Česká pošta

PKI Disclosure Statements

Version 3.4

Document contents

Records of revisions and changes

Version	Date of revision	Change reason and description	Author	Approved by
0.1	26/07/2005	first version	QCA Manager	QCA Manager
1.01	05/09/2005	smaller changes to document	QCA Manager	QCA Manager
1.02	16/09/2006	information added about issuance of the following certificates	QCA Manager	QCA Manager
1.1	12/01/2009	change of document structure, addition of a list of performed audits and information about complaint proceedings	QCA Manager	QCA Manager
2.0	02/09/2011	Merging of the report for QCA and VCA users and data updating	Petr Huptich	CA Manager
2.1	01/07/2012	updated list of audits adjusted types of issued certificates	Miroslav Trávníček	CA Manager
2.2	21/01/2013	updated list of audits	Miroslav Trávníček	CA Manager
2.3	12/04/2013	updated list of audits	Miroslav Trávníček	CA Manager
2.4	21/ 07/2014	updated list of audits, contact workplaces and certificate types	Miroslav Trávníček	CA Manager
2.5	20/ 02/2015	updated list of audits and adjusted VOP name	Miroslav Trávníček	CA Manager
2.6	01/06/2015	updated list of audits	Miroslav Trávníček	CA Manager
2.7	21/01/2016	updated list of audits	Miroslav Trávníček	CA Manager
3.0	01/07/2016	changes according to eIDAS	Vosková/Trávníček	CA Manager
3.1	08/09/2017	changes linked to the accreditation	Vosková	CA Manager
3.2	01/04/2018	updated list of audits	Vosková	CA Manager
3.3	03/12/2019	updated list of audits	Vosková	CA Manager
3.4	01/09/2020	updated list of audits and updated contact information	Miroslav Trávníček	CA Manager

1. Introduction

1.1. Document purpose

This document provides a basic overview of the hierarchy of certification authorities PostSignum QCA and PostSignum VCA, the rights and duties of holders of certificates issued by PostSignum Qualified CA, PostSignum Public CA and parties relying on them.

This document has an informative character, is not intended to replace certification policies and is not part of any contract on provision of certification services entered into between the customer and the Czech Post (hereinafter the "Czech Post").

1.2. History of performed audits and system checks

Date	Type of audit/check	Auditor's/Inspector's statement
May 2020	Audit confirming that the provided by qualified trust services are in conformity with regulation eIDAS and the relevant technical standards, conducted by Tayllorcox s.r.o.	Conformity
February 2020	Supervision audit for certification in relation to ISO 9001 and ISO 27001, conducted by CQS.	Conforms
November 2019	Conformity assessment according to the requirements of the Microsoft Root Certificate Program, made by Tayllorcox s.r.o.	Satisfactory
May 2019	Audit confirming that the provided by qualified trust services are in conformity with regulation eIDAS and the relevant technical standards, conducted by Tayllorcox s.r.o.	Conformity
February 2019	Supervision audit for certification in relation to ISO 9001 and ISO 27001, conducted by CQS.	Conforms
November 2018	Conformity assessment according to the requirements of the Microsoft Root Certificate Program, made by Tayllorcox s.r.o.	Satisfactory
February 2018	Supervision audit for certification in relation to ISO 9001 and ISO 27001, conducted by CQS.	Conforms
December 2017	Conformity assessment according to the requirements of the Microsoft Root Certificate Program, made by Tayllorcox s.r.o.	Satisfactory
April 2017	Audit confirming that the provided by qualified trust services are in conformity with regulation eIDAS and the relevant technical standards, conducted by Tayllorcox s.r.o.	Conformity
March 2017	Re-certification audit for certification in relation to ISO 9001 and ISO 27001, conducted by CQS.	Conforms
November 2016	Conformity assessment according to the requirements of the Microsoft Root Certificate Program, made by Deloitte Advisory.	Satisfactory

February 2016	Supervision audit for certification in relation to ISO 9001 and ISO 27001, conducted by CQS.	Conforms
September 2015	Partial assessment of security compliance (Czech Post's internal audit)	Satisfactory
March 2015	Supervision audit for certification in relation to ISO 9001 and ISO 27001, conducted by CQS.	Conforms
September 2014	Partial assessment of security compliance (Czech Post's internal audit)	Satisfactory
March 2014	Re-certification audit for certification in relation to ISO 9001 and ISO 27001, conducted by CQS.	Conforms
September 2013	Partial assessment of security compliance (Czech Post's internal audit)	Satisfactory
February 2013	Supervision audit for certification in relation to ISO 9001 and ISO 27001, conducted by CQS.	Conforms
December 2012	Overall assessment of security compliance, conducted by Deloitte Advisory.	Satisfactory
February 2012	Supervision audit for certification in relation to ISO 9001 and ISO 27001, conducted by CQS.	Conforms
August 2011	Partial assessment of security compliance (Czech Post's internal audit)	Satisfactory
February 2011	Re-certification audit for certification in relation to ISO 9001 and ISO 27001, conducted by CQS.	Conforms
November 2010	Partial assessment of security compliance (Czech Post's internal audit)	Satisfactory
February 2010	Partial assessment of security compliance (Microsoft Root Certificate Program), performed by Deloitte Advisory	Satisfactory
January 2010	Supervision audit for certification in relation to ISO 9001 and ISO 27001, conducted by CQS.	Conforms
October 2009	Partial assessment of security compliance (Czech Post's internal audit)	Satisfactory
December 2008	Supervision audit of certification in relation to ISO 9001 and ISO 27001, conducted by CQS.	Conforms
December 2008	Partial assessment of security compliance (Czech Post's internal audit)	Satisfactory
March 2008	Overall assessment of security compliance, conducted by Deloitte Advisory.	Satisfactory
December 2007	Re-certification audit for certification in relation to ISO 9001 and ISO 27001, conducted by CQS.	Conforms
December 2007	Partial assessment of security compliance (Czech Post's internal audit)	Satisfactory
December 2006	Overall assessment of security compliance, conducted by Ernst & Young.	Satisfactory
September 2006	Partial assessment of security compliance (Czech Post's internal audit)	Satisfactory
June 2005	Overall assessment of security compliance, conducted by Ernst & Young.	Satisfactory

2. Contact information

2.1. Certification service provider

The PostSignum certification service provider is:
Česká pošta, s.p. [Czech Post, state enterprise], ID No. 47114983
Politických vězňů 909/4
225 99 Prague 1

2.2. Contact workplaces

Entering into agreements with PostSignum customers is ensured by sales and contact locations of PostSignum and External registration authority. Contact information is available on the website of PostSignum – www.postsignum.cz.

Issuing and invalidation of certificates are ensured by branch of Czech Post and External registration authority.

Invalidation of certificates outside of working hours of branch is ensured by the following workplace

Česká pošta, s.p. [Czech Post]
User Operations Department QCA/VCA
Wolkerova 480
749 20 Vítkov
e-mail: postsignum@cpost.cz
tel.: +420 954 303 303

2.3. Communication with clients

Questions regarding provision of certification services can be sent to contact workplaces for service provision.

Expert questions will be answered by the following workplaces:

e-mail: helpdesk-ca@cpost.cz
tel.: 800 104 410

2.4. Publication of information

This report for users, certification policies and other public information can be found on the website of PostSignum:

http://www.postsignum.cz

3. Types of signatures and verification procedures

3.1. Types of issued certificates

3.1.1. PostSignum Qualified CA

The Czech Post has set up a two-level hierarchy of certification authorities named PostSignum QCA. The root of this hierarchy is the certification authority PostSignum Root QCA, which issued the certificate for certification authority PostSignum Qualified CA.

PostSignum Qualified CA issues certificates to end users, and it applies two basic registration models depending on the end user. The first registration model is focused on legal person and natural person performing business activities and the second model is focused on natural person not performing business activities.

PostSignum Qualified CA issues these types of certificates:

- Qualified certificates for electronic signature
- Qualified certificates for electronic seals

Certificates for public keys issued within the PostSignum Qualified CA hierarchy satisfy the X.509 v3 standard.

Validity of certificates is optional. A 385-day or 1115-day certificate can be requested.

3.1.2. PostSignum Public CA

The Czech Post has set up a certification authority called PostSignum Public CA (abbreviated as PostSignum VCA), which has been issued the certificate by the certification authority PostSignum Root QCA.

PostSignum Public CA issues certificates to end users, and it applies two basic registration models depending on the end user. The first registration model is focused on legal person and natural person performing business activities, and the second model is focused on natural person not performing business activities.

PostSignum Public CA issues these types of certificates:

- commercial personal certificates,
- commercial server certificates,
- commercial domain certificates,

Certificates for public keys issued within PostSignum VCA satisfy the X.509 v3 standard.

Validity of certificates is optional. A 385-day (personal and server certificates) or 397-day (domain certificate) or 1115-day (personal and server certificates) can be requested.

3.2. Verification of the applicant when issuing the initial certificate

During the process of issuing the initial certificate, the certificate applicant's identity is always verified based on the applicant's personal identity documents, and if the certificate is intended for a legal person or natural person performing business activities, then the applicant's relationship to such entity is also verified.

The applicant for the certificate must be physically present during the process of issuing the certificate and cannot appoint a representative.

If this registration process allows, it is possible to prove identity in a different way.

A detailed description of the registration procedures can be found in the relevant certification policies.

3.3. Verification of the applicant when issuing the subsequent certificate

During the process of issuing the subsequent certificate, the identity of the applicant for the subsequent certificate is verified by checking the electronic signature on the application for the subsequent certificate.

A detailed description of the registration procedures can be found in the relevant certification policies.

4. Restrictions on use

4.1.1. Qualified certificates for electronic signature

Qualified certificates for electronic signatures issued by PostSignum QCA may be used only for verifying an electronic signature in accordance with valid legislation.

The corresponding private key to the certificate issued by the qualified electronic signature can be stored on a qualified device for creating electronic signatures, but this is not required.

Qualified certificates for electronic signature issued by PostSignum QCA are not intended for communication or transactions in areas with increased risk of harm to health or damage to property, such as chemical operations, aviation, nuclear facilities, etc. or in connection with national security and defence.

4.1.2. Qualified certificates for electronic seal

Qualified certificates for electronic seal issued by PostSignum QCA may be used only for verifying an electronic signature in accordance with valid legislation.

The corresponding private key to the certificate issued by the qualified electronic seals can be stored on a qualified device for creating electronic seals, but this is not required.

Qualified certificates for electronic seal issued by PostSignum QCA are not intended for communication or transactions in areas with increased risk of harm to health or damage to property, such as chemical operations, aviation, nuclear facilities, etc. or in connection with national security and defence.

4.1.3. PostSignum VCA Commercial certificates

Certificates issued by PostSignum VCA may be used to verify electronic signatures authentication and data encryption.

Certificates issued by PostSignum VCA are not intended for communication or transactions in areas with increased risk of harm to health or damage to property, such as chemical operations, aviation, nuclear facilities, etc. or in connection with national security and defence.

5. Obligations of customers and their representatives

A customer of the certification authority PostSignum is a legal person or natural person who is in a contractual relationship with the Czech Post. The customer must in particular

- provide truthful and complete information when entering into an agreement on provision of certification services,
- immediately inform the provider of certification services about changes to information contained in the contract or certificate.

An applicant for a certificate is natural person who based on having been entrusted to do so by a customer applies for issuance of a certificate and manages the issued certificate. (If the customer is natural person not performing business activities, then the customer is the applicant.) The applicant must in particular

- become familiar with the certification policy under which the certificate is to be issued,
- provide truthful and complete information to the certification service provider,
- promptly inform the certification service provider of any changes in details contained in the contract on provision of certification services or in the issued certificate,
- handle the private key corresponding to the public key in the certificate issued based on the selected certification policy with proper care, to ensure that it is not used by anyone unauthorised and that the private key is used only for the purposes specified in the certification policy, according to which the certificate has been issued,
- to notify the certification service provider immediately of any circumstances that will lead to invalidation of the certificate, particularly if there is suspicion that the private key has been misused, and to request that the certificate be invalidated.
- in the case if the private key will be stored on a qualified device for creating electronic signatures or electronic seals:
  - have to generate and use private key under their exclusive control
  - the private key is used only for creating electronic signatures or seals, and in accordance with applicable law.

6. Basic obligations of relying parties and other users

Relying parties and other users must in particular

- obtain certificates from certification authorities PostSignum Qualified CA, PostSignum Public CA and PostSignum Root QCA from safe sources and verify the prints („fingerprints“) of these certificates,
- before using a certificate issued by PostSignum Qualified CA verify the validity of the certificate of PostSignum Qualified CA, PostSignum Root QCA and subsequently also the validity of the issued final certificate,
- before using a certificate issued by PostSignum Public CA verify the validity of the certificate of PostSignum Public CA, PostSignum Root QCA and subsequently also the validity of the issued final certificate,
- sufficiently consider (particularly based on knowledge of the particular certification policy whether a certificate issued by PostSignum Qualified CA or PostSignum Public CA based on the respective policy is suitable for the purpose for which it is planned to be used.

7. Limitations on warranty and liability

The Czech Post agrees to fulfil all obligations imposed by the certification policies, based no which it shall issue certificates, and mandatory provisions of applicable legislation.

The Czech Post is providing the warranties specified above for the entire duration of the validity of the agreement on provision of certification services entered into with the customer.

The warranties specified above are exclusive warranties of the Czech Post, and the Czech Post does not provide any other warranties.

The Czech Post shall not be liable for defects in provided services resulting from improper or unauthorised use of the services provided during fulfilment of the agreement on provision of certification services by the holder, particularly for operation in a manner that conflicts with the conditions specified in the certification policy, as well as for defects resulting from force majeure circumstances, including temporary outages of telecommunications lines, etc. The Czech Post also shall not be liable for damages stemming from use of a qualified certificate for an electronic signature or certificate for an electronic seal after the request for its invalidation has been submitted, as long as the Czech Post fulfils the defined deadline for publication of the invalidated qualified certificate for electronic signature or the certificate for the electronic seal in the list of invalidated certificates (CRL).

8. Agreements and certification policy

The relationship between the customer and the Czech Post as the provider of certification services is (except for the relevant provisions of mandatory legal regulations) governed by the contract, which includes, among other parts

- the General Commercial Terms for Certification Services,
- valid certification policies and
- the currently valid price list.

The relationship between the relying party and the Czech Post as the provider of certification services is governed by relevant provisions of valid certification policies.

The relationship between the Czech Post and relying parties is not governed by the contract.

All of the documents referred to are available on the PostSignum website or at the certification authority's business locations.

9. Personal data protection

The Czech Post agrees to protect the personal data of persons to which it gains access while providing the certification services. The basic principles for personal data protection are outlined in the certification policies, the General Commercial Terms of the certification services and in the current implementing certification directive and are based on relevant provisions of Act No. 110/2019 Coll., the Personal Data Processing, as amended.

The applicant for the certificate hereby grants permission for the Czech Post to process personal data to the extent necessary for issuance and/or invalidation of a certificate with the required data.

10. Compensation and complaint policy

If the services are not delivered in the defined quality (for example, if a certificate is issued with wrong contents), the customer shall be entitled to be refunded the price for the particular service or to be provided with new service free of charge.

More detailed information about complaint handling can be found on the PostSignum website.

11. Governing law

The activities of PostSignum QCA are governed by relevant provisions of Czech law, particularly

- Act No. 297/2016 Sb. 227/2000 Coll., on trust services for electronic transactions,
- Regulation of the European Parliament and of the Council (EU) No. 910/2014, on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS),
- Act No. 110/2019 Coll., the Personal DataProcessing, as amended.

The activities of PostSignum VCA are governed by relevant provisions of Czech law, particularly

- Act No. 110/2019 Coll., the Personal Data Processing, as amended.

12. Accreditation and conformity assessment

The Czech Post as a provider of PostSignum QCA certification services on 3/ 8/ 2005 became an accredited provider of certification services based on accreditation issued by the Ministry of Informatics of the Czech Republic.

On 21/ 12/ 2007, the information system of PostSignum QCA and PostSignum VCA received certification of conformity with ISO 9001 (QMS, Quality Management System) and ISO 27001 (ISMS, Information Security Management System).

On 1/ 07/ 2016, the Czech Post became a qualified provider of trust services in accordance with eIDAS for issuing of qualified certificate for electronic signature.

On 30/ 08 2017 have been in a trusted list of qualified services added qualified services:

- issuing of qualified certificates for electronic seal
- issuing of qualified certificates for the authentication of the web pages

The activities of the PostSignum certification authority are subject to performance of checks. Conformity assessment with applicable laws and regulations and technical standards is performed by auditor independent of the Czech Post. The intervals for performance of checks are specified in the certification policies.