider's website, or through other appropriate means,
- invalid certificates according to the rules described in the certification policy
- it shall inform the subscriber of the certificate about the fact that his certificate has been invalidated by the will of the CA or the will of the supervisory authority,
- publish the certificate revocation list, without undue delay, within the period specified in the certification policy
- examines suspect that your private key has been compromised within the scope of PostSignum Root QCA, which could lead to loss of trust this CA

- assist in checking that is performed by the external auditor or authorized employee of the Czech post

- ensure the safe operation of systems according to the requirements of applicable law.

9.6.1.2 Guarantees subordinate CAs

Subordinate certification authority acting in the hierarchy of PostSignum VCA guarantees that

- will pay due attention to all the activities associated with the provision of certification services; proper care includes operations in accordance

-with internal operational documentation

- the certification policy

- this certification practice statement,

- system security policies,

- the applicable law,

- assess and approve the establishment of a registration authority that falls within its scope,

- in the realm of its competence will enforce the rules described in this certification practice statement,

- publish the certificate policies under which certificates are issued by, on its Web site, or by other appropriate means,

- without undue delay shall examine the certificate request, shall issue a decision, whether the certificate will be issued, and shall inform the applicant of that decision,

- issue the certificate x.509 compliant and meeting the requirements of the customer

- issue a certificate containing the factually correct information based on the information that is available to the certification authority at the time of issue of the certificate, without the errors caused by operation of the CA when entering data

– inform the applicant that the certificate was issued, and shall forward the certificate issued to the applicant,

- publish the certificate that was ratified with the publication and which was accepted by the applicant, without undue delay, on its Web site, or through other appropriate means,

- certificate is revoked in accordance with the rules described in the certification policy

- it shall inform the subscriber of the certificate about the fact that his certificate has been invalidated by the will of the CA,

- publish the certificate revocation list, without undue delay, within the period specified in the certification policy

- examines suspect that your private key has been compromised within the scope of the subordinate certification authority, which could lead to loss of trust this CA

- assist in checking that is performed by the external auditor or authorised employee of the Czech post

- ensure the safe operation of systems according to the requirements of applicable law.

9.6.2 Representation and warranties RA

The registration authority acting in the hierarchy of PostSignum VCA guarantees that

- will pay due attention to all the activities associated with the provision of certification services; proper care includes operations in accordance

- the agreement between the Czech post and the registration authority, if operators are certification authorities and registration authorities different legal entities,

- with internal operational documentation

- the certification policy

- this certification practice statement,

- system security policies,

- the applicable law,

- in the realm of its competence will enforce the rules described in this certification practice statement,

- will receive certificate requests, including the relevant written documents, approve requests, or oppose according to the rules of the applicable certificate policy

- instruct the applicant of its obligations arising from the applicable certificate policy, shall provide the applicant or the certification policy information, where you can obtain the certification policy,

- proceeds to process the request that contains a factually correct information with respect to the information that is available to the registration authority at the time of receipt of the request, and without the errors caused by data entry operator registration authority,

- proceeds to process the certificate request x.509 compliant and complying with the formalities required by the applicable certificate policy

- verify the identity of the applicant for the certificate in accordance with the applicable certificate policy

- without undue delay shall examine the certificate request, shall issue a decision, whether the certificate will be issued, and shall inform the applicant of that decision,

– inform the applicant that the certificate was issued and the passes, or shall ensure that the transmission of the certificate issued to the applicant,

- ensure the revocation of the certificate according to the rules described in the certification policy

- keeps records of certificate requests that have been submitted through them,

- examines suspect that your private key has been compromised within the scope of the registration authority, which can lead to a loss of credibility of the registration authority,

- ensure the acquisition of evidence documents associated with the acceptance and processing of applications and the issuance of the certificate,

- assist in checking that is performed by the external auditor or authorized employee of the Czech post.

In the provision of services, the registration authority may be the Czech post as a provider of certification services represented by a third party on the basis of the concluded contractual relationship; referred to the level of the guarantees do not affect.

9.6.3 Representation and warranties of the applicant of the certificate

See the relevant certificate policy.

9.6.4 representation and relying party guarantee

The relying party shall be liable for the fulfillment of all the obligations that are imposed on the relying party prior to use of a commercial certificate. These obligations are listed in the relevant certification policies. In General, the relying party must in particular

- Obtain certificates of PostSignum Root QCA and the subordinate CA certificate from a safe source (provider's website, or the website of a supervisory authority) and verify the fingerprint ("fingerprint") of these certificates.

- Before using the certificate issued by the subordinate CA in the hierarchy of PostSignum this authority to validate the certificate and the validity of the issued by the end of the certificate; a check is performed on the correct signature of the issuing authority and the current CRL.

- Sufficiently consider (in particular on the basis of knowledge of the relevant certificate policy) is a certificate issued by the subordinate CA under this policy is suitable for the purpose for which it wants to use.

9.6.5 Representation and warranties of other participating entities

See the relevant certificate policy.

9.7 Disclaimers of Warranties

See the relevant certificate policy.

9.8 Limitations of liability

Arrangements for the limitation of liability specified in the certificate policy [VOP] or in the order of the services (or service contract).

9.9 Indemnities

Financial liability coverage of the certification services provider to our customers and embraces the Parties described in section 9.2 and the certification policy.

9.10 Term and termination

9.10.1 Validity period

The origin of this document defines the date of the referred to in Chapter 1.2

End of validity of the document is determined by the date of expiry.

9.10.2 Termination

See the relevant certificate policy.

9.10.3 Effect of Termination and Survival

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

9.11 Individual notices and communications with participants

9.11.1 The communication with the provider of certification services

See the relevant certificate policy.

9.11.2 Communications within the system of PostSignum VCA

See the relevant certificate policy.

9.11.3 Communication language

See the relevant certificate policy.

9.12 Amendments

9.12.1 Procedure for amendments

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

9.12.2 Notification Mechanism and Period

Issue of a new certification practice statement will be announced in the news on the website of the provider.

9.12.3 Circumstances in which OID must be changed

Czech Post has assigned according to their internal rules, object identifiers (OIDs) used in the environment of PostSignum VCA.

OIDS are assigned:

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

OIDS are not assigned to the registration authorities, or the certification practice statement.

All OIDS are recorded

- in the relevant certificate policy:
- OID assigned to PostSignum Root QCA is mentioned in each certificate issued under the policy of PostSignum VCA,
- OID CAs to PostSignum Root QCA certificate signed, is mentioned in each certificate policy, according to which issue certificates,

  Certification policy - OID specified in the corresponding certification policy and issued a certificate,

- in the internal documents of the Czech post.

Any change in the certification policy change version of a document; the greater the change in certification policy that has an impact on the applicability of a certificate, warranty, liability, or processes, raises and change of the OID.

9.13 Dispute resolution provisions

See the relevant certificate policy.

9.14 Governing law

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

9.15 Compliance with Applicable law

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

The relationship between the Czech post and the customer is governed by a written contract for the provision of certification services.

The structure of this certification practice statement is in accordance with the structure set out in RFC 3647.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No provisions in this chapter.

9.16.2 Assignment

See the relevant certificate policy.

9.16.3 Severability

See the relevant certificate policy.

9.16.4 Enforcement

The relevant provisions do not apply.

9.16.5 Force Majeure

See the relevant certificate policy.

9.16.6 Accessibility for people with disabilities

See the relevant certificate policy.

9.17 Other

9.17.1 Management documents

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

[eIDAS] REGULATION of the EUROPEAN PARLIAMENT and of the Council (EU) No. 910/2014 of 23 December 2003. July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EN 119 312 ESETSI Electronic Signatures and Infrastructures ' (ESI); Cryptographic Suites

[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

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

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

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

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

[Z101] Act 101/2000 Coll., on personal data protection, as amended

[ZoEP] Act 227/2000 Coll. on electronic signature (repealed by law 297/2016 Coll.)

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

[ZoEI] Act No. 250/2017 Coll. on electronic identification as amended

9.17.2 Links and Literature

[VOP] General terms and conditions of electronic services of Česká Pošta, s. p.

In this document reference is made also to the following internal documents:

[OZU] The command "organizing tasks of CAs and TSAs Česká Pošta, s.p." – Annex No. 2 "provision of Public jobs CA Česká Pošta, s.p." in the current text of the

[SBP] The command "system security policy CAs, TSAs and Česká Pošta, s.p." – Annex No. 2 "system security policy for the role of a Public CA United pošta, s.p." in the current text of the