Trust Service Authority of Slovenia
Issuer of qualified digital certificates
SI-TRUST eID Signature

SI-TRUST
SI-TRUST eID Podpis

SI-TRUST POLICY STATEMENT eID Signature

for qualified certificates for electronic signatures on identity cards

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

Validity: from 12 December 2023
Version: 1.2

CPName: SI-TRUST eID Signature
CPOID: 1.3.6.1.4.1.6105.9.1.1

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:	https://www.si-trust.gov.si
Label:	State-institutions

Contact details of the SI-TRUST eID issuer Signature:

Title:	SI-TRUST eID Signature Trust Service Authority of Slovenia Ministry of Digital Transformation Tržaška cesta 211000 Ljubljana
Email:	si-trust@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-TRUST eID Signature policy, it issues qualified certificates for electronic signature according to CPOID: 1.3.6.1.4.1.61.6105.9.1.1.

The code of this policy is CPName: SI-TRUST eID Signature, SI-TRUST eID Policy Identifier The signature is $CP_{OID:}$ 1.3.6.1.4.1.61.6105.9.1.1.

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

2.2. Obtaining certificates[3]

The future certificate holders are citizens of the Republic of Slovenia who submit an application for an identity card and are over 12 years of age at the time of submitting the application.

In order to obtain a certificate, the prospective holder must submit an application for an identity card in accordance with the sectoral legislation. An application for an identity card also constitutes an application for a certificate.

[1] SI-TRUST eID Policy Signature, see. 1.3.1
[2] SI-TRUST eID Policy Signature, see. 1.1, 1.2
[3] SI-TRUST eID Policy Signature, see. 4.1, 4.2, 4.3

The verification of the identity and authenticity of the prospective holder shall be carried out in accordance with the procedures for obtaining an identity card. The official of the competent authority establishes the identity of the citizen and verifies the veracity of the data contained in the application for an identity card.

An application for an identity card may be submitted by a citizen who has reached the age of 18 and also by a citizen who is not yet 18 years old, but has married or became the parent and has been recognised as having full legal capacity by a court decision.

If the application for an identity card is submitted by the legal representative, the official shall also establish the identity of the legal representative. The child or citizen of legal capacity must also be present at the time of the application, but there are no legitimate medical reasons for him or her to be unable to be present at the time of the application to the competent authority.

A qualified certificate for electronic signature is authorised by accepting an identity card application. When submitting the application, the future holder of the SI-TRUST eID Signature issuer certificate is acquainted with all the necessary documentation in accordance with the applicable legislation.

The time for issuing the certificate is defined in the legislation governing the identity card.

Based on the information on the submission of an application for an identity card, the SI-TRUST eID Signature issuer obtains data from the record of issued identity cards and prepares data for the issuance of a qualified certificate for electronic signature. Certificates are accepted exclusively on the infrastructure of the personalization provider.

An ID card chip is a device for creating a qualified electronic signature. The certificate is placed on the chip of the identity card in the process of personalization of the identity card, so that the personalization provider generates a pair of keys on the hardware security module and forwards the certificate request to the issuer in a secure way. The received certificate is stored on the chip of the ID card together with the private key. Upon completion of the process, it disables the deletion of saved records (private key and certificate) and the addition of new records by the holder.

The produced identity card shall be served on the future holder in accordance with the provisions of the legislation governing the identity card .

The initial password for accessing the digital certificate is received by the holder in the same way as an identity card, namely:

- in person when collecting an identity card at the registration service or personalization provider, or
- by postal item to the address of residence.

As soon as the ID card on which the certificate has already been collected, the holder must verify the information in this certificate. If he does not immediately inform the issuer of the SI-TRUST eID Signature of any errors, it is considered that he agrees with the content and agrees with the terms of operation and assumption of obligations and responsibilities.

Certificates are issued exclusively on the SI-TRUST infrastructure.

2.3. Use certificates and keys[4]

In order to protect the private key, the holder or future holder of the certificate is obliged:

- carefully protect the data for the use of the certificate from unauthorized persons,
- keep the private key and certificate in accordance with the notifications and recommendations of the

[4] SI-TRUST eID Policy Signature, see. 4.5

SI-TRUST eID Signature,
- protect the private key and all other confidential data with an appropriate user password in accordance with the recommendations of the SI-TRUST eID Signature or in any other way so that only the holder has access to them,
- after the expiration or revocation of the certificate, act in accordance with the SI-TRUST eID Signature notifications.

The holder must protect the private key for signing the data from unauthorised use.

3. Restrictions on use[5]

SI-TRUST eID Digital Certificates The signature can be used to:
- authentication of digitally signed data in electronic form and identification of the holder,
- services or applications for which the use of SI-TRUST qualified digital certificates is required.

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:
- carefully protect the data for the use of the certificate from unauthorized persons,
- keep the private key and certificate in accordance with the notifications and recommendations of the SI-TRUST eID Signature,
- protect the private key and all other confidential data with an appropriate user password in accordance with the recommendations of the SI-TRUST eID Signature or in any other way so that only the holder has access to them,
- after the expiration or revocation of the certificate, act in accordance with the SI-TRUST eID Signature notifications.

The holder must protect the private key for signing the data 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,
- if, after submitting an application for an identity card from a personalisation provider or a competent authority, depending on the choice of the method of service of the identity card, the holder does not receive an identity card, the holder must contact the competent authority where he applied for the identity card,
- if, after submitting an application for an identity card from a personalisation provider or a competent authority, depending on the choice of the method of service of the identity card, the holder does not receive an envelope with an initial password, the holder must submit an application to the competent authority to obtain a code to reset the user's password,
- after accepting the certificate, check the data in the certificate and immediately notify the SI-TRUST eID Signature issuer or request revocation of the certificate in case of any errors or problems,

[5] SI-TRUST eID Policy Signature, see. 1.1, 4.5, 5.4.3
[6] SI-TRUST eID Policy Signature, see. 4.5.1, 9.6.3

- monitor all notifications issued by SI-TRUST eID Signature and comply with them,
- appropriately update the necessary hardware and software for secure certificate work in accordance with notifications,
- immediately report all changes related to the certificate to the issuer of the SI-TRUST eID Signature,
- 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 (see Sub-View. 7.1) and in a manner determined by the policy SI-TRUST eID Signature,
- 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 possibility of using or misusing the holder's certificate by unauthorised persons,
- any other damage arising from non-compliance with the provisions of this Policy and other notices of the issuer of SI-TRUST's eID Signature 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 registry 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-TRUST eID Signature.

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 SI-TRUST eID issuer's policy Signature or any agreement between the holder or organisation 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,

[7] SI-TRUST eID Policy Signature, see. 4.9.6, 4.9.7, 4.9.9
[8] SI-TRUST eID Policy Signature, see. 9.7, 9.8

- 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,
- actions of the certificate holder or third party contrary to the notifications of the issuer of SI-TRUST eID Signature, policy, possible agreement or contract and other regulations,
- 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 the 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 notices from the issuer of SI-TRUST eID Signature or other applicable regulations,
- the use and reliability of the hardware and software performance of certificate holders.

The issuer of SI-TRUST eID Signature or SI-TRUST guarantees the value of individual legal transactions up to the value of 5,000 EUR.

7. Policy and applicable law[9]

The source document is the SI-TRUST eID Signature Policy for qualified certificates for electronic signatures on the identity card.

The code of this policy is CPName: SI-TRUST eID Signature, SI-TRUST eID Policy Identifier The signature is $CP_{OID:}$ 1.3.6.1.4.1.61.6105.9.1.1.

SI-TRUST and SI-TRUST eID Signatures work 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-TRUST eID Policy Signature, see. 1.2, 9.14

SI-TRUST handles all personal and confidential data on certificate holders that are strictly necessary for certificate management services in accordance with applicable law.

Protected data is all personal data obtained by the issuer of SI-TRUST eID Signature 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 responsible in accordance with the applicable legislation regarding the protection of personal data. The personalization provider is responsible for personal data necessary for the recording of the digital certificate on the identity card in accordance with the applicable legislation regarding the protection of personal data

The holder authorizes SI-TRUST or issuer SI-TRUST eID Signature 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 authorizations to do so (see previous sub-chapter) 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 included in the price of an identity card.

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]

[10] SI-TRUST eID Policy Signature, see. 9.4
[11] SI-TRUST eID Policy Signature, see. 5.5.2
[12] SI-TRUST eID Policy Signature, see. 9.1
[13] SI-TRUST eID Policy Signature, see. 9.13
[14] SI-TRUST eID Policy Signature, see. 9.15, 8

Supervision of the compliance of SI-TRUST 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 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, SI-TRUST strives to eliminate them as soon as possible.

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.