State Centre for Services of Confidence
A root provider of digital certificates for subsidiaries
and related issuers of qualified digital certificates
SI-TRUST Root

SI-TRUST
SI-TRUST Root

SI-TRUST Root
For root digital certificate issuers for subordinated and related issuers of qualified digital certificates

Public part of the internal rules of the State Trust Service Centre

validity: from 1 October 2019
version: 2.1

CP $_{Name}$: SI-TRUST Root
CP $_{OID}$: 1.3.6.1.4.1.6105.6.1.2

State Centre for Services of Confidence

Policy history

Arrangements for the operation of the SI-TRUST Root	
version: 2.1, valid: from 1 October 2019	
SI-TRUST Rouot for holders of digital certificates for subsidiaries and related issuers of qualified digital certificates CP $_{OID}$: 1.3.6.1.4.1.6105.6.1.2 CP $_{Name}$: SI-TRUST Root	*Revision of the document*
version: 2.0, valid: from 28 May 2018	
SI-TRUST Rouot for holders of digital certificates for subsidiaries and related issuers of qualified digital certificates CP $_{OID}$: 1.3.6.1.4.1.6105.6.1.2 CP $_{Name}$: SI-TRUST Root	*Changes with version 2.0:* • *under the SI-TRUST, under the SI-TRUST, the SI-TRUST has been put in place under the SI-TRUST service provider and the present policy refers to it in specific points.* • *the terms and abbreviations shall be aligned with the applicable legislation.*
version: 1.0, valid: from 23 May 2016	
SI-TRUST Rouot for holders of digital certificates for subsidiaries and related issuers of qualified digital certificates CP $_{OID}$: 1.3.6.1.4.1.6105.6.1.1 CP $_{Name}$: SI-TRUST Root	*//OR*

CONTENT

SUMMARY

Digital certificate and electronic time stamping policies constitute the complete public part of the internal rules of the National Centre for Public Administration Services (hereinafter referred to as the SI-TRUST), which determine the purpose, operation and methodology of the management with a qualified and normalised digital certificate, the allocation of qualified electronic time stamps, the liability of the SI-TRUST and the requirements to be met by users and third parties who use and rely on qualified digital certificates and other trust service providers who wish to use the SI-TRUST service.

The SI-TRUST issues qualified digital certificates and qualified electronic time stamps subject to the highest level of protection and complying 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 (eIDAS; Official Journal of the EU, no. L 257/73), ETSI standards and other applicable regulations and recommendations.

The SI-TRUST also issues normalised digital certificates and special purpose/closed systems. The operating rules of the issuers of such certificates shall be determined by the policy of action of such issuers.

Normalised digital certificates, subject to the SI-TRUST, are intended for:

- certificate issuers, time stamps, OCSP systems, information systems, software signing and registry certificates and in other cases where no qualified certificates can be used,
- to manage, access and exchange information where the use of such certificates is to be made available; and
- the service (s) for which the use of these certificates is required.

Qualified digital certificates issued by the SI-TRUST are intended for:

- the creation of electronic signatures and electronic seal, as well as the authentication of websites;
- to manage, access and exchange information where use of these certificates is envisaged,
- for secure electronic communications between certificate holders, and
- the service (s) for which the use of these certificates is required.

The qualified electronic time stamps SI-TRUST shall be reserved for:

- ensuring the existence of the document at a specified time by linking the date and time of stamping with the contents of the document in a cryptographic secure manner,
- wherever it is necessary to prove the time characteristics of transactions and other services in a secure manner,
- for other needs where a qualified electronic time stamp is required.

Under the SI-TRUST, the root publisher of the digital certificates shall be the SI-TRUST Root. The *Slovenian Trust Service Root Certification Authority*, hereinafter referred to as the *root issuer SI-TRUST Root*, or the *short SI-TRUST Root*. The SI-TRUST Root issues certificates in two volumes, within the SI-TRUST as a root publisher, and in liaising with external issuers as a bridge issuer.

The SI-TRUST's policy provides for internal rules of operation of the root broadcaster defining the purpose, operation and methodology of the management of digital certificates, responsibilities and requirements to be met by all entities.

The present document sets out the policy of the root issuer, the SI-TRUST Root, for subordinates and associated issuers of qualified digital certificates. On the basis of this document, SI-TRUST The issue of digital certificates meeting the highest safety requirements, according to CP $_{OID}$ policy: 1.3.6.1.4.1.6105.6.1.2

This document replaces the previous published policy SI-TRUST Root. All digital certificates issued after the date of validity of the new policy are dealt with under the new policy, and all the other ones are considered to be a new policy for those provisions that can usefully replace or complement the provisions of the policy according to which the digital certificate has been issued (e.g. revocation proceedings apply under the new policy).

As the changes brought about by the new policy do not affect the use or management procedures that can change the level of trust, the policy identifier (CP_{OID}) will not change.

1. INTRODUCTION

1.1. Review

(1) Common provisions are defined in the SI-TRUST.

(2) Under the SI-TRUST, the root publisher of the digital certificates shall be the SI-TRUST Root. The *Slovenian Trust Service Root Certification Authority*, hereinafter referred to as the *root issuer SI-TRUST Root*, or the *short SI-TRUST Root*. The SI-TRUST Root issues certificates in two volumes, within the SI-TRUST as a root publisher, and in liaising with external issuers as a bridge issuer.

(3) The holders of the digital certificates, which are issued by the root broadcaster SI-TRUST Root, are holders of qualified certificates. The root issuer SI-TRUST Root issues:

- issuers under the SI-TRUST certificates for subordinated issuers and unilateral certificates for related issuers;
- When liaising with other issuers (hereinafter the *external issuers*), the liaison certificates shall, as a rule, be bilateral.

(4) The present policy is prepared in line with recommendations on the structure of the document, RFC 3647 " Internet X.509 Public Key Infrastructure Certificate and Certification Practices Framework", and sets out the internal rules of the root issuer SI-TRUST Root defining the purpose, operation and methodology for the management of digital certificates, the responsibility of the SI-TRUST and the requirements to be met by holders of digital certificates from the root issuer, third parties relying on digital certificates, and other entities that use the services of the root issuer in accordance with the regulations.

(5) The interrelationships between entities under this policy may also be regulated by mutual agreement or contract or by other means, as appropriate.

(6) The root issuer SI-TRUST Role with subsidiaries or related issuers operating within the national authorities of the Republic of Slovenia shall enter into mutual agreement and with the other issuers a contract.

1.2. identification data of the operation policy

(1) The present document is the SI-TRUST policy of qualified digital certificates for subordinates and associated issuers of qualified digital certificates (*SI-TRUST Policy*).

(2) The identification mark of the document setting out the policy of performance of the root issuer SI-TRUST Root is: CP_{OID}: 1.3.6.1.4.1.6105.6.1.1, CP_{Name}: SI-TRUST Root.

(3) The digital certificates issued by the root issuer SI-TRUST Root do not include the identification mark referred to in the previous point and shall include:

- in certificates issued to issuers under the SI-TRUST, policy identifier 2.5.29.32.0 ('AnyPolicy').
- in certificates issued to external issuers, a set of policy identification codes to be used in the certificates issued to their end users.

(4) The action identification codes for external issuers linked to the SI-TRUST Root are laid down by mutual agreement or contract.

1.3. PKI participants

1.1.1. Trust service provider

(1) Common provisions are defined in the SI-TRUST.
(2) The contact details of the root issuer are SI-TRUST Root:

Address:	SI-TRUST Root State Centre for Services of Confidence Ministry of Public Administration Tržaška cesta 21 1000 Ljubljana
E-mail:	overitelj@gov.si
Tel:	01 4788 330
Website:	https://www.si-trust.gov.si
Hotline number for cancellations (24 hours total year):	01 4788 777

(3) The root issuer SI-TRUST: carries out the following tasks:

- sets out and publishes its policy of action;
- issue certificates for subordinate issuers and unilateral certificates for related issuers under the SI-TRUST;
- in liaising with external issuers, it issues the interconnection certificates which, as a general rule, are bilateral;
- concerns for a public body of certificates;
- publish a register of cancelled certificates;
- lays down operating rules for subordinate issuers;
- lays down the conditions for the interaction with other issuers;
- to draw up guidelines and recommendations for the safe use of its services;
- ensure the smooth functioning of its services, in line with policy and other regulations; and
- it shall carry out all other services in accordance with that policy, on mutual agreement with other entities and with other regulations in force.

1.1.2. registration Authority

(1) Since the SI-TRUST Root does not issue the digital certificates to end users, the SI-TRUST Root does not have a function in place for the tasks in accordance with the legislation in force.

(2) All of the functions of the Application Service required by RFC 3647 for the root issuer shall be performed by the authorised persons SI-TRUST or administrative board SI-TRUST[1].

(3) The necessary supporting documents and other requirements for issuing the digital certificates are prescribed by the root issuer SI-TRUST Root.

(4) The holders of the holders must comply with the requirements of the applicable legislation and the root issuer of the SI-TRUST, which are determined by mutual agreement/contract.

[1] The meaning is given in the pogs. 5.2 YES/NO.

(5) The responsibility for the establishment and operation of these application services is on the side of the individual issuers.

1.1.3. ~~certificate~~ holders

(1) The holders of the digital certificates, which are issued by the root broadcaster SI-TRUST Root, are qualified certifiers and not end-users of digital certificates.

(2) The root issuer SI-TRUST: issue of digital certificates for:
- subordinated issuers of qualified digital certificates; and
- associated issuers of qualified digital certificates.

(3) The root issuer SI-TRUST Root issues:
- issuers under the SI-TRUST certificates for subordinated issuers and unilateral certificates for related issuers;
- When liaising with other issuers (hereinafter the *external issuers*), the liaison certificates shall, as a rule, be bilateral.

(4) The root broadcaster SI-TRUST Rot with subsidiaries or related external issuers operating within the national authorities of the Republic of Slovenia shall enter into mutual agreement and with the other issuers a contract. The mutual agreement (s) shall define more precisely the responsibilities and procedures.

1.1.4. Third persons

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.5. Other Participants

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.4. Purpose of the use of certificates

(1) The digital certificates, which are issued by SI-TRUST Root or subordinate to the issuer, are designed to carry out a verification of the trust chain for certificates issued by subordinated or connected issuers to end-users.

(2) The use of digital certificates issued by subordinated and related issuers aims to identify subordinated and related issuers in accordance with the applicable legislation in their operations policies.

(3) The purpose of the use of the digital certificates issued by subordinated and related issuers is also set out by mutual agreement between the SI-TRUST and individual external issuers.

(4) The root issuer SI-TRUST Root also issues certificates for the OCSP system for verifying the validity of the certificates issued by the SI-TRUST Root.

1.1.6. Correct use of certificates and keys

(1) The purpose of the certificate (s) is given in the certificate in the *application of the key. Key Usage*), see1.1.150.

(2) In the case of digital certificates issued by the SI-TRUST Root, keys and associated certificates are intended to:

- The private key for signing digital certificates and a registry of cancelled certificates (hereinafter *the signature key*); and
- The public key to authenticate the signature of the digital certificates and the certificate of invalidated certificate (hereinafter *the key for signature verification*).

1.1.7. Unauthorised use of certificates and keys

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.5. Policy management

The details of the governance of the policies for the operation of the root broadcaster SI-TRUST The subordinated and the related issuers shall set them in their operational policies.

1.1.8. Policy Manager

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.9. Contact persons

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.10. Person responsible for the compliance of the issuer's operations with the policy

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.11. Procedure for the adoption of a new policy

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.6. Terms and abbreviations

1.1.12. Terms

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.13. Abbreviations

The provisions are laid down in the Sectoral Policy SI-TRUST.

2. ON NOTICE AND LIABILITY ON THE REPOSITORY

2.1. repositories

The provisions are laid down in the Sectoral Policy SI-TRUST.

2.2. Publication of certificate information

(1) The SI-TRUST makes public the following documents or data from the root provider SI-TRUST Root:
- the policy of the operation of the issuer;
- digital certificates issued,
- register of invalidated digital certificates;
- information on the applicable legislation and other rules governing the operation of the SI-TRUST and
- other information concerning the operation of the SI-TRUST Root.

(2) The digital certificates issued by the SI-TRUST Root are published in the structure of the public directory on the x500.gov.si server (given in more detail below. 7).

(3) Revoked certificates issued by SI-TRUST Root, only this publication is published in the register of invalidated certificates, which is located in the structure of the public directory on the x500.gov.si server and https://www.si-trust.gov.si (given in more detail below). 7.2).

(4) The other documents and key information on the functioning of the root broadcaster SI-TRUST Root and the general notices to the holders and to third parties are published on https://www.si-trust.gov.si.

(5) The confidential part of the internal rules of the SI-TRUST, within which the root broadcaster SI-TRUST Root is working, is not a publicly available document.

(6) Holders of digital certificates must make publicly available the documents laid down in the applicable legislation for the issuers of qualified digital certificates. In the event of the association of issuers established outside the Republic of Slovenia, they are required to publish documents in accordance with the equivalent European/domicile legislation. The root issuer SI-TRUST Rot and the holder may also specify publication requirements by mutual agreement or contract.

(7) The SI-TRUST shall be responsible for the timeliness and credibility of the documents and other data published.

(8) The root broadcaster SI-TRUST Root and the related issuers are responsible for the publication of documents and data in accordance with this policy, the mutual agreement and the applicable law.

2.3. Frequency of public announcements e

The provisions are laid down in the Sectoral Policy SI-TRUST.

2.4. Access to repositories

(1) The publicly available information/documents, digital certificates and the register of invalidated certificates are available in 24ur/7dni/365dni without restrictions.

(2) Each issuer, whether by root or downstream or associated, shall provide and be responsible for appropriate access mechanisms for authorised access to the publication and changes to the publicly available data.

(3) They have been specified in the internal rules of the SI-TRUST, but may also be specified by mutual agreement/contract between the root issuer and the holder.

3. IDENTITY AND AUTHENTICITY

3.1. naming

The root broadcaster SI-TRUST Root and the related issuers shall determine the details of the designation of the entities to which they issue the digital certificates in its operating policy in accordance with the SI-TRUST internal policy and the mutual agreement (if any).

1.1.14. Name (s) of name (s)

Each certificate shall contain, in accordance with recommendation RFC 5280, the holder and the issuer information in the form of a discriminatory name established as *UTF8Stringor* PrintableString according to RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Ref. resolution List (CRL)” and standard X.501.

1.1.15. requirement to make sense of names

(1) The distinguishing name of the holder, contained in the box *holder,* uniquely identifies the subordinate or related issuer (see sub-heading. 1.1.17).

(2) The holder’s distinct name shall be determined in accordance with ETSI standards EN 319412-1, ETSI EN319412-2 and ETSI EN 319412-3. For issuers who started operations before the implementation of the eIDAS, the distinguishing name of the holder may be determined by the SI-TRUST internal policy and any arrangement or contract between them.

1.1.16. Use of anonymous names or pseudonyms

Not foreseen.

1.1.17. rules for the interpretation of names

(1) The root issuer SI-TRUST Root shall be listed in all certificates issued by the root *issuer* in the form of a

distinctive *issuer*. *The* holder of the certificate shall, in the certificate, appear in the form *of* a discriminatory name in *the subject* box.

(2) The distinctive names in the digital certificates for holders shall be determined in accordance with the SI-TRUST internal policy and any arrangement or contract.

1.1.18. uniqueness of names

(1) The distinguishing name granted is unique for each certificate issued.

(2) The Distinguished Name shall be kept alive in the process of renewing the certificate if the holder and the root issuer have not agreed otherwise.

1.1.19. Recognition, credibility and role of trade marks

The provisions are laid down in the Sectoral Policy SI-TRUST.

3.2. initial identity validation

The underlying issuer of the SI-TRUST Root and the related issuers shall determine the details of the initial verification of the identity of their holders, to whom the digital certificates are issued, in their policy of operation in accordance with that policy and any arrangement or agreement between them.

1.1.20. Method for demonstrating private key ownership

(1) The demonstration of the possession of a private key to the public key in the certificate shall be ensured by secure procedures before and at the time of acceptance of the certificate. The certificate request contains a public key and is signed with the associated private key, e.g. in the form of PKCS # 10 according to RSA PKCS # 10 Certification Request Syntax Standard.

(2) The proof of possession of the means for secure storage of private keys and certificates granted by the issuer to the holder is kept in the SI-TRUST Root.

1.1.21. identification of organisations

(1) The prospective holder must provide proof of his identity and his/her identity to the root broadcaster SI-TRUST Root.

(2) The SI-TRUST shall check the information in relevant and accessible registers or, in the case of integration with issuers outside the Republic of Slovenia, also with the relevant other institutions.

(3) The details of the verification process are set out in the SI-TRUST, internal policy of the SI-TRUST and any mutually agreed arrangements.

1.1.22. Identity check

(1) The authorised person of the prospective holder shall submit the documents with the relevant proofs of identity and authorisation to the prospective holder. The root broadcaster SI-TRUST Rot can further verify its identity in the relevant registers or, in case of association with issuers outside the Republic of Slovenia, also with the relevant other institutions.

(2) The details of the procedure and the requirements are prescribed in the internal policy of the SI-TRUST and any mutually agreed arrangements.

1.1.23. non-verified initial verification data

(1) Any data that are not verifiable by the root issuer in the relevant registers or other institutions, or mutually agreed between the SI-TRUST and the holder, are unverified.

(2) The scope of the data is determined by the root issuer of the SI-TRUST, in the internal policy of the SI-TRUST and any mutually agreed arrangements.

1.1.24. Validation of authority

The verification of the power to obtain a digital certificate shall be carried out in the context of an identity verification procedure for a natural person in accordance with pogral. 1.1.22

1.1.25. criteria for interoperation

(1) Related issuers wishing to link public key infrastructure under the root issuer SI-TRUST Root must meet at least the following conditions:

- the issuing authority issues qualified digital certificates in accordance with its policy of action;
- is referred to in the trusted list of trust service providers if it is established in a Member State of the European Union, or is covered by another appropriate system allowing oversight of its operations, in accordance with the requirements of Slovenian and European legislation, if it is established in countries outside the European Union.

(2) In liaising with external issuers, the mode and conditions of the interconnection are determined by mutual agreement/agreement.

(3) The SI-TRUST shall not be obliged to recognise other issuers even if they meet the conditions set out in the first paragraph. The final decision on interconnection shall be taken by the SI-TRUST Administrative Committee.

(4) The SI-TRUST ensures that mutual recognition will be exercised only after signature of a written agreement or agreement with other trust service providers, which must meet a level of safety requirements comparable to or higher than the SI-TRUST, as prescribed by the SI-TRUST.

(5) The SI-TRUST may request the holder from an EU Member State to consult the latest report of conformity assessment in accordance with the IAS/an equivalent external verification report from the rest of the holders.

(6) The costs of the necessary infrastructure required by the SI-TRUST for mutual recognition shall be borne by the other trust service provider.

3.3. Identity and authenticity at the occasion of renewal of the certificate

The root broadcaster SI-TRUST Root and the associated publishers shall determine the details of the renewal process in its policy of operation in accordance with this policy and any arrangement or contract.

1.1.26. Identity and credibility in the event of renewal

Before the private signature key expires, the holder must request the renewal of the certificate in accordance with the procedure for issuing the new digital certificate as at the time of the first acquisition of a digital certificate and initial verification of identity in accordance with the subpoena. 3.2YES/NO.

1.1.27. Identity and authenticity upon renewal after cancellation

(1) The renewal of a digital certificate after cancellation is not possible.

(2) In order to regain a post-revocation digital certificate for subsidiaries and related issuers, the procedure for issuing a new digital certificate shall be carried out as at the time of the first acquisition of a digital certificate and initial verification of identity in accordance with the subpoena. 3.2YES/NO.

3.4. Identity and authenticity at the request of cancellation

(1) The root issuer SI-TRUST shall check the holder's identity and other data in accordance with the procedure laid down in the internal policy of the SI-TRUST, as well as any mutual agreement or agreement.

(2) The root broadcaster SI-TRUST Rouot and its associated publishers shall determine the details of that procedure in its policy of operation in accordance with that policy and any arrangement or agreement between them.

4. MANAGEMENT OF CERTIFICATES

4.1. Application for certificates a

All subordinated and related issuers shall determine the details of the acquisition of the digital certificates in their operations policies in accordance with this policy and any arrangement or contract.

1.1.28. Who can apply for a certificate

(1) The request to obtain the ECS may be submitted to the root broadcaster SI-TRUST Root, either by the issuer or by the prospective issuer, who fulfils the conditions of the related issuers under the policy and the agreement, if any, required by the root issuer of the SI-TRUST Root.

(2) Where the prospective holder is an external issuer, the application to be obtained under the terms and conditions of the mutual agreement shall provide the root issuer with the other documentation proving the

adequacy of its operation.

(3) The SI-TRUST may also refuse to obtain a certificate if the issuer fulfils all the required conditions (see below. 1.1.25).

1.1.29. Enrolment process and responsibilities

(1) If the prospective owner is an external issuer, the SI-TRUST is obliged to conclude a mutual agreement (s).

(2) The format of the written request and the way to apply, as well as the other details, are set out in the SI-TRUST, internal policy of the SI-TRUST and any mutually agreed arrangements.

(3) The holder shall be liable for the veracity of the data and the conduct in accordance with that policy and any mutual agreement or contract.

(4) The details of the procedure for submitting a request for a digital certificate are set out in the internal policy of the SI-TRUST and any mutually agreed arrangements.

4.2. procedure for receipt of an application for a certificate

All subordinated and related issuers shall determine the details of the acquisition of the digital certificates in their operations policies in accordance with this policy and any arrangement or contract.

1.1.30. Identity and authentication process of the prospective holder

see below. 1.1.21 YES/NO.

1.1.31. Approval/rejection of the application

(1) The request to obtain the attestation shall be approved by the SI-TRUST, as the case may be, in accordance with the decision of the SI-TRUST Administrative Committee.

(2) The procedure is described in more detail in the internal policy of the SI-TRUST and any mutually agreed arrangements.

1.1.32. Time to issue the certificate

(1) In order to obtain a digital certificate, the root broadcaster SI-TRUST shall be required to provide an answer to the applicant for approval or rejection of his application no later than thirty (30) days.

(2) The SI-TRUST Root and the prospective holder shall mutually agree on the period for issuing the certificate after all the necessary conditions for its issue have been met.

4.3. Issue of certificate

All subordinated and related issuers shall determine the details of the issue of the digital certificates in their operations policies in accordance with the applicable law and this policy and any mutual agreement or contract.

1.1.33. Issuer's procedure at the time of issue of the certificate

(1) Following the granting and conclusion of a mutual agreement/contract with an external issuer, the root issuer SI-TRUST Rot shall issue a digital certificate on the basis of the application in accordance with the subpoena. 3.2YES/NO.

(2) Issued an SI-TRUST digital certificate, published both in a public directory and on websites (see below. 1.1.36).

(3) Details of the issue procedure are set out in the internal policy of the SI-TRUST and any mutually agreed arrangements.

1.1.34. notification by the holder of the issuing of a certificate

(1) The root issuer SI-TRUST Rot shall inform the prospective holder of the issue and the details of the acquisition of the digital certificate.

(2) The SI-TRUST to the holder sends the digital certificate to the holder in the manner set out in the internal policy of the SI-TRUST and any mutual agreement or agreement.

4.4. Certificate acceptance

All subordinated and related issuers shall determine the details of the acquisition of the digital certificates in their operations policies in accordance with this policy and any arrangement or contract.

1.1.35. Certificate acceptance procedure

(1) The details of the acceptance procedure shall be determined by the root issuer of the SI-TRUST Root and shall inform the prospective holder in an agreed manner.

(2) The holder shall be responsible for verifying the data in this certificate as soon as the certificate has been accepted. If the root issuer SI-TRUST he is not informed of any errors, it is considered to be in agreement with the content and the conditions for possession and use.

1.1.36. publication of the certificate

The issued certificate shall be made publicly available, in advance, in the SI-TRUST, as indicated in the Cap0.

1.1.37. notice of issue to third parties

Unspecified.

4.5. Use of certificates and keys

1.1.38. Use of the certificate and private key of the holder

(1) The holder of the certificate shall be obliged, with regard to private key security, to:

- use private key protection equipment that meets globally accepted security and technical standards and must meet at least one of the conditions specified in ETSI Standard EN 319 411-1 (see below). 6.2),
- use software that is certified in accordance with the Common Criteria to at least EAL4 + or has been designed in accordance with ETSI Standard EN 319 401 (see below). 6.6),
- protect private keys and any other confidential information with a suitable password in line with the recommendations of the SI-TRUST and by other means such as to prevent unauthorised access to it,
- carefully protect passwords to protect private keys;
- upon expiry of the certificate, the certificate shall be handled in accordance with the SI-TRUST, as notified by the issuer.

(2) The holder must protect the private key for signing data against unauthorised use.

(3) Other duties and responsibilities are laid down in the sub-area. 1.1.182YES/NO.

1.1.39. use of the certificate and public key for third parties

The provisions are laid down in the Sectoral Policy SI-TRUST.

4.6. Re-certification of the certificate without changes in public key

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.40. Grounds for re-certification

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.41. Who may request a reissue

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.42. Procedure for re-issuing the certificate

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.43. notification to the holder of the issue of a new certificate

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.44. Acceptance of a re-certificate

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.45. Publication of a re-certificate

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.46. Issue notice to other entities

The provisions are laid down in the Sectoral Policy SI-TRUST.

4.7. Renewal of certificate

1.1.47. Circumstances for certificate re-key

(1) The renewal of the certificate shall take place with a view to the expiry of the certificate issued to the holder by the SI-TRUST Root. The holder shall then issue a new certificate with the same information about the holder.

(2) As a general rule, the procedure takes place before the date of expiry of the certificate (see below for the validity of keys.)1.1.140.

1.1.48. Who can ask for a renewal of the certificate

The renewal is requested by the holder or by an authorised person.

1.1.49. Procedure for renewal of certificate

The procedure is the same as for the first issue of the certificate, see below. 4.3

1.1.50. Notification to the holder of renewal of a certificate

The procedure is the same as for the first issue of the certificate, see below. 1.1.34YES/NO.

1.1.51. Acceptance of a renewed certificate

The procedure is the same as for the first acquisition of the certificate, see below. 4.4YES/NO.

1.1.52. Publication of a renewed certificate

The procedure is the same as for the first acquisition of the certificate, see below. 1.1.36YES/NO.

1.1.53. Issue notice to other entities

The procedure is the same as for the first acquisition of the certificate, see below. 1.1.37YES/NO.

4.8. Certificate modification

(1) If there is a change in the holder's policy that affects the confidence in the validity of the holder's certificate (s), the certificate must be cancelled.

(2) In order to obtain a new certificate, it is necessary to repeat the procedure as indicated in the sub-heading. 4YES/NO. The service provider of an issuer for a change of certificates shall not be supported.

1.1.54. Grounds for the change of certificate

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.55. Who can request a change

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.56. Procedure at the time of the amendment of the certificate

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.57. Notification to the holder of the issue of a new certificate

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.58. Acceptance of the amended certificate

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.59. Publication of the amended certificate

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.60. Issue notice to other entities

The provisions are laid down in the Sectoral Policy SI-TRUST.

4.9. Certificate revocation and suspension[2]Reasons for cancellation

(1) Revocation may be required in case of disclosure of the key or other reasons affecting the level of trust and reliability of the private key.

(2) Other reasons for a revocation may be:
- failure to comply with the conditions or requirements imposed on the holders of such a policy or of any mutual agreement or agreement,
- suspension of activities of the root broadcaster SI-TRUST Root, suspension of certification or prohibition of management of certificates,
- the termination of activities of a subordinated or related issuer;
- the takeover by the other trust service provider of the activities of the root issuer, the SI-TRUST,
- order of the competent court or administrative authority.

(3) The root issuer SI-TRUST Root shall also withdraw the certificate without the holder's request immediately after becoming aware of:
- that the information contained in the certificate is incorrect or the certificate has been issued on the basis of incorrect information,
- other circumstances affecting the validity of the certificate have changed;
- in the event of failure by the holder to comply with the holder's obligations under that policy and any mutual agreement or agreement,
- that the costs for the management of the digital certificates have not been settled,
- the SI-TRUST infrastructure has been threatened in a way that affects the reliability of the certificate,
- that the private key of the certificate holder has been compromised in a manner that affects the reliability of use;
- the SI-TRUST Root has ceased to be subject to certification or that the SI-TRUST prohibited management of certificates and its activities has not been taken over by another trust service provider,
- revocation ordered a competent court or administrative authority.

1.1.62. Who may request cancellation

(1) Common provisions are defined in the SI-TRUST.

(2) The root issuer SI-TRUST Root reserves the right to cancel an issued digital certificate in case of non-compliance for subordinated and related issuers.

1.1.63. Cancellation procedure

(1) In the event that the revocation is requested by the holder, the procedure is set out in the internal policy of the SI-TRUST and any mutual agreement or agreement.

(2) The revocation of the SI-TRUST Root issuer informs the holder and the other entities that may be affected by the revocation of the digital certificate (i.e. third parties or other entities relying on the digital certificate).

(3) The decision to revoke the certificate shall be taken by the SI-TRUST Administrative Committee no later than sixteen (16) hours from receipt of the request of cancellation in case of cancellation due to the risk of misuse or

[2] According to the recommendation of RFC 3647, this subchapter also includes a suspension procedure, which is not facilitated by the SI-TRUST.

unreliability, etc., or otherwise on the first working day following receipt of the request for cancellation.

(4) If the revocation is ordered by a court or administrative authority, this shall be done in accordance with the applicable procedures.

(5) Following the revocation, the holder shall be informed of the date and time of the revocation, the issuer of the cancellation request and the reasons for the revocation.

1.1.64. Time to issue cancellation request

The cancellation request should be requested without delay in the case of the possibility of misuse or unreliability.

1.1.65. Time spent on cancellation request received until revocation

(1) The SI-TRUST root issuer shall withdraw the SI-TRUST, following the decision of the SI-TRUST, the certificate no later than four (4) hours in the case of cancellation due to the risk of misuse or unreliability, etc., or, failing that, on the first working day following the decision of the SI-TRUST Administrative Committee.

(2) If the operation of the SI-TRUST is, due to unforeseen events, substantially reduced, the cancellation is carried out at the latest within 24 (24) hours of the decision of the SI-TRUST, at the latest within 24 hours of the decision of the SI-TRUST Administrative Committee.

(3) Following revocation, the certificate shall be immediately added to the register of cancelled certificates and to be deleted from the public register of certificates, in which only the record data of the certificate remain.

1.1.66. requirements for verification of the register of certificates for third parties withdrawn

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.67. frequency of publication of the certificate withdrawn

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.68. time until the date of publication of the register of certificates cancelled

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.69. Verification of the status of certificates

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.70. Requirements for continuous verification of the status of certificates

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.71. Other means of access to certificate status

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.72. Other requirements for private key abuse

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.73. Grounds for suspension

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.74. Who may request the suspension

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.75. Procedure for the suspension

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.76. Time of suspension

The provisions are laid down in the Sectoral Policy SI-TRUST.

4.10. Verification of the status of certificates

1.1.77. Access for verification

The register of invalidated certificates is published in a public directory on *the* server x500.gov.si and on https://www.si-trust.gov.si/sl/podpora-uporabnikom/korenski-izdajatelj-si-trust-root/, on-line verification of the status of the certificate is available at http://ocsp.ca.gov.si, and the access details are in the sub-set. 7.2And7.3.

1.1.78. Availability

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.79. Other options

The provisions are laid down in the Sectoral Policy SI-TRUST.

4.11. Termination of the relationship between the trust service holder and the trust service provider

(1) The provisions on the suspension of the relationship between an external issuer and the root issuer are laid down by mutual agreement.

(2) The relationship between an external issuer with the root issuer and the SI-TRUST Root shall be suspended if

- the holder's certificate shall expire and it shall not require it to be renewed,
- the certificate is cancelled and the holder does not request a new one.

4.12. detection of a copy of the decryption keys

Not supported.

1.1.80. Procedure for detection of decryption keys

Not supported.

1.1.81. Procedure for the detection of the meeting key

The provisions are laid down in the Sectoral Policy SI-TRUST.

5. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

5.1. Physical security

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.82. Location and structure of the trust service provider

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.83. Physical access to the infrastructure of the trust service provider

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.84. Power and air conditioning

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.85. Water exposures

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.86. Fire prevention and protection

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.87. media management

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.88. Disposal

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.89. Off-site backup

The provisions are laid down in the Sectoral Policy SI-TRUST.

5.2. organisational structure of the issuer/trust service provider

1.1.90. Organisation of a trust and trusted service provider

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.91. Number of persons required per task

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.92. Identity of individual applications

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.93. Roles requiring separation of duties

The provisions are laid down in the Sectoral Policy SI-TRUST.

5.3. Personnel controls

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.94. Qualifications, experience and clearance requirements

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.95. Background check procedures

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.96. Staff training

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.97. Training requirements

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.98. Job rotation frequency and sequence

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.99. Sanctions

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.100. Independent contractor requirements

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.101. Documentation supplied to personnel

The provisions are laid down in the Sectoral Policy SI-TRUST.

5.4. System security checks

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.102. Type of event (s)

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.103. Frequency of processing log

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.104. Retention period for audit log

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.105. Protection of audit log

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.106. Audit log backup procedures

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.107. Data collection for audit logs

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.108. notification to event-causing subject

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.109. Assessment of system vulnerabilities

The provisions are laid down in the Sectoral Policy SI-TRUST.

5.5. retention of information

1.1.110. Types of record archived

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.111. Retention period

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.112. Protection of archive

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.113. System archive and storage

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.114. Requirement of time stamping

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.115. Data collection how archived data can be collected

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.116. Procedure for access to, and verification of, archived data

The provisions are laid down in the Sectoral Policy SI-TRUST.

5.6. Renewal of the issuer's certificate

(1) The renewal and the process of transmission of the new digital certificate will be brought to the attention of the holders and other participants in a timely manner.

(2) The associated and subordinate issuers shall determine the renewal of their certificate through their policy of action.

5.7. Compromise and disaster recovery

1.1.117. Incident and compromise handling

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.118. Procedure in the event of a breakdown of hardware and software or data

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.119. Entity private key compromise procedures

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.120. Compromise and disaster recovery

The provisions are laid down in the Sectoral Policy SI-TRUST.

5.8. Extinction of the issuer

The provisions are laid down in the Sectoral Policy SI-TRUST.

6. TECHNICAL SAFETY REQUIREMENTS

6.1. Key generation and positioning

1.1.121. Key generation

(1) The generating of the key issuer, SI-TRUST Root, for signature, and authentication shall be the formal and controlled procedure at the installation of the SI-TRUST Root software, on which a separate record is kept (document 'Minutes of the process of generating SI-TRUST'). The minutes of the procedure shall ensure the completeness and the audit trail of the procedure, and shall be carried out according to detailed instructions.

(2) The minutes of the procedure shall be kept securely.

(3) Any subsequent amendments in the authorisations or relevant changes to the settings of the SI-TRUST's IT system, which are carried out when the system is set up, shall be documented in a separate record, or in the relevant journal.

(4) The root issuer pair of the root issuer pair of SI-TRUST Role shall be used for the machine security module (see below). 1.1.128).

(5) Holders of a key pair shall be generated from the holder as expected in the machine security module (see below). 1.1.128).

1.1.122. Delivery of private key to holders

The holders of the private key are generated from the holder and are not transferred.

1.1.123. Delivery of the certificate to the issuer of the certificates

The holder in the take-over process shall deliver its public key to the signature of the root broadcaster, the SI-TRUST, in the manner set out in the operation policy of the SI-TRUST and any mutually agreed arrangements.

1.1.124. Delivery of the issuer's public key to third parties

The SI-TRUST's public key certificate certificate shall be published in the SI-TRUST (see Sub-Annex). 2).

1.1.125. Key length

The key length of the SI-TRUST root issuer key and the minimal maximum length of keys for the holders are given in the table below.

entity	RSA key length [bit]
The root issuer SI-TRUST Root	3072
Sub-issuer (ies)	minimum 2048
OCSP system	2048

1.1.126. Generating and quality of public key parameters

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.127. Key purpose and certificates

The provisions are laid down in the Sectoral Policy SI-TRUST.

6.2. Private key protection and security modules

1.1.128. Cryptographic module standards

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.129. Private key control by authorised persons

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.130. Detecting a copy of the private key

Not supported.

1.1.131. backup of private keys

(1) The root issuer SI-TRUST Rot provides a backup of its private key. Details are set out in the SI-TRUST internal policy.

(2) The holder must provide a backup for his private key.

1.1.132. Private key archiving

Not supported.

1.1.133. Transfer of private key from/to cryptographic module

(1) Common provisions are defined in the SI-TRUST.

(2) If the Machine Security Module of the holder allows the transfer of the private key from/to module, the transfer must take place in encrypted form.

1.1.134. Private key record in a cryptographic module

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.135. Procedure for the activation of the private key

(1) Common provisions are defined in the SI-TRUST.

(2) Holders must ensure the safe activation of their private key.

1.1.136. Procedure for deactivation of the private key

(1) Common provisions are defined in the SI-TRUST.

(2) Holders are required to use such software which deactivate the issuer's private key when the issuer stops operating.

1.1.137. Procedure for the destruction of the private key

(1) Common provisions are defined in the SI-TRUST.

(2) The destruction of private keys on the part of holders is within their competence.

1.1.138. Cryptographic module characteristics

The provisions are laid down in the Sectoral Policy SI-TRUST.

6.3. Key Management Aspects

1.1.139. Preservation of public key

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.140. Certificate and series validity period

(1) The validity of the digital certificates issued to issuers under the SI-TRUST by the root issuer SI-TRUST:

- for subordinate issuers: twenty (20) years or until the root date of the SI-TRUST root period has elapsed,

- for unilaterally connected issuers: until the end of validity of the underlying certificate of the related issuer, i.e. until the validity of the IS-TRUST root has expired.

(2) The validity of the digital certificates in liaising with outside issuers shall be valid until the validity of the underlying certificate of the related issuer, or until the validity of the SI-TRUST root has expired.

(3) The outer issuer and the SI-TRUST Role may also agree for a different period of validity by mutual agreement/agreement.

(4) The validity of the key issuer key is SI-TRUST Rot is up to 19.01.2038.

(5) The validity of keys and certificates for the OCSP system shall be three (3) years.

6.4. Access passwords

1.1.141. Password generation

The authorised person (s) of the CSD shall use the strong passwords in the private key of the SI-TRUST to act in accordance with the SI-TRUST policy.

1.1.142. Password protection

The passwords of the authorised person (s) of the root issuer SI-TRUST Root for access to the private key of the root issuer SI-TRUST Root shall be stored in accordance with the SI-TRUST policy.

1.1.143. Other aspects of passwords

Not prescribed.

6.5. Safety requirements for issuing computer equipment by the issuer

1.1.144. Specific technical safety requirements

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.145. level of security protection

The provisions are laid down in the Sectoral Policy SI-TRUST.

6.6. Issuer's life cycle technical control

1.1.146. Control of the evolution of the system

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.147. Managing safety

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.148. Life cycle control

The provisions are laid down in the Sectoral Policy SI-TRUST.

6.7. Network security controls

(1) The system of SI-TRUST Root is inactive for most of the time and is activated only occasionally for the purpose of issuing an individual digital certificate or a list of invalidated certificates. In the course of the operation, only the network protocols which are strictly necessary to connect the system to the hardware security module and the LDAP register in the internal network segment are isolated from the rest of the network.

(2) This is specified in detail in the SI-TRUST, in accordance with the legislation in force.

6.8. Time-stamping

The provisions are laid down in the Sectoral Policy SI-TRUST.

7. CERTIFICATE PROFILE, CERTIFICATE WITHDRAWN AND ONGOING VERIFICATION OF CERTIFICATE STATUS

7.1. Certificate Profile

1.1.149. Certificate version

The digital certificates issued by the root issuer SI-TRUST and also subordinated and connected issuers follow standard *X.509*, version 3, according to RFC 5280.

1.1.150. profile of extensions

1.1.150.1. Profile of the SI-TRUST session certificate

The profile of the SI-TRUST certificate is presented in a sub-heading. **Napaka! Vira sklicevanja ni bilo mogoče najti.**YES/NO.

1.1.150.2. Certificate profile for subsidiaries and related issuers

Field names	Value or importance
Certificate (s) of the underlying (s) in the certificate	

Version \ "_blank" *Version*	3
Identification, \ "_blank" *Serial Number*	*unique internal number of the approved integer number (32 bit entropohiae)*
Signature algorithm, \ "_blank" *Algorithms*	sh256WithandeEncrConsumption (OID 1.2.840.113549.1.1.11)
Issuing body, \ "_blank" *Issuer*	c = SI, o = the Republic of Slovenia, oi = VAT-17659957, CN = SI-TRUST
The period of validity, \ "_blank" *Disability*	Not Before: <*Entry into force post-GMT* > Not After: <*End of validity after GMT* > *In format*< LLMMDUDummssZ >
Holder, \ "_blank" *Subject*	*Discriminatory name of the subsidiary or associated issuer (see below3.1), in a form suitable for printing*
Public Key Algorithm, \ "_blank" *Subject Public Key Algorithm*	vacuum Consumption (OID 1.2.840.113549.1.1.1)
Holders of a public key belonging to an appropriate key pair coded using the RSA algorithm. *RSA Public Key*	*key length min. 2048 bits*
Extensions of X.509v3	
The publication of a register of cancelled certificates, OID 2.5.29.31, \ "_blank" *CRL Distribution Points*	URI: http://www.ca.gov.si/crl/si-trust-root.crl URL: ldap://x500.gov.si/cn=SI-TRUST%20Root,oi=VATSI-17659957,o=Republika%20Slovenija,c=SI?certificateRevocationList c = SI, o = the Republic of Slovenia, OID = VAT-17659957, CN = SI-TRUST Root, CN = CRL < serial *number of the register* >
Key Usage, OID 2.5.29.15, \ *"_blank" Key Usage*	Critical) Signature of Certificates (keyCertSign), CRL signature (cRLSign)
Key of the issuer key; OID 2.5.29.35, \ "_blank" *Authority Key Identifier*	*authority Key Identifier*
The identifier of the holder's key; OID 2.5. *29.14,* \ *"_blank" Subject Key Identifier*	*subject Key Identifier*
Basic restrictions, OID 2.5.29.19, \ "_blank" *Basic Constrants*	Critical) CA: TRUE No length limitation Constraint: None)

The policy under which the certificate was issued, OID 2.5.29.32, certificatePolicies	Certificates issued to issuers under the SI-TRUST: Certificate Policy: PolicyIdentifier = 2.5.29.32.0 (anyPolicy) [1,1] Policy qualificer Info: policy qualificer Id = CPS qualificer: http://www.ca.gov.si/cps/ In certificates issued to external issuers: Certificate Policy: PolicyIdentifier = the *range of policy identification codes to be used in the certificates issued to end-users* [1,1] Policy qualificer Info: policy qualificer Id = CPS qualificer: http://www.ca.gov.si/cps/
Access to information on the issuer, OID 1.3.6.1.5.5.7.1.1, \ "_blank" *Authority Information Access*	Access Method: OCSP (OID 1.3.6.1.5.5.7.48.1) Access Location: URL = http://ocsp.ca.gov.si Access Method: CaIssuer (OID 1.3.6.1.5.5.7.48.2) Access Location: URL = http://www.ca.gov.si/crt/si-trust-root.crt
Certificate footprint (not part of the certificate)	
SHA-1 certificate footprint, \ "_blank" *Certificate Fingerprint — SHA-1*	*recognisable print of the certificate after SHA-1*
SHA-256 certificate footprint, \ "_blank" *Certificate Fingerprint — SHA-256*	*recognisable print of the certificate after SHA-256*

(1) Fields marked as *Critical* in certificates are:
- key Usage *Key Usage*), and
- basic constraints *Basic Constrants*).

(2) In the 'basic limits' field. The *Basic* Constrants) the setting of "path length limits" is also determined. *Pathh Length Constraint*), the value of which is 'not'.

(3) The digital certificate profiles issued by subordinated and related issuers are set out in their operational policies.

1.1.151. Algorithm identification markings

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.152. Name (s) of name (s)

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.153. Restriction on names

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.154. Certificate policy code

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.155. Use of expansion field to limit policy use

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.156. format and treatment of specific policy information

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.157. Consideration of a critical enlargement policy field

The provisions are laid down in the Sectoral Policy SI-TRUST.

7.2. register of invalidated certificates

1.1.158. Version

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.159. content of the register and extensions

(1) The register of certificates cancelled in addition to other data required in accordance with Recommendation *X.509* contains (basic fields and extensions are shown in more detail in the table below):

- validated certificate identification marks; and
- time and date of withdrawal.

Field name	Value or importance
Basic fields in CRL	
Version \ "_blank" *Version*	2
Issuer signature, \ "_blank" *His/her/his/her/his/her/*	P *issuer write-down*
The distinguishing name of the issuer; \ "_blank" *Issuer*	c = SI, o = the Republic of Slovenia, oi = VAT-17659957, cn = SI-TRUST Root
Time of issue of the CRL, thisUpdate	Last Update: *time of issue after GMT*
Time of issue for the next CRL, NextUpdate	Next Update: *time of subsequent issue after GMT*
Identity identifiers withdrawn and revocation time, vokedCertificate	Serial Number: <*ID of cancelled dig certificates* > Revoation Date: <*Time of revocation after GMT* >
Signature algorithm, \ "_blank" *Signature Algorthm*	sh256WithRSAEncrConsumption
Extensions of X.509v2 CRL	

Key of the issuer key; \ "_blank" *Authority Key Identifier* *(OID 2.5.29.35)*	*authority Key Identifier*
Individual Register Number (CRL1, CRL2,....), \ "_blank" *CRLnumber* *(OID 2.5.29.20)*	*individual Register serial number*
Issuer's alternative name Issues erAltName *(OID 2.5.28.18)*	*not used*
List of changes DeltaCRLindicator (*OID 2.5.29.27)*	*not used*
Publication of the list of amendments issuingDistributionPoint *(OID 2.5.29.28)*	*not used*

(2) Invalidated digital certificates, the validity of which has expired, remain published in the register of invalidated certificates.

(3) Fields in the CRL are not considered critical.

(4) The register of invalidated digital certificates is made publicly available in the repository (see below. 2).

(5) The publisher publishes both the individual registers and the full register (in one place).

7.3. Confirmation of confirmation of the status of certificates on an up-to-date basis

(1) On-line validation of the status of digital certificates is available at http://ocsp.ca.gov.si.

(2) The OCSP message profile (request/response) for continuous verification of the status of certificates is in line with RFC 2560 recommendation.

1.1.160. Version

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.161. extensions to ongoing status check

The provisions are laid down in the Sectoral Policy SI-TRUST.

8. INSPECTION

8.1. Inspection frequency

The provisions are laid down in the Sectoral Policy SI-TRUST.

8.2. technical inspection body

The provisions are laid down in the Sectoral Policy SI-TRUST.

8.3. independence of the inspection service

The provisions are laid down in the Sectoral Policy SI-TRUST.

8.4. Areas of inspection

The provisions are laid down in the Sectoral Policy SI-TRUST.

8.5. actions of the trust service provider

The provisions are laid down in the Sectoral Policy SI-TRUST.

8.6. Publication of inspection results

The provisions are laid down in the Sectoral Policy SI-TRUST.

9. OTHER BUSINESS AND LEGAL AFFAIRS

9.1. Fee schedule

1.1.162. Issuance price and renewal of certificates

The issuing and renewal price of the certificates issued by the root issuer to the SI-TRUST Root shall be issued by mutual agreement (s).

1.1.163. Access price for certificates

(1) The access to the list of digital certificates issued by the root issuer of the SI-TRUST Root is free of charge.

(2) Since that policy requires access to the public for the purposes of directories of the digital certificates managed by subordinate and associated issuers, they do not levy such access.

1.1.164. Access price of the certificate and a register of cancelled certificates

(1) Access to the certificate status and to the repository of invalidated digital certificates of the root issuer SI-TRUST Root is free of charge.

(2) Since this policy requires the public to have access to the status of the certificate and to the revoked

certificate also for subsidiaries and related issuers, they do not levy these services.

1.1.165. Prices of other services

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.166. Reimbursement of expenses

The provisions are laid down in the Sectoral Policy SI-TRUST.

9.2. Financial responsibility

1.1.167. Insurance coverage

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.168. Other cover

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.169. Holders' insurance

The provisions are laid down in the Sectoral Policy SI-TRUST.

9.3. Protection of commercial information

1.1.170. Protected data

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.171. Non-safeguarded data

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.172. Liability with regard to the protection of commercial information

The provisions are laid down in the Sectoral Policy SI-TRUST.

9.4. Protection of personal data

1.1.173. Privacy plan

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.174. Protected personal data

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.175. Personal data not protected

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.176. Responsibility for the protection of personal data

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.177. Power of attorney concerning the use of personal data

Unspecified.

1.1.178. Transfer of personal data to official request

The root issuer SI-TRUST Root shall not transfer personal data, except at the request of the competent court or administrative authority.

1.1.179. Other provisions concerning the transfer of personal data

Not prescribed.

9.5. Provisions concerning intellectual property rights

The provisions are laid down in the Sectoral Policy SI-TRUST.

9.6. Liability and accountability

1.1.180. Obligations and responsibilities of the issuer

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.181. Obligations and responsibilities of the application service

(1) The root issuer SI-TRUST Root does not have a registration service in place.

(2) The SI-TRUST Administrative Committee shall be responsible for the adequacy of the identification procedures and the accuracy of the data contained in the requests.

1.1.182. Holder's obligations and responsibilities

(1) The holder or prospective holder of the certificate shall be obliged:

- take note of this policy prior to issuing the Certificate,
- comply with this policy and determine the arrangements for mutual agreement between the parties and the other rules in force,
- upon receipt of a certificate or after acceptance of the certificate, check the information in the certificate and, if faults or any problems have occurred, immediately notify the SI-TRUST Root, or ask for the certificate to be cancelled,
- monitor and comply with the notifications of the SI-TRUST and comply with them,
- all changes linked to the certificate shall be notified immediately to the SI-TRUST Root,
- require revocation of the certificate where the private key has been compromised in a manner that affects the reliability of use or where there is a risk of abuse,
- to use the certificate solely for the purpose laid down by that policy and any mutual agreement or contract,
- provide the original signed documents and archive of these documents.

(2) The following requirements shall apply to the holder of the certificate:

- The subordinated issuer may not liaise with other issuers;
- the associated issuer shall not be associated with each other with other related issuers; subject to prior assessment and approval by the SI-TRUST Root, it may exceptionally be associated with external issuers, provided that the integrity of the interconnected system is not compromised.

(3) In the event of a breach of the integration conditions referred to in the preceding paragraph, the SI-TRUST may immediately terminate the link to the subordinated issuer (s).

(4) Each issuer that crosses the SI-TRUST Root retains all responsibilities in relation to the issue of digital certificates for its holders.

(5) The holder shall be held liable for:

- the damage suffered in the event of misuse of the certificate from the notification of the cancellation of the certificate to the revocation,
- any damage caused, either directly or indirectly, because it has been made possible to use or misuse the certificate by unauthorised persons,
- any other damage resulting from non-compliance with the provisions of this policy and other notifications from the root issuer SI-TRUST Root and the applicable regulations.

1.1.183. obligations and responsibilities of third parties

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.184. Obligations and responsibilities of other entities

The provisions are laid down in the Sectoral Policy SI-TRUST.

9.7. Contestation of liability

The provisions are laid down in the Sectoral Policy SI-TRUST.

9.8. Limits of liability

The root issuer SI-TRUST and SI-TRUST shall not be held liable for individual transactions entered into on the basis of certificates issued by subordinated and related issuers.

9.9. Redress

The provisions are laid down in the Sectoral Policy SI-TRUST.

9.10. policy validity

1.1.185. Duration

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.186. End of the policy period

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.187. Effect of the policy expiry

The provisions are laid down in the Sectoral Policy SI-TRUST.

9.11. Communication between entities

The provisions are laid down in the Sectoral Policy SI-TRUST.

9.12. amendment of a document

1.1.188. Procedure for the application of amendments

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.189. Validity and publication of amendments

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.190. Change of the policy identification code

The provisions are laid down in the Sectoral Policy SI-TRUST.

9.13. procedure in case of disputes

The provisions are laid down in the Sectoral Policy SI-TRUST.

9.14. applicable legislation

The provisions are laid down in the Sectoral Policy SI-TRUST.

9.15. compliance with applicable law

The provisions are laid down in the Sectoral Policy SI-TRUST.

9.16. General provisions

1.1.191. Comprehensive deal

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.192. Assignment of rights

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.193. Independence identified by

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.194. Receivables

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.195. Force majeure

The provisions are laid down in the Sectoral Policy SI-TRUST.

9.17. Miscellaneous provisions

1.1.196. Understanding

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.197. Conflicting provisions

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.198. Derogation from the provisions of

The provisions are laid down in the Sectoral Policy SI-TRUST.

1.1.199. Cross verification

The provisions are laid down in the Sectoral Policy SI-TRUST.