PostSignum CA Certification Policy applicable to qualified certificates for electronic signature

Version 1.0

TABLE OF CONTENTS

Change and revision record

Version	Effective from	Description and reason for change	Author	Approved by
1.0	01/07/2016	First version	PCA ČP	PAA ČP

1 INTRODUCTION

This document defines rules and procedures for issuing qualified certificates for electronic signatures (hereinafter referred to as "Certificate"). Name of the person using the issued certificate is specified in the certificate name. Certificates are issued to customers or rather to employees of customers (organizations), which are selected by a company representative.

1.1 Overview

Česká pošta, s.p. (Czech Post) (hereinafter referred to as Česká pošta or ČP/Czech Post) operates a certification authority called PostSignum QCA.

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

A customer who is interested in PostSignum QCA services shall conclude a contract describing provision of certification services with the Czech Post. This contract shall specify so-called authorized persons who act under the name of the customer and determine which applicants will be issued the relevant certificates based on individual certification policies. These applicants are registered in the system of the certification authority and apply for the certificate at the registration authority of the Czech Post.

In case of natural persons (no legal person) the authorized person as well as the applicant asking for a certificate is the customer itself and the customer pre-registration process is much simpler. A contract may be concluded and a certificate issued during one single visit at the registration authority.

The Czech Post may agree with the customer to establish special registration process conditions/requirements or to establish a new certification policy.

Qualified certificates issued according to this certification policy are for persons who are also the customer, or who share a certain relation with the customer who concludes the contract describing provision of certification services with the Czech Post. Persons who apply for certificates issued pursuant to this policy, and who will be using them, will be pursuant to applicable legislation.]. A certificate holder is a customer of the Czech Post.

The customer is responsible for the link between his own information and information about the applicant who is asking for the certificate specified on the certificate. The provider of certification services verifies the link between the applicant for a certificate and the public key in the relevant certificate.

Certificates issued according to this certification policy may only be used to verify electronic signature of the signatory pursuant to applicable legislation.

Fulfilment of requirements specified in this policy are established and enforced by the Certification Implementation Guideline PostSignum QCA.

1.2 Document Name and Identification

Tab. 1 Policy identification

Document name	PostSignum CA Certification Policy applicable to qualified certificates for electronic signature
Document version	1.0
Status	final
OID of the provider of	2.23.134

certification services	
OID PostSignum Root QCA	2.23.134.1.4.2.1
OID PostSignum Qualified CA	2.23.134.1.4.2.2
OID of this policy	2.23.134.1.4.1.17.4100
Issue date	21.6.2016
Term of validity	Until recalled, or until PostSignum QCA services are terminated.

1.3 PKI Participants

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

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

Česká pošta, s.p. (Czech Post)

ID No.:47114983, Tax ID No.: CZ47114983

Politických vězňů 909/4, 225 99, Prague 1

Phone: 267 196 111

e-mail: info@cpost.cz

Czech Post is an accredited provider of certification services based on an accreditation document issued by the Ministry of Information of the Czech Republic on 3rd August, 2005.

Czech Post became 1. 7.2016 qualified trust service provider pursuant to [eIDAS].

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

The main task of CA PostSignum QCA is to issue and manage certificates of certification authorities PostSignum Root QCA, PostSignum Qualified CA and customers of the Czech Post pursuant to defined certification policies.

1.3.2 Registration authority (hereinafter referred to as the "RA" only)

Services provided by registration authorities are ensured by the provider of certification services or by an external subject based on a contract concluded with the Czech Post - as the provider of the relevant certification services.

Registration authorities mostly provide the following services:

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

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

Registration authorities operated by an external subject may offer only selected services from the above specified list, which is also specified in a contract concluded between the external subject and the Czech Post.

1.3.3 Subscribers

Holders of qualified certificates and signatory who applied for a qualified certificate (hereinafter referred to as the "certificate" only) and who received the relevant certificate.

1.3.4 Relying parties

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

1.3.5 Other participants

Certification authority PostSignum QCA may use external subjects to provide the relevant services.

1.4 Certificate Usage

1.4.1 Appropriate certificate uses

Qualified certificates issued according to this certification policy may only be used to verify electronic signature of the signatory pursuant with the applicable legislation.

1.4.2 Prohibited certificate uses

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

Qualified certificates issued pursuant to this certification policy may only be used for proper and legal purposes and in accordance with valid legal regulations.

1.5 Policy administration

1.5.1 Organization administering the document

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

1.5.2 Contact person

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

manager.postsignum@cpost.cz

or at the webpage of the provider.

1.5.3 Person determining CPS suitability for the policy

A subject responsible for decisions focusing on the fact how the provider's procedures comply with certification services offered by other providers.
The CA Manager is responsible for managing this certification policy, and also for decisions focusing on the fact how the provider's procedures comply with certification services offered by other providers.

1.5.4 CPS approval procedures

This document has been prepared by a team which creates certification policies of the Czech Post and which is established (as necessary) by the Committee for certification policy of the Czech Post and it is governed and managed by this Committee.

The completed policy is presented by the CA Manager to the Committee for certification policies for approval, which shall also confirm the OID of the policy and will assign a version number to this policy.

1.6 Definitions and Acronyms

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

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

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

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

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

DMZ – demilitarised zone

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

Electronic time-stamp – time-stamp pursuant to [eIDAS]

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

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

Qualified certificate for electronic signature – qualified certificate pursuant to [eIDAS].

Qualified system certificate – qualified system certificate pursuant to [ZoEP].

Qualified time- stamp – qualified timestamp pursuant to [ZoEP].

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

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

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

Business location – central regional workplace/office providing certification and contract registration services.

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

Supervisory body - The supervisory body of trust service providers pursuant to [eIDAS], which is determined under applicable legislation.

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

Indicating person – a person defined in [ZoEP]

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

Creator of a seal – defined in [eIDAS]

PKI – Public Key Infrastructure – infrastructure of public keys

Applicable legislation – Are they applicable legislation regulating the area of the electronic signature, in particular the law on electronic signature then 227/2000 Coll., to their validity, the law on trust services for electronic transactions, the Decree of the Ministry of Informatics No. 378/2006 Coll. of June 19. July 2006 on the procedures of qualified providers of certification services and the REGULATION of the EUROPEAN PARLIAMENT and of the Council (EU) No 910/2014 from 23 July. July 2014 of electronic identification and services creating trust for electronic transactions in the internal market and on the repeal of Directive 1999/93/EC, including the related legislation.

Signatory– a person defined in [eIDAS].

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

PostSignum QCA – a hierarchy of certification authorities, issuing qualified certificates, non-qualified certificate and qualified system certificates pursuant to [eIDAS].

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

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

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

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

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

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

QCA ČP – see PostSignum QCA.

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

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

Private key – a collective term specifying data which are used to create an electronic signature, data necessary for creation of electronic - marks data for creating electronic seals, data for encryption and decryption, and data used for authentication.

Applicant management – application providing information support for registration and record keeping process (hereinafter also referred to as SŽ/AM).

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

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

VCA ČP – see PostSignum VCA.

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

Provider webpage – http://www.postsignum.cz – webpage of a provider offering PostSignum services.

Customer – natural person not performing any business activities, a natural person performing business activities, legal person, state or local government body. Concludes a contract with the Czech Post describing provision of certification services.

Customer – organisation – a subject which requires that the organization name and ID number are specified in the certificate.

Customer – natural person performing business activities – a person performing business activities and assigned with identification number.

Customer –natural person not performing any business activities – a natural person not performing or performing business activities, without assigned identification number.

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

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

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

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

The only exception is a storage located at postsignum.ttc.cz operated by TTC Telekomunikace, s.r.o.

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

2.2 Publication of certification information

Issued certificates are stored in the database of the certification authority.

Information about issued certificates and about operation of PostSignum QCA and documentation belonging to PostSignum QCA are published in the below specified scope.

2.2.1 Certificate and CRL publishing

Certificates of certification authorities are published

- at the webpage of the provider.

  www.postsignum.cz,

  postsignum.ttc.cz or

- at business locations of Czech Post where you may require a copy and save it on your storage media.

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

- at the webpage of the provider.

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

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

2.2.2 Publishing information about certification authority

Certification policies, user management/administ

ration and possibly other documents are published

- at the webpage of the provider, or
- at business locations (only for viewing).

Additional important information, in particular information required by applicable legislation (for example removal of an accreditation, revocation of a system certificate or certificate for electronic seal of the relevant certification authority), or information about emergency events are published

- at the webpage of the provider,
- at business locations and registration authorities in a form of a posted text messages,
- in a nationally distributed daily newspaper

2.3 Time or frequency of publication

Information is published in the following intervals:

- certification policies, certification implementation guidelines and user management/administration are published after the new version is issued and approved.
- certificates - if they were labelled for publishing, are published electronically no later than within 24 hours after the certificate is received;
- information about revoked certificates in the form of a list of revoked certificates (CRL) are published immediately after their issuance, but no later than before the validity of the last published list of revoked certificate expires.
- important information, in particular information required by applicable legislation, are published immediately.

2.4 Access controls on repositories

Certification policies (if they are labelled for publishing), certificates of certification authorities, and list of revoked certificates and other important information are available for reading only without any restrictions.

Provider of certification services does not provide unauthorized access to issued certificates, for which the certificate holder did not provide a consent for publishing.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of name

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

Email address specified in the extension Subject Alternative Name of the certificate complies with RFC-822.

3.1.1.1 MPSV client identifier

Certification authority PostSignum QCA of the Czech Post allows a placement of a client identifier into a qualified certificate issued according to this certification policy. Client identifier is assigned by the Ministry of Labour and Social Affairs (hereinafter referred to as the IK MPSV/ CI MLSA). IK MPSV is placed into the non-mandatory certificate extension Subject Alternative Name – Other Name.

Based on information obtained from a customer, the Czech Post will arrange for the assignment of the client identifier at the Ministry of Labour and Social Affairs, free of charge.

The Czech Post shall arrange for the assignment of the client identifier only if this identifier is to be shown on issued qualified certificates.

3.1.2 Need for names to be meaningful

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

3.1.3 Anonymity or pseudonymity of subscribers

PostSignum Qualified CA does not support pseudonyms of an applicant for a certificate or customer pseudonyms specified under the Certificate subject item.

3.1.4 Rules for interpreting various name forms

Certificates issued by PostSignum Qualified CA support only the following sets of characters:

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

All information documented by the authorized person or by the customer during pre-registration of application for a certificate is inserted into certificates issued by PostSignum Qualified CA in the same form as shown on the presented documents. Transcripts, for example removal of diacritical signs, is not possible.

Email address specified in the extension Subject Alternative Name of the certificate may only be encoded using US ASCII.

3.1.5 Uniqueness of names

Each person in the certification authority system is assigned with a unique identifier which is stored under the "serialNumber" item in the Subject of the certificate. Customers (except for persons not performing any business activities) also assign a number to each applicant for a certificate.

Under the item Subject of certificate you will find a combination of unique data about the customer (Company ID and customer name), as well as unique information about the applicant for a certificate, which guarantees that no two applicants will be issued a certificate with the same Subject.

In case of a collision between two distinguishing names of applicants for a certificate and therefore also a collision of the Subject item on certificates belonging to those two persons the CA Manager shall decide the solution and presents this solution to persons authorized by customers (or rather to customers), immediately upon the appearance of such collision.

3.1.6 Trademarks

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

The customer is responsible for the use of trademarks or registered trademarks in certificate fields which are not verified by the PostSignum QCA (see chapter 3.2.4).

3.2 Initial identity validation

3.2.1 Verification of data compliance - that is the procedure applied during verification focusing on the fact whether data possessed by a person necessary to create electronic signatures match data used to verify electronic signatures.

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

3.2.2 Authentication of organization identity

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

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

3.2.3 Authentication of individual identity

3.2.3.1 Verification of identity of a person performing business activities, or identity of a company employee

A natural person performing business activities demonstrates his identity during pre-registration of customer data, and when submitting an application to issue or revoke a certificate. A company/organisation employee demonstrates his identity when submitting an application to issue or revoke a certificate. One valid, not damaged document shall be presented.

The presented personal document, as specified in the below list, is accepted if the presented document provides information about nationality and identity, and has a photograph of the holder, personal ID number (or date of birth if it applies to foreigners), and information demonstrating validity of the document/expiration date.

- Citizens of the Czech Republic shall present personal ID or passport.

- Foreign citizens shall present travel, diplomatic, company or any other type of passport issued by the foreign state, or a permit issued by Czech authorities and allowing the foreign person to stay in the Czech Republic.
  Citizens of EU member states and citizens of Iceland, Liechtenstein, Norway and Switzerland may also submit a personal document, which was issued to them by the relevant country and which is used to demonstrate their identity in their country.

3.2.3.2 Verification of identity of a natural person not performing any business activities

A person not performing any business activity shall demonstrate his identity during the conclusion of a contract describing provision of certification services, and when submitting application for a certificate. One valid, not damaged personal document shall be presented plus additional, valid and undamaged document.

The presented personal document, as specified in the below list, is accepted if the presented document provides information about nationality and identity, and has a photograph of the holder, personal ID number (or date of birth if it applies to foreigners), and information demonstrating validity of the document/expiration date.

- Citizens of the Czech Republic shall present valid personal ID or passport as additional personal document.

- Foreign citizens shall present (as personal document) travel, diplomatic, company or any other type of passport issued by the foreign state, a special foreign passport valid in all world countries, travel passport demonstrating identity, or a permit issued by Czech authorities and allowing the person to stay in the Czech Republic.
  Citizens of member states of the European Union and citizens of Iceland, Liechtenstein, Norway and Switzerland may also submit a personal document, which was issued to them to demonstrate their identity in their country.

The additional personal document, from the below specified list of documents is accepted, if it is not presented as the first personal document

- Citizens of the Czech Republic shall present - as the additional personal document, a valid personal ID or passport, driver license, TP, ZTP, ZTP/P, card or birth certificate.

- Foreign citizens shall present as additional personal document a travel, diplomatic, company or any other type of passport issued by the foreign state, a special foreign passport valid in all world countries, travel passport demonstrating identity or a permit issued by Czech authorities and allowing the person to stay in the Czech Republic, or European Union driving license.
  Foreigners may also present as the additional personal document a personal document, which was issued to them to demonstrate their identity in their country. Type of document and information on the document must be written in Latin alphabet and the document must contain English translations of the above specified terms/information.

3.2.4 Non-verified subscriber information

Email address of the applicant for a certificate is located in the mandatory certificate extension under "Subject Alternative Name" item. The Czech Post, as the provider of certification services, does not verify the existence of the email address or the actual relationship between the email address and the applicant for a certificate. Therefore, this item cannot be used as the identification of the certificate holder.

The Czech Post, as the provider of certification services, does not further verify the correctness of the following:

- information describing the position of the applicant in terms of a customer,
- information about the organisational unit where the applicant for a certificate works,
- employee number,

information specified in the list of applicants which is given to the provider of certification services by a person authorized by the customer.

3.2.5 Validation of authority

No provisions available in this chapter.

3.2.6 Criteria for interoperation

Possible cooperation with other providers of certification services is possible only if the Committee for certification policy of the Czech Post approves it and based on a contract concluded under conditions defined by this Committee.

3.3 Identification and authentication for re-key requests

Identification and authentication occurring during processing of application for data exchange used to verify electronic signatures.

3.3.1 Identification and authentication for re-key after revocation

Identification and authentication occurring during a routine exchange of data used to create electronic signatures and data corresponding with data used to verify electronic signatures (hereinafter referred to as "paired data" only).

Identity of the applicant for a follow-up certificate is verified during the verification of electronic signature present on the application for the issuance of a follow-up certificate. A valid certificate (not revoked and still valid) and belonging to the applicant must be used to sign the relevant application. This certificate must be issued according to:

- PostSignum Qualified CA certification policy applicable to qualified personal certificates version 1.0 and higher or
- certification policy PostSignum Qualified CA for qualified certificate for electronic signature version 1.0 and higher.

3.3.2 Identification and authentication during exchange of paired data after certificate revocation

In case of a revoked certificate and during the identification and authentication process which occurs in connection with the issuance of a new certificate, it is necessary to proceed in the same way as during the first identity verification process done during the issuance of the first certificate (see chapter 3.2.3).

3.4 Identification and authentication for revocation request

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

- by providing a password entered during the registration for the issuance of a certificate, or

- by presenting one personal document, if it concerns an employee of an organisation or natural persons performing business activities; or one personal document and one additional document if it concerns a person not performing business activities (see chapter 3.2.3).

An authorized person shall demonstrate its identity:

- by signing a written application for certificate revocation, or

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

- by a personal document when application for a certificate revocation is presented in person at a registration authority of the Czech Post; an employee of the registration authority also verifies whether the authorized person is on the updated list of authorized persons.

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

Also supervisory body may require a revocation of a qualified certificate. In this scenario, the authorized applicant for a qualified certificate revocation is a representative of the supervisory body.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

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

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

- persons selected by an authorized person of the customer – organisation, or
- natural persons performing business activities who concluded a contract describing provision of certification services, or
- natural persons not performing business activities who concluded a contract describing provision of certification services.

4.1.2 Certificate application processing

4.1.2.1 Contract conclusion

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

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

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

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

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

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

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

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

4.1.2.2 Pre-registration of applicants for a certificate

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

services. If it concerns a person not performing any business activities, the customer will handover data about one single applicant.

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

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

Registration authority verifies the identity of the applicant for a certificate using documents specified in chapter 3.2. A link between the applicant and customer (organisation) specified on the certificate is guaranteed by an authorized person of the customer (organisation) who manages the list of applicants given to the provider of certification services.

4.1.2.3 Customer responsibilities

In particular the customer is obligated:

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

If the customer is a person not performing any business activities then applicant responsibilities specified under chapter 4.1.2.5 shall also apply to that person.

4.1.2.4 Responsibilities of authorized persons

In particular, the authorized person is responsible:

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

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

Authorized person or the actual customer informs the Czech Post on what certificates the relevant client identifier issued by the Ministry of Labour and Social Affairs must be specified.

4.1.2.5 Applicant responsibility

In particular, the applicant (signatory) is obligated:

- to provide true and complete information during the registration of an application for a certificate, and during registration of an application to issue a follow-up certificate,

- to verify whether information on the certificate is correct and correspond with the required data,
- to use and handle private key which correspond with the public key in the certificate issued pursuant to this certification policy with due diligence and to make sure that the key cannot be misused,
- to use private key and the relevant certificate issued pursuant to this certification policy only for purposes specified in this certification policy,
- immediately inform the provider of certification services about any circumstances that may result in certificate revocation, in particular, if there is a suspicion that a private key was misused, to require certificate revocation and stop using the relevant private key,
- to get acquainted with the certification policy based on which the certificate was issued,
- after paired data are generated (private and public key), to make sure that they are stored/backed up properly, if is technically possible.

4.1.2.6 Provider responsibilities

Provider of certification services is obligated:

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

4.2 Application for a certificate processing

4.2.1 Identification and authentication

The applicant for a certificate shall come to the registration authority workplace and present the following documents:

- one personal document if it concerns an employee of an organisation or a person performing business activities, or
- one personal document plus one additional personal document if it concerns a person not performing business activities.

The applicant for a certificate has an option to provide a password for possible revocation of the certificate, if the registration authority system allows such option. If the applicant applies for a follow-up certificate revocation password may be sent in an encoded format. The password must conform to the following requirements (at least 8 characters, containing at least one lowercase letter, at least one uppercase letter, at least one digit and at least one non-alphabetic character). If the applicant does not provide the password, or if the password does not comply with the requirements it will be generated automatically by the system. Password for a certificate revocation is always specified on the certificate issuance protocol.

An employee of the registration authority checks the identity of the applicant for a certificate based on the submitted personal document and in the event that the applicable legislation requires, creates and saves a copy of personal identification of the applicant for a certificate.. Using the list of applicants, the employee also verifies whether this person is allowed to apply for a certificate under the relevant certification policy.

4.2.2 Approval or rejection of certificate applications

4.2.2.1 Rejection or acceptance of the first application for a certificate

The applicant provides the employee of the registration authority with an electronic application in PKCS#10 format containing public key either saved on a storage media or through other means specified on the webpage of the provider.

Information about the valid list of applicants will be integrated into the certificate.

If all data are confirmed and approved by the applicant, the employee of the registration authority approves the issuance of the certificate and if not, the employee of the registration authority will reject the certificate.

If the employee of the registration authority is not sure about the correctness of the presented identity document, or if there are other discrepancies, he will reject to issue the certificate and inform the applicant about the relevant discrepancy.

4.2.2.2 Rejection or acceptance of an application for a follow-up certificate

The applicant provides the employee of the registration authority with an electronic application in PKCS#10 format containing electronic public-key through means specified on the webpage of the provider.

Information about the valid list of applicants will be integrated into the certificate.

The registration authority will verify electronic signature on the application, in particular, the validity of the certificate which was used to verify signature at the time of the delivery of the application by the Czech Post (it must be valid), and the issuing certification authority (PostSignum Qualified CA), and will inspect other information or elements of the application.

If the electronic signature on the application for a follow-up certificate cannot be verified, or if not all follow-up certificate issuance requirements have been complied with, the registration authority will reject to issue the certificate and will inform the applicant about it.
The Czech Post reserves its right to reject the issuance of a follow-up certificate under this certification policy.

If the employee of the registration authority is not sure about the correctness of the presented application request for a subsequent certificate, or if there are other discrepancies, he will reject to issue the certificate and will inform the applicant about the discrepancy.

4.2.3 Time to process certificate applications

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

4.3 Certificate issuance

After the application for a certificate is inspected and approved, the registration authority will enter this application into the system of the certification authority for further processing. Based on this application the certification authority system will issue the relevant certificate and will return it back to the registration authority and to publishing services (to a company providing publishing services).

The certificate will become valid immediately upon its issuance.

4.3.1 CA actions during certificate issuance

Certificate is issued by the system of the certification authority automatically after the application is received from the registration authority.

4.3.2 Notification to subscriber by the CA of issuance of certificate

Employee of the registration authority hands over to the applicant a printout of the certificate issuance protocol with data shown on the certificate immediately after the certificate is issued, or similarly as in a situation when a follow-up certificate is issued, information is sent to the email address of the applicant specifying the location of the issued certificate (URL) where the issued certificate may be accepted (certificate acceptance confirmation) and where the certificate, including certificate issuance protocol, may be downloaded.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

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

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

- that he is taking over responsibilities and obligations ensuing from certification policy according to which the certificate was issued,

- that he is not aware of any facts that could demonstrate that the private key corresponding with the public key on the certificate is owned by other person than the authorized person specified in the relevant certification policy,

- that data and information shown on the issued certificate are correct and complete (in particular, that the public key of the certificate corresponds with the public key specified on the provided PKCS#10 application).

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

The issued certificate is given to the signatory in DER format.

4.4.2 Publication of the certificate by the CA

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

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

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

This provision does not apply to the list of all qualified certificates issued based on a request of the supervisory body.

4.5 Paired data and certificate usage

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

4.5.1 The use of data for the purpose of creating electronic signatures certificates done by the certificate holder or signatory.

Signatory:

- uses and handles private key which correspond with the public key on the certificate issued pursuant to this certification policy with due diligence, while making sure that the key cannot be misused,

- in case of a loss or theft, or if there is a suspicion that the private key was compromised, the signatory must inform the provider of certification services about it immediately and stop using the specified private key,

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

4.5.2 The use of data for authentication of electronic signatures certificates by the relying party

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

- obtains PostSignum Qualified CA and PostSignum Root QCA certificates from a safe source (webpage of the provider, webpage of the supervisory body, or at the registration authority workplace) and verifies fingerprints of these certificates.

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

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

4.6 Certificate renewal

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

4.6.1 Circumstance for certificate renewal

PostSignum QCA does not provide this service.

4.6.2 Who may request renewal

PostSignum QCA does not provide this service.

4.6.3 Renewal certificate request processing

PostSignum QCA does not provide this service.

4.6.4 Notification of new certificate issuance to subscriber

PostSignum QCA does not provide this service.

4.6.5 Conduct constituting acceptance of a renewal certificate

PostSignum QCA does not provide this service.

4.6.6 Publication of the renewal certificate by the CA

PostSignum QCA does not provide this service.

4.6.7 Notification of certificate issuance by the CA to other entities

PostSignum QCA does not provide this service.

4.7 Exchange of data for authentication of electronic signatures certificate

A service called exchange of data used for authentication of electronic signatures certificate refers to the issuance of a follow-up certificate. This term will be used throughout this text.

4.7.1 Conditions for data exchange used for verification of electronic signatures in certificate

The issuance of a follow-up certificate is subject to provisions specified under chapter 3.3.1.

If not all these requirements are met the follow-up certificate cannot be issued and procedures specified under chapter 4.2 shall apply.

4.7.2 Subjects authorized to require exchange of data for verification of electronic signatures

Application to issue a follow-up certificate in line with this certification policy may be submitted by persons who were issued a certificate and who require the issuance of the necessary follow-up certificate.

4.7.3 Processing of data exchange request, used for verification of electronic signatures

An applicant requiring the issuance of a follow-up certificate shall submit his application while following procedures specified at the webpage of the provider.

Application for a follow-up certificate processing is subject to provisions specified under chapter 4.2.1 and 4.2.2.2.

4.7.4 Notification about the issuance of a certificate containing exchanged data used to verify electronic signatures sent to a signatory

Notification describing the issuance a follow-up certificate is subject to provisions specified under chapter 4.3.2.

4.7.5 Activities related to the acceptance of a certificate containing exchanged data used to verify electronic signatures

The acceptance of a follow-up certificate is subject to provisions specified under chapter 4.4.1.

4.7.6 Publishing of issued certificates containing exchanged data used to verify electronic signatures

Publishing of a follow-up certificate is subject to provisions specified under chapter 4.4.2.

4.7.7 Notification about the issuance of a certificate containing exchanged data used to verify electronic signatures sent to other subjects

Notification about the issuance of a follow-up certificate is subject to provisions specified under chapter 4.4.3.

4.8 Certificate modification

Certificate with modified data may be issued only as

- a new certificate, while following procedure specified in chapters 4.1 through 4.4, or
- as a follow-up certificate issued under condition specified in chapter 4.7, providing that only those data were changed which are allowed to be changed on follow-up certificates by this certification policy.

Data change must be reported by the customer to the provider using suitable notification method, before a new application for a new or follow-up certificate is submitted.

If any data shown on the current certificate are no longer valid, it is necessary to request a revocation of such certificate through suitable and accepted means.

4.8.1 Circumstance for certificate modification

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

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

4.8.2 Who may request certificate modification

Change list of applicants is submitted by the authorized person of the customer (organisation, a natural person performing business activities), or by the customer alone (natural person not performing business activities).

4.8.3 Processing certificate modification requests

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

- if it concerns an authorized person, the system shall verify whether this person is listed on the current list of authorized persons of the customer; if such person is physically present (a visit) then the identity of such person is checked based on presented personal ID/documents,

- if it concerns the customer itself, whether the customer has concluded a valid contract describing provision of certification services, and the identity of the customer according to presented personal ID/documents.

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

4.8.4 Notification of new certificate issuance to subscriber

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

4.8.5 Conduct constituting acceptance of modified certificate

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

4.8.6 Publication of the modified certificate by the CA

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

4.8.7 Notification of certificate issuance by the CA to other entities

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

4.9 Certificate revocation and suspension

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

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

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

- Telephone (nonstop)

Telephone: 556 316 298

- Fax (nonstop)

Fax: 556 300 013

- E-mail (nonstop)

e-mail: postsignum@cpost.cz

- Web application (nonstop)

Website: www.postsignum.cz/zneplatneni_certifikatu.html

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

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

4.9.1 Circumstances for revocation

The main reasons for end-user certificate revocation are as follows:

- any suspicion that a certificate private key may have been compromised,
- failure of a customer to comply with requirements specified in the contract describing provision of certification services,
- order issued by the supervisory body,
- request of the certificate holder or signatory,
- other reasons (death, termination, restriction or deprivation of legal rights of the signatory; loss of information accuracy based on which the certificate was issued).

4.9.2 Who can request revocation

Certificate revocation may be requested by:

- customer (certificate holder) through the use of an authorized person or statutory representative, or in person (if it concerns a person not performing any business activities),
- applicant (signatory),
- CA Manager,
- representative supervisory body,

4.9.3 Procedure for revocation request

4.9.3.1 A request for a certificate revocation submitted in person by the signatory to the registration authority

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

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

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

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

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

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

If the revocation is successful, a revocation protocol is created and emailed to the applicant to the email address specified on the revoked certificate.

4.9.3.3 A request for a certificate revocation submitted by authorized person

If the customer requires certificate revocation, he shall do so in written form. The authorized person shall come in person to the registration authority of the Czech Post, where a written application for a certificate revocation will be produced. A written revocation request may also be sent by the authorized person via fax to the fax number specified in chapter 4.9.

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

If the revocation is successful, a revocation protocol is created and emailed to the authorized person. The applicant is informed about the certificate revocation by email sent to the contact address and to the address specified in the revoked certificate.

4.9.3.4 Certificate revocation required by the certification authority

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

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

4.9.3.5 Revocation of a certificate required by the supervisory body

Also the supervisory body may decide to revoke a qualified certificate. In such scenario, PostSignum QCA will inform the customer about the certificate revocation and will specify reasons why the certificate was revoked. Representative of the supervisory body will submit written request for a certificate revocation to the CA Manager. This request must include the reason for the certificate revocation.

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

4.9.4 Revocation request grace period

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

4.9.5 Time within which CA must process the revocation request

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

4.9.6 Responsibilities of relying parties verifying the certificate revocation

The user of the certificate issued by PostSignum Qualified CA (relying party) is obligated to proceed in line with provisions specified in chapter 4.5.2.

4.9.7 Frequency of the issuance of revoked certificates

A list of revoked certificates (CRL) is issued immediately after the request to revoke a certificate is processed. If the certificate is not revoked, new CRL is issued at least every 24 hours (usually every 4 hours). The list of revoked certificates is published:

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

Primary source of the current CRL are CRL distribution locations.

4.9.8 Maximum allowed delay when issuing a list of revoked certificates

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

4.9.9 An option to verify status of the certificate online (hereinafter referred to as the "OCSP"= Online Certificate status protocol)

To verify the certificate issued under this certificate policy may be used publicly available OCSP free service, which is provided according to RFC 2560.

Link to the OCSP responder is presented in the certificate issued under this Certification Policy, refer to certificate profile - Chapter 7.

OCSP responder in certificate profile, profile requests and responses OCSP responder is listed in the certification policy for the issuance of certificate OCSP which is available on the website of the provider.

4.9.10 Requirements for online certificate status verification

See provisions under item 4.9.9.

4.9.11 Other forms of revocation advertisements available

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

4.9.12 Any possible variations in the procedure or certificate revocation - applies to situations when data used to create electronic signatures have been compromised

The certificate revocation process - if data used to create electronic signatures have been compromised, is the same as the certificate revocation process.

4.9.13 Circumstances for suspension

PostSignum QCA does not provide this service.

4.9.14 Who can request suspension

PostSignum QCA does not provide this service.

4.9.15 Procedure for suspension request

PostSignum QCA does not provide this service.

4.9.16 Limits on suspension period

PostSignum QCA does not provide this service.

4.10 Certificate status services

Certificate status may be verified:

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

4.10.1 Operational characteristics

List of revoked certificates and information about certificate status is considered public information. The list of revoked certificates (CRL) is published at locations specified under chapter 4.9.7.

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

OCSP service returns certificate status in real time (online) on the basis of sent request. Information and data about certificate status obtained through OCSP service are trusted information.

4.10.2 Service availability

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

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

OCPS service is available 7 days a week 24 hours a day.

4.10.3 Other characteristics of certificate status service

Other characteristics of certificate status services have not been established.

4.11 Termination of services used by the holder of the certificate or signatory

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

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

4.12 Storage of data used to create electronic signatures handled by trusted third party, and data recovery

PostSignum QCA does not provide this service.

4.12.1 Policies and procedures applicable to storage and recovery of data used to create electronic signatures

PostSignum QCA does not provide this service.

4.12.2 Policies and procedures for encryption key encapsulation and for recovery for recovery of the encryption key in the related session

PostSignum QCA does not provide this service.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

The following documents were processed on behalf of PostSignum QCA:

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

The above-mentioned documents were produced based on risk analysis results.

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

5.1 Physical security controls

5.1.1 Site location and construction

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

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

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

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

5.1.2 Physical access

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

5.1.3 Power and air-conditioning

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

5.1.4 Water exposures

Central workplaces are located outside of flood areas.

Central workplaces areas are equipped with flood warning system.

5.1.5 Fire prevention and protection

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

5.1.6 Media storage

Safety boxes are used to store PostSignum QCA data

5.1.7 Waste management

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

- storage media are physically destroyed or a suitable software is used ensuring complete deletion of data stored on the media,
- paper documents are destroyed using proper shredding equipment.

5.1.8 Off-site backup

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

5.2 Procedural Controls

5.2.1 Trusted roles

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

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

5.2.2 Number of persons required per task

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

5.2.3 Identification and authentication for each role

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

5.2.4 Roles requiring division of responsibilities

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

5.3 Personnel security controls

5.3.1 Requirements on qualification, experience and clearances

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

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

5.3.2 Assessment of personal reliability

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

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

5.3.3 Requirements for the preparation for role performance

All employees involved in the operation, management, maintenance and development of PostSignum QCA systems are properly trained. The training also includes a course focusing on system safety and behaviour of the system during emergency situations.

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

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

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

5.3.4 Training frequency and training requirements

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

CA Manager organizes regular operator training (in particular when PostSignum QCA procedures are changed, but at least once during every 2 years).

5.3.5 Job rotation frequency and sequence

Requirements on employee rotation frequency have not been defined.

5.3.6 Sanctions for unauthorized actions

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

5.3.7 Independent contractor requirements

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

5.3.8 Documentation supplied to personnel

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

- safety policy,
- certification policy,
- certification implementation guideline,
- operational documentation – manuals and work procedures designed for operators.

5.4 Audit Logging Procedures

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

5.4.1 Types of recorded events

In order to check, analyse or investigate emergency events (in general, to be able to demonstrate the sequence of PostSignum QCA operations and their assignment to a particular person who called them), records describing issuance of certificates, termination of certificates, the use of keys and PostSignum QCA certificates, as well as other important records are stored (for example termination of activities of a certification authority).

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

5.4.2 Record processing frequency

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

5.4.3 Auditing report storage time

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

5.4.4 Protection of auditing logs

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

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

5.4.5 Auditing log back up procedures

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

5.4.6 Auditing log collection system (internal or external)

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

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

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

5.4.8 Evaluation of vulnerability

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

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

5.5 Records Archival

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

5.5.1 Types of records archived

In PostSignum QCA the following records are being archived:

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

5.5.2 Retention period for archive

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

5.5.3 Protection of archive

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

5.5.4 Archive backup procedures

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

5.5.5 Requirements for time-stamping of records.

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

5.5.6 Archive collection system (internal or external)

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

5.5.7 Procedures to obtain and verify archive information

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

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

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

5.6 Exchange of data for verification of electronic marks or electronic seal in a superior qualified system certificate or certificate for electronic seal of the provider

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

Sufficiently in advance, but no less than one year before the validity of PostSignum Root QCA certificate expires, a new ceremonial issuance of the new certificate must take place. The result of the ceremony is the actual creation of a new self-signed certificate of root certification authority, which shall be published while following procedures specified in chapter 2.

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

Planned exchange of keys of certification authority must be reported to customers no later than 3 months before active use of the new PostSignum Root QCA certificate, or rather 1 months before the active use of PostSignum Qualified CA certificate. This notification (including the reason for the termination of the certificate validity) shall be published at the webpage of the provider and at all offices/workplaces of PostSignum QCA registration authority.

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

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

5.7 Compromise and disaster recovery

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

These documents are available (in addition to other persons) to persons inspecting PostSignum QCA.

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

5.7.1 Incident and compromise handling procedures

Protection procedures applicable to the certification authority after a natural disaster or other emergency situation occurred, have been described in documents called Building emergency plan, Emergency situation plan and Restoration plan.

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

Protection procedures applicable to the certification authority after a natural disaster or other emergency situation occurred, have been described in documents called Building emergency plan, Emergency situation plan and Restoration plan.

5.7.3 Procedure applicable to situations when data used for the creation of provider's electronic marks or electronic seal have been compromised

5.7.3.1 Subordinate certification authority key disclosure

If there is a suspicion that private key PostSignum Qualified CA has been compromised, all certificate holders, and the supervisory body and to subjects which have concluded contract directly related to the provision of certification services will be informed electronically about the fact that this authority will no longer provide its activities. This notification will also be published at the webpage of the provider and at all registration offices/workplaces of PostSignum QCA and in one nationally published newspaper. This notification shall also specify the reason for the termination of the certificate belonging to this particular certification authority.

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

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

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

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

5.7.3.2 Disclosure of PostSignum Root QCA key

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

newspaper. This notification shall also specify the reason for the termination of the certificate belonging to this particular certification authority.

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

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

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

5.7.4 Business continuity capabilities after a disaster

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

5.8 CA or RA Termination

5.8.1 Termination of activities of root certification authority

Written notification of termination of activities of PostSignum Root QCA must be delivered to all holders who possess valid certificates, to the supervisory body and to subjects which have concluded contracts directly related to the provision of certification services. This notification must also be published at the webpage of the provider and at all registration offices/workplaces of PostSignum QCA. If the termination of activities of the relevant authority also includes a termination of the validity of its certificate, the notification must also specify this information and explain the reason for the termination. If at least one certificate issued by PostSignum Root QCA remains valid, PostSignum Root QCA must provide (at least) a certificate revocation function and CRL issuance function.

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

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

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

5.8.2 Termination of activities of a subordinate certification authority

Written notification of termination of activities of PostSignum Qualified CA must be delivered to all holders possessing valid certificates, to the supervisory body and to subjects which have concluded contracts directly related to the provision of certification services. This notification must also be published at the webpage of the provider and at all registration offices/workplaces of PostSignum QCA. This

notification must also provide information about certificate termination including explanation of reasons for the termination. If at least one certificate issued by PostSignum Qualified CA remains valid, PostSignum Qualified CA must provide (at least) certificate revocation function and CRL issuance function.

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

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

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

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

5.8.3 Termination of activities of registration authority

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

5.8.4 Termination of activities of a provider of certification services

Activities of a provider of certification services are terminated pursuant to applicable legislation.

5.8.5 Accreditation removal

If an accreditation is removed, information about this removal must be delivered electronically or in written form to holders of valid certificates and to subjects which have concluded contracts directly related to the provision of certification services. This information must also be published at the webpage of the provider and at all registration offices/workplaces of PostSignum QCA, or published through other means specified under applicable legislation. This information must also include a statement saying that qualified certificates issued by this provider can no longer be used - as specified in applicable legislation.

Based on a decision issued by the supervisory body the management of the Czech Post shall decide how to proceed further.

6 TECHNICAL SECURITY CONTROLS

6.1 Paired data Generation and Installation PostSignum QCA does not provide a key (paired data) generation service on behalf of the applicant for a certificate. PostSignum QCA does not come into contact with applicant private keys, and it is not responsible for key protection or backup.

6.1.1 Generating paired data

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

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

Key pairs of PostSignum QCA operators (including RA operators; inspection keys) are generated in dedicated hardware resources which do not allow (due to their structure) private key exporting. In order to use private keys, PIN must always be entered.

Applicant private keys are generated and stored by the applicant for a certificate. Keys may be generated and then stored both in software and hardware storage units. PostSignum QCA does not prescribe specific storage requirements.

6.1.2 Transfer of data for the creation of electronic signatures over to a signatory.

PostSignum QCA does not provide key pair generation service on behalf of the applicant for a certificate.

6.1.3 Transfer of data for verification of electronic signatures over to a provider of certification services

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

6.1.4 Providing data necessary for verification of electronic signatures, data used to verify electronic marks or electronic seal by certification authority to relying parties.

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

6.1.5 Paired data sizes

Keys of certification authorities in PostSignum hierarchy for RSA algorithm have a module which is minimum 2048 bits long.

Keys of certification holders for RSA algorithm have a module which is 2048 or 4096 bits long. Other than RSA algorithms cannot be used by certificate holders.

6.1.6 Generating data parameters necessary for verification of electronic signatures generating data used to verify electronic marks or data for verify electronic seal, and inspections of their quality

Parameters used to create public keys of PostSignum QCA components are generated by adequate software and hardware. Used algorithms and their parameters comply with applicable legislation or standards or technical standards, which regulate the activities of certification services providers.

Parameters used to create public keys for applicants for a certificate are generated by adequate software and hardware of the applicant and the provider of certification services is responsible for them.

Inspection of data quality necessary for verification of electronic signatures inspection of data used to verify electronic marks is done at the level of the certification authority, which inspects the uniqueness and the allowed length of the public key.

6.1.7 Restrictions applicable to data used for verification of electronic signatures

End user public keys may only be used in compliance with regulations described in chapter 1.4

6.2 Protection of data necessary for the creation of electronic signatures necessary for the creation of electronic marks or data for verify electronic seal and safety of cryptographic modules

6.2.1 Standards and requirements of the use of cryptographic modules

Cryptographic module used to generate and store private keys of certification authorities (a tool used to create electronic signature, electronic marks or electronic seal) is active within the PostSignum QCA hierarchy, and complies with FIPS 140-2 Level 3 standards. The supervisory body has issued a compatibility standard for this module pursuant to applicable legislation.

6.2.2 Secret sharing

Public key of a certification authority is stored during operations in an activated and configured cryptographic module (safe cryptographic module), which may be turned ON or OFF by a single person.

In order to activate cryptographic module (safe cryptographic module) and to restore a private key after a breakdown (or in other cryptographic module) a cooperation of at least three persons is required.

6.2.3 Storage of data used to create electronic signatures, data for create electronic marks or data for verify electronic seals

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

6.2.4 Backup of data used to create electronic signatures data used to create electronic marks or data for verify electronic seal

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

6.2.5 Storage of data used to create electronic signatures data used to create electronic marks or data for verify electronic seal

Private keys of certification authorities in the PostSignum QCA hierarchy are not archived. When a certification authority terminates its activities, key and key backups are destroyed and report describing the actual destruction process is produced.

6.2.6 Transfer of data used to create electronic marks or data for verify electronic seal into a cryptographic module or from a cryptographic module

Private key of a certification authority is generated in cryptographic module (safe cryptographic module), and all operations using unencrypted key are done only in this module. The key only leaves the cryptographic module in a form of encrypted backups created and protected pursuant to requirements

specified in internal documents called System safety policy, Operational and safety procedures, and Auditing archiving policy (a part of [SBP]).

The key is entered (loaded) in the original cryptographic module from backups after a single employee is authorized to enter key backups and the cryptographic module.

The key is loaded in the new or initialised cryptographic module from backups, after two employees who have no access to the private key backup, and who do not have the right to activate the private key (certification authority process initiation) have been authorized.

6.2.7 Storage of data used to create electronic/marks or data for verify electronic seal in cryptographic module

Private key of a certification authority is stored in unencrypted form in activated and configured cryptographic module (safe cryptographic module), which may be turned ON or OFF by a single person.

In order to activate cryptographic module (safe cryptographic module) and to restore a private key after a breakdown (or in other cryptographic module) a cooperation of at least three persons is required.

6.2.8 Activation process of data used to create electronic signatures data used to create electronic marks or data for verify electronic seal

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

6.2.9 Deactivation process of data used to create electronic signatures data used to create electronic marks or data for verify electronic seal

Private key of a certification authority is deactivated by an authorized operating staff in accordance with internal documents called System safety policy, and Operational and safety procedures.

6.2.10 Destruction of data used to create electronic signatures data used to create electronic marks or data for verify electronic seal

A private key belonging to a certification authority stored in a cryptographic module will be destroyed through means offered by the cryptographic module, providing that the cryptographic module is to be used for other temporary purposes, or if activities of the cryptographic module are terminated, or if the certification authority - whose keys were stored in the cryptographic module, is terminated. Destruction of a private key is done by a person authorized pursuant to internal documents called System safety policy, and Operational and safety procedures, or based on requirement of the CA Manager.

The private key is destroyed by putting the cryptographic module into initialisation status which allows the user to erase safely all cryptographic information/material (including private CA key) through the use of cryptographic mechanisms. The destruction of private key also includes deletion of all backup copies of the relevant key and deactivation of cards used to access these keys.

6.2.11 Cryptographic module evaluation

Due to the fact that the cryptographic module used to save private key of a certification authority has successfully passed the evaluation according to FIPS 140–2 standards, level 3, it is not assumed that the module would contain serious errors in terms of structure. Nevertheless, the device is continuously monitored with the intention to discover possible attacks, to identify them and to respond as quickly as possible.

6.3 Other aspects of paired data management

6.3.1 Storage of data used for verification of electronic signatures

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

6.3.2 Operational period of the certificates issued to the subscriber

The length of validity of a certificate issued under this certification policy is specified on the certificate itself.

6.4 Activation data

PostSignum QCA system uses various types of activation data, for example access passwords, PINs, and others. All aspects related to activation data, their generation process, installation, and use are described in internal documents called System safety policy, Operational and safety procedures, and in applicable internal operational documents.

6.4.1 Generating and installing activation data

Activation data are usually created or entered by an employee who will be using them. In other situations, when activation data are generated by other subject, random data complying with general requirements are used and the necessary responsibility to immediately modify randomly generated data is defined and established.

All created activation data must comply with requirements on their length and structure.

6.4.2 Activation data protection

All activation data must be protected from unauthorized disclosure to third parties. All employees of PostSignum QCA must comply with these requirements, which are specified in the System safety policy document.

6.4.3 Other activation data aspects

Other aspects related to activation data, their generation process, installation and use are described in internal documents called System safety policy, Operational and safety procedures, and in applicable internal operational documents.

6.5 Computer security Controls

6.5.1 Specific technical requirements on computer controls

Each component within the PostSignum QCA hierarchy has been defined with a configuration setting ensuring safety of the relevant component at the technological level, which are based on requirements specified in applicable legislation and other related documents, in particular on [CWA 141671] and [TS 101456] standards.

6.5.2 Computer safety evaluation

PostSignum QCA system underwent and passed an external inspection focusing on compatibility and compliance with requirements specified in the relevant legislature applicable to qualified providers of trust services, in particular, requirements specified in [eIDAS].

6.6 Life-cycle safety

6.6.1 System development management

System implementation was done according to KeyStep methodology, which has been specially created for design and implementation of large PKI projects. Development of individual applications was done according to internal methodology of the Czech Post.

Following changes are implemented according to defined change management process.

6.6.2 Safety management inspections

Safety of PostSignum QCA systems is verified by means of operational controls/inspections performed under the established information system safety management ISO 27001, also by inspections of compatibility safety carried out by employees of the Czech Post and through external audits performed by an external company.

6.6.3 Life-cycle safety management

A part of the change management process is also an evaluation of impacts of the safety management process. In case of large changes or after implementation of series of smaller changes, an analysis focusing on different or repeated risks is performed.

6.7 Network security

Local networks used by central workplaces (main and backup locations) contain central PostSignum QCA systems, which are separated from the internal Czech Post network with a firewall. This firewall does not allow any communication coming from the internal network of the Czech Post towards local networks containing PostSignum QCA systems. Any communication directed towards the local network of the central workplace ends on dedicated DMZ.

In addition, internal network of the Czech Post is separated from all external networks, including the Internet, with its own firewall.

All communication occurring outside of dedicated local networks of central workplaces is encoded.

6.8 Time-stamps

See chapter 5.5.5.

7 PROFILES OF CERTIFICATES, REVOKED CERTIFICATES AND OCSP

7.1 Certificate profile

PostSignum QCA issues certificates complying with X.509 standard. Profile of a qualified certificate for electronic signature is specified in the following table. CA reserves the right to insert additional items in the certificate, if it will require a change in legislation or technical standards, which regulate the activities of certification services providers.

Tab. 2 Profile of qualified personal certificate

Item	Value	Mandatory item	Change	ORG	PFO	NFO
Version	3 (0x2)	These items are mandatory for all issued certificates and cannot be changed.				
Serial number	certificate serial number assigned by certification authority					
SignatureAlgorithm	sha256WithRSAEncryption					
Issuer						
Country Name	CZ	These items are mandatory for all issued certificates and cannot be changed. (X is a number indicating the particular subordinate CA)				
Organisation Name	Česká pošta, s.p. [Company ID No. 47114983] *the above number is the Czech Post company ID*					
CN CommonName	PostSignum Qualified CA X					
Validity						
Not Before	Beginning of validity of the issued certificate (UTC time)	These items are mandatory for all issued certificates and cannot be changed.				
Not After	End of validity of the issued certificate (UTC time)					
Subject						
C Country Name	CZ	**yes**	no	X	X	X
L Locality Name	Permanent address/contact address of a natural person	no	**yes**			X
Organization Identifier	According to the international standards organization ID in form: NTRCZ-organization ID	yes	**yes**	X	X	
O organizationName	Name of a legal person or natural person performing business activities in the following form: Customer name [customer company ID]	**yes**	**yes**	X	X	
OU organizationalUnitName	distinguishing organisational unit of a legal person or natural person performing business activities	no	**yes**	X	X	
OU organizationalUnitName	Organisational unit	no	**yes**	X	X	
OU organizationalUnitName	Number of an applicant applying for a certificate within the customer environment – organisation or natural person performing business activities serialNumber value if it concerns natural person not performing business activities	**yes**	**yes**	X	X	X
CN CommonName	name and surname of a person (including titles)	**yes**	no	X	X	X

SN surname	last name of the person	**yes**	no	X	X	X
givenName	first name of the person	**yes**	no	X	X	X
serialNumber	Unique personal identifier assigned by the provider of certification services in the following format: P*number*	**yes**	no	X	X	X
title	Position of the applicant for a certificate	no	**yes**	X	X	
Subject Public Key Info						
Algorithm	rsaEncryption	These items are mandatory for all issued certificates and cannot be changed.				
SubjectPublicKey	Public key belonging to the signatory 2048 or 4096 bits long					
Extensions	Certificate extension according to table 3					
Signature	Electronic marks or electronic seal of the provider of certification services					

Explanatory notes:
Pov mandatory certificate item
Change item may be changed on the follow-up certificate
ORG this item is a part of certificates issued to organisation employees
PFO this item is a part of certificates issued to natural persons performing business activities
NFO this item is a part of certificates issued to natural persons not performing business activities

7.1.1 Version number supported

PostSignum Qualified CA issues certificates complying with X.509 standard, version 3.

7.1.2 Extension items of a certificate

Extension items used in qualified personal certificates are specified in the following table.

Tab. 3 Certificate extension

Item	**Value**	**Mandatory item**	**Change**	**ORG**	**PFO**	**NFO**
Authority Key Identifier						
Key Identifier		These items are mandatory for all issued certificates and cannot be changed.				
Subject Key Identifier						
Subject Alternative Name						
rfc822 Name email Address	Applicant's Email Address	**yes**	**yes**	X	X	X
rfc822Name email Address	Applicant's Email Address	no	**yes**	X	X	X
rfc822Name email Address	Applicant's Email Address	no	**yes**	X	X	X
otherName	MPSV Identifier Item OID: 1.3.6.1.4.1.11801.2.1	no	**yes**	X	X	X
otherName	custom content specified by a customer the content is encoded using ASCII in hex notation - item "Description" with OID: 2.5.4.13	no	**yes**	X	X	X
Key Usage *(critical expansion)*						
DigitalSignature	yes	These items are mandatory for all issued certificates and cannot be changed.				
NonRepudiation	yes					
KeyEncipherment	yes					
DataEncipherment	no					

KeyAgreement	no	
KeyCertSign	no	
CRLSign	no	
Certificate Policies		
Policy Information [1]		
Policy Identifier	OID of this certification policy	These items are mandatory for all issued certificates and cannot be changed.
Policy Qualifier ID	CPS	
CPS URI	http://www.postsignum.cz	
User Notice	This qualified certificate for electronic signature was issued according to Regulation (EU) No 910/2014.	
Policy Information [2]		
Policy Identifier	OID 0.4.0.194112.1.0 or OID 0.4.0.194112.1.2	Compulsory is always one of the OID. OID 0.4.0.194112.1.2 is specified only if the private key is stored in a qualified resource for creating electronic signatures (QESCD) pursuant to [eIDAS]
Qualified certificate statement		
OID	0.4.0.1862.1.1 esi4-QCStatement-1	This item is mandatory for all issued certificates and cannot be changed.
OID	0.4.0.1862.1.4 *esi4-QCStatement-4*	It is shown only if the private key is stored in a qualified resource for creating electronic signatures (QESCD) pursuant to [eIDAS].
OID	0.4.0.1862.1.5 *esi4-QCStatement-5*	The item is included in all certificates issued is compulsory and can not be changed. The value of the items is a link in the message to the user in English and Czech version.
OID	0.4.0.1862.1.6.1 *esi4-QCStatement-6* *(id-etsi-qct-esign)*	The item is included in all certificates issued is compulsory and can not be changed. The item indicates that the certificate was issued as a qualified certificate for electronic signature pursuant to [eIDAS].
CRL Distribution Points		
URI	http://www.postsignum.cz/crl/psqualifiedcaX.crl	These items are mandatory for all issued certificates and cannot be changed. *(X is a number indicating the particular subordinate CA)*
URI	http://www2.postsignum.cz/crl/psqualifiedcaX.crl	
URI	http://postsignum.ttc.cz/crl/psqualifiedcaX.crl	
AuthorityInfoAccess		
accessMethod URI	id-ad-caIssuers (1.3.6.1.5.5.7.48.2) http://www.postsignum.cz/crt/psqualifiedcaX.crt	These items are mandatory for all issued certificates and cannot be changed. *(X is a number indicating the particular subordinate CA)*
accessMethod URI	id-ad-caIssuers (1.3.6.1.5.5.7.48.2) http://www2.postsignum.cz/crt/psqualifiedcaX.crt	

accessMethod URI	id-ad-caIssuers (1.3.6.1.5.5.7.48.2) http://postsignum.ttc.cz/crt/psqualifiedcaX.crt	
accessMethod URI	id-ad-ocsp (1.3.6.1.5.5.7.48.1) http://ocsp.postsignum.cz/OCSP/QCAX/	*(X is a number indicating the particular subordinate CA)*

Explanatory notes:
Pov mandatory certificate item
Change item may be changed on the follow-up certificate
ORG this item is a part of certificates issued to organisation employees
PFO this item is a part of certificates issued to natural persons performing business activities
NFO this item is a part of certificates issued to natural persons not performing business activities

Note: Some items on the certificate do not contain diacritical signs in order to allow various systems to read all entries properly.

Note: This certification policy allows up to 3 email addresses on one certificate. However, the applicant should verify in advance whether a certificate with several email addresses will be supported by applications where he intends to use the certificate.

7.1.3 Cryptographic algorithm object identifiers (hereinafter "OID")

Algorithms used in PostSignum QCA do not have any OID assigned. No specific algorithms which would be developed by the operator of PostSignum QCA, or by his supplier, are used in PostSignum QCA hierarchy except for algorithms complying with requirements applicable legislation and technical standards, which regulate the activities of certification services providers..

7.1.4 Methods used to write names and titles

Name and title writing rules are specified in chapters 3.1.1 through 3.1.4.

7.1.5 Name and title restrictions

Names and titles specified in the certificate must correspond with data shown on documents which the customer or the signatory used to demonstrate their identities. Person authorized by the customer is responsible for the correctness of data which are not shown on the presented documents.

7.1.6 Applicable certification policy OID

Each end-user certificate specifies a link to a policy based on which the certificate was issued (policy OID). OID of this policy is specified in chapter 1.2.

7.1.7 An extending item "Policy Constraints"

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

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

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

information specifying that the certificate was issued as a qualified certificate for electronic signature according to [eIDAS].

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

Writing method of "Certificate Policies" is specified in Tab. 3. This item is not marked as critical.

7.2 A profile of a list of revoked certificates

Tab. 4 CRL profile

Item Name	Value
Version	2 (0x1)
Issuer Distinguished Name	
C countryName	CZ
O organisationName	Česká pošta, s.p. [Company ID No. 47114983]
CN commonName	PostSignum Qualified CA X *(X is a number indicating the particular subordinate CA)*
Validity	
This Update	Beginning of validity of the issued CRL (UTC time)
Next Update	End of validity of the issued CRL (UTC time)
RevokedCertificates	repeated/reoccurring item for each revoked certificate
UserCertificate	serial number of a revoked certificate
RevocationDate	date and time of revocation
CrlEntryExtensions	CRL item extension according to table 5
CrlExtensions	CRL extension according to table 5
SignatureAlgorithm	sha256WithRSAEncryption
Signature	electronic marks or electronic seal of the provider of certification services

7.2.1 Version number supported for CRLs

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

7.2.2 Extending items shown on the list of revoked certificates and records on the list of revoked certificates

Tab. 5 Extension in CRL

Extension item name	Value	Critical yes/no
Extension of CrlEntryExtensions item		
InvalidityDate	date and time of the occurrence of an event causing revocation of a certificate; optional extension	no
ReasonCode	Request for certificate revocation	no
CRL extension (CrlExtensions)		
Authority Key Identifier		no
Key Identifier	in use	
AuthorityCertIssuer	in use	
AuthorityCertSerialNumber	in use	
CRL Number	CRL serial number assigned by certification authority	no

7.3 OCSP Profile

See provisions under item 4.9.9.

7.3.1 Version number

See provisions under item 4.9.9.

7.3.2 Extension items OCSP

See provisions under item 4.9.9.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Evaluation frequency or circumstances necessary to carry out evaluations

Regular internal inspections are performed within the PostSignum QCA environment (once during every 12 months). In addition to these internal inspections are performed by the external audit pursuant to applicable legislation. These regular inspections may be added (if necessary) with other inspections based on a decision issued by the CA Manager, by the management of the Czech Post or by internal Audit of the Czech Post.

8.2 Evaluator identity and qualification

Internal inspections are carried out by employees knowledgeable of PKI issues and trained for the relevant task. Employees performing the inspection are labelled in the QCA documentation as CA auditors.

And external auditor may only be a person or company knowledgeable of PKI implementation issues, and who possesses sufficient experiences in this area.

8.3 A relation of the evaluator towards the evaluated subject

An internal inspection is done by employees of the Czech Post who are not involved in the operation of PostSignum QCA certification authority.

An external inspection may only be done by a person or company independent of the Czech Post.

8.4 Evaluated areas

Areas evaluated by regular inspections are described in applicable legislation and in applicable standards.

8.5 Procedures applied to discovered defects

Inspection results are presented to the CA Manager who shall arrange for a removal/remedy of the discovered defects.

If a serious defect is discovered, which may significantly impact the ability of PostSignum QCA to fulfil customer requirements/orders and requirements specified in applicable legislation, PostSignum QCA shall interrupt issuance of certificates until these defects are removed.

8.6 Sharing evaluation results

Each inspection is recorded on a written report which is handed over to the CA Manager. CA Manager makes sure that this report is distributed and discussed. If the report is necessary CA Manager makes sure it is handed over to the supervisory body to date, which is determined by the applicable legislation.

If the report also includes auditor's statement, the CA Manager may decide to publish it.

9 OTHER BUSINESS AND LEGAL ISSUES

9.1 Fees

9.1.1 Certificate issuance or renewal fees

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

9.1.2 Certificate access fees

Access to a certificate included on the list of issued certificates is free.

9.1.3 Revocation or status information access fees

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

9.1.4 Fees for additional services

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

9.1.5 Refund policy

No provisions available in this chapter.

9.2 Financial responsibility

9.2.1 Insurance coverage

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

9.2.2 Other assets and guarantees

Assets of the Czech Post are specified in the annual report. Annual report is stored at the Commercial Registry maintained by the Municipal court in Prague under file No. A7565.

Annual report may also be viewed at the webpage of the Czech Post (www.ceskaposta.cz).

9.2.3 Insurance policy or guarantees for end-entities

PostSignum QCA does not provide this service.

9.3 Confidentiality of business information

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

9.3.1 Scope of confidential information

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

9.3.2 Information not within the scope of confidential information

The following information shall not be considered confidential:

- information that becomes publicly known otherwise than through an intentional act or omission by the receiving party;
- information the receiving party had legally possessed before conclusion of the contract describing provision of certification services, unless such information and facts were included in the subject of other contracts previously concluded between participating parties and describing protection of information, or if the information of facts alone are not considered business secret,
- information which is the results of a process, through which the receiving party acquired such information independently, provided that the receiving party can demonstrate obtainment of such information with its own records or with confidential information of a third party;
- information which were provided to the receiving party by a third party after conclusion of a contract describing provision of certification services, providing that the third party did not obtain such information directly or indirectly from the original owner of the information and providing that such information was not acquired illegally, about which the receiving party knew or must have known,
- information specified in a qualified certificate, providing that the owner of the certificate agreed with the certificate publishing.

9.3.3 Responsibility to protect confidential information

The Czech Post - as the provider of certification services, including all its employees and contractual partners are liable for processing sensitive and confidential information contained in PostSignum QCA.

9.4 Privacy of personal information

The Czech Post protects personal information acquired during provision of certification services. Requirements and principles of personal information protection are specified in this certification policy, [VOP] and in the Certification implementation guideline and in applicable legal regulations [Z101].

9.4.1 Privacy plan

The Czech Post protects personal information acquired during provision of certification services. Requirements and principles of personal information protection are specified in applicable certification policies and [VOP] and are based on applicable legal regulations [Z101].

9.4.2 Information treated as private

Personal data represent information which are protected under [Z101]. In particular, this information include all facts and data related to a specific or determinable physical person (customer – performing or not performing business activities, authorized persons or the applicant).

9.4.3 Information not deemed private

Information which is not protected under [Z101] is not regarded as sensitive, including information which has been marked for publishing based on a decision issued by the relevant person (certificates, entries or items on the certificate).

9.4.4 Responsibility to protect private information

The Czech Post - as the provider of certification services and all its employees and contractual partners are liable for protection of personal data processed in PostSignum QCA systems and within the applicable scope specified in [Z101].

9.4.5 Notice and consent to use private information

During the issuance of the first certificate the applicant for a certificate will provide the Czech Post with a consent to process the applicant's personal data.

If the applicant for a certificate wishes to have on the certificate issued by PostSignum QCA a MPSV client identifier, the applicant shall provide the Czech Post with a consent to forward personal information to the Ministry of Labour and Social Affairs in order to receive the client identifier and to specify IK MPSV on the issued certificate.

9.4.6 Disclosure pursuant to judicial or administrative process

All information and data processed in PostSignum QCA are available - within the applicable scope required by the law, to institutions authorized by the law to have access to such information. The CA Manager shall make sure that this information is available to the relevant and authorized institutions, providing that these institutions demonstrate their authorization to access such information through means common and accepted in such situations.

9.4.7 Other information disclosure circumstances

In this situation applicable provisions specified in [Z101] and in internal regulations of the Czech Post describing personal data protection requirements shall apply.

9.5 Intellectual property rights

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

9.6 Representations and warranties of other participants

The Czech Post guarantees to fulfil all obligations set forth in this certification policy and in applicable legal regulations.

The Czech Post shall provide the above specified guarantees throughout the entire validity of the contract describing provision of certification services.

9.6.1 CA representations and warranties

See provisions specified in chapter 9.6.

9.6.2 RA representations and warranties

As far as services provided by the registration authority are concerned, the Czech Post, as the provider of certification services, may be represented by a third party and based on a properly concluded contract. This clause shall not impact the level of the provided guarantees.

For other provisions see chapter 9.6.

9.6.3 Subscriber representations and warranties

Representation and guarantees provided by the certificate holder or signatory Customer (certificate holder) or applicant (signatory) guarantee that all customer obligations as well as responsibilities of an applicant for a certificate specified in the certification policy and in applicable legislation will be properly fulfilled.

9.6.4 Disclosure pursuant to judicial or administrative process

The related party guarantees that all obligations of the related party existing prior to the use of the qualified certificate will be properly fulfilled. These obligations and responsibilities are specified in this certification policy, in particular in chapter 4.5.2.

9.6.5 Representations and warranties of other participants

Subjects which are directly involved in the operational PostSignum QCA based on a contract concluded with the provider of certification services, must observe Certification policy requirements, Certification implementation guideline, Safety system policy and other internal documents.

Guaranties provided by the provider of certification services in these cases are defined in applicable legislation.

9.7 Disclaimer of guaranties/warranties

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

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

9.8 Limitation of liability

The Czech Post is not liable for damages ensuing from the use of qualified certificates, providing the holder or relying party failed to observe restrictions of use of the certificate specified in this certification policy and published at the webpage of the provider.

The Czech Post is not liable for damages ensuing from the use of the qualified certificate during a period starting on the day of the certificate acceptance until its revocation, providing that the Czech Post complied with its obligation to publish the revoked qualified certificate on the list of revoked certificates (CRL) as specified in chapter 2 of this certification policy.

As the level of experiences of the Czech Post in terms of provision of certification services increases, the Czech Post shall continuously verify whether limitations of liabilities of the Czech Post specified in this provision correspond with general conditions on the market and with adequate commercial risks of the Czech Post.

Provisions of this Article shall remain valid even after this certification policy expires.

9.9 Indemnities

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

9.10 Term and Termination

9.10.1 Term of validity

This certification policy shall remain valid from the date specified in chapter 1.2 until terminated.

9.10.2 Termination

The validity of this document shall be terminated if

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

9.10.3 Effect of termination and survival

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

9.11 Individual notices and communications with participants

9.11.1 Communication with the provider of certification services

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

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

Customer – organisation or a natural person not performing business activities communicates with the provider certification services in person and deals with the workplace/office of the registration authority or communicates with CA business locations.

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

9.11.2 Communication within PostSignum QCA system

Communication within the PostSignum QCA system is subject to valid regulations of the Czech Post and to internal documents of PostSignum QCA.

9.11.3 Communication language

All communication under PostSignum QCA must be done in Czech language unless both parties agree otherwise.

9.12 Amendments

9.12.1 Procedure for amendment

Change management procedures are specified in chapter 1.5.

9.12.2 Notification mechanism and period

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

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

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

9.12.3 Circumstances under which OID must be changed

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

OID are assigned:

- to PostSignum Root QCA,
- to each certification authority to which PostSignum Root QCA issued a certificate, in particular, to PostSignum Qualified QCA certification authority.
- to each certification policy based on which certificates are issued under PostSignum QCA.

OID are not assigned to registration authorities or to certification implementation guideline.

Any change in the certification policy requires a change in the document version and change of OID.

9.13 Dispute resolution provisions

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

- CA Manager, or
- to a registration authority (file a claim).

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

9.14 Governing law

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

9.15 Compliance with Applicable Law

Activities of PostSignum QCA is pursuant to applicable legislation of the Czech Republic.

Relations between the Czech Post and customer are specified in the contract describing provision of certification services.

Structure of this certification policy is in line with structure specified in RFC 3647.

9.16 Other provisions

9.16.1 Entire agreement

No provisions available in this chapter.

9.16.2 Assignment

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

If a qualified provider of certification services terminates its activities, the Czech Post shall exert all necessary efforts pursuant to applicable legislation in order to make sure that management of valid qualified certificates and the relevant agenda are taken over by another qualified provider of certification services. In this scenario, relationship between this qualified provider of certification services and the Czech Post shall also be specified in a special contract.

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

9.16.3 Severability

Contract describing provision of certification services concluded between the customer and the Czech Post shall remain valid even if a certain portion of this contract becomes invalid, unless both parties agree otherwise.

9.16.4 Enforcement

No provisions available in this chapter.

9.16.5 Force Majeure

The Czech Post is not liable for failure to fulfil its contractual obligations due to force majeure events, for example large natural disasters, strikes, civil unrest or war.

9.17 Other provisions

9.17.1 Outline of a Set of Provisions

When creating certification policies and certification implementation guidelines the following documents were taken into consideration:

[CWA 141671]	CWA 14167-1:2003: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements
[eIDAS]	REGULATION (EU) No. 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
ETSI EN 119 312	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
[ISO 27001]	CSN ISO/IEC 27001:2006 Information Technologies – Security Techniques - Information Security Management Systems - Requirements
[TS 101456]	ČSN ETSI TS 101 456 Electronic signatures and infrastructures; Requirements on certification authorities issuing qualified certificates, version 1.3.1.
[TR 13335]	CSN ISO/IEC TR 13335: Information technology – Guideline for IT security management
[ISO 17799]	CSN ISO/IEC 17799: Information technology – Safety techniques a Set of procedures for information safety management RFC 2511 – Internet X.509 Certificate Request Message Format
[RFC 2560]	Internet X.509 Online Certificate Status Protocol (OCSP)
[RFC 3280]	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[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
[RFC 3739]	Internet X.509 Public Key Infrastructure: Qualified Certificates Profile
[V378]	Directive of the Ministry of Informatics No. 378/2006 Coll., issued on 19th July, 2006 describing procedures applicable to qualified providers of certification services
[Z101]	Act No. 101/2000 Coll., on the protection of personal data, as amended

[ZoEP] Act No. 227/2000 Coll., on electronic signatures, as amended and related Act on trust services for electronic transactions

9.17.2 References and literature

[VOP] General Certification Service Business Terms and Conditions