State Centre for Services of Confidence

SI-TRUST
Državni center za storitve zaupanja

OVERARCHING POLICY — SI-TRUST for issuers operating under the SI-TRUST service provider

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

validity: from 1 October 2019
version: 1.1

CP$_{\text{Name}}$: SI-TRUST
CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.8.1.1

State Centre for Services of Confidence

Policy history

Overarching policy issues SI-TRUST	
version: 1.1, valid: from 1 October 2019	
holding policy — SI-TRUST for issuers operating within the SI-TRUST provider of trust services CPID: 1.3.6.1.4.1.6105.8.1.1 CPName: SI-TRUST	*Revision of the document*
version: 1.0, valid: from 28 May 2018	
Holding policy — SI-TRUST for issuers operating within the SI-TRUST provider of trust services CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.8.1.1 CP $_{\text{Name}}$: SI-TRUST	*//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.

They shall determine the details of their performance by individual issuers in their policy of operation.

This document replaces the previous published overarching policy — SI-TRUST. 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 $_{\text{OID}}$) will not change.

1. INTRODUCTION

1.1. *Review*

(1) The National Centre for Services of Confidence (hereinafter the SI-TRUST) operates under the Ministry of Public Administration (hereinafter referred to as the *MPA*).

(2) The trust service provider's policies shall constitute the complete public part of the internal rules of the SI-TRUST and 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 holders, users and third parties relying on qualified and normalised digital certificates and other trust service providers who wish to use the SI-TRUST service.

(3) 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.

(4) 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.

(5) 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.

(6) 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.

(7) 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.

(8) They shall determine the details of their performance by individual issuers in their policy of operation.

1.2. *identification data of the operation policy*

The provisions are defined in each policy.

1.3. PKI participants

1.1.1. Trust service provider

(1) The National Trust Service Centre issues digital certificates and qualified electronic time stamps, subject to the highest level of security and operating in accordance with the rules and recommendations in force.

(2) The contact details of the National Centre for Trust Services are:

Address:	Republic of Slovenia State Centre for Services of Confidence Ministry of Public Administration Tržaška cesta 21 1000 Ljubljana
Tel:	01 4788 330
Website:	https://www.si-trust.gov.si
Code:	State institutions

(3) The tasks of managing the State Centre for Services of Confidence shall be carried out by the SI-TRUST Administrative Board (see infra). 5.2).

(4) The SI-TRUST is carried out under the SI-TRUST Root and other certifiers.

(5) The contact details of the individual issuer are indicated in the associated policy.

(6) The tasks performed by an individual issuer are listed in its policy of action.

(7) At the start of its production operations, the root broadcaster SI-TRUST has formed, at the start of its production operations, its own digital certificate, which is intended to certify the certificates validated by the SI-TRUST Root, and related issuers of qualified digital certificates.

The SI-TRUST statement shall contain the following information[1]:

Field names	Value or importance
Certificate (s) of the underlying (s) in the certificate	
Version \ "_blank" *Version*	3
Certificate identification code, \ "_blank" *Serial Number*	90AE 7776 0000 0000 571D D06F
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
Holder, \ "_blank" *Subject*	c = SI, o = the Republic of Slovenia, oi = VAT-17659957, CN = SI-TRUST
Date of entry into force, *Validity: Not Before*	APR 25 07: 38: 17 2016 GMT
End of validity, *Validity: Not After*	DEC 25 08: 08: 17 2037 GMT
Public Key Algorithm, \ "_blank" *Subject Public Key Algorithm*	vacuum Consumption (OID 1.2.840.113549.1.1.1)

[1] The meaning is given in the pogs. 3.1 and 7.

Holders of a public key belonging to an appropriate key pair coded using the RSA algorithm, \ “_blank” *RSA Public Key*	*3072 bit length key*
Extensions of X.509v3	
Key Usage, OID 2.5.29.15, *\ “_blank” Key Usage*	Critical) Signature of Certificates (keyCertSign), CRL signature (cRLSign)
Basic restrictions, OID 2.5.29.19, \ “_blank” *Basic Constrants*	Critical) CA: TRUE No length limitation Constraint: None)
Key of the issuer key; OID 2.5.29.35, \ “_blank” Hash *Key Identifier*	4CA3 C368 5E08 0263
The identifier of the holder’s key; OID 2.5. *29.14,* *\ “_blank” Subject Key Identifier*	4CA3 C368 5E08 0263
Certificate footprint (not part of the certificate)	
SHA-1 certificate footprint, *Certificate Fingerprint — SHA1*	3A49 79B4 0FA8 4148 8200 B582 FBEE B63A AB99 19E
SHA-256 certificate footprint, *Certificate Fingerprint — SHA256*	“FAD5 4081 1A0DC 767C D65 72A0 88FA 3C8 493FA CD D82B 3B86 9A67 D10A AB4E 8124”

(8) The certificates of the subordinated issuers are listed in the individual policy.

1.1.2. registration Authority

The provisions are defined in each policy.

1.1.3. ~~certificate~~ holders

The provisions are defined in each policy.

1.1.4. Third persons

(1) Third parties are all end-users in the SI-TRUST public key infrastructure, and all other persons or entities relying on the issued digital certificates are SI-TRUST.

(2) Third parties must comply with the TSI TRUST and must always verify the validity of the certificate by verifying the whole chain of confidence, the purpose of the certificate, the period of validity of the certificate, etc. The more detailed obligations and responsibilities of third parties are set out in the sub-area. 1.1.39And1.1.183.

(3) A mutually agreed written agreement may be concluded between the third party and the SI-TRUST.

1.1.5. Other Participants

Not foreseen.

1.4. Purpose of the use of certificates

The provisions are defined in each policy.

1.1.6. Correct use of certificates and keys

The provisions are defined in each policy.

1.1.7. Unauthorised use of certificates and keys

(1) The digital certificates, which are issued by the SI-TRUST, must be used in accordance with the SI-TRUST and the policy of the individual issuer, the legislation in force and the arrangement between them, otherwise their use is not allowed.

(2) There are no other prohibitions relating to the use of certificates issued by the SI-TRUST.

1.5. Policy management

1.1.8. Policy Manager

The SI-TRUST Administrative Committee shall be responsible for preparing, applying, publishing, managing and interpreting the action policies.

1.1.9. Contact persons

The policy and other documentation provided by the Contact Person are the SI-TRUST (contact details given in the podfuneral. 1.3).

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

The persons responsible for the compliance of the individual issuer's operations, in accordance with the relevant policy, are entrusted to the SI-TRUST in accordance with the tasks they perform within the organisational groups (see below). 5.2).

1.1.11. Procedure for the adoption of a new policy

(1) The SI-TRUST may also issue amendments to policies, see below. 9.12YES/NO.

(2) The SI-TRUST Administrative Committee shall draw up a proposal for a new policy or amendment.

(3) In accordance with the eIDAS Regulation, the notification of the novelty of the SI-TRUST service shall be notified to the Authority under the eIDAS Regulation.

(4) The new policy or amendments are approved by the minister responsible for public administration.

1.6. *Terms and abbreviations*

1.1.12. Terms

(1) The general terms used in this policy are the following.

Digital signature	An advanced electronic signature meeting the requirements of Article 26 of the eIDAS Regulation.
Certificate/certificate	A certificate in electronic format providing the following key information: (1) information on the issuer, (2) information on the holder, (3) holders of public key, (4) time of validity and (5) the digital signature of the issuing issuer.
National authority	Ministries, government departments, government departments and administrative units, National Assembly, State Council, Constitutional Court, Court of Auditors, European Ombudsman, judicial authorities and other bodies governed by public law, who are direct users of the State budget pursuant to the Public Finance Act (Official Gazette of the Republic of Slovenia, No 11/11 — official consolidated text, 14/13 — corr., 101/13 and 55/15 — ZFisP).
Electronic signature	A set of electronic data added to or logically associated with other data in electronic form which are used by the signatory to sign.
Electronic seal	The set of electronic data added to or logically associated with other data in electronic format to ensure the origin and integrity of the related data.
Electronic time stamp	Data in electronic form linking other data in electronic form to a given moment in order to provide evidence that the latter data existed at that time.
Public key infrastructure	A set of roles, policies and procedures necessary for the formation, management, distribution, use, storage and revocation of digital certificates and for managing encryption with public keys (cf. the abbreviation of the *PKI*).
Qualified trust service	A trust service fulfilling the relevant requirements of the eIDAS Regulation.
Qualified signature	An advanced electronic signature generated by a qualified electronic signature creation device based on a qualified certificate for electronic signatures.
Qualified electronic seal	An advanced electronic seal created by a qualified electronic seal creation device and based on a qualified certificate for electronic seal.
Qualified electronic time stamp	An electronic time stamp complying with Article 42 of the eIDAS Regulation.
Qualified certificate for electronic signature	A digital certificate for electronic signature issued by a qualified trust service provider meeting the requirements of Annex I of the eIDAS Regulation.
Qualified certificate for electronic seal	A digital certificate for electronic seal issued by a qualified trust service provider meeting the requirements of Annex III of the eIDAS Regulation.
Qualified certificate for website authentication	A digital certificate for website authentication issued by a qualified trust service provider meeting the requirements of Annex IV of the eIDAS Regulation.
Business	A legal or natural person registered for the purpose of carrying out an activity.
Trust service provider	A natural or legal person providing one or more trust services as a qualified or non-qualified trust service (compare the letter of the CA).
Qualified trust service	A trust service provider providing one or more qualified trust services and

provider	the supervisory authority grants the qualified status to it.
Register of certificates cancelled	List of digital certificates that have been revoked before the expiry date (*Certification Residence List*). The SI-TRUST has this list published in its repository (cf. acronym *CRL*).
Electronic identification means	A material and/or intangible unit which contains the person identification data used for authentication for online services.
Trust service	Electronic service normally provided for remuneration including: (a) the creation, verification and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or (b) the creation, verification and validation of certificates for website authentication; or (c) the storage of electronic signatures, seals or certificates related to these services;
Third party	A legal or natural person, or any other entity relying on the issued digital certificate, or on a digital signature that can be verified by means of a public key contained in a digital certificate.
Trusted list of trust service providers	A Trusted List of a Member State of the European Union which includes information on the qualified trust service providers for which it is responsible, together with the information on the qualified trust services provided by those providers.

(2) The other terms used in this policy are given below.

Application/information system	A computer program managed by an organisation that requires the SI-TRUST service for its operation and which may be evidenced by a digital certificate SI-TRUST or by any other secure method provided by the SI-TSA.
Domain	An independent PKI infrastructure for the integration needs of issuers established within a specific organisation. Within the domain, issuers use a set of common policies that we designate as domain policies.
State Centre for Services of Confidence	Trust service provider operating within the Ministry of Public Administration.
Holder	A user who has been issued a digital certificate by the issuer. In the case of the root issuer, the SI-TRUST, is the issuer of the qualified digital certificates, who may have or are associated with the root certificate SI-TRUST.
Trust service provider infrastructure	All premises of the trust service provider, its hardware and software and the security mechanisms necessary for the safe operation of its issuers.
Internal policy SI-TRUST	The confidential part of the internal operating rules of the SI-TRUST, which is constituted by the Security Policy and subordinate and specific policy areas.
Issuer	An issuer of the digital certificates operating within the trust service provider (compare the letter of the *CA* and the expressions of the *trust service provider* and the *Certificate*).
ECS Issuer — CA	Certifier for national authorities operating within the SI-TRUST, *Slovenian governmental* certification *authority*.
Publisher of SIGEN-CA	Certifier for natural persons and business entities operating within the SI-TRUST, *Slovenian General Certification Authority*.
SI-Pass-CA issuer	An issuer of certificates issuing certificates for natural persons for the purpose of the online registration and e-signing service of the SI-PASS

	service and operating within the SI-TRUST, *Slovenian Authentication and e-Signature Service Certification Authority*.
The issuer of the SI-TSA	The issuer of qualified time stamps, which operates within the SI-TRUST, *Slovenian Time Age Authority.*
Public directory	A public directory, in which the issued digital certificates and the register of invalidated certificates are published. For the needs of the root broadcaster SI-TRUST the public directory is established *on* the x500.gov.si server.
By the end-user;	Holder of a certificate issued from an affiliated or a subordinate issuer.
Root publisher	In a hierarchical model of public key infrastructure, a root publisher presents a basic starting point of trust within a given domain, its certificate shall be used for verifying the validity of certificates within the trust chain.
The root issuer SI-TRUST Root	The root provider of digital certificates that operates within the SI-TRUST and issues the digital certificates for subordinated and related issuers of qualified digital certificates (qualified digital certificates). *Slovenian Trust Service Root Certification Authority*.
Interlinking	Interconnection, or also cross-authentication, is used to build confidence both between issuers within a single domain and for the integration of issuers from different domains (intra-domain (intra-national) and cross-domain authentication).
Qualified electronic signature creation device	Electronic signature creation device fulfilling the requirements of Annex II of the eIDAS Regulation (QSCD, *Qualified Signature Creation Device*). The private key of a qualified electronic signature creation device cannot be exported or copied.
Announcement of the SI-TRUST	Public announcement on the SI-TRUST website, https://www.si-trust.gov.si.
SI-TRUST alert	All instructions, explanations, lists, conditions, individual notices, recommendations, standards and other documents established or recommended by the SI-TRUST, or SI-TRUST, to be published or otherwise communicated to the holders, organisations or third parties.
Organisation	A national authority, a legal or natural person that manages the certificate to which the SI-TRUST has issued a liaison certificate (compare the service of *trust service provider*).
A smart card or a secure signature creation tool	See the *term 'Qualified electronic signature creation*'.
Subordinated issuer	The subordinate issuer does not have a self-issued certificate in the hierarchical model of the public key infrastructure, but has been issued with his basic digital certificate by the immediate parent. The performance of the subordinated issuer is determined by the rules of the parent body. In a public key infrastructure set up by a root broadcaster SI-TRUST Root, the latter, in its capacity as parent issuer, shall issue digital certificates for subordinate issuers. At the same time, the SI-TRUST Root provides a basic basis for trust within the domain under the SI-TRUST Root.
Policy	J shall be subject to the internal rules of the trust service provider, specifying the purpose, operation and methodology of the digital certificate management, the liability of the trust service provider and the requirements to be fulfilled by users and third parties using and relying on digital certificates by the trust service provider.
Special certificate	A digital certificate with two pairs of keys linking data from the certificate

	with the holder's private keys. The special certificate consists of a signature verification certificate and a encryption certificate.
Associated issuer	Issuing of the ECS on the basis of the ECS issued by the root issuer SI-TRUST Root.
Interconnection certificate	A digital certificate establishing trust between the two issuers.
Registration Authority	It is authorised by the issuer to accept applications for registration, revocation and regeneration of certificates and to verify the identity of the holders/future holders (RA, *Registration Authority*).
smsPASS	An electronic identification means that allows the registration through the SI-PASS service using the one-time password sent by the SMS message.
Online certification	One pair digital certificate linking data from the certificate with the holder's private key.
SI-PASS service	Service for online registration and e-signature *Authentication and e-Signature Service*, https://sicas.gov.si.
Chain of Trust	A set of certificates to be used for the verification of the validity of the end-user certificate. In addition to the end-user certificate, it also includes a certificate from the root issuer, as well as certificates from subsidiaries or related issuers.
Link certificate	A digital certificate in which the new public key is signed with the previous private key and vice versa
Request	A form for obtaining, withdrawing or validating certificates that can be accessed via the SI-TRUST website or, in the case of authorised persons, to the application services.
Employed	A natural person who is in an employment relationship with an organisation, or who has a different legal basis for the organisation of work for an organisation and for whom the responsible person of that organisation wishes to obtain a certificate which that person needs to carry out his duties for that organisation.

1.1.13. Abbreviations

CA	Issuing authority of digital certificates, *Certification Authority.*
CP $_{Name}$	The policy name of the service provider (s) of trust (s) of the provider (s) of trust (s)*. Certification Policy Name*), related to the unique activity policy code (cf. acronym *CP* $_{OID}$).
CP $_{OID}$	The unique code of action policy based on the OID number, *Certification Policy Object Identifier*
CRL	Certificates withdrawn (CRL) *Certification Relocation List*) (cf. the *Register of withdrawals of certificates*).
DCF77	A debt radio transmitter, located in Masisi, Frankfurt, providing 77.5 kHz with an official reference time frame.
eIDAS	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	International recommendations in the field of telecommunications, *European Telecommunications Standards Institute,* http://www.etsi.org.
FIPS	U.S. administration set of standards for use in computer systems, *Federal Information Processing Standard*
GPS	Satellite positioning system, *Global positioning system.*
HSM	Private key storage hardware or machine security module, *Hardware Security Module.*
LDAP	A protocol providing access to the directory and specified according to IETF. *Internet Engineering Task Force* Recommendation RFC 1777 “Leightweight Directory Access Protocol”.
MPA	Ministry of Public Administration, Tržaška cesta 21, 1000 Ljubljana.
NTP	Time synchronisation protocol. *Network Time Protocol*, http://www.ntp.org.
OCSP	A protocol for the ongoing verification of the validity of qualified digital certificates, as recommended by RFC 2560 “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol”, *Online Certificate Status* Protocol).
OI	Field in digital certificate with the name of the organisation identifier and OID number 2.5.4.97 containing an organisation identification code different from the organisation’s official name. The SI-TRUST shall apply, in accordance with ETSI standards, the tax number of the organisation using the prefix VATSI.
OID	International number uniquely identifying each installation in accordance with ITU-T X.208 (ASN.1), *Object Identifier.*
PKCS # 7 and PKCS # 10	Recommendations (*Public Key Cryptography Standards*) RSA Security for IT systems developers that use asymmetric cryptographic algorithms. • PKCS # 7 provides a syntax for cryptographic processed data such as digital signatures and digital envelopes. It shall apply, for example, to the transmission of digital certificates and lists of invalidated certificates. • PKCS # 10 determines the syntax of the call for authentication of the public key, names and other attributes.
CIP	Public Key Infrastructure. *Public Key Infrastructure*
PKI-CMP	It provides for a procedure for the exchange of data relating to digital certificates between entities of an infrastructure service provider’s infrastructure. It also includes *de facto* standard PKCS # 7 and PKCS # 10. It is published as RFC 4210 “*Public Key Infrastructure (based) X.509 — Certificate Management Protocols*”.
QSCD	Qualified electronic signature creation device fulfilling the requirements of Annex II of the eIDAS Regulation, *Qualified Signature Creation Device*.
QTSP	Qualified trust service provider, *Qualified Trust Service Provider.*
RFC	International recommendations for the Internet of IETF. *Internet Engineering Task Force* in IESG, *Internet Engineering Steering Group Request for Comments*, http://www.ietf.org/rfc.html.

SI-TRUST	See the term 'State Centre for Services of Confidence'.
SI-TRUST Root	The root provider of the digital certificates, *Slovenian Trust Service Root Certification Authority.*
TSP	Trust service provider, *Trust Service Provider.*
UTF-8	The mode of encoding the international sign code by which ASCII characters remain single-fold and the other signs can occupy several syllables.
X.501	Recommendations for distinctive names: ITU-T Recommendation X.501 — Information technology — Open Systems Interconnection — The Directory: Models".
X.509	Recommendations for the profile of digital certificates and register of cancelled certificates: RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile.
TSA	The issuer of the electronic time stamps (TSA; *Time seniority Authority*).
UTC	Coordinated universal time. *Coordinated Universal Time,* International Standard for Time Measurements, expired on 1972.

2. ON NOTICE AND LIABILITY ON THE REPOSITORY

2.1. repositories

The SI-TRUST documents or particulars of an individual issuer are made public in two trade repositories:

- in a public directory on a x500.gov.si server; and
- https://www.si-trust.gov.si.

2.2. Publication of certificate information

The provisions are defined in each policy.

2.3. Frequency of public announcements e

(1) The new policies shall be published in accordance with the indication in the subplace. 9.10YES/NO.

(2) The publicly available information or documents shall be published immediately after their creation.

(3) The certificates shall be published in a public directory immediately after their issuance, and record information on the certificate (holder name, e-mail address, serial number...) as soon as the booking of the certificate has been made.

(4) Certificates withdrawn shall be published immediately in the register of certificates (detailed topics below). 1.1.68).

(5) Other publicly available information or documents shall be published as necessary.

2.4. Access to repositories

The provisions are defined in each policy.

3. IDENTITY AND AUTHENTICITY

3.1. naming

The provisions are defined in each policy.

1.1.14. name (s) of name (s)

The provisions are defined in each policy.

1.1.15. requirement to make sense of names

The provisions are defined in each policy.

1.1.16. Use of anonymous names or pseudonyms

The provisions are defined in each policy.

1.1.17. rules for the interpretation of names

The provisions are defined in each policy.

1.1.18. uniqueness of names

The provisions are defined in each policy.

1.1.19. Recognition, credibility and role of trade marks

(1) The proprietor or organisation may not require any distinctive name that would fall to someone else, thereby infringing any rights of the trade mark or other copyright of other persons.

(2) Liability in respect of the right to use names or protected trade marks and other rights shall lie exclusively on the part of the proprietor. The SI-TRUST shall not be obliged to check and/or to bring this to the attention of the holder or organisation.

(3) Possible conflicts will be resolved exclusively by the party and the holder or the organisation.

3.2. initial identity validation

The provisions are defined in each policy.

1.1.20. Method for demonstrating private key ownership

The provisions are defined in each policy.

1.1.21. identification of organisations

The provisions are defined in each policy.

1.1.22. Identity check

The provisions are defined in each policy.

1.1.23. Non-verified initial verification data

The provisions are defined in each policy.

1.1.24. Validation of authority

The provisions are defined in each policy.

1.1.25. criteria for interoperation

The provisions are defined in each policy.

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

The provisions are defined in each policy.

1.1.26. Identity and credibility in the event of renewal

The provisions are defined in each policy.

1.1.27. Identity and authenticity upon renewal after cancellation

The provisions are defined in each policy.

3.4. Identity and authenticity at the request of cancellation

The provisions are defined in each policy.

4. MANAGEMENT OF CERTIFICATES

4.1. Application for certificates a

The provisions are defined in each policy.

1.1.28. Who can apply for a certificate

The provisions are defined in each policy.

1.1.29. Enrolment process and responsibilities

The provisions are defined in each policy.

4.2. procedure for receipt of an application for a certificate

The provisions are defined in each policy.

1.1.30. Identity and authentication process of the prospective holder

The provisions are defined in each policy.

1.1.31. Approval/rejection of the application

The provisions are defined in each policy.

1.1.32. Time to issue the certificate

The provisions are defined in each policy.

4.3. Issue of certificate

The provisions are defined in each policy.

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

The provisions are defined in each policy.

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

The provisions are defined in each policy.

4.4. Certificate acceptance

The provisions are defined in each policy.

1.1.35. Certificate acceptance procedure

The provisions are defined in each policy.

1.1.36. publication of the certificate

The provisions are defined in each policy.

1.1.37. notice of issue to third parties

The provisions are defined in each policy.

4.5. use of certificates and keys

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

The provisions are defined in each policy.

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

(1) The third party relying on the ECS must act and use the certificate in accordance with the policy and other applicable regulations.

(2) The third party may only rely on the certificate for the purpose specified in the certificate (see below. 1.1.127) and in the manner prescribed by the policy;

(3) When using the Certificate, the third party shall always verify the validity of the digital certificate in accordance with the instructions given by the individual issuer*:*

- at the time of use, check that the certificate is not revoked,
- verify at the time of use the certificate if the digital signature of the certificate has been creosote in the period of validity and with the appropriate purpose of the certificate,
- verify, at the time of the certificate, the signature of the issuer of the certificate, which is published in this policy as well as in any other manner communicated to third parties,
- to comply with the other provisions, provided that an arrangement has been agreed with the SI-TRUST to use the certificates.

(4) In order to authenticate the signature/other cryptographic operation, the third party shall use the software and

hardware used to verify all the above requirements for the safe use of the certificates in a credible manner.

(5) Other duties and responsibilities are laid down in the sub-area. 1.1.183YES/NO.

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

Not supported.

1.1.40. Grounds for re-certification

Not supported.

1.1.41. Who may request a reissue

Not supported.

1.1.42. Procedure for re-issuing the certificate

Not supported.

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

Not supported.

1.1.44. Acceptance of a re-certificate

Not supported.

1.1.45. Publication of a re-certificate

Not supported.

1.1.46. Issue notice to other entities

Not supported.

4.7. Renewal of certificate

The provisions are defined in each policy.

1.1.47. Circumstances for certificate re-key

The provisions are defined in each policy.

1.1.48. Who can ask for a renewal of the certificate

The provisions are defined in each policy.

1.1.49. Procedure for renewal of certificate

The provisions are defined in each policy.

1.1.50. Notification to the holder of renewal of a certificate

The provisions are defined in each policy.

1.1.51. Acceptance of a renewed certificate

The provisions are defined in each policy.

1.1.52. Publication of a renewed certificate

The provisions are defined in each policy.

1.1.53. Issue notice to other entities

The provisions are defined in each policy.

4.8. Certificate modification

The provisions are defined in each policy.

1.1.54. Grounds for the change of certificate

Not supported.

1.1.55. Who can request a change

Not supported.

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

Not supported.

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

Not supported.

1.1.58. Acceptance of the amended certificate

Not supported.

1.1.59. Publication of the amended certificate

Not supported.

1.1.60. Issue notice to other entities

Not supported.

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

The provisions are defined in each policy.

1.1.62. Who may request cancellation

(1) Revocation of an attestation may require:

- the authorised person SI-TRUST,
- holder,
- the competent court; or
- administrative authority.

(2) In the event that the SI-TRUST has acquired the information on the misuse of the certificate by a third party, it shall, before the revocation of the certificate, obtain the consent of its holder.

1.1.63. Cancellation procedure

The provisions are defined in each policy.

1.1.64. Time to issue cancellation request

The provisions are defined in each policy.

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

1.1.65. Time spent on cancellation request received until revocation

The provisions are defined in each policy.

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

(1) Third parties relying on the certificate must check the latest register of invalidated certificates before use.

(2) For the sake of authenticity and integrity, it is always necessary to verify the validity and credibility of that register, which is digitally signed by the individual issuer.

(3) For each digital certificate used, the third party has to carry out a complete process of verification of the chain of confidence in accordance with RFC 5280.

(4) If a third party is unable to verify the status of a digital certificate in the register, he/she may nevertheless refuse to use the digital certificate or accept the digital certificate, and accept it.

1.1.67. frequency of publication of the certificate withdrawn

The register of certificates cancelled is kept up (see below for access to the register. 1.1.159):

- after each withdrawal of the certificate,
- at least once a year if there are no new records or changes in the register of cancelled certificates at the root broadcaster SI-TRUST Root,
- once a day, if there are no new records or changes in the register of invalidated certificates, approximately twenty four (24) hours after the last refreshments in the other issuers.

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

(1) The publication of a new register of cancelled certificates shall be carried out:

- In a public directory on a *x500.gov.si* server immediately,
- and on the Internet site, with a delay of up to one (1) at the root broadcaster SI-TRUST Root, or with a delay of up to ten (10) minutes in other Issuers.

(2) The register of withdrawals of certificates shall be communicated to potential third parties and to other entities that rely on the issued digital certificates SI-TRUST.

1.1.69. Verification of the status of certificates

A protocol for ongoing verification of the status of certificates (OCSP) is supported in line with RFC 2560 “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol”. See detailed below. 7.3YES/NO.

1.1.70. Requirements for continuous verification of the status of certificates

When using the Certificate, third parties shall at all times verify whether the certificate you are relying on is cancelled.
See also below. 1.1.66YES/NO.

1.1.71. Other means of access to certificate status

Not supported.

1.1.72. Other requirements for private key abuse

Not prescribed.

1.1.73. Grounds for suspension

Not supported.

1.1.74. Who may request the suspension

Not supported.

1.1.75. Procedure for the suspension

Not supported.

1.1.76. Time of suspension

Not supported.

4.10. Verification of the status of certificates

1.1.77. Access for verification

The provisions are defined in each policy.

1.1.78. Availability

Verification of the status of the certificates shall be available 24 (24) h all days in the year.

1.1.79. Other options

Not prescribed.

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

trust service provider

The provisions are defined in each policy.

4.12. detection of a copy of the decryption keys

The provisions are defined in each policy.

1.1.80. Procedure for detection of decryption keys

The provisions are defined in each policy.

1.1.81. procedure for the detection of the meeting key

Not supported.

5. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

5.1. Physical security

(1) The SI-TRUST equipment shall be protected by a multi level physical and electronic security system.

(2) The security of the SI-TRUST infrastructure shall be carried out in accordance with the recommendations of the profession for the highest level of protection.

(3) The full description of the SI-TRUST and the management and management procedures are determined by the SI-TRUST policy.

1.1.82. Location and structure of the trust service provider

(1) The SI-TRUST equipment is located in specific, secure, separate rooms within the infrastructure of the Ministry of Public Administration.

(2) It is protected by a multi-level physical and electronic security system.

(3) Detailed provisions have been set out in the SI-TRUST, on the internal market.

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

(1) The SI-TRUST infrastructure shall be accessible only to authorised persons SI-TRUST in accordance with their duties and powers, see below. 5.2YES/NO.

(2) All accesses are protected in accordance with the applicable legislation and recommendations.

(3) Detailed provisions have been set out in the SI-TRUST, on the internal market.

1.1.84. Power and air conditioning

(1) The SI-TRUST infrastructure shall be provided with an uninterrupted supply and adequate air conditioning systems.

(2) This is set out in detail in the SI-TRUST, on the internal market.

1.1.85. water exposures

(1) The SI-TRUST infrastructure is not exposed to flood risks.

(2) This is set out in detail in the SI-TRUST, on the internal market.

1.1.86. Fire prevention and protection

(1) The SI-TRUST facilities shall be protected from any outbreak of fire.

(2) This is set out in detail in the SI-TRUST, on the internal market.

1.1.87. media management

(1) Data in physical or electronic format shall be recorded on data carriers which are securely stored in secure facilities.

(2) Backup software and encrypted SI-TRUST are regularly renovated and stored in two separate and physically protected spaces, at different locations.

(3) This is set out in detail in the SI-TRUST, on the internal market.

1.1.88. Disposal

(1) The SI-TRUST ensures the secure disposal and destruction of documents in physical and electronic format.

(2) Disposal of waste is carried out by a special committee under the SI-TRUST policy.

1.1.89. Off-site backup

See below. 1.1.87YES/NO.

5.2. organisational structure of the trust service provider

1.1.90. Organisation of a trust and trusted service provider

(1) The operational, organisational and professional operation of the SI-TRUST is managed by the authorised person, SI-TRUST, who is authorised to perform those tasks by the head of the internal organisational unit within the Ministry of Public Administration, who is responsible for the management of the digital certificates (hereinafter *leader of NOE*).

(2) The persons authorised include the SI-TRUST:

- Employed in the SI-TRUST and
- Of the registration service.

(3) The SI-TRUST employed in the SI-TRUST is arranged in six organisational groups covering the following subject areas:

- the governance of the trust service provider;
- management of certificates,
- infrastructure management;
- security and control,
- internal verification of compliance,
- legal-linguistic administration.

(4) Trusted roles are performed by employees performing tasks in the following substantive areas:

- the governance of the trust service provider;
- management of certificates,
- infrastructure management;
- security and control.

Organisation group	Role	Primary tasks	Number of persons
Governance of the trust service provider	System operator	– Operation strategy SI-TRUST – Determination of the first safety engineer – The operational management of the SI-TRUST	3
Management of certificates	First security engineer	– Determination and implementation of safe operation rules for the certification scheme – Determination of other security engineers	1
	Other safety engineers	– Determination and implementation of safe operation rules for the certification scheme	2
	Certificate administrators	– Management of certificates *	2
Infrastructure management	System Administrator	– Operating system (installation, configuration, maintenance...) – Telecommunications management (intrusion detection and detection system, fire barrier,...)	2
Security and control	Security Administrator	– Inspection of logs – Back-up of safety copies	1
Internal verification of compliance	Internal auditor		1
Legal — administrative	Lawyer		1

* In view of the specificities of the issuer SI-TRUST Root, the administrators' role in it was accepted by the safety engineers.

(5) The SI-TRUST is composed of the system operator, the security engineer, the lawyer and the head of NOE.

(6) The tasks of the SI-TRUST Administrative Board shall be:

- the appointment of staff performing trusted roles;
- preparing changes and new versions of policy
- carrying out conformity assessment under the eIDAS,
- deciding on the issue and revocation of certificates of subsidiaries and related issuers;
- other tasks of the management of the State Trust Service Centre.

1.1.91. Number of persons required per task

(1) Certain sensitive tasks must be carried out simultaneously in accordance with the applicable legislation and the SI-TRUST policy. These may include:

- key recovery;
- detection of a copy of the decryption keys; and
- other tasks set out in the SI-TRUST policy.

(2) Infrastructure shall ensure that security or critical procedures are approved by two authorised persons at the same time.

(3) The number of persons indicated in the table in the table. 5.2It represents a minimum number of persons.

1.1.92. Identity of individual applications

Identification and access rights for the performance of specific tasks in accordance with the role of each organisational group as well as the performance of the functions of the registration service shall be ensured by means of the SI-TRUST's security mechanisms and control procedures.

1.1.93. Roles requiring separation of duties

(1) All the SI-TRUST organisational groups listed in the table below. 5.2They are incompatible with each other.

(2) In the absence of suitable qualified staff, teams of specific groups of the same or similar privileges may be combined with similar types of staff.

(3) Notwithstanding the provisions of the preceding Article, critical operations, the performance of which has the effect of increasing risks, shall be mutually incompatible.

(3) The roles of individual organisational groups are determined by the SI-TRUST policy.

5.3. Personnel controls

According to the legislation in force, more detailed arrangements on staff supervision are set out in the SI-TRUST, on the other hand.

1.1.94. Qualifications, experience and clearance requirements

(1) The SI-TRUST staff shall have appropriate qualifications and experience in accordance with the requirements of the applicable legislation and shall be suitable for the performance of their duties, in accordance with the requirements of the applicable legislation.

(2) The person (s) SI-TRUST shall sign a declaration concerning the carrying out of tasks with specific responsibilities prior to the commencement of the tasks for the purpose of the SI-TRUST.

(3) The employees of the SI-TRUST engaged in trusted roles:

- must be designated for the purpose of carrying out these applications by the SI-TRUST,
- they may not carry out other functions which would be contrary to the performance of duties in the SI-TRUST,
- they must not be dismissed on previous similar duties (e.g. custodian of cryptographic devices, security engineer) as a result of negligence or failure; and
- hold a PSC for at least CONFIDENTIAL.

1.1.95. Background check procedures

(1) Prior to the conclusion of the employment relationship, checking the suitability of the SI-TRUST staff shall be carried out by the HR department of the Ministry of Public Administration in accordance with the applicable law for civil servants.

(2) Verifications of the suitability of the SI-TRUST staff carrying out trusted roles shall be carried out by the body approved under the Classified Information Act (ZSTG, Official Gazette of the Republic of Slovenia, Nos 50/06 — official consolidated text, 9/10 and 60/11) at the time of the authorisation for access to classified information.

1.1.96. Staff training

All the necessary education shall be provided to persons performing the tasks of the organisational groups mentioned above and the tasks of the application department.

1.1.97. Training requirements

Staff will be trained depending on the needs/innovations regarding the operation of the SI-TRUST infrastructure.

1.1.98. job rotation frequency and sequence

Not prescribed.

1.1.99. Sanctions

In the case of an unauthorised or negligent failure, the sanctions shall be applied to the authorised persons in the SI-TRUST in accordance with the applicable law for civil servants and other applicable legislation.

1.1.100. Independent contractor requirements

Potential external operators are subject to the same requirements as the SI-TRUST as authorised persons.

1.1.101. Documentation supplied to personnel

Under the SI-TRUST, authorised persons all the necessary documentation shall be made available in accordance with their respective duties and tasks.

5.4. System security checks

(1) The SI-TRUST shall, in accordance with the legislation in force, have permanent surveillance of the operation of its infrastructure, under which it shall be verified that:

- the physical security of the ICT infrastructure,
- seamless operation of all security systems;
- the smooth functioning of all information and communication systems and
- whether in the meantime there has been an intrusion or an attempt by unauthorised persons to be accessed by equipment or data.

(2) In accordance with the legislation in force, detailed information on this point is set out in the SI-TRUST, on the one hand, and the Commission, on the other hand, on the other hand.

1.1.102. Type of event (s)

(1) The SI-TRUST shall, in accordance with the legislation in force, record the following types of event:

- occurrence on the individual issuer's operating system, software and hardware;
- events on operating systems, software and hardware components of the communication system,
- events relating to the keys of an individual issuer,
- events related to keys and digital certificates of holders (issuance, acquisition, renewal, revocation, detection of a copy of the decryption keys),
- occurrences related to security policy and management of the information system of an individual issuer;
- occurrences related to security policy and management of the communication system.

(2) The SI-TRUST shall also collect and record, in electronic or written form, security data which are not part of the trust service provider's information and communication system:

- events relating to physical access to the systems of an individual issuer and physical location,
- staffing changes for the SI-TRUST,
- events related to the destruction of sensitive material (such as cryptographic keys and key holders, activation data, personal data on holders).

(3) The index logs shall be stored in written form or in electronic form in the secure area of the SI-TRUST.

1.1.103. Frequency of processing log

(1) The SI-TRUST shall carry out regular security inspections of its infrastructure using surveillance and alert alarm systems for occurrence.

(2) The SI-TRUST staff reviews audit logs on the occasion of any warning from the control systems. The review shall include:

- check the integrity of the logs;
- an overview of log records; and
- analysis and reporting of relevant events — problem solving.

1.1.104. Retention period for audit log

(1) The log of keys and digital certificates events shall be kept for a period of at least seven (7) years after the expiry date of the certificate to which the log refers.

(2) Other audit logs shall be kept for a period of at least seven (7) years after the occurrence of the event.

(3) The record of the events referred to in the preceding paragraph containing personal data shall be kept in accordance with the legislation in force.

1.1.105. Protection of audit log

(1) The logs shall be protected in accordance with security mechanisms providing the highest level of security.

(2) The details are set out in the SI-TRUST, in accordance with the legislation in force.

1.1.106. Audit log backup procedures

(1) Back-up copies of logs shall be performed on a regular back-up of systems on a daily basis.

(2) The details are set out in the SI-TRUST, in accordance with the legislation in force.

1.1.107. Data collection for audit logs

(1) Data shall be collected either automatically or manually depending on the type of data.

(2) The details are set out in the SI-TRUST, in accordance with the legislation in force.

1.1.108. Notification to event-causing subject

It shall not be necessary to inform the agent of the event.

1.1.109. Assessment of system vulnerabilities

(1) The analysis of logs and the monitoring of the implementation of all procedures shall be carried out on a regular basis by the authorised persons SI-TRUST or by automated means with other security mechanisms on all computer communications devices under the authority of the SI-TRUST.

(2) The vulnerability assessment shall be carried out on the basis of an analysis of the logs and a finding of

control over the conduct of the proceedings.

(3) The details are set out in the SI-TRUST, in accordance with the legislation in force.

5.5. retention of information

1.1.110. Types of record archived

The SI-TRUST shall, in accordance with the applicable legislation, retain the following information or documents:

- logs,
- minutes,
- all supporting documents relating to the verification of identity and other data on the holders,
- concluded between themselves;
- all requests,
- certificates issued and register of certificates cancelled,
- operation policies;
- SI-TRUST — Publication and notification
- private decryption keys according to the sub-area. 6And
- other documents in accordance with the rules in force.

1.1.111. retention period

(1) Archived data concerning keys and digital certificates shall be kept for a period of at least seven (7) years after the expiry of the certificate to which the data relates.

(2) The remaining archived data shall be kept for a period of at least seven (7) years after their creation.

(3) The archived data referred to in the preceding paragraph containing personal data shall be kept in accordance with the legislation in force.

1.1.112. Protection of archive

(1) Archived data, which are contained in documentary material (right of right holders, agreements and contracts, and record of event in writing), shall be stored and archived in accordance with the procedures for documentary material on the MPA.

(2) The archived data to be recorded under the information system (automatically generated index logs, digital certificates, invalidated certificate registers and private decryption keys) shall be kept in at least two copies in separate locations.

(3) According to the legislation in force, this is set out in detail in the SI-TRUST, in line with the legislation in force.

1.1.113. System archive and storage

(1) For data subject to documentary material (Holder’s requests, agreements and contracts, as well as the written record of the events), it shall be made available in accordance with the procedural workflow of documentary

material on the MPA.

(2) A backup shall be made at the time of production of the data archive to be recorded in the information system (automatically generated index logs, digital certificates, registers of invalidated certificates and private decryption keys). A copy of archived data shall be stored securely in two physical locations.

(3) The details of this are set out in the SI-TRUST, in accordance with the legislation in force.

1.1.114. Requirement of time stamping

Not prescribed.

1.1.115. Data collection how archived data can be collected

(1) The data shall be collected in a manner consistent with the type of document.

(2) According to the legislation in force, this is specified in the Interni Policy SI-TRUST.

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

(1) Access to archived data is permitted:

- the SI-TRUST Administrative Board,
- persons authorised to be SI-TRUST and
- for inspection purposes.

(2) According to the legislation in force, this is specified in the Interni Policy SI-TRUST.

5.6. Renewal of the issuer's certificate

The provisions are defined in each policy.

5.7. Compromise and disaster recovery

1.1.117. Incident and compromise handling

Under the current legislation, this is set out in the SI-TRUST.

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

Under the current legislation, this is set out in the SI-TRUST.

1.1.119. Entity private key compromise procedures

Under the current legislation, this is set out in the SI-TRUST.

1.1.120. Compromise and disaster recovery

Under the current legislation, this is set out in the SI-TRUST.

5.8. *Extinction of the issuer*

If the SI-TRUST is terminated by its activity or by an individual issuer, the SI-TRUST will take action in accordance with the legislation in force and any mutual agreement or agreement. The process of winding up is set out in more detail in the Intern Policy SI-TRUST.

6. TECHNICAL SAFETY REQUIREMENTS

6.1. *Key generation and positioning*

1.1.121. Key generation

The provisions are defined in each policy.

1.1.122. Delivery of private key to holders

The provisions are defined in each policy.

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

The provisions are defined in each policy.

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

The provisions are defined in each policy.

1.1.125. Key length

The provisions are defined in each policy.

1.1.126. Generating and quality of public key parameters

The quality of the key parameter of the individual issuer is ensured by the private key hardware manufacturer, which uses a *random number generator* in accordance with the FIPS standard 140-2 Level 3.

1.1.127. Key purpose and certificates

(1) The purpose of the use of keys or certificates shall be in accordance with *X.509 v.3* as specified *in* the certificate in the *key application* field *and*the extended *application key.*

(2) The signature of the digital certificates and the register of cancelled certificates is intended for the private key of the individual issuer and for authentication the public key in the issuer's certificate is reserved.

(3) The profile of the issuer's certificate and the certificate of the holders is given in the rat. 7YES/NO.

6.2. *Private key protection and security modules*

1.1.128. Cryptographic module standards

(1) The private key of an individual issuer is generated and stored on hardware for the secure storage of private keys (or machine security module, HSM. *Hardware Security Module*) which complies with the FIPS standard 140-2 Level 3.

(2) The equipment used by the holders of the SI-TRUST's certificate holders must conform to the globally accepted security and technical standards and comply at least with one of the conditions set out in ETSI Standard EN 319 411-1, Chapter. 1.1.145

1.1.129. Private key control by authorised persons

The provisions on access to the private key of an individual issuer are set out in the SI-TRUST, in accordance with the legislation in force.

1.1.130. Detecting a copy of the private key

The provisions are defined in each policy.

1.1.131. backup of private keys

The provisions are defined in each policy.

1.1.132. Private key archiving

The provisions are defined in each policy.

1.1.133. Transfer of private key from/to cryptographic module

(1) The transfer of the private key of an individual issuer from a hardware security module shall be carried out in encrypted form after the generation of a backup private key pair (see below), following the generation of a backup private key pair (see below). 1.1.131). The transfer of the private key to the hardware security module

shall be done in encrypted form in the event of a security module being replaced or reset.

(2) The transfer of the private key from or to the cryptographic module shall be carried out with the approval of at least two SI-TRUST persons.

(3) Details on the delegation of the issuer's private key are set out in the SI-TRUST Internet policy.

(4) The details of the generic company's private key shall be determined by the individual issuers in its policy of operation.

1.1.134. Private key record in a cryptographic module

(1) The private key is protected in a machine security module by mechanisms according to the FIPS standard 140-2 Level 3.

(2) The details of the access to the private key of the holder shall be determined by the individual issuers in their policy of operation.

1.1.135. Procedure for the activation of the private key

(1) The activation of the private key of an individual issuer shall be carried out at the moment of the start-up of the software of the issuer and shall take place in accordance with the provisions of the Interne policy SI-TRUST.

(2) The details of the private key activation of the holder shall be determined by the individual issuers in its policy of operation.

1.1.136. Procedure for deactivation of the private key

(1) In the event of a suspension of the performance of an individual issuer, the issuer's software shall deactivate the private key of the issuer.

(2) The details of the deactivation of the private key of the holder shall be determined by the individual issuers in its policy of operation.

1.1.137. Procedure for the destruction of the private key

(1) The procedure for the destruction of the private key of an individual issuer shall take place in a safe manner consistent with the provisions of the Interne policy SI-TRUST. The private key shall be destroyed in such a way that it cannot be restored.

(2) The details of the destruction of the private key of the holder shall be determined by the individual issuers in their policy of operation.

1.1.138. Cryptographic module characteristics

The machine security module shall comply with the standards laid down in the sub-area. 6.2YES/NO.

6.3. Key Management Aspects

1.1.139. Preservation of public key

An individual issuer shall archive its public key and the holders' public keys as given in the sub-area. 5.5YES/NO.

1.1.140. Certificate and series validity period

The provisions are defined in each policy.

6.4. Access passwords

1.1.141. Password generation

The provisions are defined in each policy.

1.1.142. Password protection

The provisions are defined in each policy.

1.1.143. Other aspects of passwords

The provisions are defined in each policy.

6.5. Safety requirements for issuing computer equipment by the issuer

1.1.144. Specific technical safety requirements

Under the current legislation, this is set out in the SI-TRUST.

1.1.145. level of security protection

Under the current legislation, this is set out in the SI-TRUST.

6.6. Issuer's life cycle technical control

1.1.146. Control of the evolution of the system

(1) An individual issuer uses an Entrust software that is certified in accordance with the Common Criteria EAL4 +.

(2) The detailed technical requirements are set out in the Interni Policy SI-TRUST.

(3) Holders of certificates of a root issuer shall use software certified in accordance with the Common Criteria to at least EAL4 + or established in accordance with ETSI Standard EN 319 401.

1.1.147. managing safety

Under the current legislation, this is set out in the SI-TRUST.

1.1.148. Life cycle control

Under the current legislation, this is set out in the SI-TRUST.

6.7. Network security controls

The provisions are defined in each policy.

6.8. Time-stamping

Unspecified.

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

7.1. Certificate Profile

1.1.149. Certificate version

The provisions are defined in each policy.

1.1.150. profile of extensions

The provisions are defined in each policy.

1.1.151. Algorithm identification markings

(1) Certificates issued by an individual issuer are signed by the issuer using an algorithm defined in the *needle algorithm*: the value of “sh256WithRSAEncrConsumption”, the identification code: OID 1.2.840.113549.1.1.11.

(2) The full range of algorithms, data formats and protocols are available from the SI-TRUST.

(3) The root issuer SI-TRUST Root may also support other algorithms if it is concluded in a possible mutual agreement or contract with the holder.

1.1.152. Name (s) of name (s)

see below.1.1.14

1.1.153. Restriction on names

There are no restrictions on names (the box in the *instructions*) is not prescribed.

1.1.154. Certificate policy code

See below. 1.1.150 YES/NO.

1.1.155. Use of expansion field to limit policy use

Restrictions on the use of policies (*Policy results*) do not apply.

1.1.156. format and treatment of specific policy information

Certificates issued by an individual issuer shall use *the* specific polycyQualificiers information to be treated in accordance with RFC 5280.

1.1.157. Consideration of a critical enlargement policy field

Policy extension field (policy extension) *CertificatePolicies* is not labelled as critical.

7.2. register of invalidated certificates

1.1.158. Version

(1) The register of invalidated certificates issued by the root issuer SI-TRUST and also subordinated and its related issuers comply with ITU-T Recommendation X.509 (1997) and ISO/IEC 9594-8: 1997 including ver. 2

(2) The register of invalidated certificates is permanently accessible to the repository (see below. 2.1):
- according to the LDAP protocol, and
- according to the HTTP protocol.

1.1.159. content of the register and extensions

The provisions are defined in each policy.

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

The provisions are defined in each policy.

1.1.160. Version

An individual issuer uses OCSP version 1 messages in accordance with RFC 2560 recommendation.

1.1.161. Extensions to ongoing status check

OCSP messages (request/response) services for ongoing verification of status of certificates support the extension of Nons, which are not rated as critical.

8. INSPECTION

8.1. Inspection frequency

Inspection frequency is the responsibility of the inspection service, which is competent according to the legislation in force.

8.2. technical inspection body

(1) The SI-TRUST inspection supervision shall be carried out by the competent inspection service in accordance with the legislation in force.

(2) The external verification of the compliance of operations shall be carried out by a conformity assessment body in accordance with the applicable legislation.

(3) The internal verification of compliance shall be carried out by the internal auditor and the other authorised persons under the SI-TRUST.

8.3. independence of the inspection service

The inspection service shall be the supervisory authority competent according to the applicable legislation.

8.4. Areas of inspection

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

8.5. actions of the trust service provider

In the event of any deficiencies or deficiencies found, the SI-TRUST shall endeavour to eliminate them as soon as possible.

8.6. *publication of inspection results*

(1) The SI-TRUST shall make publicly available on its websites a summary of the inspection decisions.

(2) The SI-TRUST shall make publicly available on its websites information on the conformity assessment body which, in accordance with the applicable legislation, has carried out an external verification of compliance of the operation with the SI-TRUST.

9. OTHER BUSINESS AND LEGAL AFFAIRS

9.1. *Fee schedule*

1.1.162. Issuance price and renewal of certificates

The provisions are defined in each policy.

1.1.163. Access price for certificates

The provisions are defined in each policy.

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

The provisions are defined in each policy.

1.1.165. Prices of other services

The cost of the necessary hardware or software required or recommended by an individual issuer for the safe storage and use of the certificates shall be borne by the holder of the certificate or organisation.

1.1.166. Reimbursement of expenses

Not prescribed.

9.2. *Financial responsibility*

1.1.167. Insurance coverage

With regard to the operation of the SI-TRUST, the Ministry of Public Administration shall take due care of its liability in accordance with the legislation in force.

1.1.168. other cover

Unspecified.

1.1.169. Holders' insurance

Unspecified.

9.3. Protection of commercial information

1.1.170. Protected data

(1) The SI-TRUST shall treat as confidential the following information:

- all applications for a certificate or other service,
- confirmation of private keys for certificates when kept by the issuer,
- any confidential information relating to financial liabilities,
- any confidential information which has been the subject of mutual agreement with the organisation or third parties; and
- all other issues that are registered under the applicable law in the SI-TRUST.

(2) The SI-TRUST acts in accordance with the legislation in force, by any confidential information relating to the organisations or third parties strictly necessary for the certification of the management of the certificates.

1.1.171. Non-safeguarded data

The SI-TRUST shall make publicly available only such business data which, in accordance with the applicable law, are not of a confidential nature.

1.1.172. Liability with regard to the protection of commercial information

The SI-TRUST shall forward only those details of the organisations which are indicated in the certificate or in any mutual agreement or contract. Other information may be transmitted only where it is specifically required for the performance of a specific certificate (s) related to the certificates, or approved by the certificate holder or at the request of the competent court or administrative authority in the application for the certificate or at a later date. The data shall also be transmitted without the written consent, if provided for by the legislation or regulations in force.

9.4. Protection of personal data

1.1.173. Privacy plan

The SI-TRUST acts in accordance with the legislation in force, by means of any personal and confidential information relating to the holders of the certificates which are strictly necessary for the certification of the management of the certificates.

1.1.174. Protected personal data

Protected data are all personal data obtained by an individual issuer on requests for its services or in any mutual agreement or in any relevant register or in the relevant registers to establish the identity of the holder.

1.1.175. Personal data not protected

No other potentially hazardous personal data other than those indicated in the certificate and in the certificate withdrawn register.

1.1.176. Responsibility for the protection of personal data

The SI-TRUST shall be responsible in accordance with the legislation in force concerning the protection of personal data.

1.1.177. Power of attorney concerning the use of personal data

The provisions are defined in each policy.

1.1.178. Transfer of personal data to official request

The provisions are defined in each policy.

1.1.179. Other provisions concerning the transfer of personal data

The provisions are defined in each policy.

9.5. Provisions concerning intellectual property rights

Provisions relating to copyright, related and other intellectual property rights in respect of a particular issuer:

- politicians belong to all the rights of the SI-TRUST.
- all the rights of the SI-TRUST are attached to the certificate directory and to the register of cancelled certificates.
- all data in the certificates belong to all the rights of the SI-TRUST,
- all the rights of the holder or organisation shall belong to the private signing key.

9.6. Liability and accountability

1.1.180. Obligations and responsibilities of the issuer

(1) The SI-TRUST shall be responsible:

- to act in accordance with its internal rules and other applicable regulations and legislation,
- to work in accordance with international recommendations;
- to publish all relevant documents determining its operation (performance policies, claims, price lists,

instructions, etc.);
- publish on their websites all information on those changes in the SI-TRUST activity, which in any way affect the holders of certificates, organisations and third parties,
- ensure the functioning of the application services in accordance with the provisions laid down by the individual issuer and the other rules in force,
- comply with the provisions on the safe handling of personal, operational and confidential information about the trust service provider, certificate holders, organisations or third parties;
- to revoke the certificate and to publish the cancelled certificate in the register of invalidated certificates when it determines that the reasons given lie within the scope of this policy or other applicable regulations,
- issue certificates in accordance with the policy of the individual issuer and other regulations and recommendations.
- they shall carefully protect the private keys of the certificates from unauthorised access if they are kept by the issuer.

(2) The SI-TRUST shall be responsible:
- to ensure the correctness of the data issued;
- before issuing the certificate, check that the holder has certified the private key to which the public key certificate belongs (see below. 3.2),
- ensure the secure reception of digital certificates through the mandatory use of smart cards and ensure the secure delivery of smart cards with digital certificates to holders,
- ensure the correctness of the publication of the register of certificates cancelled,
- ensure the regularity of the operation of the current verification of the status of the certificates,
- ensure uniformity of names;
- ensure adequate physical security of premises and accesses to the premises of the trust service provider themselves;
- as a good holder, care is taken to ensure the smooth operation and maximum availability of services;
- as a good holder, care is taken to ensure that services are as accessible as possible;
- as a good holder, care is taken to ensure the smooth functioning of all other accompanying services,
- try to remedy the problems encountered to the best of their abilities and in the shortest possible period of time,
- ensure the optimisation of hardware and software; and
- inform all relevant entities on relevant matters; and
- comply with all other policy requirements.

(3) The SI-TRUST ensures the widest possible accessibility of its services, namely 24ur/7dni/365dni, without taking into account the following examples:
- planned and pre-announced infrastructure technical or service interventions;
- unplanned technical or service interventions in the infrastructure as a result of unforeseen failures,
- technical or service interventions due to failure of the infrastructure, outside the scope of the SI-TRUST, and
- unavailability due to force majeure or extraordinary events.

(4) The SI-TRUST shall announce the maintenance or upgrading of the infrastructure at least three (3) days before the start of works.

(5) The SI-TRUST shall be responsible for all references in this document and for the implementation of all the provisions laid down in this policy.

(6) The other obligations/responsibilities of the SI-TRUST are set out in the internal policy of the SI-TRUST and may be agreed by mutual agreement with the holder, organisation or third party.

1.1.181. Obligations and responsibilities of the application service

The provisions are defined in each policy.

1.1.182. Holder's obligations and responsibilities

The provisions are defined in each policy.

1.1.183. obligations and responsibilities of third parties

(1) Third parties should examine all requirements and circumstances before deciding to rely on certificates issued by an individual issuer.

(2) Third parties relying on certificates issued by an individual issuer must:

- carefully consider all risk and accountability options in the use of certificates and define policy on how to use it;
- use software and hardware to authenticate the signature/other cryptographic operation by which all requirements for the safe use of certificates can be checked in a credible way;
- Inform the issuer if they learn that the private keys of the certificate holder, on which they rely, have been at risk in a way that affects the reliability of the use, or if there is a risk of misuse or if the information given in the certificate has changed,
- manage documents;
- to take account of other provisions contained in any mutual agreement,
- follow any issuer's instructions or recommendations relating to reliable use;
- immediately inform the issuer of any errors or problems,
- take note of this policy and take into account all provisions on their obligations, responsibilities, and limitations on trust and the use of certificates,
- monitor and comply with any notices and notices issued by the issuer,
- take account of any other rules which are outside the scope of the issuer's jurisdiction and which are laid down elsewhere.

(3) Third parties shall bear all the consequences of any failure to comply with the terms of that policy, the possible agreement with the SI-TRUST and the applicable legislation.

1.1.184. Obligations and responsibilities of other entities

Not prescribed.

9.7. Contestation of liability

The SI-TRUST shall not be liable for damage caused by:

- the use of certificates for the purpose and in a manner not specifically provided for in the policy of the individual issuer or any agreement reached between the holder and the organisation and the SI-TRUST,
- incorrect or lack of protection of the holders' passwords or private keys, issuing of confidential data or key to third parties and irresponsible behaviour of the holder,

- misuse or intrusion into the holder's information system and thus data on certificates by unauthorised persons;
- the failure or malfunctioning of the information infrastructure of the certificate holder or of third parties,
- non-verification of data and validity of certificates,
- failure to verify the period of validity of the certificate,
- the behaviour of the certificate holder or the third party, contrary to the notifications of the individual issuer, the policy, the agreement (s), if any, and the other regulations,
- facilitate the use or misuse of the holder's attestation by unauthorised persons,
- certificates with false data and inaccurate data or other acts of the holder or organisation issued,
- the use of certificates and the validity of certificates in the event of changes in the certificate or changes in particulars of the holder or organisation,
- failure of the infrastructure which is not under the management of the SI-TRUST,
- data to be encrypted or signed using corresponding certificates/private keys,
- the behaviour of the holders in the use of the certificates, even if the holder or the third party has complied with all the provisions of that policy and arrangement and has informed the individual issuer or other applicable rules,
- the use and reliability of the operation of certificate holders' hardware and software.

9.8. Limits of liability

The provisions are defined in each policy.

9.9. Redress

The applicant shall be liable for the damage caused by non-compliance with the provisions of this policy, the legislation in force and any reciprocal arrangements.

9.10. policy validity

1.1.185. Duration

The new version (s) of the SI-TRUST policy 7 (7) days before force will be pre-published on the SI-TRUST website with the date of its entry into force.

1.1.186. End of the policy period

(1) The end of the policy is not determined and linked to the validity of certificates issued on the basis of a policy.

(2) At the time of publication of the new policy, all certificates issued on the basis of that policy shall remain in force in force, which cannot reasonably be replaced by appropriate provisions under the new policy (for example, the procedure establishing the manner in which the certificate was issued, etc.).

(3) For individual provisions of the policies in force, an individual issuer may issue amendments such as that made in the sub-area. 9.12YES/NO.

1.1.187. Effect of the policy expiry

(1) When a new policy is issued, all digital certificates issued or renewed after that date are dealt with under the new policy.

(2) The new policy does not affect the validity of certificates issued under previous policies. Such certificates shall remain valid until the end of their expiry and, where possible, shall be dealt with under the new policy.

9.11. Communication between entities

(1) The contact details of the provider of the trust service or the individual issuer are published on the website and set out in the sub-area. **Napaka! Vira sklicevanja ni bilo mogoče najti.**YES/NO.

(2) The contact details of the holder (s) and/or of the organisation (s) are given in the requests and any mutual agreement (s).

(3) The third party contact details are provided in a possible mutual agreement between the third party and the SI-TRUST.

(4) The individual issuer shall keep the other entities informed by means of notices published on the Internet and by e-mail.

(5) The individual as well as the third party may determine the method of communication by mutual agreement.

(6) The root issuer SI-TRUST Rouot and the external issuer can determine the mode of communication by mutual agreement.

9.12. amendment of a document

1.1.188. Procedure for the application of amendments

(1) Before any change occurs in the SI-TRUST policy, the Authority shall inform the supervisory authority of any planned change in the provision of its qualified trust services, as well as of any intention to cease the provision of those services.

(2) The SI-TRUST reserves the right to amend this document without prior information of the holders and other entities, provided that the changes do not affect the intended use and the management procedures capable of changing the level of trust.

(3) Amendments or additions to the present policy may be published by an individual issuer in the form of amendments to that policy where no significant changes are made to the functioning of the issuer.

(4) The amendments shall be adopted by the same procedure as the policy.

(5) The holders/prospective holders may submit their observations to the SI-TRUST by email with regard to the policy content considered by the SI-TRUST. The SI-TRUST reserves the right to take the comments into account at their discretion.

1.1.189. Validity and publication of amendments

The SI-TRUST policy changes seven (7) days before entry into force on the SI-TRUST website under the new document identification code (CP $_{OID}$) and the date of its entry into force.

1.1.190. Change of the policy identification code

(1) The new policy version of an individual issuer shall be identified by the new document identifier (CP $_{OID}$).

(2) The root broadcaster SI-TRUST Root, or its related issuers, shall assess whether or not the amendments adopted require the allocation of new policy identification codes (CP $_{OIDs}$) to be used in the certificates issued to end-users. If the change affects the intended use or the management procedures that can change the level of trust, they must assign new policy identification marks.

9.13. procedure in case of disputes

(1) The parties will endeavour to settle the disputes amicably or, if this is not possible, the Court of Ljubljana has jurisdiction to settle the dispute. The dispute settlement parties shall agree exclusively on the application of the provisions of the Republic of Slovenia.

(2) In the case of integration of the root broadcaster SI-TRUST Root with issuers located outside the Republic of Slovenia, the proceedings shall be determined by mutual agreement or the agreement in the case of disputes.

9.14. applicable legislation

The SI-TRUST and the individual issuer shall 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,
- A Regulation implementing Regulation (EU) on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (Official Gazette of the Republic of Slovenia No 46/16);
- 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 (Official Journal of the EU, L 119/1),
- The law on the protection of personal data;
- The Law on classified information;
- recommendations of ETSI in the field of qualified certificates and trust services;
- recommendations of RFC in the area of X.509 certificates,
- and other applicable regulations and recommendations.

9.15. compliance with applicable law

Monitoring of compliance of the operation with the applicable legislation and regulations laid down in the sub-heading. 9.14It shall be carried out by the competent inspection service (see sub-heading. 8.2).

9.16. General provisions

1.1.191. Comprehensive deal

The provisions of this policy shall not in any way alter, restrict or otherwise affect liabilities, liabilities and guarantees under the SI-TRUST under other contracts or arrangements, or other applicable legislation.

1.1.192. Assignment of rights

The certificate issued by an individual issuer to the holder, as well as any rights attached to the use of the Certificate, shall be exclusively reserved to the holder and shall not be transferable to any third party.

1.1.193. Independence identified by

Any one of the terms of a policy or a possible agreement or contract is or becomes invalid, has no bearing on other provisions. The term ‘invalid’ shall be replaced by a term which must be as close as possible to the purpose for which the term is invalid.

1.1.194. Receivables

Not specified.

1.1.195. Force majeure

The SI-TRUST shall not be liable for damage caused by force majeure which the trust service provider does not have the power to influence, such as acts of war, acts of terrorism, unrest, natural disasters, etc.

9.17. Miscellaneous provisions

1.1.196. Understanding

The policy mix uses a male self-permanent form which refers to *both sexes. All terms written in the singular refer to the plural and vice versa.*

1.1.197. Conflicting provisions

Where the provisions of this policy conflict with the provisions of any contract or arrangement between the SI-TRUST and the holder or a third party, the terms of the contract or arrangement shall apply.

1.1.198. Derogation from the provisions of

If, on an exceptional basis, an individual issuer departs from the specific provisions of that policy in a particular case, that does not mean that the exemption would continue to apply in future and in all other cases.

1.1.199. Cross verification