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 May 20, 2026
Version: 3.0

CPName: SI-PASS-CA

- **Policy for Qualified Digital Certificates for Natural Persons for Qualified Electronic Signature**
  CP_{OID}: 1.3.6.1.4.1.6105.7.1.2
- **Policy for Qualified Digital Certificates for Natural Persons**
  CP_{OID}: 1.3.6.1.4.1.6105.7.2.2
- **Policy for Normalised Digital Certificates for Natural Persons**
  CP_{OID}: 1.3.6.1.4.1.6105.7.3.2

CONTENTS:

1. Trust Service Provider Information[1]

Contact details of the National Centre for Trust Services operating 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 21 1000 Ljubljana
Phone:	+386 1 4788 330
Website:	http://www.si-trust.gov.si
Label:	State-institutions

Contact details of the issuer SI-PASS-CA:

Title:	SI-PASS-CA Trust Service Authority of Slovenia Ministry of Digital Transformation Tržaška cesta 21 1000 Ljubljana
Email:	si-pass-ca@gov.si
Phone:	01 4788 330
Website:	https://www.si-trust.gov.si
Telephone number on duty for cancellations (24 hours every day of the year):	+386 1 4788 777
Single Contact Centre:	080 2002, +386 1 4788 590 ekc@gov.si

2. Digital certificates, their acquisition and use

2.1. Types of certificates[2]

According to the current policy, SI-PASS-CA issues the following digital certificates for the needs of the online login and e-signature service:

- qualified digital certificates for natural persons for qualified electronic signatures;
- qualified digital certificates for natural persons; and
- Normalized digital certificates for natural persons.

According to this policy, SI-PASS-CA also represents the SI-PASS qualified trust service policy for managing remote devices for creating a qualified electronic signature. The SI-PASS service for remote e-signature provides a server-side signing service in accordance with ETSI TS 119 431-1, Annex A (EUSPv2 Policy) and manages the lifecycle of signing keys on behalf of signatories. It shall ensure that signature keys are created, activated and used exclusively within the qualified electronic signature creation device under the sole control of the signatory.

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

[1] SI-PASS-CA Policy, Chapter 1.3.1
[2] SI-PASS-CA Policy, Chapter 1.1, 1.2

- CPOID: 1.3.6.1.4.1.6105.7.1.2 for qualified digital certificates for natural persons for qualified electronic signatures,
- CPOID: 1.3.6.1.4.1.6105.7.2.2 for qualified digital certificates for natural persons, and
- CPOID: 1.3.6.1.4.1.6105.7.3.2 for normalised digital certificates for natural persons.

Each certificate shall contain an indication of the relevant policy in the form of a CPOID designation.

The SI-PASS qualified trust service policy identifier for managing remote devices for creating a qualified electronic signature is 0.4.0.19431.1.1.4.

2.2. Obtaining certificates[3]

Prospective certificate holders shall always be natural persons.

The application for obtaining the certificate is submitted by the future holder electronically on the SI-PASS user pages on the basis of logging in to the SI-PASS service.

In order to obtain a qualified digital certificate for natural persons for a qualified electronic signature, the prospective certificate holder may log in to the SI-PASS service in one of the following ways:

- by means of electronic identification of a confidence level of "medium" or "high" in accordance with ZEISZ,
- with a qualified digital certificate for a qualified electronic signature,
-
- with an electronic identification means, a confidence level of "high" in accordance with eIDAS.

In order to obtain a qualified digital certificate for natural persons, the prospective certificate holder can log in to the SI-PASS service in one of the following ways:

- with a qualified digital certificate,
- with an electronic identification means of assurance level "medium" in accordance with eIDAS.

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

The future holder of the certificate proves his/her identity by logging in to the SI-PASS service with a valid qualified digital certificate or other appropriate means of electronic identification.

An application for a certificate shall be approved automatically on the basis of a successful certification procedure.

In the case of an approved application, the SI-PASS-CA shall issue it to the prospective holder of the certificate immediately after the approval of the application.

Certificates are issued exclusively on the SI-TRUST infrastructure.

2.3. Use certificates and keys[4]

The holder's private key and its certificate are securely stored on the infrastructure of the SI-PASS-CA issuer, which ensures that the corresponding certificate is valid at the time of use of the holder's private key.

[3] SI-PASS-CA Policy, Chapter 4.1, 4.2, 4.3
[4] SI-PASS-CA Policy, Chapter 4.5

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

The holder of a qualified digital certificate for natural persons for a qualified electronic signature may log in to the SI-PASS service in one of the following ways:

- by means of electronic identification of a confidence level of "medium" or "high" in accordance with ZEISZ,
- with a qualified digital certificate for a qualified electronic signature,
-
- with an electronic identification means, a confidence level of "high" in accordance with eIDAS.

The holder of a qualified digital certificate for natural persons may log in to the SI-PASS service in one of the following ways:

- with a qualified digital certificate,
- with an electronic identification means of assurance level "medium" in accordance with eIDAS.

The holder of a normalised digital certificate for natural persons may log in to the SI-PASS service using one of the other login methods supported in the SI-PASS service, which enable the acquisition of information on the name and surname of the future holder.

With regard to the protection of the private key, the holder or prospective holder of the certificate is obliged to:

- make sure that the login method used in the SI-PASS service is not jeopardized,
- protect the private key with an appropriate password in accordance with the SI-PASS-CA recommendations 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 SI-PASS-CA notifications.

The holder must protect the private key from unauthorized use.

2.4. Use of SI-PASS for remote e-signature[5]

SI-TRUST provides the SI-PASS service for remote e-signature in accordance with Regulation (EU) No 910/2014, Commission Implementing Regulation (EU) 2025/1567 and ETSI EN 319 421, ETSI EN 319 422 and ETSI EN 391 401 standards.

The SI-PASS service for remote e-signature includes the following components as defined by ETSI TS 119 431-1:

- Signing Key Creation Service: Creates signing keys within a qualified electronic signature creation device.
- Certificate linking service: links certificates issued by SI-PASS-CA to the corresponding signing keys,
- service of linking electronic identification means or signatory identity: connects the signatory's authentication (via the SI-PASS service for online login) with the appropriate signing keys,
- Signature Activation Data: Validates Signature Activation Data (SAD) and activates signature keys to create a signature.
- Delete Signing Key Service: Destroys signing keys when necessary.

The SI-PASS service for Remote E-Signature supports two models of Signature Creation Application (SCA) installation:

- External SCA application: An in-house service provider manages its own SCA application. It sends a pre-calculated Data To Be Signed Representation (DTBS/R) value to the SI-PASS interface and receives the raw value of the signature.

[5] SI-PASS-CA Policy, Chapter 1.1

- SCA SI-PASS application: The provider of its own service sends the document to the SI-PASS interface. The SCA SI-PASS calculates DTBS/R data, orchestrates the signing via the Server Signing Application (SSA), and returns the signed document.

3. Restrictions on use[6]

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

The holder's private key and its certificate are securely stored on the infrastructure of the SI-PASS-CA issuer, which ensures that the corresponding certificate is valid at the time of use of the holder's private key.

Logs of logged events relating to keys and digital certificates shall be retained for at least ten (10) years after the expiry of the certificate to which the log relates.

Other logs of recorded events shall be kept for at least ten (10) years after the occurrence of the event.

Logs of recorded events referred to in the previous paragraph, which contain personal data, are kept in accordance with the applicable legislation.

4. Duties and responsibilities of the holder[7]

With regard to the protection of the private key, the holder or prospective holder of the certificate is obliged to:
- make sure that the login method used in the SI-PASS service is not jeopardized,
- protect the private key with an appropriate password in accordance with the SI-PASS-CA recommendations 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 SI-PASS-CA notifications.

The holder must protect the private key from unauthorized use.

The holder or prospective holder of the certificate is obliged to:
- familiarise yourself with this policy before issuing the certificate;
- act in accordance 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 the cancellation of the certificate in the event of any errors or problems,
- monitor and comply with all SI-PASS-CA notifications,
- update the necessary hardware and software for safe work with certificates in accordance with the notifications,
- report any changes related to the certificate immediately to the SI-PASS-CA,
- request the revocation of the certificate if the private keys have been compromised in a way that affects the reliability of use, or if there is a risk of misuse,
- use the certificate for the purpose specified in the certificate and in the manner specified by the SI-PASS-CA policy,
- take care of the originally signed documents and the archive of these documents.

The holder is responsible for:

[6] SI-PASS-CA Policy, Chapter 1.1, 4.5, 5.4.3
[7] SI-PASS-CA Policy, Chapter 4.5.1, 9.6.3

- the damage incurred in the event of misuse of the certificate from the notification of the revocation to the revocation,
- any damage caused either directly or indirectly by the fact that the use or misuse of the holder's certificate by unauthorized persons was enabled through the fault of the holder,
- any other damages resulting from failure to comply with the provisions of this policy and other SI-PASS-CA notices and applicable regulations.

5. Requirements for third-party verification of the register of revoked certificates[8]

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

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

A third party must perform a full chain of trust verification process in accordance with RFC 5280 for each digital certificate used.

If a third party is unable to verify the status of a digital certificate in the register of revoked certificates, they may refuse to use the digital certificate or use the digital certificate anyway and consciously accept it.

The register of revoked certificates shall be updated:
- no later than two (2) hours after the revocation of the certificate,
- once a day, if there are no new records or changes in the register of revoked certificates, approximately twenty-four (24) hours after the last refresh.

The Real-Time Certificate Status Verification Protocol (OCSP) is supported in accordance with RFC 2560 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP".

6. Disclaimer and Limitation of Liability[9]

SI-TRUST shall not be liable for damages resulting from:
- the use of certificates for a 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,
- improper or deficient protection of passwords or private keys of holders, issuance of 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 into the data on certificates by unauthorized persons,
- malfunctioning or malfunctioning of the IT infrastructure of the certificate holder or third parties,
- failure to verify the data and validity of certificates;
- failure to verify the validity period of the certificate,
- the conduct of the certificate holder or a third party contrary to the notices of the SI-PASS-CA issuer, the policy, any agreement or contract and other regulations,
- enabling the use or misuse of the holder's certificate by unauthorized persons,
- a certificate issued with false information and unreliable information or other actions of the holder or organization,
- the use of certificates and the validity of certificates in the event of changes in the data contained in the certificate or changes in the information of the holder or organisation,
- failure of infrastructure that is not within the domain of SI-TRUST management,

[8] SI-PASS-CA Policy, Chapter 4.9.6, 4.9.7, 4.9.9
[9] SI-PASS-CA Policy, Chapter 9.7, 9.8

- data that is encrypted or signed using the associated certificates or private keys,
- the conduct of holders in the use of certificates, including if the holder or a third party has complied with all the provisions of this policy and agreement and the notices of the SI-PASS-CA issuer or other applicable regulations,
- the use and reliability of the operation of the hardware and software of the certificate holders.

The issuer of SI-PASS-CA or SI-TRUST guarantees the value of an individual 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[10]

The underlying 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 vary depending on the type of certificate:

- CPOID: 1.3.6.1.4.1.6105.7.1.2 for qualified digital certificates for natural persons for qualified electronic signatures,
- CPOID: 1.3.6.1.4.1.6105.7.2.2 for qualified digital certificates for natural persons, and
- CPOID: 1.3.6.1.4.1.6105.7.3.2 for normalised digital certificates for natural persons.

SI-TRUST and the issuer SI-PASS-CA shall act 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,
- Personal Data Protection Act,
- The Classified Information Act,
- the Act on the Protection of Documentary and Archival Records and Archives,
- Regulation on the designation of electronic identification means and the use of a central service for online sign-in and electronic signature,
- ETSI recommendations in the field of qualified certificates and trust services;
- RFC recommendations in the field of X.509 certificates,
- CA/Browser Forum requirements ("Baseline Requirements" and "EV SSL Certificate Guidelines"),
- and other applicable regulations and recommendations.

8. Personal data protection and retention period

8.1. Personal data protection[11]

All personal and confidential information about certificate holders that is strictly necessary for certificate management services is handled by the SI-PASS-CA issuer in accordance with applicable law.

Protected data are all personal data that the SI-PASS-CA issuer obtains on requests for its services or in any mutual agreement or contract or in appropriate registers for proving the identity of the holder.

[10] SI-PASS-CA Policy, Chapter 1.2, 9.14
[11] SI-PASS-CA Policy, Chapter 9.4

There is no other potentially non-proprietary personal data other than those listed in the certificate and the register of revoked certificates.

SI -TRUST is responsible in accordance with the 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 application for obtaining a certificate or later in writing.

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

The data is also provided without written consent, if this is stipulated by law or applicable regulations.

8.2. Retention time[12]

Archived data relating to keys and digital certificates shall be stored 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 its creation.

The archived data referred to in the previous paragraph, which contain personal data, are stored in accordance with the applicable legislation.

9. Reimbursement of costs[13]

No costs of administering certificates shall be charged to holders.

10. Dispute procedure[14]

The parties will endeavour to resolve disputes amicably, and if this is not possible, the court in Ljubljana shall have jurisdiction to resolve disputes. For the purpose of resolving disputes, the parties agree exclusively to apply the regulations of the Republic of Slovenia.

11. Compliance with applicable legislation[15]

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

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

The implementation of SI-TRUST inspections is carried out by the competent inspection service in accordance with the applicable legislation.

External verification of the conformity of performance shall be carried out by a conformity assessment body

[12] SI-PASS-CA Policy, Chapter 5.5.2
[13] SI-PASS-CA Policy, Chapter 9.1
[14] SI-PASS-CA Policy, Chapter 9.13
[15] SI-PASS-CA Policy, Chapter 9.15, 8

in accordance with the applicable legislation.

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

The inspection service is the supervisory authority competent in accordance with the legislation in force.

The areas of control are determined by the applicable legislation and regulations.

In the event of identified deficiencies or errors, the issuer of SI-PASS-CA or SI-TRUST shall endeavour to eliminate them as soon as possible.

SI-TRUST publishes a summary of the inspection decisions on its website.

SI-TRUST shall publicly publish on its website information on the conformity assessment body that has carried out an external verification of the compliance of SI-TRUST's operations in accordance with the applicable legislation.