POLICY STATEMENT

for qualified digital certificates for government authorities

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

Validity: from 12 December 2023
Version: 8.5

CPName: SIGOV-CA

- Policy for Online Qualified Digital Certificates for Employees
  CPOID: 1.3.6.1.4.1.6105.1.1.9
- Policy for online qualified digital certificates for employees with mandatory use of smart cards
  CPOID: 1.3.6.1.4.1.6105.1.2.9
- Policy for specific qualified digital certificates for employees
  CPOID: 1.3.6.1.4.1.6105.1.3.9
- Policy for special qualified digital certificates for employees with mandatory use of smart cards
  CPOID: 1.3.6.1.4.1.6105.1.4.9
- Policy for online qualified digital certificates for employees with generic title
  CPOID: 1.3.6.1.4.1.6105.1.5.9
- Policy for online qualified digital certificates for general title employees with mandatory use of smart cards
  CPOID: 1.3.6.1.4.1.6105.1.6.9
- Policy for specific qualified digital certificates for employees with generic title
  CPOID: 1.3.6.1.4.1.6105.1.7.9
- Policy for specific qualified digital certificates for general title employees with mandatory use of smart cards
  CPOID: 1.3.6.1.4.1.6105.1.8.9
- Policy for online normalised digital certificates for information systems
  CPOID: 1.3.6.1.4.1.6105.1.9.9
- Policy for online normalized certificates for code signature
  CPOID: 1.3.6.1.4.1.6105.1.10.9
- Policy for normalised certificates for issuers of qualified timestamps
  CPOID: 1.3.6.1.4.1.6105.1.11.9
- Policy for normalized digital certificates for certificate validation systems
  CPOID: 1.3.6.1.4.1.6105.1.12.9
- Policy for online qualified digital certificates for website authentication
  CPOID: 1.3.6.1.4.1.6105.1.13.9
- Policy for online qualified electronic seal certificates
  CPOID: 1.3.6.1.4.1.6105.1.14.9
- Policy for online qualified electronic seal certificates with mandatory use of smart cards
  CPOID: 1.3.6.1.4.1.6105.1.15.9

Content

© Trust Service Authority of Slovenia

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 21 1000 Ljubljana
Telephone:	01 4788 330
Web page:	https://www.si-trust.gov.si
Label:	State-institutions

Contact details of SIGOV-CA issuer:

Title:	SIGOV-CA Trust Service Authority of Slovenia Ministry of Digital Transformation Tržaška cesta 21 1000 Ljubljana
Email:	sigov-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, SIGOV-CA issues the following digital certificates:

- special qualified digital certificates for employees of organizations,
- special qualified digital certificates for employees of organizations with mandatory use of smart cards,
- special qualified digital certificates for employees with the general name of the organization or organizational unit,
- special qualified digital certificates for employees with the general name of the organization or organizational unit with the obligatory use of smart cards,
- online qualified digital certificates for employees of organizations,
- Online qualified digital certificates for employees of organizations with mandatory use of smart cards,
- online qualified digital certificates for employees with the general name of the organisation or organizational unit,
- online qualified digital certificates for employees with the general name of an organization or organisational unit with the mandatory use of smart cards,
- online qualified digital certificates for the authentication of websites operated by organisations;
- online qualified digital certificates for electronic seals of organisations;
- online qualified digital certificates for electronic seals of organisations with mandatory use of smart cards;

[1] SIGOV-CA policy, see. 1.3.1
[2] SIGOV-CA policy, see. 1.1, 1.2

© Trust Service Authority of Slovenia

- Online normalised digital certificates for information systems managed by organisations
- Online normalized digital certificates for signing codes for the needs of the organization,
- normalised digital certificates for issuers of qualified timestamps,
- Normalized digital certificates for real-time certificate validation systems.

The designation of this policy is CPName: SIGOV-CA, and the SIGOV-CA policy identifiers vary depending on the type of certificate:

- CPOID: 1.3.6.1.4.1.6105.1.1.9 for online qualified digital certificates for employees,
- CPOID: 1.3.6.1.4.1.6105.1.2.9 for online qualified digital certificates for employees with mandatory use of smart cards,
- CPOID: 1.3.6.1.4.1.6105.1.3.9 for specific qualified digital certificates for employees,
- CPOID: 1.3.6.1.4.1.6105.1.4.9 for specific qualified digital certificates for employees with mandatory use of smart cards,
- CPOID: 1.3.6.1.4.1.6105.1.5.9 for online qualified digital certificates for employees with generic title,
- CPOID: 1.3.6.1.4.1.6105.1.6.9 for online qualified digital certificates for employees with the generic title required to use smart cards,
- CPOID: 1.3.6.1.4.1.6105.1.7.9 for specific qualified digital certificates for employees under the common title,
- CPOID: 1.3.6.1.4.1.6105.1.8.9 for specific qualified digital certificates for employees with the general title required to use smart cards,
- CPOID: 1.3.6.1.4.1.6105.1.9.9 for online normalized certificates for servers,
- CPOID: 1.3.6.1.4.1.6105.1.10.9 for online normalised certificates for code signature,
- CPOID: 1.3.6.1.4.1.6105.1.11.9 for normalised certificates for qualified timestamp issuers (*hereinafter* TSA).*Time Stamp Authority*),
- CPOID: 1.3.6.1.4.1.6105.1.12.9 for normalized digital certificates for certificate validation systems (hereinafter referred to as *OCSP). Online Certificate Status Protocol*),
- CPOID: 1.3.6.1.4.1.6105.1.13.9 for online qualified digital certificates for website authentication,
- CPOID: 1.3.6.1.4.1.6105.1.14.9 for online qualified electronic seal certificates;
- CPOID: 1.3.6.1.4.1.6105.1.15.9 for online qualified electronic seal certificates with mandatory use of smart cards.

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 employed by the organization for whom it seeks certification. In the case of certificates for information systems, code signature, website authentication and electronic seals, the holder of such a certificate is authorised by the head or, in the case of a certificate for the issuer of qualified time stamps and the system for real-time verification of the validity of digital certificates, the head of the organization or the person authorised by the head.

To obtain a certificate, the future holder and head must correctly complete and sign the application for a certificate.

The head of the organization where the future holder of the certificate is employed guarantees the identity of the future holder of the certificate, who verified it in accordance with the current legislation.

The request for obtaining a certificate is approved or, in case of incorrect or incomplete data or non-fulfillment of obligations from the agreement by the organization, is rejected by SI-TRUST authorized persons.

SIGOV-CA shall transmit the smart card, together with the digital certificate and instructions for acting in a

[3] SIGOV-CA policy, see. 4.1, 4.2, 4.3

© Trust Service Authority of Slovenia

secure manner, to the future holder of the digital certificate with the mandatory use of the smart card, no later than ten (10) days from the approval of the request.

SIGOV-CA shall provide the prospective holder of the digital certificate without the obligation to use the smart card with the authorisation code and reference number no later than ten (10) days from the approval of the request.

Certificates are issued exclusively on the SI-TRUST infrastructure.

In the case of an approved request for a certificate with the mandatory use of a SIGOV-CA smart card, the future certificate holder will forward a smart card with a digital certificate to the future certificate holder via the contact person of the organization that applied for the holder's certificate, and the preset password for accessing the digital certificate by mail item marked "Personal" to the address of his organization.

In the case of an approved request for a certificate without the mandatory use of a SIGOV-CA smart card, the SIGOV-CA smart card shall provide the prospective certificate holder with the reference number and the authorisation code through two separate channels: the reference number by e-mail, and the authorisation code by post, and exceptionally the SIGOV-CA authorised person may also hand them over them in person. Both data are needed by the prospective holder to collect the digital certificate.

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 certificate in accordance with SIGOV-CA notifications and recommendations,
- protect the private key and any other confidential data with an appropriate password in accordance with the SIGOV-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 SIGOV-CA notifications.

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

3. Restrictions on use[5]

SIGOV-CA digital certificates (hereinafter referred to as 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.

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 or organisation[6]

[4] SIGOV-CA policy, see. 4.5
[5] SIGOV-CA policy, see. 1.1, 4.5, 5.4.3

© Trust Service Authority of Slovenia

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 certificate in accordance with SIGOV-CA notifications and recommendations,
- protect the private key and any other confidential data with an appropriate password in accordance with the SIGOV-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 SIGOV-CA 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:

- get acquainted with this policy and any agreement between the organization and SI-TRUST before issuing the certificate,
- comply with the policy and provisions of any agreement between the organization and SI-TRUST and other applicable regulations,
- if, after submitting the request for obtaining a certificate or other service, the SIGOV-CA issuer does not receive a notification by e-mail specified in the request, he must contact the authorised persons of the SIGOV-CA issuer,
- after receiving or after receiving the confirmation, check the data in the confirmation and immediately inform SIGOV-CA or request revocation of the certificate in case of any errors or problems,
- monitor and comply with all SIGOV-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 SIGOV-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 SIGOV-CA policy,
- take care of the originally signed documents and the archive of these documents.

The head or organization is obliged:

- carefully read the policy and provisions of the agreement between the organization and SI-TRUST before signing the application for certification,
- ensure that the holders of certificates for its organisation comply with all the requirements of this policy and applicable regulations,
- regularly monitor all SIGOV-CA notifications,
- comply with the notices, policy and agreement between the organization and SI-TRUST and other applicable regulations,
- ensure that certificate holders keep the necessary hardware and software to work securely with certificates up to date;
- take care of the archive of electronic documents and the necessary data for the use of certificates,
- any changes concerning the holder and the organisation related to the holder's certificate should be communicated without delay to SIGOV-CA,
- request revocation of the certificate if the private keys of the certificate holder have been compromised in a way that affects the reliability of use, or if there is a risk of abuse, or if the information provided in the certificate has changed.

The organisation shall be responsible 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,

[6] SIGOV-CA policy, see. 4.5.1, 9.6.3

© Trust Service Authority of Slovenia

- any other damage arising from non-compliance with the provisions of this Policy and other SIGOV-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 register, digitally signed by SIGOV-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 SIGOV-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 contrary to the notifications of the SIGOV-CA issuer, 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 and with the notices of the SIGOV-CA issuer or other applicable regulations,
- the use and reliability of the hardware and software performance of certificate holders.

[7] SIGOV-CA policy, see. 4.9.6, 4.9.7, 4.9.9
[8] SIGOV-CA policy, see. 9.7, 9.8

© Trust Service Authority of Slovenia

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

- for digital certificates with mandatory use of smart cards up to EUR 5,000, and
- for certificates without the obligatory use of smart cards up to EUR 1,000.

7. Policy and applicable law[9]

The source document is SIGOV-CA Qualified Digital Certificates Policy for State Authorities.

The designation of this policy is CPName: SIGOV-CA, and the SIGOV-CA policy identifiers vary depending on the type of certificate:

- CPOID: 1.3.6.1.4.1.6105.1.1.9 for online qualified digital certificates for employees,
- CPOID: 1.3.6.1.4.1.6105.1.2.9 for online qualified digital certificates for employees with mandatory use of smart cards,
- CPOID: 1.3.6.1.4.1.6105.1.3.9 for specific qualified digital certificates for employees,
- CPOID: 1.3.6.1.4.1.6105.1.4.9 for specific qualified digital certificates for employees with mandatory use of smart cards,
- CPOID: 1.3.6.1.4.1.6105.1.5.9 for online qualified digital certificates for employees with generic title,
- CPOID: 1.3.6.1.4.1.6105.1.6.9 for online qualified digital certificates for employees with the generic title required to use smart cards,
- CPOID: 1.3.6.1.4.1.6105.1.7.9 for specific qualified digital certificates for employees under the common title,
- CPOID: 1.3.6.1.4.1.6105.1.8.9 for specific qualified digital certificates for employees with the general title required to use smart cards,
- CPOID: 1.3.6.1.4.1.6105.1.9.9 for online normalized certificates for servers,
- CPOID: 1.3.6.1.4.1.6105.1.10.9 for online normalised certificates for code signature,
- CPOID: 1.3.6.1.4.1.6105.1.11.9 for normalised certificates for qualified timestamp issuers (*hereinafter* TSA).*Time Stamp Authority*),
- CPOID: 1.3.6.1.4.1.6105.1.12.9 for normalized digital certificates for certificate validation systems (hereinafter referred to as *OCSP). Online Certificate Status Protocol*),
- CPOID: 1.3.6.1.4.1.6105.1.13.9 for online qualified digital certificates for website authentication,
- CPOID: 1.3.6.1.4.1.6105.1.14.9 for online qualified electronic seal certificates;
- CPOID: 1.3.6.1.4.1.6105.1.15.9 for online qualified electronic seal certificates with mandatory use of smart cards.

SI-TRUST and SIGOV-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,

[9] SIGOV-CA policy, see. 1.2, 9.14

© Trust Service Authority of Slovenia

- 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 SIGOV-CA issuer on requests for its services or in any mutual agreement or contract, or in appropriate 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 or responsible person of the organisation authorizes SI-TRUST or the SIGOV-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 listed in the certificate, unless certain data are specifically required for the provision of specific services or applications related to certificates, and SI-TRUST has authorized the holder or head of the organization 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 to the organization according to the published price list on the https://www.si-trust.gov.si/sl/digitalna-potrdila/drzavni-organi/ 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

[10] SIGOV-CA policy, see. 9.4
[11] SIGOV-CA policy, see. 5.5.2
[12] SIGOV-CA policy, see. 9.1
[13] SIGOV-CA policy, see. 9.13

© Trust Service Authority of Slovenia

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.

[14] SIGOV-CA policy, see. 9.15, 8

© Trust Service Authority of Slovenia