State Centre for Services of Confidence
Issuer of eligible digital certificates of SIGEN-CA

SI-TRUST
SIGEN-CA

SIGEN-CA POLICY

for qualified digital certificates for commercial entities

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

validity: From 1 October 2019
version: 7.1

CP$_{\text{Name}}$: SIGEN-CA-1

- **Online Qualified Certificate Policy for**
  CP$_{\text{OIDs}}$: 1.3.6.1.4.1.6105.2.1.1.5
- **Policy for Special Qualified Digital Certificates for staff** of
  CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.2.1.2.5
- **Policy for online qualified digital certificates for employees using**
  CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.2.1.3.5
- **Policy for special qualified digital certificates for employees of**
  CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.2.1.4.5
- **Policy for Online normalised digital certificates for**
  CP$_{\text{OID}}$ **information systems**: 1.3.6.1.4.1.6105.2.1.5.5
- **Policy for Online normalised digital certificates to sign**
  CP$_{\text{OID}}$ Code: 1.3.6.1.4.1.6105.2.1.6.5
- **Policy for online qualified digital certificates for the authentication of** the
  CP$_{\text{OID}}$ website: 1.3.6.1.4.1.6105.2.1.7.5
- **Policy for online qualified digital certificates for**
  CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.2.1.8.5

State Centre for Services of Confidence

Policy history

Issues of SIGEN-CA operations	
version: 7.1, valid: from 1 October 2019	
• Policy for online qualified digital certificates for employees, CP OID: 1.3.6.1.4.1.6105.2.1.1.5 • Policy for special qualified digital certificates for employees, CP OID: 1.3.6.1.4.1.6105.2.1.2.5 • Policy for online qualified digital certificates for employees with a general title, CP OID: 1.3.6.1.4.1.6105.2.1.3.5 • Policy for special qualified digital certificates for employees with a general title, CP OID: 1.3.6.1.4.1.6105.2.1.4.5 • Policy for Online normalised digital certificates for information systems, CP OID: 1.3.6.1.4.1.6105.2.1.5.5 • Policy for Online normalised digital certificates for code signature, CP OID: 1.3.6.1.4.1.6105.2.1.6.5 • Policy for online qualified digital certificates for website authentication, CP OID: 1.3.6.1.4.1.6105.2.1.7.5 • Policy for online qualified digital certification for stamp, CP OID: 1.3.6.1.4.1.6105.2.1.8.5 CP Name: SIGEN-CA-1	*Change from version 7.1:* • *qualified digital certificates for general names are renamed as qualified digital certificates for employees with a general title.* • *revision of the document.*
amendment to the policy version 7.0, validity: from 18 February 2019	
Amendment to Politiki SIGEN-CA qualified digital certificate for business operators no 1/7.0	*Amendment by amendment 1/7.0:* • *in the case of certificates for electronic seals, the title included in the Distinguished Name is changed.*
version: 7.0, valid: from 28 May 2018	
• Policy for online qualified digital certificates for employees, CP OID: 1.3.6.1.4.1.6105.2.1.1.5 • Policy for special qualified digital certificates for employees, CP OID: 1.3.6.1.4.1.6105.2.1.2.5 • Policy for online qualified digital certificates for general titles, CP OID: 1.3.6.1.4.1.6105.2.1.3.5 • Policy for specific qualified digital certificates for general titles, CP OID: 1.3.6.1.4.1.6105.2.1.4.5 • Policy for Online normalised digital certificates for information systems, CP OID: 1.3.6.1.4.1.6105.2.1.5.5 • Policy for Online normalised digital certificates for code signature, CP OID: 1.3.6.1.4.1.6105.2.1.6.5 • Policy for online qualified digital certificates for website authentication, CP OID: 1.3.6.1.4.1.6105.2.1.7.5 • Policy for online qualified digital certification for stamp, CP OID: 1.3.6.1.4.1.6105.2.1.8.5 CP Name: SIGEN-CA-1	*Changes with version 7.0:* • *normalised certificates for servers are renamed as qualified certificates for website authentication.* • *the validity of certificates for website authentication is 27 months.* • *the distinguishing name of certificates for website authentication has been modified;* • *a qualified certificate for electronic seal and normalised certificates for information systems are introduced.* • *the certificates indicate the policy codes as set out in the new standards.* • *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: 6.0, valid: from 6 June 2016	

• Policy for online qualified digital certificates for employees, CP OID: 1.3.6.1.4.1.6105.2.1.1.4 • Policy for special qualified digital certificates for employees, CP OID: 1.3.6.1.4.1.6105.2.1.2.4 • Policy for online qualified digital certificates for general titles, CP OID: 1.3.6.1.4.1.6105.2.1.3.4 • Policy for specific qualified digital certificates for general titles, CP OID: 1.3.6.1.4.1.6105.2.1.4.4 • Policy for online normalised digital certificates for servers, CP OID: 1.3.6.1.4.1.6105.2.1.5.4 • Policy for Online normalised digital certificates for code signature, CP OID: 1.3.6.1.4.1.6105.2.1.6.4 CP Name: SIGEN-CA-1	*Changes with version 6.0:* • *the second self-digital certificate from the SIGEN-CA was formed on the basis of a private key of 3072 bits, which is stored on the hardware for the secure storage of private keys.* • *the issuer SIGEN-CA certificate and all holders' certificates shall use the SHA-256 hash algorithm,* • *the distinguishing name of the digital certificate from the issuer of SIGEN-CA has been modified;* • *the distinction names of the holders' certificates, which may include characters from the code table UTF-8, have been modified.* • *on-line verification of the status of certificates under the OCSP protocol is supported,* • *the issuer of SIGEN-CA is recognised by the root broadcaster SI-TRUST Root;* • for *certificates for employees and general titles, the field use key. Key Usage) added value of ContentCommitment;* • *servers and code signature are renamed normalised certificates.*
version: 5.0, valid: from 7 November 2015	
• Policy for online qualified digital certificates for employees, CP OID: 1.3.6.1.4.1.6105.2.1.1.3 • Policy for special qualified digital certificates for employees, CP OID: 1.3.6.1.4.1.6105.2.1.2.3 • Policy for online qualified digital certificates for general titles, CP OID: 1.3.6.1.4.1.6105.2.1.3.3 • Policy for specific qualified digital certificates for general titles, CP OID: 1.3.6.1.4.1.6105.2.1.4.3 • Online Qualified Certificate Policy for servers, CP OID: 1.3.6.1.4.1.6105.2.1.5.3 • Policy for Online Qualified Digital Certificates to sign the Code, CP OID: 1.3.6.1.4.1.6105.2.1.6.3 CP Name: SIGEN-CA-1	*Changes with version 5.0:* • *use of the new title for CA at the Home Office, now called the National Centre for Services of Confidence.* • *SHA-256 compression algorithm is used for servers.* • *the validity of web certificates for servers is 3 years.* • *the validity of the encryption certificate and the private signing key for the special certificates for employees and general titles is 5 years.* • *it is possible to issue web certificates for servers with multiple server names;* • *the issue of specific server certificates is abolished;* • *new SIGEN-CA contact details.*
amendment to the policy version 4.0, validity: from 21 March 2014	
Amendment to Politiki SIGEN-CA qualified digital certificate for business operators no 2/4.0	*Amendment by amendment 2/4.0:* • *use of the new title for certification service providers at the Ministry of Justice and Public Administration, new to the Ministry of the Interior.*
amendment to the policy version 4.0, validity: from 23 July 2012	
Amendment to Politiki SIGEN-CA qualified digital certificate for business operators no 1/4.0	*Amendment by amendment 1/4.0:* • *the use of the new title for certification authorities at the Ministry of Public Administration, new to which is the 'Prosecutor at the Ministry of Justice and Public Administration'.*
version: 4.0, valid: from 14 September 2009	
• Policy SIGEN-CA for online qualified digital certificates for employees and general titles, CP OID: 1.3.6.1.4.1.6105.2.1.1.2 • Policy SIGEN-CA for special qualified digital certificates for employees and general titles, CP OID: 1.3.6.1.4.1.6105 2.1.2.2 • Policy SIGEN-CA for online qualified digital certificates for servers and code signature, CP OID: 1.3.6.1.4.1.6105 2.1.3.2 • SIGEN-CA policy for servers, CP OID: 1.3.6.1.4.1.6105.2.1.4.2 CP Name: SIGEN-CA-1	*Changes with version 4.0:* • *the issuer of SIGEN-CA issues qualified digital certificates with a minimum length of 2048 bits;* • *in qualified employment-friendly certificates for staff and general titles, the corresponding qualified certificate code shall be added;* • *it is amended to provide for a guarantee of the value of each legal transaction.*
amendment to the policy version 3.0, validity: from 18 May 2007	

Amendment to Politiki SIGEN-CA qualified digital certificate for business operators no 1/3.0	*Amendment by amendment 1/3.0:* • *the issuer of the SIGEN-CA shall not transmit the certificate code to the prospective holder by registered mail.*
version: 3.0, valid: from 28 February 2006	
● Policy SIGEN-CA for online qualified digital certificates for employees and general titles, CP OID: 1.3.6.1.4.1.6105.2.1.1.1 ● Policy SIGEN-CA for special qualified digital certificates for employees and general titles, CP OID: 1.3.6.1.4.1.6105 2.1.2.1 ● Policy SIGEN-CA for online qualified digital certificates for servers and code signature, CP OID: 1.3.6.1.4.1.6105 2.1.3.1 ● SIGEN-CA policy for servers, CP OID: 1.3.6.1.4.1.6105.2.1.4.1 CP Name: SIGEN-CA-1	*Changes with version 3.0:* • *use of the new title for certification service providers at the Centre of the Government for Informatics, newly designated by the Ministry of Public Administration;* • *'Personal qualified digital certificates' are newly referred to as 'special qualified digital certificates';* • *the revocation is only possible within the official hours, except in urgent cases;* • *the use of the new title for SIGEN-CA holders, for holders of 'legal and natural persons registered for the purposes of the activity', uses the term 'business entities';* • *the structure of the document is in line with RFC 3647 recommendations.*
version: 2.0, valid: from 15 July 2002	
Policy SIGEN-CA for legal and natural persons registered for activities CP OID: 1.3.6.1.4.1.6105.2.1.2 CP Name: SIGEN-CA-1	*Changes with version 2.0:* • *it is also issued with qualified digital certificates for the general titles and organisational units of the institutions;* • *the issue of a qualified digital certificate for servers and the signature of the code is also issued.*
version: 1.0, valid: from 15 October 2001	
Policy SIGEN-CA for legal and natural persons registered for activities CP OID: 1.3.6.1.4.1.6105.2.1.1 CP Name: SIGEN-CA-1	//OR

CONTENT

SUMMARY

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

The SI-TRUST issues qualified digital certificates and qualified electronic time stamps subject to the highest level of protection and complying with Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS; Official Journal of the EU, no. L 257/73), ETSI standards and other applicable regulations and recommendations.

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

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

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

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

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

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

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

for other needs where a qualified electronic time stamp is required.

Within the SI-TRUST, an issuer of qualified digital certificates (SIGEN-CA) shall be operational. *Slovenian General Certification Authority*, https://www.si-trust.gov.si/sl/digitalna-potrdila/poslovni-subjekti/, which issues certificates for business entities and natural persons.

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

The SIGEN-CA action policy shall specify the internal operating rules of the issuer 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 policies of the issuer of SIGEN-CA for business entities, i.e. legal and natural persons registered for the purpose of carrying out activities (hereinafter referred to as ‘ *organisations*’) for several types of qualified digital certificates complying with the highest safety requirements. On the basis of this document SIGEN-CA issues a specific and online digital certificate following the following policies of CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.2.1.1.5, CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.2.1.2.5, CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.2.1.3.5, CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.2.1.4.5, CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.2.1.5.5, CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.2.1.6.5, CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.2.1.7.5 and CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.2.1.8.5

The present document replaces the previously published SIGEN-CA policies for business operators. 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).

The changes made to the present document are the following:

- qualified digital certificates for general names are renamed as qualified digital certificates for the general title (s).

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 $_{\text{OIDs}}$) are not altered.

Qualified digital certificates shall be obtained on the basis of an application to be signed by the responsible person of the business entity and by the prospective holders. In the case of a digital certificate for information systems, the signature of the code, the website and the electronic seals, the prospective holder is the employee or person authorised by the responsible person to use this certificate. The person responsible shall, by means of the signature of the request, guarantee the identity of the prospective holder. The request will be submitted to the application service (list published at https://www.si-trust.gov.si/sl/digitalna-potrdila/poslovni-subjekti/).

On the basis of an approved request, the SIGEN-CA shall develop a reference number and an authorisation code, which shall be unique for each prospective holder of a qualified digital certificate and shall be required by the prospective holder to take over his certificate, carried out at his workstation, in accordance with the instructions given by the issuer of SIGEN-CA. the prospective holder shall receive the reference number by e-mail and the authorisation code by post to the service address.

An online digital certificate is connected to one pair of keys generated by the holder's software or hardware. The SIGEN-CA never holds or does not have access to the private key. The public key is sent to the SIGEN-CA issuing the certificate, of which the public key is an integral part. The online certificate is stored at the holder and has been made available in the public directory of the certificates.

In the case of a dedicated digital certificate, separate signature/authentication keys and decryption and encryption are separate and two confirmed. To this end:

- The signature keys pair/authentication pair shall be produced by the holder of the software. The SIGEN-CA never stores and does not have access to the private signature key. The public key to signature verification shall be sent to the SIGEN-CA issuing the signature verification certificate, of which the public key for the verification of signature forms an integral part. The certificate for signature verification shall be filed with the holder.
- The decryption/encryption keys pair shall be formed on the SIGEN-CA page. the private key to decrypt the holder shall be held by the holder. For the purposes of possible access (decryption) to important data encrypted, if the private decryption key is no longer accessible for any reason, this key, under the specific regime set out in the SI-TRUST policy, shall also be safely stored in the SIGEN-CA archives, which shall issue the encryption certificate of which the public key for encryption is an integral part. The encryption certificate shall be published in the public directory of the certificates.

In addition to the data included in the digital certificate, the SIGEN-CA shall keep the other necessary information on the holder and the organisation for the purpose of electronic commerce, in accordance with the rules in force.

The holder is obliged to carefully protect private keys and their digital certificates and to comply with the policy, to inform the issuer of the SIGEN-CA and the applicable legislation.

1. INTRODUCTION

1.1. *Review*

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

(2) Within the SI-TRUST, the issuer of the SIGEN-CA is operational. *Slovenian General Certification Authority*, https://www.si-trust.gov.si/sl/digitalna-potrdila/poslovni-subjekti/, which issues digital certificates for business entities and natural persons. The present document sets out the policies of the issuer of SIGEN-CA for all types of digital certificates for the needs of business operators (hereinafter*: organisation*).

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

(4) Following the present policy SIGEN-CA issues the following qualified digital certificates:

- special qualified digital certificates for organisations working in organisations,
- special qualified digital certificates for employees with the general title of the organisation (s).
- online qualified digital certificates for organisations working in organisations,
- online qualified digital certificates for employees with the general title of the organisation/organisational unit,
- online qualified digital certificates for website authentication managed by organisations;
- online qualified digital certificates for organisations' electronic seals
- online normalised digital certificates for organisations managed by organisations,
- online normalised digital certificates for code signature.

(5) The SIGEN-CA certificates may be used for:

- encryption of data in electronic format;
- authentication of digitally signed data and identification of the holder,
- 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 issuer of SIGEN-CA for the protection of private keys or use of secure cryptographic modules.

(7) The present policy is prepared in line with RFC 3647 " Internet X.509 Public Key Infrastructure Certificate and Certification Practices Framework", and sets out the internal rules of the issuer of SIGEN-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 digital certificates from the SIGEN-CA, third parties relying on digital certificates, and other entities that, in accordance with the regulations, use the services of the SIGEN-CA.

(8) Mutual relations are also implemented on the basis of a possible written agreement between the organisations and the SI-TRUST or between third parties relying on the SIGEN-CA certificates and the SI-TRUST.

(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 SIGEN-CA Policy Certificate for Business Operators (*SIGEN-CA*).

(2) This policy code is CP $_{\text{Name}}$: SIGEN-CA-1, and the SIGEN-CA-1 policy identification markings vary according to the type of certificate:

- CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.2.1.1.5 for online qualified certificates for employees,
- CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.2.1.2.5 for special qualified certificates for employees,
- CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.2.1.3.5 for online qualified certificates for employees with a general title,
- CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.2.1.4.5 for special qualified certificates for employees holding a general title,
- CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.2.1.5.5 for online normalised certificates for information systems,
- CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.2.1.6.5 for online normalised certificates for code signature,
- CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.2.1.7.5 for online qualified certificates for website authentication,
- CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.2.1.8.5 for online qualified certificates for electronic seals.

(3) Each certificate shall contain an indication of the relevant policy in the form of a CP $_{\text{OID}}$ code, see below. 7.1.2YES/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 shall be operational.

(3) The SIGEN-CA contact details are:

Address:	SIGEN-CA State Centre for Services of Confidence Ministry of Public Administration Tržaška cesta 21 1000 Ljubljana
E-mail:	sigen-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 shall perform 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;
- concerns for a public body of certificates;
- 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 or her application; and

- provides all other services in accordance with this policy and with other regulations.

(5) Upon the launch of its production operation, the issuer of the SIGEN-CA generated its own digital certificate, which is intended to certify the certificates issued by the SIGEN-CA to the holders.

Certificate No 1 SIGEN-CA shall contain the following information[1]:

Field name	Value of the SIGEN-CA certificate
Certificate (s) of the underlying (s) in the certificate	
Version \ “_blank” *Version*	3
ID, *Serial Number*	3B3C F9C9
Signature algorithm, \ “_blank” *Signature Algorthm*	sh1WithRSAEncrConsumption
Issuing body, \ “_blank” *Issuer*	c = SI, o = stage institutions, ou = sigen-ca
Holder, *Subject*	c = SI, o = stage institutions, ou = sigen-ca
Date of entry into force, *Validity: Not Before*	June 29 21: 27: 46 2001 GMT
End of validity, *Validity: Not After*	June 29 21: 57: 46 2021 GMT
Public Key Algorithm, \ “_blank” *Public Key Algorthm*	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*	*2048 bit length key*
Extensions of X.509v3	
Key Usage, OID 2.5.29.15, *\ “_blank” Key Usage*	Signature of Certificates (keyCertSign), CRL signature (cRLSign)
Basic restrictions, OID 2.5.29.19, \ “_blank” *Basic Constrants*	CA: TRUE No length limitation Constraint: None)
Key of the issuer key; OID 2.5.29.35, \ “_blank” *Authority Key Identifier*	717B 8A06 1AF31 0555 AB60 1277 4720 1E03 8818 EC89
The identifier of the holder's key; OID 2.5.29.14, \ “_blank” *Subject Key Identifier*	717B 8A06 1AF31 0555 AB60 1277 4720 1E03 8818 EC89
Certificate footprint (not part of the certificate)	
The footprint of the MD-5 certificate, \ “_blank” *Certificate Fingerprint — MD5*	49EF A6A1 F0DE 8EA7 6A5AAB7D 1E5F C446
SHA-1 certificate footprint, *Certificate Fingerprint — SH* A-1	3E42 A187 06BD 0C9C CF59 4750 D2E4 D6AB 0048 FDC4
SHA-256 certificate footprint, *Certificate Fingerprint — SH* A-256	12D4 80C1 A3C6 6478 1B99 D9DF 0E9F AF3F 1CAC EE1B 3C30A33 7A4A312 3F FED2

(6) Five (5) years before the date of expiry of the first own digital certificate, the issuer of the SIGEN-CA formed a

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

second own digital certificate, intended to certify the certificates issued by SIGEN-CA to the holders or issuers of safe time stamps from 6.6.2016 onwards.

Certificate No 2 SIGEN-CA shall contain the following information:

Field name	Value of the SIGEN-CA certificate
Version \ “_blank” *Version*	3
ID, *Serial Number*	CD81 8601 0000 0000 571E 043E
Signature algorithm, \ “_blank” *Signature Algorthm*	sh256WithRSAEncrConsumption
Issuing body, \ “_blank” *Issuer*	c = SI, o = Republic of Slovenia, oi = VAT-17659957, cn = SIGEN-CA G2
Holder, *Subject*	c = SI, o = Republic of Slovenia, oi = VAT-17659957, cn = SIGEN-CA G2
Date of entry into force, *Validity: Not Before*	APR 25 11: 19: 25 2016 GMT
End of validity, *Validity: Not After*	APR 25 11: 49: 25 2036 GMT
Public Key Algorithm, \ “_blank” *Public Key Algorthm*	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*	4C25 278C A82D 729E
The identifier of the holder’s key; OID 2.5. *29.14,* *\ “_blank” Subject Key Identifier*	4C25 278C A82D 729E
Certificate footprint (not part of the certificate)	
SHA-1 certificate footprint, *Certificate Fingerprint — SH* A-1	335F 27AE EE7A EA9B D4E3 FE59 EB65 B4AC 8926 E0E7
SHA-256 certificate footprint, *Certificate Fingerprint — SH* A-256	C4B9 BE09 EA4E F4A1 37EC 573A EFC1 23C4 B509 62CF B99A 13DB 4A34 274D

(7) The root issuer SI-TRUST Root has issued a pairing certificate to the SIGEN-CA with the following information:

Field names	Value or importance
Certificate (s) of the underlying (s) in the certificate	
Version \ “_blank” *Version*	3

ID, *Serial Number*	A668 BD51 0000 0000 571D D0E8
Signature algorithm, \ "_blank" *Signature Algorthm*	sh256WithRSAEncrConsumption
Issuing body, \ "_blank" *Issuer*	c = SI, o = the Republic of Slovenia, oi = VAT-17659957, cn = SI-TRUST Root
Holder, *Subject*	c = SI, o = stage institutions, ou = sigen-ca
Date of entry into force, *Validity: Not Before*	May 24 11: 58: 27 2016 GMT
End of validity, *Validity: Not After*	June 27 22: 00: 00 2021 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*	*2048 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*	717B 8A06 1AF31 0555 AB60 1277 4720 1E03 8818 EC89
Certificate footprint (not part of the certificate)	

SHA-1 certificate footprint, *Certificate Fingerprint — SH* A-1	EF9B C82D C8B0 F209 4529 447F 3BB6 6AC9 9C25 7C66
SHA-256 certificate footprint, *Certificate Fingerprint — SH* A-256	E016 01D8 F0D6 9434 E699 735C 4F34 8FC1 5FB4 8FBF2C 2B20 03FE E0F5 4A90 E819 48FD

Field names	Value or importance
Certificate (s) of the underlying (s) in the certificate	
Version \ "_blank" *Version*	3
ID, *Serial Number*	28C3 981D 0000 0000 571D D0E7
Signature algorithm, \ "_blank" *Signature Algorthm*	sh256WithRSAEncrConsumption
Issuing body, \ "_blank" *Issuer*	c = SI, o = the Republic of Slovenia, oi = VAT-17659957, cn = SI-TRUST Root
Holder, *Subject*	c = SI, o = Republic of Slovenia, oi = VAT-17659957, cn = SIGEN-CA G2
Date of entry into force, *Validity: Not Before*	May 24 11: 49: 41 2016 GMT
End of validity, *Validity: Not After*	APR 23 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*	4C25 278C A82D 729E
Certificate footprint (not part of the certificate)	
SHA-1 certificate footprint, *Certificate Fingerprint — SH* A-1	D3C6 C554 C171 F9BA 952C E04C AC2C 1C9B D68B 08D4
SHA-256 certificate footprint, *Certificate Fingerprint — SH* A-256	7950 15CA ACA7 4715 D341 120D 3F0E FD19 2A03 2F1C 0039 1797 F54E F998 0804 A175

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 conditions for carrying out the tasks of the SI-TRUST and act in accordance with the regulations in force.

(2) The role of the application service is:

- verification of the identity of holders/future holders, details of organisations and other necessary data,
- accepting applications for certificates,
- accepting requests for cancellation of certificates,
- acceptance of requests for renewal of special certificates
- verification of claims data,
- issue the necessary documentation to the holders or future holders,
- forward requests and other data in a secure manner to SIGEN-CA.

(3) The role of the registration service for the purposes of the SIGEN-CA is carried out by the authorised person of the application department to check the data on the holders/future holders, the organisation’s data and other necessary data, and to carry out the other tasks mentioned above.

(4) The issuer of SIGEN-CA has established the respective offices in various locations, and the information on this is published on the websites.

1.3.3 Certificate holders

(1) The Subscriber is the subject of certificates *issued* by the organisation or the responsible person of the *subject*.

(2) By signing a certificate request, the responsible person guarantees the organisation and identity of future holders and authorises them to use the certificates on behalf of the organisation.

(3) Holders of certificates are always natural persons. In the case of an information system certificate, code

signature, website and electronic seals, the holder of such certification shall be authorised by the person responsible. The holders may then be:

- Employees
- Employees entrusted with the management of information systems (services or applications),
- staff authorised to use the code signature software;
- The staff authorised to operate the websites,
- Employees authorised to operate electronic seals.

(4) A mutually agreed written agreement shall be concluded between the organisation and the SIGEN-CA/SI-TRUST.

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 specific and online SIGEN-CA certificates issued in the context of the present policy may be used for:

- encryption of data in electronic format;
- authentication of digitally signed data and identification of person signing;
- services or applications for which the use of qualified digital certificates are required under the SI-TRUST.

(2) The use of certificates is linked to the purpose of the corresponding keys. The following options are distinguished:

- The private signing key (hereinafter the *signature key*); and
- The public key for the verification of the signature (hereinafter *the key for signature verification*),
- The private decryption key (hereinafter the *decryption key*); and
- The public encryption key (hereinafter referred to as *the encryption key*).

(3) The issuer of SIGEN-CA also issues certificates for an OCSP for verifying the validity of certificates issued by SIGEN-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*, and in cases where certificates are validated for website authentication and the code signature additionally in the field of the *extended use of the key. Extended Key Message*, see7.1.2.

(2) Each holder of a special certificate belongs to two separate key pairs — for the digital signature/authentication of the signature and for the decryption/encryption of data. Both pairs have one private and public key.

(3) Each holder of an online certificate shall belong to a single key pair, which shall consist of a private and public

key designed for signing/authentication, decryption and encryption of data.

(4) An overview of the use of certificates and keys is given in the table below.

Certificate type	Key pair	Associated keys	Purpose
specific to employees and to employees with a general title	digital signature/authentication pair (certificate for signature verification)	- Signature key - Signature authentication key	signature/authentication
	decryption/encryption pair (encryption certificate)	- Decryption key - Encryption key	decryption/encryption
online for employees and for employees with a general title	digital signature/authentication and decryption/encryption	- Private key - Public Key	signature/authentication and decryption/encryption
information systems online	digital signature/authentication and decryption/encryption	- Private key - Public Key	signature/authentication and decryption/encryption
online for the signature of the code[2]	digital signature/authentication pair (certificate for signature verification)	- Signature key - Signature authentication key	signature/authentication enforceable software codes
website authentication[3]	digital signature/authentication and decryption/encryption	- Private key - Public Key	signature/authentication and decryption/encryption of secure links
electronic seal online	digital signature/authentication pair (certificate for signature verification)	- Signature key - Signature authentication key	signature/authentication

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.

[2] The purpose of the code signature certificate is further limited to the authentication of an executable code.

[3] The purpose of using a certificate for website authentication is further limited to creating a secure connection.

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 issuer of SIGEN-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 operation of the SIGEN-CA.

(2) In the structure of a public digital certificate directory, located on the x500.gov.si *server, they publish with* e:
- registration details of the certificate (holder name, e-mail address, serial number...),
- valid digital certificates (set out in more detail below. 7.1) and
- register of invalidated digital certificates (set out in more detail below. 7.2).

(3) The other documents or key information on the operation of the issuer of SIGEN-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 SIGEN-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) The publicly available information/documents, digital certificates and the register of invalidated certificates are available in 24ur/7dni/365dni without restrictions.

(2) The public directory, which holds the certificates, is accessible to the public *on* the x500.gov.si server protocol.

(3) The certificates are also available via the SIGEN-CA website under the HTTPS protocol:

https://www.si-trust.gov.si/sl/ss-obrazci/iskanje-digitalnih-potrdil-si-trust/.

(4) The SI-TRUST or issuer of SIGEN-CA concerns the authorised and safe addition, modification or deletion of information in the public directory of the certificates.

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 background information, including the organisation, in *the subject field,* see the table below.

(4) In the case of a certificate, the name included in the discriminatory name shall be:

- for employees, the holder’s name and surname,
- For employees with the general name (s) of the organisation (s) of organisation and/or organisation unit of the organisation, as well as the holder’s first name and surname,
- for the information systems, the name of the system,
- to sign the code, the name of the organisation (s) of its organisational unit (s),

- in order to authenticate the websites, the website has the registered name;
- for electronic seals, a label unambiguously representing the organisation or its service.

(5) The details of the organisation are given in the distinctive name in the form of a code of organisation and its tax number (see also the following subchapter).

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

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

Type of certificate	Field name	Distinguished Name[6]

certificate from the issuer of SIGEN-CA	issuing body, *issued*	c = SI,
		o = the Republic of Slovenia,
		OI = VATSI-17659957,
		CN = SIGEN-CA G2

special certificates for employees	Holder, Subject	c = SI,
		ST = Slovenia,
		o = the organisation code >,
		OI = VATSI —< Taxation No of Organisation >,
		CN = < name >,
		GN = < Name >,
		SurName = < Surname >
		SN = serial number >

special certificates for employees with the general title of the organisation (s)	Holder, Subject	c = SI,
		ST = Slovenia,
		o = the organisation code >,
		OI = VATSI —< Taxation No of Organisation >,
		CN =,
		GN = < Name >,
		SurName = < Surname >
		SN = serial number >

online employee certificates	Holder, Subject	c = SI,
		ST = Slovenia,
		o = the organisation code >,
		OI = VATSI —< Taxation No of Organisation >,
		CN = < name >,
		GN = < Name >,
		SurName = < Surname >
		SN = serial number >

online certificates for employees with the general title of the	Holder, Subject	c = SI,
		ST = Slovenia,

[4] The SIGEN-CA certificate shall not contain any serial number.

[5] The rules for the production of discriminatory names for other types of certificate shall be determined and published by the SIGEN-CA.

[6] importance of individual designations: general government ("c"), organisation ("o"), organisational unit ("ou"), name ("cn"), a serial number ("sn").

organisation (s)		o = the organisation code >,
		OI = VATSI —< Taxation No of Organisation >,
		CN =,
		GN = < Name >,
		SurName = < Surname >
		SN = serial number >

online certificates for information systems	Holder, Subject	c = SI,
		ST = Slovenia,
		o = the organisation code >,
		OI = VATSI —< Taxation No of Organisation >,
		CN =,
		SN = serial number >

online certification for the signature of the code	Holder, Subject	c = SI,
		ST = Slovenia,
		o = the organisation code >,
		OI = VATSI —< Taxation No of Organisation >,
		CN =,
		SN = serial number >

web certificates for website authentication	Holder, Subject	c = SI,
		ST = Slovenia,
		o = the organisation code >,
		OI = VATSI —< Taxation No of Organisation >,
		L = < Place of Organisation >,
		BC = < type of organisation >,
		JUR = level of registration >,
		CN =,
		SN = NTRSI — < identification No of the organisation >/SITRUST — < serial number >

online certificates for electronic seals	Holder, Subject	c = SI,
		ST = Slovenia,
		o = the organisation code >,
		OI = VATSI —< Taxation No of Organisation >,
		CN =,
		SN = serial number >

3.1.2 requirement to make sense of names

(1) Code of the organisation complying with the sub-items. 3.1.1Included in the discriminatory name must meet the following requirements:

- Be registered in a commercial or other official register[7],
- The maximum length may be sixty (60) characters[8].

[7] The mark must be derived from the registered short or full name of the organisation.

[8] In the case of a registered name of more than 60 characters, the mark shall be designated as the first 60 characters of the name.

(2) The SIGEN-CA reserves the right to refuse the title if it finds:

- improper or offensive,
- that it is misleading for third parties or belongs to another legal or natural person,
- that it is contrary to the rules in force.

(3) In case of a certificate for website authentication, the website name should be populated with a full domain name *(Fully validated native name*).

(4) 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 certificate issued by SIGEN-CA	2	
2-8 City	unique number of holder	//OR	
9 — 10 rd place	label for special certificate	employed	20
		employed by common title	22
	tag for web certificate	employed	16
		employed by common title	18
		information system	10
		signature of the code	19
		website	13
		electronic seal	15
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

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

(2) Proof of possession of the means for secure storage of private keys and certificates granted by the issuer to the holder shall be held at SIGEN-CA.

3.2.2 Identification of organisations

(1) Information about the organisation is given in the form of an organisation's code and its tax number, see below. 3.1.1And3.1.2.

(2) The responsible person of the organisation shall guarantee the accuracy of the data by signing the certificate request.

(3) The issuer of the SIGEN-CA verifies the accuracy of the data on the organisation and identity of the person responsible in the relevant services or in the official records.

(4) In online authentication certificates for websites, the issuer of SIGEN-CA controls ownership of, and control over, the online domain in primary and all additional names of websites in one of the following ways:

- the issuer of the SIGEN-CA sends a unique tag to the email addresses 'admin', 'Administrator', 'Webmaster', 'hostmaster' and 'post-master' web domains on behalf of the website; allow the certificate to be issued when it has been approved for each domain domain.
- The issuer of the SIGEN-CA sends the unique identifier to the email address set out in the label *Contactemail* of the CAA message; allow the certificate to be issued when it has been approved for each domain domain.
- for web domains registered with the Ministry of Public Administration, the issuer of the SIGEN-CA shall check the domain ownership of the domain owner's contact person; the issue of the certificate shall be made available once it has been approved for each domain domain.

(5) In online authentication certificates for websites, the issuer of SIGEN-CA verifies the credentials of the CAA for the online domain into basic and all additional names of websites and allows the certificate to be issued if for each web domain:

- There is no *issue marking issued by the* CAA of the CAA; or
- An *issue label of* the CAA of the CAA with the value "sis-trust.gov.si" exists.

3.2.3 Identity check

(1) For its employed persons, the organisation shall verify their identity by means of the SIGEN-CA, that is to say

the responsible person of the organisation shall guarantee:

- For the identity of the prospective holder of the certificate, which he has verified in accordance with the applicable legislation; and
- that the proposed holder is either employed by the organisation and wishes to obtain a certificate or performs tasks for the organisation for which that certificate is to be obtained,

(2) The issuer of SIGEN-CA verifies the identity of the holders in the relevant registers.

(3) The e-mail address of the holder of the SIGEN-CA verifies that the email address given in the request is valid, in such a way that the SIGEN-CA sends the message to the prospective holder at the time of acceptance of the request. If this message is rejected, acceptance of the ECS is not possible.

3.2.4 Non-verified initial verification data

(1) The unverified information in the certificate is the name for:

- General titles;
- information systems and
- signature of the code; and
- the name of the websites.

(2) The organisation and the holder shall guarantee the accuracy of the information referred to above.

3.2.5 Validation of authority

The organisation or the responsible person of the organisation shall, by means of a signature, guarantee that he/she wants a specific person who is an employee or who performs tasks for that organisation, to obtain a certificate either for himself or for an information system, the signature of a code, a website or an electronic seal with which that person will operate.

3.2.6 criteria for interoperation

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

(2) The issuer of SIGEN-CA shall not liaise with other issuers on each other.

(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

(1) The renewal of special certificates shall take place under the protocol of the PKI-CMP protocol where the holder identifies himself by holding a valid private key.

(2) However, when the online certificate is renewed, the identity of the holder must be checked again in accordance with the procedure laid down in the box. 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 revocation of the certificate shall be submitted by the holder or the responsible person:

- in person, with the application service, where the person responsible shall verify the identity of the applicant;
- electronically, however, the request must be digitally signed by the private key that belongs to the digital certificate, which has been issued by the SI-TRUST and thus also demonstrates the identity of the applicant.

(2) In case of cancellation by telephone on the SIGEN-CA hotline number, the holder must provide the password chosen for this purpose.

(3) 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 employed by the organisation for which they wish to obtain a certificate. In the case of an information system certificate, code signature, website authentication, and electronic seal authentication, the holder of such certificate shall be authorised by the person responsible. This will be done in detail in the sub-area. 1.3.3 YES/NO.

4.1.2 Enrolment process and responsibilities

(1) In order to obtain the certificate, the prospective holder and the person responsible must duly complete and sign the application for the certificate.

(2) The acquisition requests are made available through the application services or other authorised persons of the issuer of SIGEN-CA and on the SIGEN-CA web pages.

(3) The person responsible may, by his or her signature, authorise another person to bring a claim to the application service.

(4) In order to obtain a certificate, the prospective holder and the person responsible shall be required to:

- complete the certificate request with real and correct data;
- provide it in a secure manner with the application service,
- carry out the acceptance of the certificate in a secure manner on the instructions of the SIGEN-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

(1) The responsible person of the organisation where the prospective holder of the certificate is employed shall guarantee the identity of the prospective holder of the certificate, which it has verified in accordance with the applicable legislation.

(2) The issuer shall verify the identity of the prospective holder and any information on the future holder and organisation indicated in the application and made available in the official records or other official documents in force.

4.2.2 Approval/rejection of the application

(1) Before submitting the request, the issuer shall inform the responsible person and the prospective holder of the documentation required in accordance with the applicable legislation.

(2) The request for a certificate shall be approved or, in the case of incorrect or incomplete information or failure to comply with the obligations set out in the agreement by the organisation, the duly authorised persons shall refuse the SI-TRUST.

(3) Approval or refusal is notified to the prospective holder by e-mail.

4.2.3 Time to issue the certificate

Following an approved application and arrangement between the organisation and the SI-TRUST, the authorisation code and the reference number shall be transmitted by the SIGEN-CA to the holder of the digital certificate at the latest within ten (10) days of the 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 SIGEN-CA, the authority shall forward to the future holder of the certificate a reference number and an authorisation code along two separate routes: the reference number is sent by e-mail and by mail delivery by email and, exceptionally, can be handed over by the designated person under the authority of SIGEN-CA. Both information will need to be taken over by the prospective holder to take over the digital certificate.

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

(3) The issued SIGEN-CA certificate is published both in a public directory and on websites (see below. 4.4.2).

4.3.2 notification by the holder of the issuing of a certificate

(1) The prospective holder shall be informed of the authorisation or rejection of the request to obtain a digital certificate.

(2) Two (2) months before the date of the certificate or key issuer SHALL be notified by e-mail of the holder.

4.4. Certificate acceptance

4.4.1 Certificate acceptance procedure

(1) To take over the certificate, the prospective holder needs a reference number and an authorisation code issued by the SIGEN-CA, see below. 4.3 YES/NO.

(2) Detailed instructions for taking over all types of certificates under this policy can be found on the website https://www.si-trust.gov.si/sl/digitalna-potrdila/poslovni-subjekti/. Also, all new developments relating to the way certificates are accepted have also been published on the website.

(3) Immediately upon receipt of the certificate, the titular holder shall check the information contained in this certificate. To the extent that the issuer does not inform the SIGEN-CA of any errors, it is considered to agree with the contents of the agreement and to agree to the conditions of operation and assumption of liabilities and responsibilities.

(4) After receiving the reference number and the authorisation code, the prospective holder of the certificate must accept the certificate within 60 (60) days of the reservation of the certificate. At the request of the prospective holder, it is possible to extend the take-over time for the new sixty (60), otherwise the booking of the certificate shall be cancelled by the SIGEN-CA.

(5) Once the certificate has been taken over, they become the reference number and the authorisation code unusable.

4.4.2 publication of the certificate

The certificate issued shall be made publicly available in the SI-TRUST, as indicated in the funeral. 2YES/NO.

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) In order to protect the private keys, the holder or prospective holder of the certificate shall be obliged to:

- carefully protect the data to take over the certificate against unauthorised persons,
- store the private key and the certificate in accordance with the notices and recommendations of the SIGEN-CA;
- protect private keys and any other confidential information by means of a suitable password in accordance with the recommendations of the SIGEN-CA or in any other way such that only the holder has access to it;
- carefully protect passwords to protect private keys;
- once the certificate has expired, the certificate shall be handled in accordance with the SIGEN-CA

notifications.

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

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

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 a certificate (valid for special certificates only)

(1) In the case of special certificates, it shall be possible to renew the certificate which may be carried out automatically before the expiry of the certificate or as recovery of keys at the holder's request.

(2) The special certificate to be renewed shall contain the same distinguishing name as the original certificate.

(2) The automatic generating of new key pairs and the extension of the validity of the special certificate shall be performed automatically under the safe-harbour protocol of the PKI-CMP certificate at the first use of the holder's certificate with direct access to the SIGEN-CA infrastructure over a hundred (100) days prior to the last day of validity of the certificate.

(4) The automatic extension of the validity of special certificates issued before 6.6.2016 and signed with certificate No 1 from the SIGEN-CA is not supported.

4.7.1 keys to key regeneration

(1) The renewal of the keys for the special certificate shall be carried out if the holder of the certificate:
- remember to forget your password to private keys.
- loses or damages media for the storage of key data for the use of the certificate;
- does not automatically extend the validity of the Certificate,
- it has not accessed its confirmation until such time as the digital signature key has expired and thus has access to the certificate.

(2) Subject to safety conditions, the SI-TRUST shall reserve an autonomous decision between:
- keys regenerated
- or a revocation.

(3) The recovery of keys of special certificates issued before 6.6.2016 and signed with certificate No 1 of the issuer of SIGEN-CA is allowed only for the purposes of accessing the decryption keys history of the decryption keys of prior agreement with the SIGEN-CA. the procedure may only be run until the expiry date of certificate No 1 of the SIGEN-CA certificate until 29.6.2021.

4.7.2 who can ask for the key to be regenerated

Regeneration may be requested by the holder of the certificate together with the responsible person.

4.7.3 Process for key recovery

(1) The clearance of the certificate keys is carried out on the basis of a completed recovery request from the holder of the certificate and the responsible person submitted to the SIGEN-CA application service.

(2) As for the issuance of a new certificate, the holder of the reference number and the authorisation code for accessing the encryption key pair shall receive the reference number and the creation of a new source pair.

(3) The SIGEN-CA shall transmit to the holder the authorisation code and the reference number at the latest within ten (10) days of the processing of the request for regeneration (Podstl. 4.7.1).

(4) The regeneration process must be carried out by the titular holder within sixty (60) days of the reservation of the certificate. At the request of the holder, it is possible to prolong the regeneration time for the new sixty (60), otherwise the booking of the certificate shall be cancelled by the SIGEN-CA.

(5) Upon completion of regeneration, the reference number and the authorisation code are rendered unusable.

4.7.4 Notification to the holder about the recovery of keys

The procedure is the same as for the first issue of the certificate, see below. 4.3.2YES/NO.

4.7.5 Acceptance of a regenerated certificate

The procedure is the same as for the first acquisition of the certificate, see below 4.4.1.

4.7.6 Publication of a renewed certificate

The procedure is the same as for the first acquisition of the certificate, see below 4.4.2.

4.7.7 Issue notice to other entities

The procedure is the same as for the first acquisition of the certificate, see below 4.4.3.

4.8. Certificate modification

(1) If there is a change in the data affecting the validity of the distinguishing name entered in the certificate, the certificate shall be cancelled.

(2) In order to obtain a new certificate, it is necessary to repeat the procedure 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[9]

4.9.1 Reasons for cancellation

(1) Revocation of a certificate must be requested by the holder or the responsible person of the organisation in the case of:

- where private keys of the certificate holder were compromised in a manner that affects the reliability of use,
- if there is a risk of misuse of private keys or certificates from the holder,
- if the incorrect key information indicated in the certificate has changed or is incorrect,
- if the holder ceases to be employed by the organisation, or has ceased working for the organisation, or is no longer authorised to use the certificate.

(2) The issuer of the SIGEN-CA shall also withdraw the certificate without the request of the holder or the responsible person of the organisation as soon as it becomes aware of:

- that the holder of the certificate has ceased to work in or for an organisation,
- 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;
- failure of the holder/organisation from this policy and the arrangement between the organisation and the SI-TRUST,
- that the costs for the management of the digital certificates have not been settled,
- the SI-TRUST infrastructure has been threatened in a way that affects the reliability of the certificate,
- that private keys of the certificate holder have been compromised in a manner that affects the reliability of use;
- that the SIGEN-CA has ceased to issue certificates, or that the SI-TRUST prohibited management of certificates and its activities has not been taken over by another trust service provider,
- revocation ordered a competent court or administrative authority.

[9] According to the recommendation of RFC 3647, this subchapter includes a suspension procedure, which is not facilitated by the SIGEN-CA.

4.9.2 Who may request cancellation

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

(2) The revocation of the certificate may also be requested by the responsible person of the organisation.

4.9.3 Cancellation procedure

(1) Revocation may be requested by the holder:

- in person during official opening hours,
- by electronic mail twenty four (24) hours a day, every day of the year in the case of the possibility of misuse or unreliability of the certificate, at the time considered by the applicable legislation for the business time of the public authorities,
- the frequency of 24 (24) hours per day for all days of the year in the case of the possibility of misuse or unreliability of the certificate, at the time considered by the applicable legislation for the business time of the public authorities.

(2) Revocation may be requested by the person responsible for the organisation:

- in person during official opening hours,
- by electronic mail of 24 (24) hours a day, every day of the year in the case of misuse of the certificate, at the time considered by the applicable legislation for the business time of the public authorities.

(3) If the operation of the SI-TRUST is substantially reduced as a result of unforeseen events, the holder or the responsible person may only request the cancellation in person during the official hours of the application.

(4) Where revocation is required:

- in person, an appropriate request for revocation of the certificate must be completed and submitted to the application service;
- electronically, the holder or the responsible person of the organisation must send to the SIGEN-CA an email with a revocation request, digitally signed with a trusted certificate for its authentication. When doing so, the issuer of a cancellation request must at the same time notify the SIGEN-CA of this telephone call number for cancellations (see below). 1.3.1);
- the telephone must be called on by the holder by means of a telephone hotline for cancellations (see below. 1.3.1The holder must indicate the password provided by the holder in the corresponding application for certification as a password for revocation of the certificate or otherwise securely relayed to the SIGEN-CA. without a revocation password, the holder may not override the certificate by telephone.

(5) The date and time of withdrawal, the issuer of the cancellation request and the reasons for the revocation shall be communicated to the holder and the person responsible by e-mail.

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

4.9.4 Time to issue cancellation request

The cancellation request should be requested without delay in the case of the possibility of an abuse or unreliability, etc., of urgency, or otherwise the first working day for the time applicable to the business time of the national authorities or official hours of the application services (cf. the following subchapter).

4.9.5 Time spent on cancellation request received until revocation

(1) Following receipt of a valid cancellation request, the SI-TRUST:

- to cancel the certificate within a maximum of four (4) hours if the risk of misuse or unreliability, etc.,
- otherwise, on the first working day following receipt of the request for cancellation.

(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 cancelled certificates and to be deleted from the public directory of the certificates[10].

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

[10] Only the record details of the certificate remain in the public directory.

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-sigen-ca/, on-line verification of the status of the certificate is available at http://ocsp.sigen-ca.si, and the access details are in the sub-set. 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 (valid only for special certificates)

(1) The SIGEN-CA keeps the history of the decryption keys and discovers a copy of it only in exceptional cases, where the latter are not accessible for any reason, for access to the service data that is encrypted and accessible only with the decryption key of the holder.

(2) The SIGEN-CA reserves the right not to authorise the discovery of a copy of the decryption keys in the case of a certificate that has been cancelled due to incorrect information in the certificate.

(3) The detection of the copy of the decryption keys for certificates issued before 6.6.2016 and signed with certificate No 1 from the issuer of SIGEN-CA can only be carried out until certificate No 1 of the issuer of SIGEN-CA is valid until 29.6.2021.

4.12.1.1 Who requests the detection of a copy of the decryption keys

A copy of the decryption keys may be requested by:

- the responsible person, on the basis of an application for the detection of a copy of the decryption keys for access to data that is encrypted and accessible with the decryption keys of the person's decryption key,
- the competent court or administrative authority.

4.12.1.2 Procedure in case of request for the detection of a copy of the decryption keys

(1) The responsible person must complete the request to detect the copy of the decryption keys and transmit it in a secure manner to the SIGEN-CA.

(2) SIGEN-CA detection of a copy of the decryption keys:

- inform the holder of the certificate of the date and the issuer of the copy of its data keys for the decryption of the data by e-mail, and
- it shall revoke the certificate and inform the holder of the revocation by electronic means.

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 service provider and trusted role

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 Type of event (s)

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 case of renewal of an SIGEN-CA certificate, the process is published on the SIGEN-CA web pages.

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 generation of the SIGEN-CA pair of keys for signing and authentication is the formal and controlled procedure with the installation of the SIGEN-CA software for which a separate record is kept (document "publisher of the process of generating the SIGEN-CA-2 keys"). 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 SIGEN-CA's IT system shall be documented in a separate report or in an appropriate log.

(4) To generate the SIGEN-CA pair of key pairs, the machine security module shall be used (see below). 6.2.1).

(5) The holders' keys shall be generated depending on the type of certificate according to the table below.

Certificate type	Certificate	The key is generated
specific to employees and to employees with a general title	digital signature key pair (certificate for signature verification)	at the holder
	pair of decryption/encryption keys (encryption certificate)	In the case of SIGEN-CA
online for employees, for employees with a general title, information systems and website authentication	digital signature key pair/authentication and decryption/encryption	at the holder
certificate for signature of code and electronic seals	digital signature key pair (certificate for signature verification)	at the holder

6.1.2 Delivery of private key to holders

The method of secure private key transfer is given in the table below.

Certificate type	Certificate	Key	Delivery

special	digital signature/authentication pair (certificate for signature verification)	private signing key	no transfer[11]
	decryption/encryption pair (encryption certificate)	private decryption key	transfer from issuer to holder through PKI-CMP
online	digital signature/authentication and decryption/encryption	private key	no transfer

6.1.3 delivery of the certificate to the issuer of the certificates[12]

In the acceptance procedure, holders shall deliver their public key for signature by SIGEN-CA under the PKI-CMP protocol for special certificates and PKCS # 7 protocol for online certificates.

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

(1) The ECS Public Key Certificate shall be published in the SI-TRUST Repository (see sub-items. 2.1).

(2) The certificate with the public key of the issuer of SIGEN-CA has been delivered to the holder (s) delivered to, or made available to, the holder:

- In the public directory *x500.gov.si* on the LDAP protocol (see below. 2.3),
- in the form of PEM at https://www.si-trust.gov.si/assets/si-trust-root/povezovalni-podrejeni/sigenca/sigen-ca.xcert.pem or https://www.si-trust.gov.si/assets/si-trust-root/povezovalni-podrejeni/sigenca-g2/sigen-ca-g2.xcert.pem
- via the PKI-CMP protocol for special certificates and PKCS # 7 for online certificates.

6.1.5 Key length

Certificate	RSA key length [bit]
certificate from the issuer of SIGEN-CA	3072
certificate for: • employed • employees with a general title • information systems • signature of the code • website authentication • electronic seals	2048[13]
OCSP certificate	2048

6.1.6 Generating and quality of public key parameters

[11] The key is generated by the holder and never stored in the SIGEN-CA.

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

[13] Value means the prescribed minimum length.

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

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

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

6.2.2 Private key control by authorised persons

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

6.2.3 detecting a copy of the private key

(1) The SIGEN-CA detects copies of the private key for decryption for special certificates for which it is determined from the rat. A6.1.1 key on the side of the issuer of SIGEN-CA.

(2) The procedure for detecting a copy of the private key for decryption for special certificates is laid down in the subpoena. 4.12YES/NO.

6.2.4 backup of private keys

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

(2) Backup private keys for decryption of special certificates (in accordance with the determination of the rat. They6.1.1 are stored and stored regularly in two separate and physically protected areas in the encrypted SIGEN-CA bases.

6.2.5 Private key archiving

The SIGEN-CA shall archive copies of the private keys for the decryption of specific certificates (in accordance with the determination of the rat. 6.1.1), as specified in the sub-area. 5.5YES/NO.

6.2.6 Transfer of private key from/to cryptographic module

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

(2) The private keys for the decryption of special holders' certificates shall be transferred from the place where they are created, i.e. to the issuer of the SIGEN-CA, to the holder of the site under the protocol of the PKI-CMP

protocol.

(3) The other private keys of the holders are generated from the holder.

6.2.7 Private key record in a cryptographic module

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

(2) Holders shall have access to their private key by means of a password with relevant applications.

6.2.8 Procedure for the activation of the private key

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

(2) Holders must use both a software environment that requires an appropriate password to be entered for the activation of their private key.

6.2.9 Procedure for deactivation of the private key

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

(2) Holders must use both the software that prevents access to their private key at the time of departure or at the specified time of time without entering an appropriate password.

6.2.10 procedure for the destruction of the private key

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

(2) The destruction of private keys on the part of the holders is the responsibility of the holders. They must use the relevant secure certificate deletion applications.

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
special certificate for employees and employees with a general title	digital signature/authentication pair (special certificate — for signature verification)	private signing key	5 years
		public key for signature verification	5 years
	decryption/encryption pair (special certificate — for encryption)	private decryption key	5 years
		public key for encryption	5 years
online certificate for employees, for employees with a general title and for information systems	digital signature/authentication and decryption/encryption	private key	5 years
		public Key	5 years
web certificate for website authentication	digital signature/authentication and decryption/encryption	private key	27 months
		public Key	27 months
web certificate for the signature of code and electronic seals	digital signature/authentication pair (certificate for signature verification)	private signing key	5 years
		public key for signature verification	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) Authorised persons of the issuer to access the private key of SIGEN-CA shall use the strong passwords with which they comply with the SI-TRUST policy.

(2) The activation data, i.e. the reference number and the authorisation code required for the acceptance of the certificate, are generated on the SIGEN-CA page.

(3) Holders shall determine a password to protect access to their private keys.

(4) The SIGEN-CA recommends the use of secure passwords:
- mixed use of large and small letters, numbers and special characters,
- a length of at least 8 characters,
- It advises against the use of the words written in the dictionaries.

6.4.2 Password protection

(1) The passwords of the issuer of the SIGEN-CA issuer shall be stored under the SI-TRUST policy.

(2) Activation data for certification shall be secure from SIGEN-CA.

(3) The SIGEN-CA shall forward to the future holder of the certificate the reference number and the authorisation code along the following two separate routes:
- reference number by e-mail,
- Author’s code by post,
- however, they shall also, exceptionally, be handed over in person.

(3) Until the certificate is taken over, the prospective holder must carefully protect the activation data to take over the certificate, become unusable after acceptance of the certificate and can be discarded by the holder.

(4) The SIGEN-CA recommends that the private key access password is not stored or stored in a safe place and that only the holder has access to it.

(5) The SIGEN-CA advises 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 SIGEN-CA issues and deals with the following types of certificate for organisations' needs in this section[14]:

- special certificates for employees,
- online certificates for employees,
- special certificates for employees with the general title of the organisation or organisational unit,
- online certificates for employees with the general title of the organisation or organisational unit,
- online certificates for information systems,
- online certification for the signature of the code,
- web certificates for website authentication, and
- online certificates for electronic seals.

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

(3) Issuer SIGEN-CA certificates shall be followed by standard *X.509.*

7.1.1 Certificate version

All certificates issued by the issuer of SIGEN-CA are followed by standard *X.509*, version 3, according to RFC 5280.

7.1.2 profile of extensions

7.1.2.1 Profile of SIGEN-CA certificate

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

7.1.2.2 Certificate Profile for Holders

The basic information contained in the certificate is given below and the other data are contained according to the type of certificate below:

Field names	Value or importance
Certificate (s) of the underlying (s) in the certificate	
Version \ "_blank" *Version*	3

[14] Certificate from the issuer of SIGEN-CA is already given in detail 1.3.1YES/NO.

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 = Republic of Slovenia, oi = VAT-17659957, cn = SIGEN-CA G2
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, depending on the type of certificate (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*	The *holder’s e-mail address, see out 7.1.2.3.* the *name of the website for website authentication certificates, see below. 7.1.2.4*

The publication of a register of cancelled certificates, OID 2.5.29.31,
\ “_blank” *CRL Distribution Points*
	URI: http://www.sigen-ca.si/crl/sigen-ca-g2.crl
	URL: ldap://x500.gov.si/cn=SIGEN-CA G2;
	OI = VATSI-17659957,
	o = the Republic of Slovenia,
	c = SI? certificateRequationList
	c = SI,
	o = the Republic of Slovenia,
	OI = VATSI-17659957,
	CN = SIGEN-CA G2,
	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.sigen-ca.si Access Method: CaIssuer (OID 1.3.6.1.5.5.7.48.2) Access Location: URL = http://www.sigen-ca.si/crt/sigen-ca-g2-certs.p7c
Key Usage, OID 2.5.29.15, \ *“_blank” Key Usage*	*depending on the type of certificate, see below. 7.1.2.2.1 and 7.1.2.2.2*
The extended application of the key; OID 2.5.29.37, \ “_blank” *Extended Key Usage*	*depending on the type of certificate, see below. 7.1.2.2.1 and 7.1.2.2.2*
Key of the issuer key; OID 2.5.29.35, \ “_blank” Hash *Key Identifier*	4C25 278C A82D 729E
The identifier of the holder’s key; OID 2.5. *29.14,* \ *“_blank” Subject Key Identifier*	*subject Key Identifier*

The policy under which the certificate was issued, OID 2.5.29.32, certificatePolicies	Certificate Policy: PolicyIdentifier = *depending on the type of certificate, see below.* *7.1.2.2.1 and 7.1.2.2.2* [1,1] Policy qualifier Info: policy qualifier 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. 7.1.2.2.1 and 7.1.2.2.2*
Basic restrictions, OID 2.5.29.19, \ "_blank" *Basic Constrants*	CA: FALSE No length limitation Constraint: None)
Certificate footprint (not part of the certificate)	
SHA-1 certificate footprint \ "_blank" *Certificate Fingerprint — SHA-1*	*recognisable print of the certificate after SHA-1*
SHA-256 certificate footprint \ "_blank" *Certificate Fingerprint — SHA-256*	*recognisable print of the certificate after SHA-256*

7.1.2.2.1 Profile of special certificates

(1) Both certificates of the special certificate, i.e. the encryption certificate and the certificate for the verification of signature, shall include the data set out in the above table. However, certain fields in the certificate, which depend on the nature of the certificate, are set out below.

(2) The values of the *key* fields, the *policy* and the *code of the qualified certificate* for the encryption certificate are given in the table below.

Field name	Value in the encryption certificate	
	employed	employed by common title
Key Usage, *Key Usage*	Key Encipherment	
The extended use of the key, *Extended Key Usage*	//OR	
The policies under which the certificate (OID) has been issued and which also indicate that it is a qualified certificate, *Certificate Policies*	Policy: 1.3.6.1.4.1.6105.2.1.2.5	Policy: 1.3.6.1.4.1.6105.2.1.4.5
Qualified certificate identifier, OID 1.3.6.1.5.5.7.1.3, QcStatements *statement*	//OR	

(3) The values of the *key* fields, the *policy* and the *code of the qualified certificate* for the certificate for the verification of signature are given in the table below.

Field name	Signature verification certificate value	
	employed	employed by common title
Key Usage, *Key Usage*	Digital Signature, ContenPurpose ment	
The extended use of the key, *Extended Key Usage*	//OR	

The policies under which the certificate (OID) has been issued and which also indicate that it is a qualified certificate, *Certificate Policies*	Policy: 1.3.6.1.4.1.6105.2.1.2.5 0.4.0.194112.1.0	Policy: 1.3.6.1.4.1.6105.2.1.4.5 0.4.0.194112.1.0
Qualified certificate identifier, OID 1.3.6.1.5.5.7.1.3, QcStatements *statement*	QcCompliance statement QcType: eSign PdsLocation: https://www.ca.gov.si/cps/sigenca1_pds_en.pdf https://www.ca.gov.si/cps/sigenca1_pds_sl.pdf	

(4) Field *Application* field *The key* message shall be marked as critical for all types of special certificates.

7.1.2.2.2 Web certificate profile

(1) The web certificate shall include the data set out in the table in the table below. 7.1.2 YES/NO. The values of the *key fields,* the *extended use of the key, the policy and the qualified certificate code,* but which depend on the type of certificate*,* are given in the table below for the online certificate.

Field name	Online certificate value			
	employed	employed by common title	information system	signature of the code
Key Usage, *Key Usage*	Digital Signature, Key Encipherment, ContenPurpose ment		Digital Signature, Key Encipherment	Digital Signature
The extended use of the key, *Extended Key Usage*	//OR		//OR	Code Signing
The policies under which the certificate (OID) has been issued and which also indicate that it is a qualified certificate, *Certificate Policies*	Policy: 1.3.6.1.4.1.6105.2.1.1.5 0.4.0.194112.1.0	Policy: 1.3.6.1.4.1.6105.2.1.3.5 0.4.0.194112.1.0	Policy: 1.3.6.1.4.1.6105.2.1.5.5	Policy: 1.3.6.1.4.1.6105.2.1.6.5
Qualified certificate identifier, OID 1.3.6.1.5.5.7.1.3, QcStatements *statement*	QcCompliance statement QcType: eSign PdsLocation: https://www.ca.gov.si/cps/sigenca1_pds_en.pdf https://www.ca.gov.si/cps/sigenca1_pds_sl.pdf		//OR	

Field name	Online certificate value	
	website authentication	electronic seal
Key Usage, *Key Usage*	Digital Signature, Key Encipherment,	Digital Signature, ContenPurpose ment
The extended use of the key, *Extended Key Usage*	serverAuth, climentAuth	//OR
The policies under which the certificate (OID) has been issued and which also indicate that it is a qualified certificate, *Certificate*	Policy: 1.3.6.1.4.1.6105.2.1.7.5 0.4.0.194112.1.4	Policy: 1.3.6.1.4.1.6105.2.1.8.5 0.4.0.194112.1.1

Policies		
Qualified certificate identifier, OID 1.3.6.1.5.5.7.1.3, QcStatements *statement*	QcCompliance statement QcType: web PdsLocation: https://www.ca.gov.si/cps/sigenca2_pds_en.pdf https://www.ca.gov.si/cps/sigenca2_pds_sl.pdf	QcCompliance statement QcType: onesal PdsLocation: https://www.ca.gov.si/cps/sigenca2_pds_en.pdf https://www.ca.gov.si/cps/sigenca2_pds_sl.pdf

(2) Field *Application* field *The key* message shall be marked as critical for all types of online certificates.

7.1.2.3 Requests for e-mail address

(1) The e-mail address must meet the following requirements:
- be valid, and
- must have a strong link with the holder or organisation.

(2) The SIGEN-CA reserves the right to refuse the application for certification if it finds that the e-mail address is:
- abusive or offensive,
- that it is misleading to third parties,
- represents another legal or natural person,
- it is contrary to the rules and standards in force.

7.1.2.4 Requirements for the name of the website

(1) The name of the website shall be the full domain name indicated on the distinctive name (s) (see paragraph 2 below. 3.1.2).

(2) In addition to the name of the website mentioned in the distinctive name, the holder may add up to 4 additional names of the website.

7.1.3 Algorithm identification markings

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

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 SIGEN — CA*
The distinguishing name of the issuer; \ "_blank" *Issuer*	c = SI, o = Republic of Slovenia, oi = VAT-17659957, cn = SIGEN-CA G2
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 = SIGEN-CA G2, cn = CRL < *serial number* of the register >	- Ldap://x500.gov.si/cn=CRL< *register serial number* >, cn = SIGEN-CA G2, oi = VAT-17659957, o = Slovenia, c = SI
full Register	C = SI, o = the Republic of Slovenia, oi = VAT-17659957, cn = SIGEN-CA G2 (*in "CertificationRevolationList")*	- Http://www.sigen-ca.si/CRL/sigen-Ta-g2.crl - Ldap://x500.gov.si/cn= SIGEN-CA G2, 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 is available at http://ocsp.sigen-ca.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

The costs of management of certificates are calculated on the basis of the published price list on the website https://www.si-trust.gov.si/sl/digitalna-potrdila/poslovni-subjekti/.

9.1.2 Access price for certificates

Access to the directory issued by the issuer of SIGEN-CA is free of charge.

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

Access to the certificate status and to the registry of the cancelled certificates issued by the Validator 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 or responsible person of an organisation authorises the SI-TRUST or issuer of SIGEN-CA to use personal data for a certificate or later in a written form.

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 the holder or the responsible person of the organisation (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 the holders/future holders and the information on the organisation,
- accept requests for SIGEN-CA services;
- check claims,
- to deliver the necessary documentation to the holders or future holders and organisations,
- forward requests and other data in a secure way to the SIGEN-CA.

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

9.6.3 liability and liability of the holder or organisation

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

- to take note of this policy and the arrangements agreed between the organisation and the SI-TRUST before issuing the certificate,
- comply with the policy and the terms of the arrangement between the organisation and the SI-TRUST and other applicable regulations;
- if, following the request to obtain a certificate or another service from the issuer of SIGEN-CA, you have not received the e-mail notification specified in the request, the issuer must contact the authorised persons of the SIGEN-CA;
- Upon acceptance of the certificate, check the information in the certificate and inform the SIGEN-CA immediately in case of any errors or problems, or ask for the certificate to be cancelled,
- if, after the application for a certificate or other service has been awarded from the issuer, the SIGEN-CA does not receive the e-mail notification specified in the request, then to contact the authorised persons of the SIGEN-CA;
- follow up all SIGEN-CA notifications and comply with them.
- duly updated, in accordance with the notifications, the necessary hardware and software for safe work with certificates,
- all changes linked to the certificate shall immediately be reported to the SIGEN-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 laid down in the SIGEN-CA policy,
- provide the original signed documents and archive of these documents.

(2) The responsible person or organisation is required to:

- carefully read the policy and set out the agreement between the organisation and the SI-TRUST before signing the certificate request;
- ensure that holders of certificates for its organisation meet all the requirements laid down in this policy and the applicable rules;
- regularly follow all notices from the issuer of SIGEN-CA;
- comply with notices, policies and arrangements between the organisation and the SI-TRUST and other applicable regulations;
- ensure that holders of certificates duly update the necessary hardware and software for safe work with certificates,
- manage the archive of electronic documents and the necessary data for the use of the certificates;
- all changes concerning the holder and the organisations linked to the holder’s certificate shall immediately be reported to the SIGEN-CA.
- require revocation of the certificate where the private keys of the certificate holder have been compromised in a manner that affects the reliability of use or there is a risk of misuse or if the particulars shown in the

certificate have changed.

(3) The organisation shall be responsible 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, as a result of the use or misuse of the holder's certificate by unauthorised persons;
- any other damage resulting from non-compliance with the provisions of this policy and other SIGEN-CA notifications and applicable regulations.

(4) The holder's or organisation's obligations with regard to the use of the certificates are defined in the following sentence. 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 SIGEN-CA/SI-TRUST guarantees the value of each legal transaction up to a value 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.