POŠTA® CA Certification Agency

Policy Disclosure Statement

POŠTA SLOVENIJE

POŠTA SLOVENIJE, d.o.o. | Slomškov trg, 2500 Maribor | info.postarca@posta.si | postarca.posta.si

Content

1 TRUST SERVICE PROVIDER IDENTITY AND CONTACT INFORMATION

The trust service provider POŠTA SLOVENIJE d.o.o., Maribor, Slovenia, operates a certification authority, the Certification Agency of Post of Slovenia, or POŠTA®CA. POŠTA®CA issues various types of qualified and normalized digital certificates.

Naslov:	Pošta Slovenije, d.o.o. POŠTA®CA Slomškov trg 10 2000 Maribor
Telefon:	02 449 2941
Fax:	02 449 2807
Spletna stran:	http://postarca.posta.si/
E-mail	info.postarca@posta.si
Pomoč uporabnikom:	080 44 40

2 CATEGORIES OF DIGITAL CERTIFICATES, CERTIFICATE HOLDER IDENTITY VALIDATION AND PURPOSES OF USE

The certification authority issues the following categories of qualified certificates for employees of legal persons:

- **Advanced qualified certificates –** qualified certificates with two key pairs for natural persons employed by legal persons who are required to use a QSCD device. Such certificates can be used for qualified electronic signatures, encryption and authentication.
- **Qualified certificates with compulsory use of QSCD device –** qualified certificates with one key pair for natural persons employed by legal persons. Use of a QSCD device is compulsory. Such certificates can be used for qualified electronic signatures, encryption and authentication.
- **Qualified certificates -** qualified certificates with one key pair for natural persons employed by legal persons. Such certificates can be used for advanced electronic signatures, encryption and authentication.
- **Qualified certificates issued on a QSCD device** – qualified certificates with one key pair for natural persons employed by legal persons. The certificates are issued on QSCD devices. Such certificates can be used for qualified electronic signatures, encryption and authentication.
- **Qualified certificates issued on a remote QSCD device** – qualified certificates with one set of keys for natural persons employed by legal persons, issued on a remote QSCD device. Such certificates can be used for qualified electronic signatures.
- **Qualified certificates with a general name and compulsory use of QSCD device** - qualified certificates with one key pair for natural persons employed by legal persons, with an additional general name in the commonName field and compulsory use of a QSCD device. Such certificates can be used for qualified electronic signatures, encryption and authentication.

  ***NOTE**: No longer issued since the release of policy version 1.3. All certificates issued shall remain in use until the expiry date.*

- **Qualified certificates with a general name** - qualified certificates with one set of keys for natural persons employed by legal persons, with an additional general name in field commonName. Such certificates can be used for advanced electronic signatures, encryption and authentication.

  ***NOTE**: No longer issued since the release of policy version 1.3. All certificates issued shall remain in use until the expiry date.*

- **Qualified certificates with a general name issued on QSCD device** - qualified certificates with one key pair for natural persons employed by legal persons with an additional general name in the commonName field and compulsory use of QSCD device. Such certificates can be used for qualified electronic signatures, encryption and authentication.

  ***NOTE**: No longer issued since the release of policy version 1.3. All certificates issued shall remain in use until the expiry date.*

The certification authority issues the following categories of qualified certificates for natural persons:

- **Advanced qualified certificates –** qualified certificates with two key pairs for natural persons and compulsory use of QSCD device. Such certificate can be used for qualified electronic signatures, encryption and authentication.
- **Qualified certificates with compulsory use of QSCD device -** qualified certificates with one key pair for natural persons and compulsory use of QSCD device. Such certificates can be used for qualified electronic signatures, encryption and authentication.
- **Qualified certificates -** qualified certificates with one key pair for natural persons. Such certificates can be used for advanced electronic signatures, encryption and authentication.
- **Qualified certificates issued on a QSCD device –** qualified certificates with one key pair for natural persons, issued on a QSCD device. Such certificates can be used for qualified electronic signatures, encryption and authentication.
- **Qualified certificates issued on a remote QSCD device –** qualified certificates with one key pair for natural persons, issued on a remote QSCD device. Such certificates can be used for qualified electronic signatures.
- **Qualified certificates issued on professional cards in the health insurance card scheme -** qualified certificates with one key pair, issued on a professional card in the health insurance card scheme. Such certificates can be used for qualified electronic signatures, encryption and authentication.

The certification authority issues the following categories of qualified certificates for legal persons:

- **Qualified certificates for legal persons with compulsory use of QSCD device –** qualified certificates with two key pairs and compulsory use of QSCD device. Such certificates can be used for qualified electronic seals.
- **Qualified certificates for legal persons –** qualified normalized certificates for legal persons with one key pair. Such certificates can be used for advanced electronic seals.
- **Qualified certificates for legal persons, issued on a QSCD device -** qualified certificates for legal persons with one key pair, issued on a QSCD device. Such certificates can be used for qualified electronic seals.
- **Qualified certificates for legal persons, issued on a remote QSCD device -** qualified certificates for legal persons with one key pair, issued on a remote QSCD device. Such certificates can be used for qualified electronic seals.

The certification authority issues the following categories of qualified certificates for web servers or website authentication:

- **Qualified certificates for web servers –** qualified certificates for web servers with one key pair. Such certificates can be used for web server identity verification.

The certification authority issues the following categories of normalized certificates:

- **Normalized certificates for web servers –** such certificates can be used for verifying the identity of web servers and VPN devices.
- **Normalized certificates for timestamp services –** such certificates can be used for verifying advanced electronic signatures of timestamp services.
- **Normalized certificates for OCSP services -** such certificates can be used for verifying advanced electronic signature of OCSP service.

All categories of digital certificates ensure the certificate holder's proof of identity. Identity validation is carried out as follows:

- The identity of a legal or natural person registered to perform business activities is verified based on officially validated documentation or by data from official sources. The legal person is represented by a legal representative or by a person authorized by a legal representative. The legal representative or person authorized by a legal representative is verified based on an official identification document.
- The identity of natural persons is verified based on an official identification document.

3 RELIANCE LIMITS

The trust service provider stores all data pertaining to the content of digital certificates and their validity verification for at least seven years after the certificate expiry date. Digital certificates can only be used for the purposes set out in the chapter *Categories of digital certificates, validation of certificate holders' identity and permitted purposes of use* and in the latest published version of the certification practice statement (*POŠTA®CA Politika za kvalificirana in normalizirana potrdila*), published at http://postarca.posta.si/dokumenti. The POŠTA®CA certification authority is not responsible for certificates which are no longer valid.

4 OBLIGATIONS OF SUBSCRIBERS AND CERTIFICATE HOLDERS

The certificate holder is obliged to:

- protect their private passwords and private keys. They must not disclose or provide their private passwords or private keys to third parties, otherwise they shall bear full responsibility for any direct or indirect damage incurred through the use of the certificate holder's qualified certificate by unauthorized parties;
- digitally sign only those documents for which the requirement for the validity of the digital signature is no longer than the certificate validity (except for signed documents for which the maintenance of the long-term validity of the electronic signature is provided in another way, e.g., the documents are stored in an electronic archive that supports the maintenance of the signature's long-term validity);
- ensure the use of digital certificates only within their validity period;
- ensure the use of digital certificates only for purposes approved by the certification authority;

- immediately request the revocation of a digital certificate in case of suspected misuse or private key disclosure;
- notify the certification authority within 48 hours of any change of data in the certificate or in the application for the digital certificate;
- take into account the certification authority's rules of operation and check all of the certification authority's notices and act in accordance with them;
- keep up with technological developments and update their software and hardware in accordance with the certification authority's notifications. The following recommendations for providing security on computers on which digital certificates are used shall also be taken into account:
    - install and regularly update antivirus protection;
    - install a firewall;
    - regularly install security updates to the operating system and software;
    - log out from the system or lock the desktop when not using computer;
    - remove the smart card from the smart card reader when not using computer;
- when a subscriber or certificate holder generates the key pairs themselves, they must take into account the certification practice statement (*POŠTA®CA Politika za kvalificirana in normalizirana potrdila*), Chapter 6.1.5 and the requirements set out in ETSI TS 119 312;
- settle all financial commitments to the certification authority within the deadline;
- use the digital certificate for web servers only for SSL or TLS protocol on web servers for which it was issued.

This document contains summary of the certification authority POŠTA®CA's operating rules. Certificate holders and subscribers must also be familiar with the certification practice statement (*POŠTA®CA Politika za kvalificirana in normalizirana potrdila*), published at http://postarca.posta.si/dokumenti.

5 OBLIGATIONS OF THIRD PARTIES REGARDING CERTIFICATE STATUS VERIFICATION

Third parties that rely on the certification authority's digital certificates are obliged to:

- limit their trust in the digital certificate solely to the purposes set out in this policy;
- verify the validity of the digital certificate;
- read this document carefully and familiarise themselves with the certification authority's obligations and restrictions;
- if the digital certificate contains information on a third party, that party shall be obliged to demand the cancellation of the digital certificate if it learns that the private key has been exposed to a threat that affects its reliability, or if there is a threat of abuse, or if the information stated in the digital certificate has been changed.

6 TRUST SERVICE PROVIDER LIMITATIONS OF LIABILITY

The trust service provider shall not be liable for any damages, liabilities or other claims arising from the use of digital certificates in the following cases:

- if the digital certificate was issued due to an error, inaccurate data or other irregularities on the part of the certificate holder;
- if the digital certificate has expired;

- if the digital certificate is used after revocation and after being published in the Certificate Revocation List;
- if the digital certificate has been falsified or otherwise altered or modified;
- if a subscriber, certificate holder or third party fails to comply with the provisions of this document, the certification authority's rules of operation or applicable laws and regulations issued on their basis;
- if the private key has been compromised or if there are reasonable grounds for believing it has been compromised;
- if the digital certificate was used for purposes other than those specified in the contract, the certification authority's rules of operation or applicable laws and regulation issued on their basis;
- in case of damage due to a malfunction of the subscriber's, certificate holder's or third party's hardware or software.

7 CERTIFICATION PRACTICE STATEMENTS AND OTHER PUBLIC DOCUMENTS PUBLISHED BY THE TRUST SERVICE PROVIDER

The trust service provider publishes the following documents on its website:

- a public Certification Practice Statement for each individual type of digital certificate, published at http://postarca.posta.si/dokumenti;
- applications for issuing, revocation or renewal of certificates, published at http://postarca.posta.si/dokumenti;
- instructions for the acceptance of individual types of digital certificates;
- list of registration offices;
- price list.

The trust service provider will also publish all notices at http://postaca.posta.si relevant to all users of certificates issued by the trust service provider.

8 DATA PROTECTION

All data obtained, created or transmitted are protected as confidential information, except:

- digital certificates and certificate revocation lists, and the personal or business information contained therein;
- this document and other documents published on the certification authority's website.

9 REFUND POLICY

If a subscriber withdraws their application before the registration process is completed, or if the trust service provider rejects the application, the entire fee will be refunded.

By signing the application for a certificate, the subscriber agrees that it shall not be entitled to withdraw from the order after the certification authority fully completes the order or delivery of digital content, since the certificate is issued according to the applicant's needs as set out on the application form and is adapted to its personal needs.

In the event of a refund due to an eligible claim, the POŠTA® certification authority shall only cover the costs of issuing the digital certificate and the procedure according to the valid price list.

10 APPLICABLE LAW, COMPLAINTS AND DISPUTE RESOLUTION

The trust service provider operates in accordance with:

- 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;
- The Electronic Commerce and Electronic Signature Act of the Republic of Slovenia (Official Gazette of the RS, no. 98/2004-UPB-1, 61/2006-ZEPT);
- other applicable regulations and recommendations.

The format of this document, the POŠTA®CA PKI Disclosure Statement, follows the recommendations of ETSI EN 319 411-1, Annex A.2 The PDS structure.

The format and content of the certification practice statement (*POŠTA® CA Politika za kvalificirana in normalizirana potrdila*) is consistent with:

- RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework;
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.

All complaints and will be resolved by negotiation if possible. If this is not possible, the local court in Maribor shall be competent.

11 TSP AND REPOSITORY LICENSES, TRUST MARKS, AND AUDIT

The trust service provider POŠTA®CA, operated by Pošta Slovenije, has the status of a qualified trusted service provider in accordance with the eIDAS Regulation for the assignment of qualified certificates for electronic signatures, electronic seals and website authentication.

The status of the qualified trust service provider is confirmed by the competent supervisory authority in the Republic of Slovenia by decision and published on the EU Trusted List (https://webgate.ec.europa.eu/tl-browser).

The compliance of the operation of the POŠTA®CA trust service provider with the requirements of the eIDAS Regulation and the relevant standards (see 10) is verified by an appropriately accredited conformity assessment body.