Trust Service Authority of Slovenia
Issuer of SIGEN-CA qualified digital certificates

SIGEN-CA POLICY STATEMENT

for online qualified digital certificates for natural persons

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

Validity: from 12 December 2023
Version: 7.5

CPName: SIGEN-CA-2
CPOID: 1.3.6.1.4.1.6105.2.2.3.5

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 SIGEN-CA issuer:

Title:	SIGEN-CA Trust Service Authority of Slovenia Ministry of Digital Transformation Tržaška cesta 211000 Ljubljana
Email:	sigen-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 policy, SIGEN-CA issues online qualified digital certificates for natural persons according to the CPOID: 1.3.6.1.4.1.61.6105.2.2.3.5.

The policy code is CP_{Name}: SIGEN-CA-2 and the SIGEN-CA-2 policy identifier is CPOID: 1.3.6.1.4.1.6105.2.2.3.5.

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

2.2. Obtaining certificates[3]

Prospective certificate holders are always natural persons.

To obtain a certificate, the future holder must correctly fill out and sign the application for obtaining a certificate. A claim may be submitted by a person over 15 years of age with legal capacity.

In the event that the future holder is a disabled person, the application for obtaining a certificate may be submitted on his behalf by another person, who must attach a notarized or administratively certified power of attorney and his valid photo identity document.

[1] SIGEN-CA policy for natural persons, see. 1.3.1
[2] SIGEN-CA policy for natural persons, see. 1.1, 1.2
[3] SIGEN-CA policy for natural persons, see. 4.1, 4.2, 4.3

The prospective holder may submit to the SIGEN-CA issuer by electronic means an application digitally signed with its valid qualified digital certificate for natural persons issued to him by the SIGEN-CA issuer.

In case of submitting a claim in person to the registration service, the authorized person verifies the identity of the future holder at the registration service in accordance with the applicable legislation. The prospective holder must prove his identity by means of a valid identity document.

In case of submission of the request electronically, the SIGEN-CA issuing officer shall authenticate the electronic signature. The identity of the prospective holder shall be proven by the validity of his electronic signature.
The application for a certificate is approved or, in case of incorrect or incomplete data or non-fulfillment of obligations, is rejected by the authorised persons issuing SIGEN-CA.

On the basis of an approved application, SIGEN-CA shall provide the prospective holder of the digital certificate with the authorisation code and reference number no later than ten (10) days from the approval of the request.

In case of an approved request, SIGEN-CA shall provide the future certificate holder with the reference number and authorisation code through two separate channels: the reference number by e-mail, and the authorisation code by post, and exceptionally the SIGEN-CA authorised person may also hand them over in person. Both data are needed by the prospective holder to collect the digital certificate.

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 receipt of the certificate from unauthorized persons,
- keep the private key and confirmation in accordance with SIGEN-CA notifications and recommendations,
- protect the private key and any other confidential data with an appropriate password in accordance with the SIGEN-CA recommendations or in any other way so that only the holder has access to them,
- carefully protect passwords to protect the private key,
- after the expiration or revocation of the certificate, act in accordance with SIGEN-CA notifications.

The holder must protect the private key from unauthorised use.

3. Restrictions on use[5]

SIGEN-CA digital certificates may be used for:
- encryption of data in electronic form,
- 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.

[4] SIGEN-CA policy for natural persons, see. 4.5
[5] SIGEN-CA policy for natural persons, see. 1.1, 4.5, 5.4.3

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 receipt of the certificate from unauthorized persons,
- keep the private key and confirmation in accordance with SIGEN-CA notifications and recommendations,
- protect the private key and any other confidential data with an appropriate password in accordance with the SIGEN-CA recommendations or in any other way so that only the holder has access to them,
- carefully protect passwords to protect the private key,
- after the expiration or revocation of the certificate, act in accordance with SIGEN-CA notifications.

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,
- if, after submitting the request for a certificate or other service, the SIGEN-CA issuer does not receive a notification by e-mail specified in the request, it must contact the authorised persons of the SIGEN-CA issuer,
- after accepting the certificate, check the data in the certificate and immediately inform SIGEN-CA or request cancellation of the certificate in case of any errors or problems,
- if, after submitting the request for obtaining a certificate or other service, the SIGEN-CA issuer does not receive a notification by e-mail specified in the request, then it must contact the authorised persons of the SIGEN-CA issuer,
- monitor and comply with all SIGEN-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 SIGEN-CA without delay,
- 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 SIGEN-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 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 SIGEN-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 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

[6] SIGEN-CA policy for natural persons, see. 4.5.1, 9.6.3
[7] SIGEN-CA policy for natural persons, see. 4.9.6, 4.9.7, 4.9.9

register, digitally signed by SIGEN-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 SIGEN-CA issuer's policy 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,
- 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,
- the conduct of the certificate holder or third party in violation of the SIGEN-CA issuer's notifications, 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,
- the conduct of holders in the use of certificates, including if the holder or a third party has complied with all provisions of this policy and agreement, as well as notices from the SIGEN-CA issuer or other applicable regulations,
- the use and reliability of the hardware and software performance of certificate holders.

The SIGEN-CA or SI-TRUST issuer guarantees the value of each legal transaction up to EUR 1,000.

7. *Policy and applicable law*[9]

The source document is the SIGEN-CA Policy for Qualified Digital Certificates for Natural Persons.

The code of this policy is CPName: SIGEN-CA-2 and the SIGEN-CA-2 policy identifier is $CP_{OID:}$ 1.3.6.1.4.1.61.6105.2.2.3.5.

[8] SIGEN-CA policy for natural persons, see. 9.7, 9.8
[9] SIGEN-CA policy for natural persons, see. 1.2, 9.14

SI-TRUST and SIGEN-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]

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 SIGEN-CA issuer 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 holder authorizes SI-TRUST or the SIGEN-CA issuer 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.

[10] SIGEN-CA policy for natural persons, see. 9.4
[11] SIGEN-CA policy for natural persons, see. 5.5.2

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/digitalna-potrdila/fizicne-osebe/ 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]

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.

[12] SIGEN-CA policy for natural persons, see. 9.1
[13] SIGEN-CA policy for natural persons, see. 9.13
[14] SIGEN-CA policy for natural persons, see. 9.15, 8