State Centre for Services of Confidence

Issuer of qualified digital certificates for service for
on-line registration and e-signing for SI-PAS-SCA

SI-TRUST
SI-PASS-CA

SI-PASS-CA POLICY

for a qualified digital certificate for online registration and e-signature

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

validity: From 1 October 2019
version: 2.1

CP $_{Name}$: SI-SC-SCA

- **Policy for a qualified digital certificate for natural persons for a qualified electronic signature** of
  CP $_{OID}$: 1.3.6.1.4.1.6105.7.1.1
- **Policy for natural persons**
  CP $_{OID}$: 1.3.6.1.4.1.6105.7.2.1
- **Normalised digital certificate policy for natural persons**
  CP $_{OID}$: 1.3.6.1.4.1.6105.7.3.1

Policy history

Issuing of policies for the operation of the SI-PASS-CA	
version: 2.1, valid: from 1 October 2019	
• SI-Pass-CA policy for qualified digital certificates for natural persons for a qualified electronic signature, CP $_{OID}$: 1.3.6.1.4.1.6105.7.1.1 • SI-Pass-CA policy for natural persons qualified digital certificates, CPID: 1.3.6.1.4.1.6105.7.2.1. • SI-Pass-CA policy for normalised digital certificates for natural persons, CPID: 1.3.6.1.4.1.6105.7.3.1 CP $_{Name}$: SI-SC-SCA	*Revision of the document*
version: 2.0, valid: from 28 May 2018	
• SI-Pass-CA policy for qualified digital certificates for natural persons for a qualified electronic signature, CP $_{OID}$: 1.3.6.1.4.1.6105.7.1.1 • SI-Pass-CA policy for natural persons qualified digital certificates, CPID: 1.3.6.1.4.1.6105.7.2.1. • SI-Pass-CA policy for normalised digital certificates for natural persons, CPID: 1.3.6.1.4.1.6105.7.3.1 CP $_{Name}$: SI-SC-SCA	*Changes with version 2.0:* • *editorial changes to the policy are made.* • *the specific method of obtaining a one-time password for odour can be abolished on the basis of a declaration in the SI-PASS service with a qualified digital certificate in a secure electronic signature tool issued in Slovenia.* • *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 28 June 2016	
• SI-Pass-CA policy for qualified digital certificates for natural persons for a qualified electronic signature, CP $_{OID}$: 1.3.6.1.4.1.6105.7.1.1 • SI-Pass-CA policy for natural persons qualified digital certificates, CPID: 1.3.6.1.4.1.6105.7.2.1. • SI-Pass-CA policy for normalised digital certificates for natural persons, CPID: 1.3.6.1.4.1.6105.7.3.1 CP $_{Name}$: SI-SC-SCA	*//OR*

CONTENT

1 INTRODUCTION 11

1.1 Review 11

1.2 Identification data of the operation policy 11

1.3 PKI participants 12
1.3.1 Trust service provider 12
1.3.2 Registration Authority 14
1.3.3 Certificate holders 15
1.3.4 Third persons 15
1.3.5 Other Participants 15

1.4 Purpose of the use of certificates 15
1.4.1 Correct use of certificates and keys 15
1.4.2 Unauthorised use of certificates and keys 16

1.5 Policy management 16
1.5.1 Policy Manager 16
1.5.2 Contact persons 16
1.5.3 Person responsible for the compliance of the issuer's operations with the policy 16
1.5.4 Procedure for the adoption of a new policy 16

1.6 Terms and abbreviations 16
1.6.1 Terms 16
1.6.2 Abbreviations 16

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES 16

2.1 Repositories 16

2.2 Publication of certificate information 16

2.3 Frequency of publication 17

2.4 Access to repositories 17

3 IDENTITY AND AUTHENTICITY 17

3.1 Naming 17
3.1.1 Name (s) of name (s) 17
3.1.2 Requirement to make sense of names 18
3.1.3 Use of anonymous names or pseudonyms 18
3.1.4 Rules for the interpretation of names 19
3.1.5 Uniqueness of names 19
3.1.6 Recognition, credibility and role of trade marks 19

3.2 Initial identity validation 19
3.2.1 Method for demonstrating private key ownership 19
3.2.2 Identification of organisations 19
3.2.3 Identity check 19
3.2.4 Non-verified initial verification data 20
3.2.5 Validation of authority 20
3.2.6 Criteria for interoperation 20

3.3 Identity and authenticity at the occasion of renewal of the certificate 20
3.3.1 Identity and credibility in the event of renewal 20
3.3.2 Identity and authenticity upon renewal after cancellation 20

3.4 Identity and authenticity at the request of cancellation 20

4 MANAGEMENT OF CERTIFICATES 20

4.1 Application for a certificate 20
4.1.1 Who can apply for a certificate 21
4.1.2 Enrolment process and responsibilities 21

4.2 Procedure for receipt of an application for a certificate 21
4.2.1 Verification of the identity and credibility of the prospective holder 21
4.2.2 Approval/rejection of the application 22
4.2.3 Time to issue the certificate 22

4.3 Issue of certificate 22
4.3.1 Issuer's procedure at the time of issue of the certificate 22
4.3.2 Notification by the holder of the issuing of a certificate 23

4.4 Certificate acceptance 23
4.4.1 Certificate acceptance procedure 23
4.4.2 Publication of the certificate 24
4.4.3 Notice of issue to third parties 24

4.5 Use of certificates and keys 24
4.5.1 Use of the certificate and private key of the holder 24
4.5.2 Use of the certificate and public key for third parties 25

4.6 Re-certification of the certificate without changes in public key 25
4.6.1 Grounds for re-certification 25
4.6.2 Who may request a reissue 25
4.6.3 Procedure for re-issuing the certificate 25
4.6.4 Notification to the holder of the issue of a new certificate 25
4.6.5 Acceptance of a re-certificate 25
4.6.6 Publication of a re-certificate 25
4.6.7 Issue notice to other entities 26

4.7 Renewal of certificate 26
4.7.1 Circumstances for certificate re-key 26
4.7.2 Who can ask for a renewal of the certificate 26
4.7.3 Procedure for renewal of certificate 26
4.7.4 Notification to the holder of renewal of a certificate 26
4.7.5 Acceptance of a renewed certificate 26
4.7.6 Publication of a renewed certificate 26
4.7.7 Issue notice to other entities 26

4.8 Certificate modification 26
4.8.1 Grounds for the change of certificate 27
4.8.2 Who can request a change 27
4.8.3 Procedure at the time of the amendment of the certificate 27
4.8.4 Notification to the holder of the issue of a new certificate 27
4.8.5 Acceptance of the amended certificate 27
4.8.6 Publication of the amended certificate 27
4.8.7 Issue notice to other entities 27

4.9 Certificate revocation and suspension 27
4.9.1 Reasons for cancellation 27
4.9.2 Who may request cancellation 28
4.9.3 Cancellation procedure 28
4.9.4 Time to issue cancellation request 28
4.9.5 Time spent on cancellation request received until revocation 28
4.9.6 Requirements for verification of the register of certificates for third parties withdrawn 29
4.9.7 Frequency of publication of the certificate withdrawn 29
4.9.8 Time until the date of publication of the register of certificates cancelled 29

4.9.9 Verification of the status of certificates 29
4.9.10 Requirements for continuous verification of the status of certificates 29
4.9.11 Other means of access to certificate status 29
4.9.12 Other requirements for private key abuse 29
4.9.13 Grounds for suspension 29
4.9.14 Who may request the suspension 29
4.9.15 Procedure for the suspension 29
4.9.16 Time of suspension 30

4.10 Verification of the status of certificates 30
4.10.1 Access for verification 30
4.10.2 Availability 30
4.10.3 Other options 30

4.11 End of subscription 30

4.12 Detection of a copy of the decryption keys 30
4.12.1 Procedure for detection of decryption keys 30
4.12.2 Procedure for the detection of the meeting key 30

5 GOVERNANCE AND SECURITY CONTROLS OF INFRASTRUCTURE 30

5.1 Physical security 30
5.1.1 Location and structure of the trust service provider 31
5.1.2 Physical access to the infrastructure of the trust service provider 31
5.1.3 Power and air conditioning 31
5.1.4 Water exposures 31
5.1.5 Fire prevention and protection 31
5.1.6 Media management 31
5.1.7 Disposal 31
5.1.8 Off-site backup 31

5.2 Organisational structure of the issuer/trust service provider 31
5.2.1 Organisation of a trust and trusted service provider 31
5.2.2 Number of persons required per task 31
5.2.3 Identity of individual applications 32
5.2.4 Roles requiring separation of duties 32

5.3 Personnel controls 32
5.3.1 Qualifications, experience and clearance requirements 32
5.3.2 Background check procedures 32
5.3.3 Staff training 32
5.3.4 Training requirements 32
5.3.5 Job rotation frequency and sequence 32
5.3.6 Sanctions 32
5.3.7 Independent contractor requirements 32
5.3.8 Documentation supplied to personnel 33

5.4 System security checks 33
5.4.1 Species of log 33
5.4.2 Frequency of processing log 33
5.4.3 Retention period for audit log 33
5.4.4 Protection of audit log 33
5.4.5 Audit log backup procedures 33
5.4.6 Data collection for audit logs 33
5.4.7 Notification to event-causing subject 33
5.4.8 Assessment of system vulnerabilities 33

5.5 Retention of information 33
5.5.1 Types of record archived 34

5.5.2 Retention period 34
5.5.3 Protection of archive 34
5.5.4 System archive and storage 34
5.5.5 Requirement of time stamping 34
5.5.6 Data collection how archived data can be collected 34
5.5.7 Procedure for access to, and verification of, archived data 34

5.6 Renewal of the issuer's certificate 34

5.7 Compromise and disaster recovery 34
5.7.1 Incident and compromise handling 34
5.7.2 Procedure in the event of a breakdown of hardware and software or data 34
5.7.3 Entity private key compromise procedures 35
5.7.4 Compromise and disaster recovery 35

5.8 Extinction of the issuer 35

6 TECHNICAL SAFETY REQUIREMENTS 35

6.1 Key generation and positioning 35
6.1.1 Key generation 35
6.1.2 Delivery of private key to holders 35
6.1.3 Delivery of the certificate to the issuer of the certificates 36
6.1.4 Delivery of the issuer's public key to third parties 36
6.1.5 Key length 36
6.1.6 Generating and quality of public key parameters 36
6.1.7 Key purpose and certificates 36

6.2 Private key protection and security modules 36
6.2.1 Cryptographic module standards 36
6.2.2 Private key control by authorised persons 37
6.2.3 Detecting a copy of the private key 37
6.2.4 Backup of private keys 37
6.2.5 Private key archiving 37
6.2.6 Transfer of private key from/to cryptographic module 37
6.2.7 Private key record in a cryptographic module 37
6.2.8 Procedure for the activation of the private key 37
6.2.9 Procedure for deactivation of the private key 38
6.2.10 Procedure for the destruction of the private key 38
6.2.11 Cryptographic module characteristics 38

6.3 Key Management Aspects 38
6.3.1 Preservation of public key 38
6.3.2 Certificate and key validity period 38

6.4 Access passwords 38
6.4.1 Password generation 38
6.4.2 Password protection 39
6.4.3 Other aspects of passwords 39

6.5 Safety requirements for issuing computer equipment by the issuer 39
6.5.1 Specific technical safety requirements 39
6.5.2 Level of security protection 39

6.6 Issuer's life cycle technical control 39
6.6.1 Control of the evolution of the system 39
6.6.2 Managing safety 39
6.6.3 Life cycle control 39

6.7 Network security controls 40

6.8 Time-stamping 40

7 CERTIFICATE PROFILE, CERTIFICATE WITHDRAWN AND ONGOING VERIFICATION OF CERTIFICATE STATUS 40

7.1 Certificate Profile 40
7.1.1 Certificate version 40
7.1.2 Profile of extensions 40
7.1.3 Algorithm identification markings 42
7.1.4 Name (s) of name (s) 42
7.1.5 Restriction on names 43
7.1.6 Certificate policy code 43
7.1.7 Use of expansion field to limit policy use 43
7.1.8 Format and treatment of specific policy information 43
7.1.9 Consideration of a critical enlargement policy field 43

7.2 Register of invalidated certificates 43
7.2.1 Version 43
7.2.2 Content of the register and extensions 43

7.3 Confirmation of confirmation of the status of certificates on an up-to-date basis 44
7.3.1 Version 44
7.3.2 Extensions to ongoing status check 45

8 INSPECTION 45

8.1 Inspection frequency 45

8.2 Technical inspection body 45

8.3 Independence of the inspection service 45

8.4 Areas of inspection 45

8.5 Actions of the trust service provider 45

8.6 Publication of inspection results 45

9 OTHER BUSINESS AND LEGAL AFFAIRS 45

9.1 Fee schedule 45
9.1.1 Issuance price and renewal of certificates 45
9.1.2 Access price for certificates 46
9.1.3 Access price of the certificate and a register of cancelled certificates 46
9.1.4 Prices of other services 46
9.1.5 Reimbursement of expenses 46

9.2 Financial responsibility 46
9.2.1 Insurance coverage 46
9.2.2 Other cover 46
9.2.3 Holders' insurance 46

9.3 Protection of commercial information 46
9.3.1 Protected data 46
9.3.2 Non-safeguarded data 46
9.3.3 Liability with regard to the protection of commercial information 46

9.4 Protection of personal data 47
9.4.1 Privacy plan 47
9.4.2 Protected personal data 47
9.4.3 Personal data not protected 47
9.4.4 Responsibility for the protection of personal data 47
9.4.5 Power of attorney concerning the use of personal data 47
9.4.6 Transfer of personal data to official request 47

9.4.7 Other provisions concerning the transfer of personal data 47

9.5 Provisions concerning intellectual property rights 47

9.6 Liability and accountability 47
9.6.1 Obligations and responsibilities of the issuer 48
9.6.2 Obligation and responsibility of the registration service 48
9.6.3 Liability and liability of the holder 48
9.6.4 Liability and liability of third parties 48
9.6.5 Obligations and responsibilities of other entities 49

9.7 Contestation of liability 49

9.8 Limits of liability 49

9.9 Redress 49

9.10 Policy validity 49
9.10.1 Duration 49
9.10.2 End of the policy period 49
9.10.3 Effect of the policy expiry 49

9.11 Communication between entities 49

9.12 Amendment of a document 49
9.12.1 Procedure for the application of amendments 49
9.12.2 Validity and publication of amendments 50
9.12.3 Change of the policy identification code 50

9.13 Procedure in case of disputes 50

9.14 Applicable legislation 50

9.15 Compliance with applicable law 50

9.16 General provisions 50
9.16.1 Comprehensive deal 50
9.16.2 Assignment of rights 50
9.16.3 Independence identified by 50
9.16.4 Receivables 50
9.16.5 Force majeure 50

9.17 Miscellaneous provisions 51
9.17.1 Understanding 51
9.17.2 Conflicting provisions 51
9.17.3 Derogation from the provisions of 51
9.17.4 Cross verification 51

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.

Within the SI-TRUST, an issuer of qualified digital certificates of the SI-PASS-CA is operational. *Slovenian Authentication and e-Signature Service Certification Authority,* https://www.si-trust.gov.si/sl/si-pass/, which issues certificates for physical persons for the purpose of the online registration and e-Signature service of the SI-PASS.

The SI-Pass-CA issuer is registered in accordance with the applicable legislation and recognised by the root issuer of the SI-TRUST Root. *Slovenian Trust Service Root Certification Authority*.

The policy of operation of the SI-PASS-CA defines the internal rules of operation of the issuing body 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 an issuer of SI-PASS-CA for qualified digital certificates to be issued for the purpose of the online registration and e-Signature service of the SI-PASS. On the basis of this

document, SI-PASS-CA issues digital certificates that meet the highest safety requirements, according to the following policies: CP $_{OID}$: 1.3.6.1.4.1.6105.7.1.1, CP $_{OID}$: 1.3.6.1.4.1.6105.7.2.1 and CP $_{OID}$: 1.3.6.1.4.1.6105.7.3.1

This document replaces the previous published SI-PASS-CA policy for qualified digital certificates issued for the purpose of the online registration and e-Signature service of the SI-PASS. 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 identification marks (CP $_{OIDs}$) are not altered.

Following this policy, the SI-PASS-CA issues the following digital certificates:

- qualified digital certificates for natural persons for qualified electronic signatures,
- qualified digital certificates for natural persons; and
- normalised digital certificates for natural persons.

Digital certificates are obtained on the basis of a request submitted by the prospective holder electronically using the SI-PASS user pages on the basis of a declaration in the SI-PASS service.

In order to obtain a qualified digital certificate for natural persons for a qualified electronic signature, the prospective holder of a certificate in the SI-PASS service may apply one of the following ways:

- with a one-time password;
- with a qualified digital certificate in a secure electronic signature means;
- using an electronic ID level assurance level ‘high’ in accordance with eIDAS.

In order to obtain a qualified digital certificate for natural persons, the prospective holder of the certificate in the SI-PASS service may be declared in one of the following ways:

- with a qualified digital certificate,
- the electronic identification of the level of assurance ‘medium’ under the eIDAS.

In order to obtain a normalised digital certificate for natural persons, the prospective holder of the certificate in the SI-PASS service may apply to one of the other applications supported by the SI-PASS.

In the case of an approved request of the SI-PASS-CA, the holder of the certificate shall be issued to the prospective holder of the certificate as soon as the application has been approved.

The holder’s digital certificate is linked to one pair of keys generated by a dedicated machine security module, which is used as a secure electronic signature tool operated by the originator of the SI-Pass-CA. the SI-Pass-CA is stored in encrypted form by the holders of the private key in a dedicated secure database and shall not have access to it. The private key shall be located outside the dedicated hardware security module only in encrypted form. The holder shall have access to the private key of the holder in unencrypted form only the holder.

In addition to the data included in the digital certificate, the SI-CA holds the other necessary details of the holder for the purpose of electronic commerce, in accordance with the rules in force.

The holder must ensure that the application form used in the SI-PASS service is not compromised and that the password for protection of the private key is protected and the policy followed, the SI-PASS-CA and the applicable legislation are followed up.

1. INTRODUCTION

1.1. Review

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

(2) Within the SI-TRUST, an issuer of qualified digital certificates of the SI-PASS-CA is operational. *Slovenian Authentication and e-Signature Service Certification Authority,* https://www.si-trust.gov.si/sl/si-pass/, which issues certificates for physical persons for the purpose of the online registration and e-Signature service of the SI-PASS.

(3) The SI-Pass-CA issuer is registered in accordance with the applicable legislation and recognised by the root issuer of the SI-TRUST Root. *Slovenian Trust Service Root Certification Authority*.

(4) Following this policy, the SI-Pass-CA policy for the online registration and e-signing service of the SI-PASS gives the following digital certificates:

- qualified digital certificates for natural persons for qualified electronic signatures,
- qualified digital certificates for natural persons; and
- normalised digital certificates for natural persons.

YES/NO.

(5) The SI-Pass-CA digital certificates may be used for:

- authentication of digitally signed data,
- services or applications for which the use of qualified digital certificates are required under the SI-TRUST.

(6) For certificates issued on the basis of this policy, it is necessary to follow the recommendations made by the originator of SI-PASS-CA for the protection of private keys.

(7) The present policy is prepared in line with RFC 3647 " Internet X.509 Public Key Infrastructure Certificate and Certification Practices Framework", which provides for the internal rules of the issuing party SI-PASS-CA, 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 the digital certificates of the SI-PASS-CA, third parties relying on digital certificates, and other entities that comply with the provisions of the SI-Pass-CA issuer.

(8) Mutual relationships between third parties relying on the attestations of the issuer of SI-PASS-CA and the SI-TRUST shall also be implemented on the basis of a possible written agreement.

(9) The SI-TRUST may liaise with other trust service providers through the root issuer of the SI-TRUST, governed by mutual agreement.

1.2. Identification data of the operation policy

(1) The present document is the SI-Pass-CA policy for a qualified digital certificate for the online registration and e-signature service (hereinafter " *SI-Pass-CA policy*").

(2) This policy code is CP $_{Name}$: The SI-PASS-CA and the SI-Pass-CA policy identification markings vary according to the type of certificate:

- CP $_{OID}$: 1.3.6.1.4.1.6105.7.1.1 for qualified digital certificates for natural persons,
- CP $_{OID}$: 1.3.6.1.4.1.6105.7.2.1 for qualified digital certificates for natural persons, and
- CP $_{OID}$: 1.3.6.1.4.1.6105.7.3.1 for normalised digital certificates for natural persons.

(3) Each certificate shall contain an indication of the relevant policy in the form of a CP_{OID} code, see below. 7.1.2 YES/NO.

1.3. PKI participants

1.3.1 Trust service provider

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

(2) Under the SI-TRUST, an issuer of qualified digital certificates for the SI-PASS-CA is operational.

(3) The contact details of the originator of the SI-PASS-CA are:

Address:	SI-SC-SCA State Centre for Services of Confidence Ministry of Public Administration Tržaška cesta 21 1000 Ljubljana
E-mail:	si-pass-ca@gov.si
Tel:	01 4788 330
Website:	https://www.si-trust.gov.si
Hotline number for cancellations (24 hours total year):	01 4788 777
Single contact centre:	080 2002, 01 4788 590 ekc@gov.si

(4) The issuer of the SI-PASS-CA carries out the following tasks:
- issuance of a qualified and normalised digital certificate;
- sets out and publishes its policy of action;
- sets out the claim forms for their services,
- it sets out and publishes instructions and recommendations for the safe use of its services;
- publish a register of cancelled certificates;
- ensure the smooth functioning of its services, in line with policy and other regulations,
- inform its users;
- he/she is in charge of the functioning of his/her application office and
- provides all other services in accordance with this policy and with other regulations.

(5) At the start of its production operation, the issuer of the SI-PASS-CA has generated its own digital certificate, which is intended to certify the certificates issued by the SI-Pass-CA to the holders.

The SI-Pass-CA certificate shall contain the following information[1]:

Field name	Value of the ECS certificate issued by SI-PASS-CA
R azlic, \ "_blank" *Version*	3
ID, *Serial Number*	5A2A3BA 0000 0000 574E AE10

[1] The meaning is given in the pogs. 3.1 and 7.1.

Signature algorithm, \ "_blank" *Signature Algorithm*	sh256WithRSAEncrConsumption
Issuing body, \ "_blank" *Issuer*	c = SI, o = the Republic of Slovenia, oi = VAT-17659957, cn = SI-PASS-CA
Holder, *Subject*	c = SI, o = the Republic of Slovenia, oi = VAT-17659957, cn = SI-PASS-CA
Date of entry into force, *Validity: Not Before*	June 1 09: 12: 41 2016 GMT
End of validity, *Validity: Not After*	June 1 09: 42: 41 2036 GMT
Public Key Algorithm, \ "_blank" *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, \ "_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*	4832 CA46 4E33 CB0A
The identifier of the holder's key; OID 2.5. *29.14,* \ *"_blank" Subject Key Identifier*	4832 CA46 4E33 CB0A
Certificate footprint (not part of the certificate)	
SHA-1 certificate footprint, *Certificate Fingerprint — SH* A-1	271E 1C16 BC2C 72DE 1243 9F79 CD9B 3FAE FECA 2E78
SHA-256 certificate footprint, *Certificate Fingerprint — SH* A-256	10D4 20E2 C8BF E438 D696 7038 16E1 58E4 79C8 D825 82AC 691B9 ACD4 51B7 4986

(6) The root issuer SI-TRUST Root has issued a liaison certificate for the issuer of the SI-Pass-CA with the following data:

Field names	Value or importance
Certificate (s) of the underlying (s) in the certificate	
Version \ "_blank" *Version*	3
ID, *Serial Number*	9D0E9E3A 0000 0000 571D10C
Signature algorithm, \ "_blank" *Signature Algorithm*	sh256WithRSAEncrConsumption
Issuing body, \ "_blank" *Issuer*	c = SI, o = the Republic of Slovenia, oi = VAT-17659957, cn = SI-TRUST Root
Holder, *Subject*	c = SI, o = the Republic of Slovenia, oi = VAT-17659957, cn = SI-PASS-CA
Date of entry into force, *Validity: Not Before*	June 10 10: 24: 15 2016 GMT

End of validity, *Validity: Not After*	May 30 22: 00: 00 2036 GMT
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, \ "_blank" *RSA Public Key*	*3072 bit length key*
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 Rot, OI = VATSI-17659957, o = the Republic of Slovenia, c = SI? certificateRequationList c = SI, o = the Republic of Slovenia, OI = VATSI-17659957, CN = SI-TRUST Root, CN = CRL1
Access to information on the issuer, OID 1.3.6.1.5.5.7.1.1, \ "_blank" *Authority Information Access*	Access Method = OCSP http://ocsp.ca.gov.si Access Method = CA Issuers http://www.ca.gov.si/crt/si-trust-root.crt
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)
The policy under which the certificate was issued, OID 2.5.29.32, certificatePolicies	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/
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*	4832 CA46 4E33 CB0A
Certificate footprint (not part of the certificate)	
SHA-1 certificate footprint, *Certificate Fingerprint — SH* A-1	4FAE 2C20 DED9 3559 4D57 D544 19D5 0D3A 496B B8D7
SHA-256 certificate footprint, *Certificate Fingerprint — SH* A-256	B394 3BD0 C0FF B4B4 1C9E1AD E986 ABE3 3583 12D6 AA6C 5DD2 45B7B0D 63A5 F851

1.3.2 Registration Authority

(1) The organisation carrying out the functions of the registration service authorises the SI-TRUST. They must

comply with the tasks of the SI-TRUST, application services and comply with the regulations and procedures in place for the work of the emergency services TSI SI-TRUST.

(2) The role of the application service is:
- verification of the identity of the holders/future holders, their data and other necessary data,
- accepting applications for certificates,
- verification of claims data,
- issue the necessary documentation to the holders or future holders,
- transmission of requests and other data in a secure manner to SI-PAS-SCA.

(3) The SI-Pass-CA issuer has a wide range of facilities in place in various locations, and the data on this is published on the websites of the SI-PASS-CA.

1.3.3 Certificate holders

Holders of certificates under this policy are always natural persons (*subject*), see the definition in a Cap. 1.6 YES/NO.

1.3.4 third persons

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

1.3.5 Other Participants

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

1.4. Purpose of the use of certificates

(1) The SI-SCk-CA certificates issued in this policy can be used for:
- authentication of digitally signed data,
- services or applications for which the use of qualified digital certificates are required under the SI-TRUST.

(2) The holder's digital certificate is linked to one pair of keys generated by a dedicated machine security module, which is used as a secure electronic signature tool operated by the originator of the SI-PASS-CA.

(3) The use of certificates is linked to the purpose of the corresponding keys. The following options are distinguished:
- The private signing key (hereinafter referred to as the *private key*); and
- The public key to authenticate the signature (hereinafter referred to as *public key*).

(4) The authorising officer SI-PASS-CA also issues certificates for an OCSP for verifying the validity of certificates issued by the SI-Pass-CA.

1.4.1 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*).

(2) Each certificate holder shall belong to one pair of keys, which shall consist of a private and public key to sign/authenticate the signature.

1.4.2 Unauthorised use of certificates and keys

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

1.5. Policy management

1.5.1 Policy Manager

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

1.5.2 contact persons

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

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

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

1.5.4 Procedure for the adoption of a new policy

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

1.6. terms and abbreviations

1.6.1 Terms

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

1.6.2 Abbreviations

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

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

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 information from the originator of the SI-PASS-CA:
- the policy of the operation of the issuer;
- price list,
- claims for services provided by the issuer,
- instructions for the safe use of the digital certificates;
- information on the applicable legislation concerning the operation of the SI-TRUST and
- other information related to the functioning of the SI-PASS-CA.

(2) In the structure of a public digital certificate directory, located on the x500.gov.si *server, it publishes a* register of invalidated digital certificates (given in more detail below. 7.2).

(3) The other documents or key information on the functioning of the originator of the SI-PASS-CA and the general notices to the holders and to third parties are published on the websites https://www.si-trust.gov.si.

(4) The confidential part of the internal rules of the SI-TRUST, within which the issuer of the SI-PASS-CA operates, is not a publicly available document.

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

2.3. frequency of publication

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

2.4. Access to repositories

(1) Publicly available information/documents and a register of cancelled certificates are available without restrictions.

(2) The public directory, which holds a register of cancelled certificates, is publicly available *on* the x500.gov.si LDAP.

(3) In accordance with the SI-TRUST, the SI-TRUST or the issuing of SI-SCk-CA is responsible for the authorised and secure management of data in a public directory.

3. IDENTITY AND AUTHENTICITY

3.1. naming

3.1.1 name (s) of name (s)

(1) 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 UTF8String or PrintableString according to RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Ref. resolution List (CRL)” and standard X.501.

(2) Each certificate issued is issued by the *issuer, see the* table below.

(3) The distinguishing name of the holder contains the *holder's* basic information, see the table below.

(4) Each distinguishing name shall also include a serial number as determined by the issuer of the SI-PASS-CA[2] (see below). 3.1.5).

(5) The distinguishing name shall be, according to the type of identity or certificates, according to the following rules[3].

Type of certificate	Field name	Distinguished Name[4]
certificate issued by SI-PASS-CA	Issuing body, \ "_blank" *Issuer*	c = SI, o = the Republic of Slovenia, OI = VATSI-17659957, CN = SI-PASS-CA
qualified certificate for natural persons for qualified electronic signatures	Holder, \ "_blank" *Subject*	c = SI, ST = Slovenia, MA = individuals, MA = QcQscd, cn = < name and surname >, GN = < Name >, SurName = < Surname > SN = serial number >
qualified certificate for natural persons	Holder, \ "_blank" *Subject*	c = SI, ST = Slovenia, MA = individuals, MA = Qc, cn = < name and surname > GN = < Name >, SurName = < Surname > SN = serial number >
a normalised certificate for natural persons	Holder, \ "_blank" *Subject*	c = SI, ST = Slovenia, MA = individuals, MA = Nc, cn = < name and surname > GN = < Name >, SurName = < Surname > SN = serial number >

3.1.2 requirement to make sense of names

(1) The holder of the certificate shall be unambiguously designated by a distinctive name in accordance with the previous section.

2 The certificate issued by the SI-Pass-CA issuer does not contain the serial number.

3 The rules for the production of discriminatory names for other types of certificate are laid down and published by the SI-Pass-CA.

4 importance of individual designations: country ('c'), country name ('st'), Organisation ('o'), organisational unit ('ou'), title ('cn'), name ('gn'), serial number ('sn').

(2) The owner/title data contains characters from the code table UTF-8.

3.1.3 Use of anonymous names or pseudonyms

Not foreseen.

3.1.4 rules for the interpretation of names

The rules are set out in the sub-area. 3.1.1And3.1.2.

3.1.5 uniqueness of names

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

(2) The unique serial number included in the discriminatory name is also unique.

(3) The serial number shall be a 13-digit number and uniquely identify the holder or issued the certificate. The table below specifies the meaning and value of individual lots of the serial number:

Serial number	Importance	Value	
1 rd place	label for the certificate issued by the authorising officer SI-PASS-CA	3	
2-8 City	unique number of holder	//OR	
9 — 10 rd place	tag for Service for Online Registration and eSignature	certificate for a qualified electronic signature	31
		qualified Certificate	32
		a normalised certificate	33
11 — 12 rd place	sequence number of certificates of the same type	//OR	
13 rd place	control number	//OR	

3.1.6 Recognition, credibility and role of trade marks

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

3.2. Initial identity validation

3.2.1 method for demonstrating private key ownership

The key pair shall be generated through a dedicated machine security module, which is used as a secure electronic signature medium managed by the issuer of the SI-PASS-CA, and therefore the demonstration by the prospective holder is not required. When issuing the certificate, the link between the private and the public key shall be verified using the request in the form of PKCS # 10 in accordance with RSA PKCS # 10 Certification Request Syntax Standard.

3.2.2 identification of organisations

Unspecified.

3.2.3 Identity check

(1) The verification of the identity of the holders is carried out either by the SI-TRUST or following a registration in the SI-PASS with a valid qualified digital certificate or other appropriate means of electronic identification.

(2) The SI-Pass-CA issuer shall verify the holder's personal details of the holder in the relevant registers or in the applicable qualified certificates or other electronic identification means.

3.2.4 Non-verified initial verification data

Unverified data contained in a qualified certificate. The data in the normalised certificate are not verified.

3.2.5 Validation of authority

Unspecified.

3.2.6 criteria for interoperation

(1) The SI-Pass-CA issuer is mutually recognised by the root issuer of the SI-TRUST Root.

(2) The issuer of the SI-PASS-CA shall not be associated with each other by other issuers.

(3) The SI-TRUST may liaise with other trust service providers through the root issuer of the SI-TRUST, governed by mutual agreement.

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

3.3.1 Identity and credibility in the event of renewal

The control of the holders shall be carried out in accordance with the provisions laid down in the subsection. 3.2.3YES/NO.

3.3.2 Identity and authenticity upon renewal after cancellation

The control of the holders shall be carried out in accordance with the provisions laid down in the subsection. 3.2.3YES/NO.

3.4. Identity and authenticity at the request of cancellation

(1) The request for cancellation of the certificate shall be submitted by the holder electronically on the basis of a

declaration in the SI-PASS service, thus demonstrating the identity of the applicant.

(2) Detailed cancellation proceedings are given in the rat. 4.9.3YES/NO.

4. MANAGEMENT OF CERTIFICATES

4.1. application for a certificate

4.1.1 Who can apply for a certificate

Prospective holders of certificates are always natural persons, see definition in the rat. 1.3.3 YES/NO.

4.1.2 Enrolment process and responsibilities

(1) The application for a certificate is submitted by the future holder electronically using the SI-PASS user pages on the basis of a declaration in the SI-PASS service.

(2) In order to obtain a qualified digital certificate for natural persons for a qualified electronic signature, the prospective holder of a certificate in the SI-PASS service may apply one of the following ways:
- with a one-time password;
- with a qualified digital certificate in a secure electronic signature means;
- using an electronic ID level assurance level 'high' in accordance with eIDAS.

(3) In order to obtain a qualified digital certificate for natural persons, the prospective holder of the certificate in the SI-PASS service may be declared in one of the following ways:
- with a qualified digital certificate,
- the electronic identification of the level of assurance 'medium' under the eIDAS.

(4) In order to obtain a normalised digital certificate for natural persons, the prospective holder of the certificate in the SI-PASS service may apply to one of the other applications supported by the SI-PASS.

4.1.2.1 Pass the smsPASS procedure

E, then, the password of the certificate may be obtained by the prospective holder of the certificate on the basis of:
- activation codes sent to the email address following the submission of an acquisition request to the application service,
- activation codes sent to the address of the domicile, following registration in the SI-PASS service with a qualified digital certificate issued in Slovenia.

Procedure for the application service

(1) In order to obtain the pass, the prospective holder is required to fill in the application for an acquisition and to appear in person at the application department, where he/she indicates his/her identity and his/her claim in person at the application file. A claim may be submitted by a person aged over 15 years.

(2) In the event that the prospective holder is a disabled person, the request for an award may be made on his behalf by another person who must attach to that person a notarial or administrative authorisation and his valid identity document with the image.

(3) The prospective holder shall be obliged to:
- apply for genuine and correct data on the SI-PASS user pages;
- show your identity and sign in the application to the application service,
- activate the talc in a secured manner on the instructions of the authorising officer of the SI-PASS-CA.

4.2. procedure for receipt of an application for a certificate

4.2.1 Verification of the identity and credibility of the prospective holder

The prospective holder of the certificate demonstrates his identity on the basis of a registration in the SI-PASS with a valid qualified digital certificate or other appropriate means of electronic identification.

4.2.1.1 Identification to obtain a unique password for smsPASS

(1) In the case of a personal submission to an application service, an authorised person shall check the identity of the prospective holder in accordance with the legislation in force at the application service. The prospective holder must prove his/her identity by means of a valid identification document.

(2) It is necessary to verify the identity of the prospective holder or all of the information provided in the application and made available in the official records or other official documents in force.

(3) In the case of an application for PASS by an electronic means, the prospective holder shall demonstrate his identity on the basis of a declaration in SI-PASS with a valid qualified digital certificate issued in Slovenia.

4.2.2 Approval/rejection of the application

(1) Before submitting an application, the SI-Pass-CA issuer shall inform the prospective holder of any necessary documentation in accordance with the applicable legislation.

(2) The application for a certificate is granted automatically on the basis of a successful procedure for obtaining a certificate (see below. 4.1.2).

4.2.2.1 Approval of the request for a one-time password of smsPASS

(1) In case of personal submission of an application for talcum powder to the application service, the request for acquisition shall be approved or, in the case of incorrect or deficient data or a failure to comply with the obligations, the prospective holder shall be notified directly to the application service.

(2) In the case of submission of an application for odours by electronic means, the application shall be approved automatically.

4.2.3 Time to issue the certificate

Following an approved request to the prospective holder of a digital certificate, the SI-SCk-CA shall issue this certificate to the prospective holder of the digital certificate as soon as the application has been approved.

4.2.3.1 Pass time for smsPASS

(1) In the case of a personal submission to the SI-Pass-CA application service, an e-mail address shall be transmitted to the prospective TalASS holder by an email address immediately after the request has been approved.

(2) In the case of an electronic claim for talc based on a declaration in the SI-PASS service, a qualified digital certificate issued in Slovenia, the SI-PASS-CA will send the holder of the TalPASS holder the activation code to the address of the domicile no later than ten (10) days from the date of approval of the request.

4.3. issue of certificate

4.3.1 Issuer's procedure at the time of issue of the certificate

(1) In the case of an approved request of the SI-PASS-CA, the holder of the certificate shall be issued to the prospective holder of the certificate as soon as the application has been approved.

(2) Certificates shall be issued exclusively on the SI-TRUST infrastructure.

4.3.1.1 Procedure for the issuance of the unique password of the smsPASS

(1) In case of a personal submission to the SI-Pass-CA application service, an activation code shall be provided by the SI-PASS-CA to the prospective holder of the TalPASS holder by an email address.

(2) In the case of an electronic claim programme based on a declaration in the SI-PASS service with a qualified digital certificate issued in Slovenia, the SI-PASS-CA sends to the holder of the TalPASS holder the activation code at the address of the permanent residence.
YES/NO.

4.3.2 notification by the holder of the issuing of a certificate

The holder of the certificate informed about the issue of a digital certificate on the SI-PASS user pages.

4.3.2.1 Pass notice for TalsPASS

The holder of the TalPASS is informed by the SI-PASS user pages of the version of the TalPASS user page.

4.4. Certificate acceptance

4.4.1 Certificate acceptance procedure

(1) In the case of an approved request of the SI-PASS-CA, the holder of the certificate shall be issued to the prospective holder of the certificate as soon as the application has been approved.

(2) The method and detailed instructions for acceptance of certificates under this policy are described in the SI-PASS user pages.

(3) Immediately upon receipt of the certificate, the titular holder shall check the information contained in this certificate. If the issuer of SI-PASS-CA does not notify any errors, it is considered to agree with the contents of the file and to agree to the terms of operation and assumption of liabilities and responsibilities.

4.4.1.1 Unique password activation process

(1) For the activation of the talc, the prospective holder needs the activation code issued by the SI-Pass-CA, see below. 4.3 YES/NO.

(2) In the activation process, the prospective holder shall enter his mobile telephone number, to which the SI-Pass-CA is sent a unique password by means of the entry of which the prospective holder provides evidence of the possession of a mobile telephone number and thus registers it.

(3) The method and detailed instructions for the activation of the talc under this policy are described in the SI-PASS user pages.

(4) After receipt of the activation code, the prospective holder of the talc shall actuate the single password of the talc in sixty (60) days after the approval of the talcum powder. At the request of a prospective holder, it is possible to extend the activation time for the new sixty (60), namely SI-PASS-CA, to revoke the activation code.

(5) After the activation of the odour of the odour, the activation code is not usable.

(6) The holder of the TalPASS can change the mobile phone number in the SI-PASS user pages on the basis of a declaration in the SI-PASS service.

4.4.2 Publication of the certificate

Unspecified.

4.4.3 notice of issue to third parties

Unspecified.

4.5. Use of certificates and keys

4.5.1 use of the certificate and private key of the holder

(1) The holder's private key and its certificate are securely stored on the infrastructure of the ATV issuer.

(2) Before the certificate is used, the holder must be able to sign the SI-PASS in an appropriate manner and enter a password protected by his/her private key.

(3) The holder of a qualified digital certificate for a qualified electronic signature may apply in the SI-PASS service in one of the following ways:
- with a one-time password;
- with a qualified digital certificate in a secure electronic signature means;
- using an electronic ID level assurance level 'high' in accordance with eIDAS.

(4) The holder of a qualified digital certificate for natural persons may apply in the SI-PASS service in one of the following ways:
- with a qualified digital certificate,
- the electronic identification of the level of assurance 'medium' under the eIDAS.

(5) The holder of the normalised digital certificate for natural persons can apply for the SI-PASS service to one of the other applications supported by the SI-PASS.

(6) The holder or prospective holder of the certificate shall be obliged, for the protection of the private key:
- ensure that the application form used in the SI-PASS Service is not compromised,
- the private key shall be protected by the private key, in accordance with the recommendations of the SI-PASS-CA, in such a way that it is accessible only to the holder,
- carefully protect the password for the protection of the private key;
- upon expiry of the certificate, the certificate shall be handled in accordance with the SI-PASS-CA notifications.

(7) The holder must protect the private key from unauthorised use.

(8) Other duties and responsibilities are laid down in the sub-area. 9.6.3YES/NO.

4.5.1.1 Use of the TalPASS one-time password

(1) The unique password of the odour of the odour is first registered by the SI-PASS and password, followed by a one-time password received by SMS to the registered mobile phone number.

(2) The holder, or the prospective holder, of the TalPASS is obliged to:
- it is closely protected from unauthorised persons by the data used for the activation of the talc;
- protect mobile phone numbers and associated mobile phone against unauthorised persons;
- it shall be protected by a suitable password in accordance with the SI-Pass-CA recommendations by the holder only,
- carefully protect the motto of the talcum powder;
- following the expiry date and/or withdrawal of talc, comply with the SI-PASS-CA notifications.

4.5.2 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.

4.6.1 Grounds for re-certification

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

4.6.2 Who may request a reissue

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

4.6.3 Procedure for re-issuing the certificate

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

4.6.4 Notification to the holder of the issue of a new certificate

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

4.6.5 Acceptance of a re-certificate

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

4.6.6 publication of a re-certificate

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

4.6.7 Issue notice to other entities

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

4.7. Renewal of certificate

4.7.1 Circumstances for certificate re-key

Not supported.

4.7.2 Who can ask for a renewal of the certificate

Not supported.

4.7.3 Procedure for renewal of certificate

Not supported.

4.7.4 Notification to the holder of renewal of a certificate

Not supported.

4.7.5 Acceptance of a renewed certificate

Not supported.

4.7.6 Publication of a renewed certificate

Not supported.

4.7.7 Issue notice to other entities

Not supported.

4.8. Certificate modification

(1) If there is a change in the data affecting the validity of the discriminatory name (s) in the certificate, the certificate must be cancelled.

(2) In order to obtain a new certificate, it is necessary to repeat the procedure for obtaining a new certificate, as indicated in the sub-heading. 4.1YES/NO. The service provider of an issuer for a change of certificates shall not be supported.

4.8.1 Grounds for the change of certificate

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

4.8.2 Who can request a change

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

4.8.3 Procedure at the time of the amendment of the certificate

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

4.8.4 Notification to the holder of the issue of a new certificate

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

4.8.5 Acceptance of the amended certificate

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

4.8.6 Publication of the amended certificate

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

4.8.7 Issue notice to other entities

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

4.9. Certificate revocation and suspension[5]

4.9.1 Reasons for cancellation

(1) Revocation of the certificate must be requested by the holder in the event of:
- the private key of the certificate holder has been compromised in a manner that affects the reliability of use;
- if there is a risk of misuse of the private key or certificate of the holder,
- if the incorrect key information indicated in the certificate has changed or is incorrect.

(2) The issuer of SI-PASS-CA 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,
- an error check has been made on the identity of the data at the application service,
- other circumstances affecting the validity of the certificate have changed;
- for failure of the holder to comply with the obligations of the holder,
- that the potential costs for the management of the digital certificates have 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-PASS-CA has ceased to be issuing certificates, or that the SI-TRUST has been prohibited from managing certificates and its activities has not been taken over by another trust service provider,
- revocation ordered a competent court or administrative authority.

4.9.2 Who may request cancellation

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

4.9.3 Cancellation procedure

(1) The revocation can be requested by the keeper electronically twenty four (24) hours a day, for all days of the year in the SI-PASS user pages on the basis of a TSI application.

(2) When it comes to the possibility of misuse or unreliability of the certificate, the holder may, in case of revocation or unreliability of the certificate, call the CSD hotline number twenty-four (24) hours a day, all days a year.

(3) If the operation of the SI-TRUST is significantly reduced as a result of unforeseen events and registration in the SI-PASS service is not possible, the holder of the APA cannot request, but there is no possibility of misusing his or her certificate.

(4) The holder shall be informed on the SI-PASS user pages of the date and time of the revocation, the issuer of the cancellation request and the reasons for the revocation.

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

[5] According to the recommendation of RFC 3647, this subchapter includes a suspension procedure for which the SI-Pass-CA issuer does not allow it.

4.9.4 Time to issue cancellation request

A request for cancellation should be requested without delay in the event of an abuse or unreliability, etc., of urgency, or as soon as possible and before the first subsequent use of the certificate.

4.9.5 time spent on cancellation request received until revocation

(1) The SI-TRUST shall, after receipt of a valid request to cancel the certificate, be revoked at the latest within four (4) hours.

(2) If the operation of the SI-TRUST is, due to unforeseen events, substantially reduced, the cancellation is carried out at the latest within twenty-four (24) hours after receipt of a valid cancellation request, due to the risk of misuse or unreliability.

(3) Following revocation, the certificate shall be immediately added to the register of invalidated certificates.

4.9.6 requirements for verification of the register of certificates for third parties withdrawn

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

4.9.7 frequency of publication of the certificate withdrawn

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

4.9.8 time until the date of publication of the register of certificates cancelled

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

4.9.9 Verification of the status of certificates

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

4.9.10 Requirements for continuous verification of the status of certificates

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

4.9.11 Other means of access to certificate status

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

4.9.12 Other requirements for private key abuse

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

4.9.13 Grounds for suspension

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

4.9.14 Who may request the suspension

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

4.9.15 Procedure for the suspension

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

4.9.16 Time of suspension

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

4.10. Verification of the status of certificates

4.10.1 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/digitalna-potrdila-si-pass-ca/, on-line verification of the status of the certificate is available at http://ocsp. sy-can-ca.gov.si, and access details are in the sub-place. 7.2And7.3.

4.10.2 Availability

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

4.10.3 Other options

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

4.11. End of subscription

The relationship between the holder and the SI-TRUST shall be terminated if

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

4.12. detection of a copy of the decryption keys

4.12.1 procedure for detection of decryption keys

Not supported.

4.12.2 Procedure for the detection of the meeting key

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

5. GOVERNANCE AND SECURITY CONTROLS OF INFRASTRUCTURE

5.1. Physical security

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

5.1.1 location and structure of the trust service provider

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

5.1.2 Physical access to the infrastructure of the trust service provider

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

5.1.3 Power and air conditioning

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

5.1.4 Water exposures

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

5.1.5 Fire prevention and protection

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

5.1.6 media management

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

5.1.7 disposal

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

5.1.8 Off-site backup

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

5.2. Organisational structure of the issuer/trust service provider

5.2.1 organisation of a trust and trusted service provider

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

5.2.2 Number of persons required per task

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

5.2.3 Identity of individual applications

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

5.2.4 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.

5.3.1 Qualifications, experience and clearance requirements

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

5.3.2 Background check procedures

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

5.3.3 staff training

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

5.3.4 Training requirements

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

5.3.5 Job rotation frequency and sequence

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

5.3.6 Sanctions

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

5.3.7 Independent contractor requirements

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

5.3.8 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.

5.4.1 Species of log

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

5.4.2 Frequency of processing log

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

5.4.3 Retention period for audit log

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

5.4.4 protection of audit log

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

5.4.5 Audit log backup procedures

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

5.4.6 Data collection for audit logs

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

5.4.7 Notification to event-causing subject

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

5.4.8 Assessment of system vulnerabilities

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

5.5. retention of information

5.5.1 Types of record archived

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

5.5.2 Retention period

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

5.5.3 Protection of archive

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

5.5.4 System archive and storage

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

5.5.5 Requirement of time stamping

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

5.5.6 Data collection how archived data can be collected

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

5.5.7 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

In the case of renewal of an ATV certificate, the procedure is published on the websites of the SI-PASS-CA.

5.7. Compromise and disaster recovery

5.7.1 Incident and compromise handling

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

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

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

5.7.3 Entity private key compromise procedures

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

5.7.4 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

6.1.1 Key generation

(1) The generating of the SI-Pass-CA key pair is a formal and controlled procedure in the case of the installation of the SI-PASS-CA software for which a separate record is kept (document 'document generic manufacturing process for SI-PASS-CA'). 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-Pass-CA IT system provided for the establishment of the system shall be documented in a separate record, or in the relevant journal.

(4) The generating pair of the SI-Pass-CA key pair shall be used in the machine security module (see below). 6.2.1).

(5) For generating the pairs of key holders, a dedicated machine safety module shall be used, which shall be used as a secure electronic signature tool operated by the issuer of the SI-PASS-CA (see below). 6.2.1).

(6) The machine security module shall be used to generate the infrastructure control keys that are used to activate user private keys for the secure storage of private key holders (see below). 6.2.1). The generic process shall be carried out every three (3) years or at an earlier stage and shall be described in more detail in the SI-TRUST.

6.1.2 Delivery of private key to holders

The private key is generated on a dedicated hardware security module and stored in a dedicated secure database, managed by an issuer of SI-PASS-CA, and therefore will not be delivered to the holder.

6.1.3 Delivery of the certificate to the issuer of the certificates[6]

The public key is generated on a dedicated hardware security module and stored in a dedicated secure database, and therefore, delivery to the issuer is not required.

6.1.4 Delivery of the issuer's public key to third parties

(1) The certificate with the public key of the issuer of SI-PASS-CA is published in SI — TRUST (see below). 2.1).

(2) The certificate issued to the holder of the SI-PAS-SCA public key is accessible to the holder or to third parties:

- in the public directory x500.gov.si on the LDAP protocol (see below. 2.3),
- in the form of PEM on https://www.si-trust.gov.si/assets/si-trust-root/povezovalni-podrejeni/si-pass-ca/si-pass-ca.xcert.pem.

6.1.5 Key length

Certificate	RSA key length [bit]
certificate issued by SI-PASS-CA	3072
certificate for holders	2048[7]
OCSP certificate	2048

6.1.6 Generating and quality of public key parameters

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

6 RFC 3647 does not provide a description of how the certificates are delivered to holders.

7 Value means the prescribed minimum length.

6.1.7 Key purpose and certificates

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

6.2. Private key protection and security modules

6.2.1 Cryptographic module standards

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

(2) Holders' private keys shall be generated and used by machine tools for secure storage of private keys complying with the FIPS standard 140-2 Level 3 and the requirements for a secure signature creation medium in accordance with applicable legislation.

(3) The infrastructure key control key (s) used to activate user private keys for the secure storage of private key holders is generated, used and stored on machine tools for secure private key storage compliant with the FIPS standard 140-2 Level 3.

6.2.2 Private key control by authorised persons

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

(2) The holder shall have access to the private key of the holder in unencrypted form only the holder.

6.2.3 Detecting a copy of the private key

Not supported.

6.2.4 backup of private keys

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

(2) The issuer of the SI-PASS-CA provides a backup for the private keys of the holders. Details are set out in the SI-TRUST internal policy.

6.2.5 Private key archiving

Not supported.

6.2.6 Transfer of private key from/to cryptographic module

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

(4) The holder's private key is generated on a dedicated hardware security module which is used as a secure

electronic signature tool operated by the issuer of SI-PASS-CA. the transfer of the holder's private key from a hardware security module shall be carried out in encrypted format, following a key pair, for the purpose of secure storage of the private key into a dedicated secure database and making its backup copy (see below. 6.2.4). The transfer of the private key to the hardware security module shall be done in encrypted form before any use of the private key of the holder. The private key shall be located outside the dedicated hardware security module only in encrypted form.

6.2.7 Private key record in a cryptographic module

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

(2) The holder's private key is protected in the Machine Security Module by mechanisms according to the FIPS 140-2 Level 3 and the holder's password for private key protection.

6.2.8 procedure for the activation of the private key

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

(2) The activation of the private key of the holder shall be carried out before any use of the private key for the purpose of the authentication of the electronic signature. Prior to activating the private key, the holder must apply the SI-PASS service in an appropriate manner and enter a password protected by his/her private key (see below). 4.5.1).

6.2.9 Procedure for deactivation of the private key

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

(2) After the authentication of the electronic signature, the holder's private key will be permanently removed and thus deactivated in a dedicated machine security module.

6.2.10 Procedure for the destruction of the private key

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

(2) The destruction of the private key of the holder shall be carried out as soon as the request for cancellation has been submitted so that the private key in encrypted form is permanently removed from the dedicated protected database.

6.2.11 Cryptographic module characteristics

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

6.3. Key Management Aspects

6.3.1 Preservation of public key

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

6.3.2 Certificate and key validity period

(1) The validity of the certificates and keys are given in accordance with the table below.

Certificate type	Key pair	Keys	Validity
holder's certificate	digital signature/authentication couple	private key	5 years
		public Key	5 years

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

6.4. access passwords

6.4.1 Password generation

(1) The authorised person (s) person authorised to access the private key of SI-PASS-CA shall use the strong passwords with which they comply with the SI-TRUST policy.

(2) Holders themselves determine a password to protect access to their private keys using strong passwords, which is provided through the SI-PASS service.

(3) The SI-SCk-CA for keepers requires the use of secure passwords:
- mixed use of large and small letters and numbers;
- a length of at least 6 characters,
- The use of the words contained in the dictionaries is advised.

6.4.2 Password protection

(1) The passwords of the AEO Holders of the SI-PASS-CA for access to the private key of the ATV holder are stored under the SI-TRUST policy.

(2) The SI-Pass-CA recommends that the holder's password for access to the private key is not stored or stored in a safe place and that only the holder has access to it.

(3) The SI-SCk-CA recommends the holders to ensure that the password is replaced at least every six (6) months.

6.4.3 Other aspects of passwords

Not prescribed.

6.5. Safety requirements for issuing computer equipment by the issuer

6.5.1 Specific technical safety requirements

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

6.5.2 Level of security protection

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

6.6. Issuer's life cycle technical control

6.6.1 Control of the evolution of the system

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

6.6.2 Managing safety

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

6.6.3 Life cycle control

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

6.7. Network security controls

(1) Only the network protocols which are strictly necessary for the operation of the system are enabled.

(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) Based on this policy, the SI-PASS-CA issues certificates for natural persons for the purposes of the online registration and e-signing service of the SI-PASS.

(2) All qualified certificates shall include data that are specified for qualified certificates in accordance with applicable legislation.

(3) The SI-Pass-CA issuer's certificates are followed by standard *X.509.*

7.1.1 Certificate version

All certificates from the ATV issuer are followed by standard *X.509*, version 3, according to RFC 5280.

7.1.2 profile of extensions

7.1.2.1 Profile of the SI-Pass-CA certificate

The profile of the SI-Pass-CA certificate is presented in a sub-heading. 1.3.1YES/NO.

7.1.2.2 Certificate Profile for Holders

(1) The information in the certificate is given below.

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*
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-PASS-CA
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*	*the distinguishing name of the holder, which includes the holder's name and the serial number (see below. 3.1.1*), *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*	the *key length is min. 2048 bits, see below. 6.1.5*
Extensions of X.509v3	
Alternative name OID 2.5.29.17, \ "_blank" *Subject Alternative Name*	*not used*

The publication of a register of cancelled certificates, OID 2.5.29.31, \ "_blank" *CRL Distribution Points*	URI: http://www.si-pass-ca.gov.si/crl/si-pass-ca.crl URL: ldap://x500.gov.si/cn=SI-PASS-CA OI = VATSI-17659957, o = the Republic of Slovenia, c = SI? certificateRequationList c = SI, o = the Republic of Slovenia, OI = VATSI-17659957, CN = SI-PASS-CA, CN = CRL < serial *number of the register, see below. 7.2.2* >
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.si-pass-ca.gov.si Access Method: CaIssuer (OID 1.3.6.1.5.5.7.48.2) Access Location: URL = http://www.si-pass-ca.gov.si/crt/si-pass-ca-certs.p7c
Key Usage, OID 2.5.29.15, \ *"_blank" Key Usage*	ContentCommitment
The extended application of the key; OID 2.5.29.37, \ "_blank" *Extended Key Usage*	*not used*
Key of the issuer key; OID 2.5.29.35, \ "_blank" Hash *Key Identifier*	4832 CA46 4E33 CB0A
The identifier of the holder's key; OID 2.5. *29.14,* \ *"_blank" Subject Key Identifier*	*subject Key Identifier*
The policies under which the certificate was issued, OID 2.5.29.32, certificatePolicies	Certificate Policy: PolicyIdentifier = *depending on the type of certificate, see below. 7.1.2.3* [1,1] Policy qualificer Info: policy qualificer Id = CPS qualificer: http://www.ca.gov.si/cps/
Qualified certificate identifier, OID 1.3.6.1.5.5.7.1.3, QcStatements *statement*	*depending on the type of certificate, see below. 7.1.2.3*
Basic restrictions, OID 2.5.29.19, \ "_blank" *Basic Constrants*	CA: FALSE No length limitation Constraint: None)
Certificate footprint (not part of the certificate)	
Resultsa-SHA-1 \ "_blank" Certificate Fingerprint — SHA-1	*recognisable print of the certificate after SHA-1*
Resultsa-SHA-256 \ "_blank" *Certificate Fingerprint — SHA-256*	*recognisable print of the certificate after SHA-256*

(2) Field *Application* field *The key* message shall be marked as *critical*.

(3) The holder may have a single valid certificate of the same type.

7.1.2.3 gauges of individual attestations

All certificate holders' certificates shall include the data set out in the table in the floor. 7.1.2 YES/NO. The values of the *policy fields and the code of the qualified certificate that depend on the type of certificate are* given in the table below for each type of certificate.

Field name	Type of certificate		
	qualified certificate for a qualified electronic signature	qualified Certificate	a normalised certificate
The policies under which the certificate (OID) has been issued and which also indicate that it is a qualified certificate, *Certificate Policies*	Policy: 1.3.6.1.4.1.6105.7.1.1 0.4.0.194112.1.2	Policy: 1.3.6.1.4.1.6105.7.2.1 0.4.0.194112.1.0	Policy: 1.3.6.1.4.1.6105.7.3.1
Qualified certificate identifier, OID 1.3.6.1.5.5.7.1.3, QcStatements *statement*	QcCompliance statement QcSSCD statement QcType: eSign PdsLocation: https://www.ca.gov.si/cps/sipassca_pds_en.pdf https://www.ca.gov.si/cps/sipassca_pds_sl.pdf	QcCompliance statement QcType: eSign PdsLocation: https://www.ca.gov.si/cps/sipassca_pds_en.pdf https://www.ca.gov.si/cps/sipassca_pds_sl.pdf	//OR

7.1.3 Algorithm identification markings

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

(2) The infrastructure key control keys that are used to activate user private keys for the secure storage of holders' private keys are generated by the AES256 and HASH-MAC-SHA256 algorithm.

7.1.4 Name (s) of name (s)

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

7.1.5 Restriction on names

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

7.1.6 Certificate policy code

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

7.1.7 Use of expansion field to limit policy use

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

7.1.8 Format and treatment of specific policy information

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

7.1.9 Consideration of a critical enlargement policy field

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

7.2. register of invalidated certificates

7.2.1 Version

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

7.2.2 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 *write-down* of *SI-PASS-CA*
The distinguishing name of the issuer; \ "_blank" *Issuer*	c = SI, o = the Republic of Slovenia, oi = VAT-17659957, cn = SI-PASS-CA
Time of issue of the CRL, thisUpdate	Last Update: *Time of release after GMT* >
Time of issue for the next CRL, NextUpdate	Next Update: <*Time of next 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 a single register and are only published in the full register until the expiration date.

(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. 2.1).

(5) The publisher publishes both the individual registers and the full register. Access for LDAP and HTTP protocols and publication shows the table below.

Publication of the CRL		Access to CRL
individual registers	C = SI, o = Republic of Slovenia, oi = VAT-17659957, cn = SI-PASS-CA, cn = CRL < *serial number* of the register >	- Ldap://x500.gov.si/cn=CRL< *register serial number* >, cn = SI-Pass-CA, oi = VAT-17659957, o = Slovenia, c = SI
full Register	C = SI, o = the Republic of Slovenia, oi = VAT-17659957, cn = *SI-PASS-CA (* in CertificationRevocationList)	- Http://www.si-pass-ca.gov.si /crl/si-pass.crl - Ldap://x500.gov.si/cn= SI-PASS-CA, oi = VAT-17659957, o = Slovenia, c = SI? certificateRequationList

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 can be found at http://ocsp. si-pass.gov.si.

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

7.3.1 Version

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

7.3.2 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

9.1.1 Issuance price and renewal of certificates

Certification costs are calculated on the basis of a published price list on the website https://www.si-trust.gov.si/sl/si-pass/.

9.1.2 Access price for certificates

Certificate holders' certificates shall not be published in a public directory (see place. 0).

9.1.3 Access price of the certificate and a register of cancelled certificates

Access to the status of the certificate and the register of certificates cancelled by the originator of the SI-PASS-CA is free of charge.

9.1.4 Prices of other services

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

9.1.5 Reimbursement of expenses

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

9.2. Financial responsibility

9.2.1 Insurance coverage

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

9.2.2 Other cover

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

9.2.3 Holders' insurance

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

9.3. Protection of commercial information

9.3.1 Protected data

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

9.3.2 Non-safeguarded data

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

9.3.3 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

9.4.1 Privacy plan

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

9.4.2 Protected personal data

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

9.4.3 Personal data not protected

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

9.4.4 Responsibility for the protection of personal data

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

9.4.5 Power of attorney concerning the use of personal data

The holder authorises the use of personal data in a request for the purpose of obtaining a certificate, or at a later date in writing, for the use of personal data.

9.4.6 Transfer of personal data to official request

(1) The SI-TRUST shall not transmit data on holders of certificates other than those stated in the certificate, unless specific data are specifically requested for the implementation of the specific certification service (s) and the SI-TRUST is authorised by the proxy holder (see previous subchapter) or at the request of the competent court or administrative authority.

(2) The data shall also be transmitted without the written consent, if provided for by the legislation or regulations in force.

9.4.7 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

9.6.1 Obligations and responsibilities of the issuer

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

9.6.2 Obligation and responsibility of the registration service

(1) The registration service is required to:
- verify the identity of holders/future holders,
- accept requests for SI-PAS-SCA services;
- check claims,
- supply the holders or prospective holders with the necessary documentation,

- forward requests and other data in a secure manner to SI-PASS-CA.

(2) The application service is responsible for the implementation of all the provisions of these policies and other requirements that have been agreed with the SI-TRUST.

9.6.3 Liability and liability of the holder

(1) The holder or prospective holder of the certificate shall be obliged:
- take note of this policy prior to issuing the Certificate,
- comply with the policy and other applicable regulations;
- if, following the submission of an application to obtain a one-time password of smassSS from the issuer of the SI-PASS-CA, no notification is received by e-mail or postal item to the address of the registered office, the designated person (s) of the SI-PASS-CA,
- upon acceptance of the certificate, check the information in the certificate, and if faults or any problems have occurred, immediately notify the SI-PASS-CA or ask for the certificate to be cancelled,
- monitor and comply with all notifications and comply with the SI-PASS-CA notifications,
- duly updated, in accordance with the notifications, the necessary hardware and software for safe work with certificates,
- all amendments related to the certificate shall be notified immediately to the SI-Pass-CA,
- require the withdrawal of a certificate where private keys have been compromised in a manner that affects the reliability of use or there is a risk of abuse,
- use the certificate for the purpose specified in the certificate (see below. And7.1 in the manner prescribed by the SI-Pass-CA policy,
- provide the original signed documents and archive of these documents.

(2) 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 the holder has been able, through the fault of the proprietor, to use or abuse the holder's certificate by unauthorised persons,
- any other damage resulting from non-compliance with the provisions of this policy and other TSI-SAS-CA notifications and applicable regulations.

(3) The holder's obligations with regard to the use of the certificates are set out in the sub-area. 4.5.1YES/NO.

9.6.4 liability and liability of third parties

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

9.6.5 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 issuer of SI-Pass-CA/SI-TRUST guarantees the value of each transaction by type of certificate to the value of:

- for qualified certificates for a qualified electronic signature up to the amount of EUR 5,000; and
- for qualified certificates up to the amount of EUR 1,000.

9.9. Redress

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

9.10. policy validity

9.10.1 Duration

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

9.10.2 End of the policy period

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

9.10.3 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

9.12.1 Procedure for the application of amendments

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

9.12.2 Validity and publication of amendments

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

9.12.3 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

9.16.1 Comprehensive deal

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

9.16.2 Assignment of rights

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

9.16.3 independence identified by

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

9.16.4 Receivables

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

9.16.5 Force majeure

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

9.17. Miscellaneous provisions

9.17.1 Understanding

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

9.17.2 Conflicting provisions

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

9.17.3 Derogation from the provisions of

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

9.17.4 Cross verification

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