Česká pošta

Disclosure Statements TSA

Version 2.4

Document contents

Records of revisions and changes

Version	Date of revision	Change reason and description	Author	Approved by
0.1	21. 1. 2009	Draft	Daniel Joščák	
0.2	22. 2. 2009	Commenting on the document	Martin Šlancar	
0.3	24. 2. 2009	The incorporation of comments	Ondřej Steiner	
1.0	26. 2. 2009	"Milestone" version approved by the Manager of the TSA	Martin Šlancar	Manažer QCA
1.1	22. 5. 2009	"Milestone" Manager of TSA-approved version, incorporating the comments of the Ministry of the Interior	Martin Šlancar	Manažer QCA
1.2	1. 8. 2012	Document updates	H. Radová Švecová	Manažer CA
1.3	21. 1. 2013	Update list of audits	Miroslav Trávníček	Manažer CA
1.4	12. 4. 2013	Update list of audits	Miroslav Trávníček	Manažer CA
1.5	21. 7. 2014	Update list of audits	Miroslav Trávníček	Manažer CA
1.6	20. 2. 2015	Update list of audits, adjusted VOP name	Miroslav Trávníček	Manažer CA
1.7	1. 6. 2015	Update list of audits	Miroslav Trávníček	Manažer CA
1.8	21. 1. 2016	Update list of audits	Miroslav Trávníček	Manažer CA
2.0	1. 7. 2016	Changes according to eIDAS	Vosková/Trávníček	Manažer CA
2.1	8. 9. 2017	Changes linked to the accreditation	Miroslav Trávníček	Manažer CA
2.2	1. 4. 2018	Update list of audits	Vosková/Trávníček	Manažer CA
2.3	3.12.2019	Update list of audits	Vosková	Manager CA
2.4	1.9.2020	updated list of audits and updated contact information	Miroslav Trávníček	CA Manager

1. Introduction

1.1. Document purpose

This document provides a basic information about the time stamp authority PostSignum TSA, the rights and obligations of users of qualified electronic timestamps (hereinafter referred to as the time stamps) issued by PostSignum, the TSA and the relying party.

This document is for information only, does not replace the policy for issuing time stamps and is not part of the contract on the provision of certification services concluded between the customer and the Czech post, s.p. (Czech post or CP).History of performed audits and system checks

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
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

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. Contact information is available on the website of PostSignum – www.postsignum.cz.

Issuing time stamps ensures the provider through the application on a special server that accepts requests on the issue of time stamps.

2.3. Communication with clients

Questions regarding provision of PostSignum services TSA 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 issued timestamp and the issuance

3.1 Types of timestamps

The time stamp that is issued by PostSignum, the TSA means a qualified electronic time stamp in accordance with regulation eIDAS.

As to the data message by the certification services provider and a trusted way combines the data in electronic form, with the time at the moment, and guarantees that the data in electronic form existed before that time.

Postsignum publishes the TSA one type of a timestamp that is described in the document "the politics of the issue time stamps of PostSignum TSA". Policy OID is referred to in the document.

Time stamps issued by PostSignum TSA complies with the RFC 3161.

3.2 Conclusion of the contract

A customer service issue time stamps of PostSignum TSA is a legal entity, the individual entrepreneur (entrepreneur), the nonentrepreneurial natural person, State authority or local government authority.

3.2.1 Written agreement

The customer gets access to the services of PostSignum TSA to the conclusion of a written contract for the provision of certification services. This agreement shall be concluded in accordance with the terms and conditions of certification services.

The contract is signed by the customer, as in the normal course of trade. The identity of the natural person is verified on the basis of a single identity document (identity card or passport).

Customer in the contract defines the responsible person who is authorized to act on behalf of the customer in case of the provision of services, the issue of time stamps. Delegate defines a method of authentication when sending a request for the release of the timestamp, and other parameters for the service.

3.2.2. Electronic contract (prepaid package, time stamps)

The customer gets access to the services of PostSignum TSA purchased a prepaid package time stamps through the ordering system of the provider. This agreement shall be concluded in accordance with the terms and conditions of certification services.

The customer in the order (electronic contract) defines the contact person. Contact person defines how authentication when sending a request for the release of time stamp.

3.3. Verification procedures and request a time stamp

Extradition request time stamp serves customers CP on the basis of the concluded contract between CP and the customer. The applicant for a time stamp (person or application acting on behalf of the customer) creates a secure authenticated connection with PostSignum TSA over HTTPS, which identifies and authenticates:

- ▪ commercial certificate issued by a certification authority PostSignum VCA, or
- ▪ name and password.

After a valid identification and authentication of the applicant creates a thumbprint (hash) of electronic data (messages, document, transactions, etc.), which is then stored in a request for a qualified timestamp (according to RFC 3161). This data structure is through the connection passed to PostSignum TSA. The request is then sent to one of the sites TSU (the issuing time stamps itself, hereinafter referred to as TSU) for the assessment of the correctness and designation.

An application may occur in particular in the case of:

- ▪ identification and authentication is unsuccessful,
- ▪ the time stamp request does not meet the requirements defined by the policy for issuing time stamps
- ▪ termination of the private key of the TSA.

The allowed algorithm for calculation of the fingerprint (hash), which is stored in the time stamp request are: SHA-1, SHA-256, SHA-384, SHA-512, The algorithm for calculation fingerprint is not validated.

3.4. Release of time stamp

After receipt of the request time stamp makes the formal correctness of control TSA PostSignum request and in case of a positive outcome of the checks of the application is to fingerprint (hash) of the data contained in the request is added to the data structures of the time from a reliable gauge of the time. This data structure is electronically flagged data for creating electronic seals the TSA, thus creating a time stamp according to RFC 3161, which is archived.

In response, including the time stamp is sent to the applicant about the time stamp.

3.5. Verification of the timestamp

To verify a time stamp, perform the following steps:

- ▪ verification of the fingerprint (hash) of the verified data referred to in the time stamp to the newly calculated fingerprint (hash) from electronic data available attesting to the side,
- ▪ the validation of electronic seals using the TSA's certificate.

Furthermore, it is downloaded to the current certificate revocation list (CRL) and verifies the validity of:

- ▪ the used certificate TSA, which is marked with the stamp,
- ▪ PostSignum Qualified CA certificate of the CA that issued the certificate of the TSA,
- ▪ certificate certification authority PostSignum Root QCA, which issued the certificate of the authority PostSignum Qualified CA.

If the fingerprint (hash) are identical when the same algorithm and has been verified the validity of any electronic seal and of the appropriate certificate, the time stamp is valid.

The minimum lifetime electronic seals on the time stamp of PostSignum TSA TSA is equal to the validity of the certificate.

4. Restrictions on use

Time stamps issued by the authority PostSignum TSA are not primarily intended for communication or transactions in areas with an increased risk of damage to persons or property, such as chemical plants, air traffic, the operation of nuclear facilities, etc. or in areas related to security and System State.

In addition to the above, no further restrictions are laid down for the application of the electronic time stamp, issued in accordance with the contents of the policy for issuing time stamps.

Time stamp, issued by PostSignum, the TSA can be used for the following purposes:

- ▪ where required the use of a qualified electronic time stamp pursuant to Act No. 297/2016 Coll. on trust services for electronic transactions;
- ▪ where required the use of a qualified electronic time stamp under regulation eIDAS, as amended;
- ▪ in other cases, where there is a need to establish the existence of a specific data (the document) before that time's moment.

4.1. Accuracy of the time in the time stamp

The maximum deviation of the time in the issued time stamp from the value of the qualified world UTC time is 1 second.

4.2. Retention period of audit records

Audit records (including the issued time stamps) are held in accordance with the legislation of the Czech Republic.

5. Obligations of customers and their representatives

A customer of authority PostSignum TSA 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, or order a prepaid package time stamps
- immediately inform the provider of certification services about changes to information contained in the contract

Contact person or authorized person of the customer shall in particular:

- ensure the confidentiality of authentication information

By the time stamp is a natural person or system that on behalf of the customer is asking for the release of time stamp. The applicant must in particular:

- to ensure the confidentiality of the authentication information needed to verify the customer's identity when applying for the time stamp,
- become familiar with the policy, according to which he was the time stamp is issued.

6. Basic obligations of relying parties and other users

The relying party performs the following activities:

- ▪ authenticates the fingerprint (hash) of the verified data,
- ▪ verifies the validity of electronic seals using the TSA's certificate.

The relying party also gets the current certificate revocation list (CRL) and verifies the validity of:

- ▪ the used certificate TSA, which is the stamp of pečetěno,
- ▪ PostSignum Qualified CA certificate of the CA that issued the certificate of the TSA,
- ▪ certificate certification authority PostSignum Root QCA, which issued the certificate of the authority PostSignum Qualified CA;

The relying party shall consider whether the time stamp issued in accordance with this policy is suitable for the purpose for which it was used.

A detailed description of the expiration timestamp is set out in the document "the politics of the issue time stamps of PostSignum TSA".

7. Limitations on warranty and liability

The Czech Post agrees to fulfil all obligations imposed by the policies of the issuing time stamps, based no which it shall issue time stamps, 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, or the validity of the purchased a prepaid package of time stamps.

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 users, particularly for operation in a manner that conflicts with the conditions specified in the policies of the issuing time stamps, as well as for defects resulting from force majeure circumstances, including temporary outages of telecommunications lines, etc.

8. Agreements and certification policy

The relationship between the customer and the Czech Post as the provider of issuing time stamps 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 issuing time stamps 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 service of issuing time stamps. The basic principles for personal data protection are outlined in the the policies of the issuing time stamps, the General Commercial Terms of the certification services and in the rertification practice statement PostSignum TSAS and are based on relevant provisions of Act No. 101/2000 Coll., the Personal Data Protection Act, as amended.

10. Compensation and complaint policy

If the services are not delivered in the defined, 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 TSA 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 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 1. 7. 2009 CP spread provided by certificate services on the issue of service time stamp with the name of PostSignum TSA (even just the TSA).

On 21. 2. 2011 an information system of PostSignum 2011 TSA certification of compliance with ISO 9001 (quality management system) and ISO 27001 (ISMS information security management system).

On 1. 7. 2016 the Czech post has become a qualified trust service provider according to eIDAS.

On 30. 8. 2017 was in a trusted list of professional services added qualified service issue qualified electronic timestamps.

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.