Trust Service Authority of Slovenia

Issuer of qualified certificates for the service for
online registration and SI-PASS-CA e-signature

SI-TRUST
SI-PASS-CA

SI-PASS-CA POLICY STATEMENT

for qualified digital certificates, online login and eSignature services

Summary of the public part of the internal rules of the Trust Service Authority of Slovenia

Validity: from 12 December 2023
Version: 2.5

CPName: SI-PASS-CA

- Policy for Qualified Digital Certificates for Natural Persons for CPOID Qualified Electronic Signature : 1.3.6.1.4.1.6105.7.1.1
- Policy for Qualified Digital Certificates for CPOID Natural Persons : 1.3.6.1.4.1.6105.7.2.1
- Policy for Normalised Digital Certificates for Natural Persons CPOID : 1.3.6.1.4.1.6105.7.3.1

CONTENT:

1. Information about the trust service provider[1]

Contact details of the National Centre for Trust Services within the Ministry of Digital Transformation (hereinafter referred to as *SI-TRUST):*

Title:	Republic of Slovenia Trust Service Authority of Slovenia Ministry of Digital Transformation Tržaška cesta 211000 Ljubljana
Telephone:	01 4788 330
Web page:	http://www.si-trust.gov.si
Label:	State-institutions

Contact details of the issuer of SI-PASS-CA:

Title:	SI-PASS-CA Trust Service Authority of Slovenia Ministry of Digital Transformation Tržaška cesta 211000 Ljubljana
Email:	si-pass-ca@gov.si
Telephone:	01 4788 330
Web page:	https://www.si-trust.gov.si
Telephone number on duty for cancellations (24 hours every day of the year):	01 4788 777
Single Contact Centre:	080 2002, 01 4788 590 ekc@gov.si

2. Digital certificates, their acquisition and use

2.1. Certificate types[2]

According to this SI-PASS-CA policy, SI-PASS issues the following digital certificates for the purposes of the online registration and e-signature service:

- qualified digital certificates for natural persons for a qualified electronic signature,
- qualified digital certificates for natural persons, and
- Normalized digital certificates for natural persons.

The policy code is CPName: SI-PASS-CA, and the SI-PASS-CA policy identifiers are different depending on the type of certificate:

- CPOID: 1.3.6.1.4.1.6105.7.1.1 for qualified digital certificates for natural persons for a qualified electronic signature,
- CPOID: 1.3.6.1.4.1.6105.7.2.1 for qualified digital certificates for natural persons; and
- CPOID: 1.3.6.1.4.1.6105.7.3.1 for normalised digital certificates for natural persons.

Each certificate shall indicate the relevant policy in the form of a CPOID code.

2.2. Obtaining certificates[3]

[1] SI-PASS-CA POLICY, see. 1.3.1
[2] SI-PASS-CA POLICY, see. 1.1, 1.2
[3] SI-PASS-CA POLICY, see. 4.1, 4.2, 4.3

Prospective certificate holders are always natural persons.

The future holder shall submit the request for the certificate electronically on the SI-PASS user pages on the basis of logging into the SI-PASS service.

In order to obtain a qualified digital certificate for natural persons for a qualified electronic signature, the future certificate holder can apply to the SI-PASS service in one of the following ways:
- by means of electronic identification of assurance level "medium" or "high" according to ZEISZ,
- a qualified digital certificate on a secure means of electronic signatures,
- by means of electronic identification assurance levels "high" according to eIDAS.

In order to obtain a qualified digital certificate for natural persons, the future certificate holder can apply to the SI-PASS service in one of the following ways:
- with a qualified digital certificate,
- by means of electronic identification of assurance level "medium" according to eIDAS.

In order to obtain a normalized digital certificate for natural persons, the future certificate holder can log in to the SI-PASS service using one of the other login methods supported in the SI-PASS service, which enable obtaining information about the name and surname of the future holder.

The prospective holder of the certificate shall prove its identity by logging into the SI-PASS service with a valid qualified digital certificate or other appropriate means of electronic identification.

The application for a certificate is automatically approved on the basis of a successful certification process.

In case of an approved request from SI-PASS-CA to the future certificate holder, it shall be issued immediately after the application has been approved.

Certificates are issued exclusively on the SI-TRUST infrastructure.

2.3. Use certificates and keys[4]

The holder's private key and certificate are securely stored on the issuer's infrastructure SI-PASS-CA, which ensures that the corresponding certificate is valid while using the holder's private key.

Before using the certificate, the holder must log in to the SI-PASS service in an appropriate manner and enter a password that protects his private key.

The holder of a qualified digital certificate for natural persons for a qualified electronic signature can log in to the SI-PASS service in one of the following ways:
- by means of electronic identification of assurance level "medium" or "high" according to ZEISZ,
- a qualified digital certificate on a secure means of electronic signatures,
- by means of electronic identification assurance levels "high" according to eIDAS.

The holder of a qualified digital certificate for natural persons can log in to the SI-PASS service in one of the following ways:
- with a qualified digital certificate,
- by means of electronic identification of assurance level "medium" according to eIDAS.

The holder of a normalized digital certificate for natural persons can log in to the SI-PASS service by one of the other login methods supported in the SI-PASS service, which enable obtaining information about the name and surname of the future holder.

[4] SI-PASS-CA POLICY, see. 4.5

In order to protect the private key, the holder or future holder of the certificate is obliged:
- ensure that the login method used in SI-PASS is not compromised,
- protect the private key with an appropriate password in accordance with the recommendations of SI-PASS-CA in such a way that only the holder has access to it,
- carefully protect the password to protect the private key,
- After the expiration or revocation of the certificate, act in accordance with the notifications of SI-PASS-CA.

The holder must protect the private key from unauthorised use.

3. Restrictions on use[5]

SI-PASS-CA digital certificates can be used for:
- authentication of digitally signed data in electronic form,
- services or applications for which the use of SI-TRUST qualified digital certificates is required.

The holder's private key and certificate are securely stored on the issuer's infrastructure SI-PASS-CA, which ensures that the corresponding certificate is valid while using the holder's private key.

Logs of recorded events related to keys and certificates are retained for at least ten (10) years after the certificate to which the log relates expires.

The remaining logs of recorded events shall be retained for at least ten (10) years after the occurrence of the event.

The event logs referred to in the preceding paragraph containing personal data shall be retained in accordance with applicable law.

4. Duties and responsibilities of the holder[6]

In order to protect the private key, the holder or future holder of the certificate is obliged:
- ensure that the login method used in SI-PASS is not compromised,
- protect the private key with an appropriate password in accordance with the recommendations of SI-PASS-CA in such a way that only the holder has access to it,
- carefully protect the password to protect the private key,
- After the expiration or revocation of the certificate, act in accordance with the notifications of SI-PASS-CA.

The holder must protect the private key from unauthorised use.

The holder or future holder of the certificate is obliged:
- familiarize yourself with this policy before issuing a certificate,
- comply with the policy and other applicable regulations,
- after receiving the certificate, check the data in the certificate and immediately notify SI-PASS-CA or request revocation of the certificate in case of any errors or problems,
- monitor and comply with all SI-PASS-CA notifications,
- appropriately update the necessary hardware and software for secure certificate work in accordance with notifications,
- report all changes related to the certificate to SI-PASS-CA IMMEDIATELY,

[5] SI-PASS-CA POLICY, see. 1.1, 4.5, 5.4.3
[6] SI-PASS-CA POLICY, see. 4.5.1, 9.6.3

- request certificate revocation if private keys have been compromised in a way that affects usage reliability, or if there is a risk of misuse,
- use the certificate for the purpose specified in the certificate and in the manner specified in the SI-PASS-CA policy,
- take care of the originally signed documents and the archive of these documents.

The holder shall be liable for:
- damage incurred in case of misuse of the certificate from cancellation report to revocation,
- any damage caused, either directly or indirectly, due to the fault of the holder it has been possible to use or abuse the holder's certificate by unauthorised persons,
- any other damage arising from non-compliance with the provisions of this Policy and other SI-PASS-CA notifications and applicable regulations.

5. Requirements for verification of the registry of revoked certificates for third parties[7]

Third parties relying on the certificate should check the latest published register of revoked certificates before use.

For the sake of authenticity and integrity, it is always necessary to verify the validity and authenticity of this register, which is digitally signed by SI-PASS-CA.

For each digital certificate used, the third party must perform a complete trust chain verification process in accordance with RFC 5280.

If a third party is unable to verify the status of the digital certificate in the registry of revoked certificates, it may refuse to use the digital certificate or nevertheless use the digital certificate and knowingly accept.

The register of revoked certificates shall be updated:
- after each revocation of the certificate,
- once a day, if there are no new records or changes in the registry of revoked certificates, approximately twenty-four (24) hours after the last refresh.

The Real-time Certificate Status Protocol (OCSP) according to RFC recommendation 2560 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP" is supported.

6. Disclaimer and Limitation of Liability[8]

SI-TRUST is not liable for damages caused by:
- the use of certificates for the purpose and in a manner not expressly provided for in the policy of the issuer of SI-PASS-CA or any agreement between the holder or organization and SI-TRUST,
- incorrect or incomplete protection of the passwords or private keys of the holders, issuing confidential data or keys to third parties and irresponsible behaviour of the holder,
- misuse or intrusion into the information system of the certificate holder and thus data on certificates by unauthorized persons,
- the non-functioning or malfunctioning IT infrastructure of the certificate holder or third parties,
- non-verification of data and validity of certificates,
- failure to check the period of validity of the certificate,
- conduct of the certificate holder or third party contrary to the notifications of the issuer of SI-PASS-CA, policy, possible agreement or contract and other regulations,

[7] SI-PASS-CA POLICY, see. 4.9.6, 4.9.7, 4.9.9
[8] SI-PASS-CA POLICY, see. 9.7, 9.8

- enable the use or misuse of the holder's certificate by unauthorised persons,
- the certificate issued containing false data and untrue data or other actions of the holder or organisation,
- the use of certificates and the validity of certificates in the event of changes to the particulars given in the certificate or changes to the particulars of the holder or organisation,
- a failure of infrastructure that is not within the domain of SI-TRUST management,
- data that is encrypted or signed using associated certificates or private keys,
- conducting holders in the use of certificates, even if the holder or a third party has complied with all provisions of this policy and agreement, as well as notifications from the issuer of SI-PASS-CA or other applicable regulations,
- the use and reliability of the hardware and software performance of certificate holders.

The issuer of SI-PASS-CA or SI-TRUST guarantees the value of each legal transaction according to the type of certificate up to the value of:

- for qualified certificates for qualified electronic signatures up to EUR 5,000; and
- for qualified certificates up to EUR 1,000.

7. Policy and applicable law[9]

The source document is the SI-PASS-CA policy for qualified digital certificates for the online login and e-signature service.

The policy code is CPName: SI-PASS-CA, and the SI-PASS-CA policy identifiers are different depending on the type of certificate:

- CPOID: 1.3.6.1.4.1.6105.7.1.1 for qualified digital certificates for natural persons for a qualified electronic signature,
- CPOID: 1.3.6.1.4.1.6105.7.2.1 for qualified digital certificates for natural persons; and
- CPOID: 1.3.6.1.4.1.6105.7.3.1 for normalised digital certificates for natural persons.

SI-TRUST and the issuer of SI-PASS-CA operate in accordance with:

- Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC,
- Regulation (EU) No 679/2016 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 1995/46/EC,
- the Electronic Identification and Trust Services Act,
- the Identity Card Act,
- the Personal Data Protection Act,
- the Classified Information Act,
- the Protection of Documents and Archives and Archives Act,
- Regulation determining electronic identification means and using the central online registration and electronic signature service;
- ETSI recommendations in the field of qualified certificates and trust services,
- RFC recommendations in the field of X.509 certificates,
- CA/Browser Forum ("Baseline Requirements" and "EV SSL Certificate Guidelines")
- and other applicable regulations and recommendations.

8. Protection of personal data and storage period

8.1. Protection of personal data[10]

[9] SI-PASS-CA POLICY, see. 1.2, 9.14

All personal and confidential data on certificate holders, which are strictly necessary for certificate management services, is handled by the issuer of SI-PASS-CA in accordance with the applicable legislation.

Protected data is all personal data obtained by the issuer of SI-PASS-CA on requests for its services or in any mutual agreement or contract or in the relevant registers for proving the identity of the holder.

There are no other potentially non-protected personal data other than those mentioned in the certificate and the register of revoked certificates.

SI-TRUST is liable in accordance with applicable legislation regarding the protection of personal data.

The holder authorizes SI-TRUST or the issuer of SI-PASS-CA to use personal data on the request for obtaining a certificate or later in writing.

SI-TRUST does not provide data on certificate holders that are not specified in the certificate, unless certain data are specifically required for the provision of specific services or applications related to certificates, and SI-TRUST is the holder of the authorizations to do so, or at the request of the competent court or administrative authority

Data is also transmitted without written consent, if provided for by law or applicable regulations.

8.2. Storage time[11]

Archived data relating to keys and certificates shall be kept for at least ten (10) years after the expiry of the certificate to which the data relates.

Other archived data is stored for at least ten (10) years after their creation.

The archived data referred to in the preceding paragraph containing personal data shall be stored in accordance with applicable law.

9. Reimbursement[12]

Certificate management costs are charged according to the published price list on the https://www.si-trust.gov.si/sl/si-pass website.

10. Procedure in case of disputes[13]

The parties will endeavour to resolve disputes amicably, but if this is not possible, the court in Ljubljana shall have jurisdiction to resolve disputes. The parties shall agree on the exclusive application of the regulations of the Republic of Slovenia for the settlement of disputes.

11. Compliance with applicable legislation[14]

The supervision of the compliance of SI-TRUST or the issuer of SI-PASS-CA with the applicable legislation and regulations is carried out by the competent inspection service.

[10] SI-PASS-CA POLICY, see. 9.4
[11] SI-PASS-CA POLICY, see. 5.5.2
[12] SI-PASS-CA POLICY, see. 9.1
[13] SI-PASS-CA POLICY, see. 9.13
[14] SI-PASS-CA POLICY, see. 9.15, 8

The frequency of inspections is the responsibility of the inspection service, which is responsible in accordance with the legislation in force.

SI-TRUST inspections are carried out by the competent inspection service in accordance with the applicable legislation.

External verification of conformity of operations shall be carried out by a conformity assessment body in accordance with applicable legislation.

Internal verification of compliance is carried out by the internal auditor and other authorized persons within SI-TRUST.

The inspection service is the supervisory authority competent under the applicable legislation.

Areas of control are determined by current legislation and regulations.

In case of identified deficiencies or errors, the issuer of SI-PASS-CA or SI-TRUST strives to eliminate them in the shortest possible time.

SI-TRUST shall make a summary of inspection decisions publicly available on its website.

SI-TRUST shall make publicly available on its website information about the conformity assessment body that has carried out external verification of SI-TRUST compliance in accordance with the applicable legislation.