State Centre for Services of Confidence
Issued by the issuer of qualified digital certificates
SIGOV-CA

SI-TRUST
SIGOV-CA

SIGOV-CA POLICY

for qualified digital certificates for public authorities

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

validity: From 1 October 2019
version: 8.1

CP$_{\text{Name}}$: SIGOV-CA

- **Policy for online qualified digital certificates for employees**
  CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.1.9
- **Policy for online qualified digital certificates for employees with mandatory smart card usage**
  CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.2.9
- **Policy for special qualified digital certificates for employees**
  CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.3.9
- **Policy for special qualified digital certificates for employees with the mandatory use of smart cards**
  CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.4.9
- **Policy for online qualified digital certificates for employees with a general title**
  CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.5.9
- **Policy for online qualified digital certificates for employees with a general title by making use of smart cards mandatory**
  CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.6.9
- **Policy for special qualified digital certificates for employees with a general title**
  CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.7.9
- **Policy for specially qualified digital certificates for employees with a general title by mandatory use of smart cards**
  CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.8.9
- **Policy for Online normalised digital certificates for information systems**
  CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.9.9
- **Policy for Online normalised digital certificates for code signature**
  CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.10.9
- **Normalised digital certificate policy for qualified time stamps issuers**
  CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.11.9
- **Normalised digital certificate policy for digital certificate validation systems**
  CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.12.9
- **Policy for online qualified certificates for website authentication**
  CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.13.9
- **Policy for online qualified digital certificates for electronic seal**
  CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.14.9
- **Policy for online qualified digital certification for the mandatory use of smart cards**
  CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.15.9

State Centre for Services of Confidence

Policy history

Issues Policies Issues — CA	
version: 8.1, valid: from 1 October 2019	
● Policy for online qualified digital certificates for employees, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.1.9 ● Policy for online qualified digital certificates for employees with mandatory smart card use, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.2.9 ● Policy for special qualified digital certificates for employees, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.3.9 ● Policy for special qualified digital certificates for employees with mandatory smart card use, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.4.9 ● Policy for online qualified digital certificates for employees with a general title, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.5.9 ● Policy for online qualified digital certificates for employees with a general title by mandatory use of smart cards, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.6.9 ● Policy for special qualified digital certificates for employees with a general title, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.7.9 ● Policy for specially qualified digital certificates for employees with a general title by mandatory use of smart cards, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.8.9 ● Policy for Online normalised digital certificates for information systems, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.9.9 ● Policy for Online normalised digital certificates for code signature, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.10.9 ● Normalised Digital Certificate Policy for Qualified Time Stamp Issuers, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.11.9 ● Normalised digital certificate policy for digital certificate validation systems, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.12.9 ● Policy for online qualified digital certificates for website authentication, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.13.9 ● Policy for online qualified digital certification for stamp, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.14.9 ● Policy for online qualified digital certificates for the mandatory use of smart cards, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.15.9 CP$_{\text{Name}}$: REPLY — CA	*Change from version 8.1:* • *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 8.0, validity: from 18 February 2019	
Amendment to PSC — CA for qualified digital certificates for national authorities no 1/8.0	*Amendment by amendment 1/8.0:* • *in the case of certificates for electronic seals, the title included in the Distinguished Name is changed.*
version: 8.0, valid: from 28 May 2018	

• Policy for online qualified digital certificates for employees, CP $_{OID}$: 1.3.6.1.4.1.6105.1.1.9 • Policy for online qualified digital certificates for employees with mandatory smart card use, CP $_{OID}$: 1.3.6.1.4.1.6105.1.2.9 • Policy for special qualified digital certificates for employees, CP $_{OID}$: 1.3.6.1.4.1.6105.1.3.9 • Policy for special qualified digital certificates for employees with mandatory smart card use, CP $_{OID}$: 1.3.6.1.4.1.6105.1.4.9 • Policy for online qualified digital certificates for general titles, CP $_{OID}$: 1.3.6.1.4.1.6105.1.5.9 • Policy for online qualified digital certificates for general names with mandatory smart card use, CP $_{OID}$: 1.3.6.1.4.1.6105.1.6.9 • Policy for specific qualified digital certificates for general titles, CP $_{OID}$: 1.3.6.1.4.1.6105.1.7.9 • Policy for special qualified digital certificates for general titles with mandatory use of smart cards, CP $_{OID}$: 1.3.6.1.4.1.6105.1.8.9 • Policy for Online normalised digital certificates for information systems, CP $_{OID}$: 1.3.6.1.4.1.6105.1.9.9 • Policy for Online normalised digital certificates for code signature, CP $_{OID}$: 1.3.6.1.4.1.6105.1.10.9 • Normalised Digital Certificate Policy for Qualified Time Stamp Issuers, CP $_{OID}$: 1.3.6.1.4.1.6105.1.11.9 • Normalised digital certificate policy for digital certificate validation systems, CP $_{OID}$: 1.3.6.1.4.1.6105.1.12.9 • Policy for online qualified digital certificates for website authentication, CP $_{OID}$: 1.3.6.1.4.1.6105.1.13.9 • Policy for online qualified digital certification for stamp, CP $_{OID}$: 1.3.6.1.4.1.6105.1.14.9 • Policy for online qualified digital certificates for the mandatory use of smart cards, CP $_{OID}$: 1.3.6.1.4.1.6105.1.15.9 CP $_{Name}$: REPLY — CA	*Changes with version 8.0:* • *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 is introduced, qualified certificates for electronic seal with the mandatory use of smart cards and normalised certificates for information systems;* • *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: 7.0, valid: from 6 June 2016	

• Policy for online qualified digital certificates for employees, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.1.8 • Policy for online qualified digital certificates for employees with mandatory smart card use, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.2.8 • Policy for special qualified digital certificates for employees, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.3.8 • Policy for special qualified digital certificates for employees with mandatory smart card use, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.4.8 • Policy for online qualified digital certificates for general titles, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.5.8 • Policy for online qualified digital certificates for general names with mandatory smart card use, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.6.8 • Policy for specific qualified digital certificates for general titles, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.7.8 • Policy for special qualified digital certificates for general titles with mandatory use of smart cards, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.8.8 • Policy for online normalised digital certificates for servers, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.9.8 • Policy for Online normalised digital certificates for code signature, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.10.8 • Normalised digital certificate policy for certifiers, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.11.8 • Normalised digital certificate policy for digital certificate validation systems, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.12.8 CP$_{\text{Name}}$: REPLY — CA	*Changes with version 7.0:* • *the issuer SIGOV-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;* • *the distinguishing names of the certificates for general titles have been modified.* • *servers, code signature, certifiers of safe time stamps and digital certificate validity systems are renamed normalised certificates.*
version: 6.0, valid: from 11 January 2016	
• Policy for online qualified digital certificates for employees, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.1.7 • Policy for online qualified digital certificates for employees with mandatory smart card use, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.2.7 • Policy for special qualified digital certificates for employees, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.3.7 • Policy for special qualified digital certificates for employees with mandatory smart card use, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.4.7 • Policy for online qualified digital certificates for general titles, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.5.7 • Policy for online qualified digital certificates for general names with mandatory smart card use, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.6.7 • Policy for specific qualified digital certificates for general titles, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.7.7 • Policy for special qualified digital certificates for general titles with mandatory use of smart cards, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.8.7 • Online Qualified Certificate Policy for servers, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.9.7 • Policy for Online Qualified Digital Certificates to sign the Code, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.10.7 • Policy for Qualified Digital Certificates for certifiers of safe time stamps, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.11.7 • Certificate policy for digital certificate validation systems, CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.1.12.7 CP$_{\text{Name}}$: REPLY — CA	*Changes with version 6.0:* • *it was the second own digital certificate issued by the issuer of SIGOV-CA with a private key of 3072 bits, which is stored on the hardware for the secure storage of private keys.* • *the SHA-256 hash algorithm is used in the issuer's certificate and in all holders' certificates;* • *the distinguishing name of the digital certificate of the issuer SIGOV-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.*
version: 5.0, valid: from 7 November 2015	

• Policy for online qualified digital certificates for employees, CP$_{OID}$: 1.3.6.1.4.1.6105.1.1.6 • Policy for online qualified digital certificates for employees with mandatory smart card use, CP$_{OID}$: 1.3.6.1.4.1.6105.1.2.6 • Policy for special qualified digital certificates for employees, CP$_{OID}$: 1.3.6.1.4.1.6105.1.3.6 • Policy for special qualified digital certificates for employees with mandatory smart card use, CP$_{OID}$: 1.3.6.1.4.1.6105.1.4.6 • Policy for online qualified digital certificates for general titles, CP$_{OID}$: 1.3.6.1.4.1.6105.1.5.6 • Policy for online qualified digital certificates for general names with mandatory smart card use, CP$_{OID}$: 1.3.6.1.4.1.6105.1.6.6 • Policy for specific qualified digital certificates for general titles, CP$_{OID}$: 1.3.6.1.4.1.6105.1.7.6 • Policy for special qualified digital certificates for general titles with mandatory use of smart cards, CP$_{OID}$: 1.3.6.1.4.1.6105.1.8.6 • Online Qualified Certificate Policy for servers, CP$_{OID}$: 1.3.6.1.4.1.6105.1.9.6 • Policy for Online Qualified Digital Certificates to sign the Code, CP$_{OID}$: 1.3.6.1.4.1.6105.1.10.6 • Policy for Qualified Digital Certificates for certifiers of safe time stamps, CP$_{OID}$: 1.3.6.1.4.1.6105.1.11.6 • Certificate policy for digital certificate validation systems, CP$_{OID}$: 1.3.6.1.4.1.6105.1.12.6 CP$_{Name}$: REPLY — CA	*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.* • *in the distinct name of special certificates, no organisation code,* • *it is possible to issue web certificates for servers with multiple server names;* • *the issue of specific server certificates is abolished;* • *new contact details of the issuer SIGOV-CA.*
amendment to the policy version 4.0, validity: from 21 March 2014	
Amendment to PSC — CA for qualified digital certificates for national authorities 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 PSC — CA for qualified digital certificates for national authorities 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 for online qualified digital certificates for employees and general titles, CP$_{OID}$: 1.3.6.1.4.1.6105.1.1.5 • Policy for specially qualified digital certificates for employees and general titles, CP$_{OID}$: 1.3.6.1.4.1.6105.1.2.5 • Policy for servers and code signing for servers and code signature, CP$_{OID}$: 1.3.6.1.4.1.6105.1.3.3 • Policy for servers, CP$_{OID}$: 1.3.6.1.4.1.6105.1.4.3 • Policy for Qualified Digital Certificates for certifiers of safe time stamps, CP$_{OID}$: 1.3.6.1.4.1.6105.1.5.3 • Certificate policy for digital certificate validation systems, CP$_{OID}$: 1.3.6.1.4.1.6105.1.6.2 • Policy for online qualified digital certificates for employees and general titles with mandatory use of smart cards, CP$_{OID}$: 1.3.6.1.4.1.6105.1.7.1 • Policy for special qualified digital certificates for employees and general titles with the mandatory use of smart cards; CP$_{OID}$: 1.3.6.1.4.1.6105.1.8.1 CP$_{Name}$: REPLY — CA	*Changes with version 4.0:* • *the issuer of the digital certificate SHALL issue a qualified digital certificate with a minimum length of 2048 bits;* • *the issuer of the digital certificate SHALL also issue online and specific qualified digital certificates for employees and general titles without the mandatory use of smart cards. If the prospective holder chooses to accept the certificate using the smart card, the latter will be delivered with the ECS together with the digital certificate in a secure manner;* • *in qualified digital certificates for employees and general titles, the appropriate marking for qualified certificates or certificates with the mandatory use of smart cards 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 CTP for qualified digital certificates for national authorities no 1/3.0	*Amendment by amendment 1/3.0:* • *the issuer SIGOV-CA does not transmit to the prospective holder the certificate code by registered mail, but by means of a simple postal item.*
version: 3.0, valid: from 28 February 2006	
• SIMGOV-CA policy for online qualified digital certificates for employees and general titles, CP$_{OID}$: 1.3.6.1.4.1.6105.1.1.4 • Policy SIGOV-CA policy for special qualified digital certificates for employees and general titles, CP$_{OID}$: 1.3.6.1.4.1.6105.1.2.4 • SGOV-CA policy for online qualified digital certificates for servers and code signature, CP$_{OID}$: 1.3.6.1.4.1.6105.1.3.2 • SIGOV-CA policy for special qualified digital certificates for servers, CP$_{OID}$: 1.3.6.1.4.1.6105.1.4.2 • SGOV-CA policy for qualified digital certificates for certifiers of safe time stamps, CP$_{OID}$: 1.3.6.1.4.1.6105.1.5.2 • SGOV-CA policy for qualified digital certificates for digital certificates validation systems, CP$_{OID}$: 1.3.6.1.4.1.6105.1.6.1 CP$_{Name}$: REPLY — CA	*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 ECS certificate holders are limited to national authorities, namely direct budget holders;* • *the issue is also issued with qualified digital certificates for OCSP systems;* • the *revocation is only possible within the business time, except in urgent cases;* • *the structure of the document is in line with RFC 3647 recommendations.*
version: 2.1, valid: from 28 October 2003	
• SIMGOV-CA policy for online qualified digital certificates for employees and general titles, CP$_{OID}$: 1.3.6.1.4.1.6105.1.1.3 • SIMGOV-CA policy for personal qualified digital certificates for employees and general titles, CP$_{OID}$: 1.3.6.1.4.1.6105.1.2.3 • SGOV-CA policy for online qualified digital certificates for servers and code signature, CP$_{OID}$: 1.3.6.1.4.1.6105.1.3.1 • SIMGOV-CA policy for personal qualified digital certificates for servers, CP$_{OID}$: 1.3.6.1.4.1.6105.1.4.1 • SGOV-CA policy for qualified digital certificates for certifiers of safe time stamps, CP$_{OID}$: 1.3.6.1.4.1.6105.1.5.1 CP$_{Name}$: REPLY — CA	*Changes with version 2.1:* • *issuance of qualified digital certificates for certifiers of safe time stamps;* • *policies are new separate for certificates for which funds are required for secure preservation of certificates;* • *the structure of the document is in line with RFC 2527 recommendations.*
version: 2, valid: from 15 July 2002	
• Policy SIGOV-CA for Qualified Digital Certificates for Public Administration Institutions, CP$_{OID}$: 1.3.6.1.4.1.6105.1.1.2 and 1.3.6.1.4.1.6105.1.2.2 CP$_{Name}$: REPLY — CA	*Change from version 2:* • *it is also issued with qualified digital certificates for the general titles and organisational units of the institutions;* • *a qualified digital certificate for the signing of the code is also issued.*
version: 1, valid: from 17 January 2001	
• Certificate policy for online qualified digital certificates, CP$_{OID}$: 1.3.6.1.4.1.6105.1.1.1, CP$_{Name}$: SGOV-CA-1 • SGOV-CA policy for the service of personal qualified digital certificates, CP$_{OID}$: 1.3.6.1.4.1.6105.1.2.1, CP$_{Name}$: SGOV-CA-2	*//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.

The issuer of qualified digital certificates SIGOV-CA shall be subject to the SI-TRUST. *Slovenian governmental certification authority*), https://www.si-trust.gov.si/sl/digitalna-potrdila/drzavni-organi/, which issues certificates to public authorities and other bodies that are regarded under the current legislation as direct spending units of the state budget.

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

The third-party policy of operation of the ECS determines 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 policy of the issuer of SIGOV-CA for several types of qualified digital certificates complying with the highest safety requirements. On the basis of this document, the SIGOV-CA document issues a specific and online digital certificate according to the following policies: CP $_{OID}$: 1.3.6.1.4.1.6105.1.1.9, CP $_{OID}$: 1.3.6.1.4.1.6105.1.2.9, CP $_{OID}$: 1.3.6.1.4.1.6105.1.3.9, CP $_{OID}$: 1.3.6.1.4.1.6105.1.4.9, CP $_{OID}$: 1.3.6.1.4.1.6105.1.5.9, CP $_{OID}$: 1.3.6.1.4.1.6105.1.6.9, CP $_{OID}$: 1.3.6.1.4.1.6105.1.7.9, CP $_{OID}$: 1.3.6.1.4.1.6105.1.8.9, CP $_{OID}$: 1.3.6.1.4.1.6105.1.9.9, CP $_{OID}$: 1.3.6.1.4.1.6105.1.10.9, CP $_{OID}$: 1.3.6.1.4.1.6105.1.11.9, CP $_{OID}$: 1.3.6.1.4.1.6105.1.12.9, CP $_{OID}$: 1.3.6.1.4.1.6105.1.13.9, CP $_{OID}$: 1.3.6.1.4.1.6105.1.14.9 and CP $_{OID}$: 1.3.6.1.4.1.6105.1.15.9

The present document replaces the previously published policy SIGOV-CA. 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 under the new policy for those provisions that can reasonably be replaced or supplemented by a policy where 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 $_{OIDs}$) are not altered.

Qualified digital certificates are obtained on the basis of a request to be signed by the head of the organisation or organisational unit and prospective holders. In the case of a digital certificate for information systems, the signature of the code, the website, the electronic seal, the issuing of a time stamps or systems for continuous verification of the validity of the digital certificates shall be the prospective holder of the employee or person authorised by the President to use this certificate. By signing the application, the head shall guarantee the identity of the prospective holder. The completed application is based on the application service set up at the headquarters of the SI-TRUST (contact details published at https://www.si-trust.gov.si/sl/digitalna-potrdila/drzavni-organi/).

As a general rule, online and specific qualified digital ECS certificates for employees, and employees with a general title, shall be issued as certificates through the mandatory use of smart cards and, on the basis of an approved request, are taken over by the holder of a smart card on the infrastructure of the issuer SIGOV-CA. exceptionally, the prospective holder may request otherwise on the application to obtain a qualified certificate, provided that the use of the smart card is not technically possible in his or her environment. In the case of a certificate with the mandatory use of a smart card, it is presented to the prospective holder together with the digital certificate in a secure manner by the ICA, so that the prospective holder receives a smart card with a digital certificate through a contact person of the organisation, and the pre-set password for access to a digital certificate is received by a postal item classified as “Personal” to the address of his/her organisation.

In the case of digital certificates without the mandatory use of the SIMGOV-CA smartcards, it shall, on the basis of an approved request, draw up a reference number and an authorisation code, which shall be unique for each prospective holder of a qualified digital certificate and are required by it to take over his certificate, carried out in accordance with the instructions of the originator SGOV-CA. the prospective holder shall receive the reference number by e-mail and the authorisation code by the postal item, to the address of its organisation.

An online digital certificate is connected to one pair of keys generated by the holder’s software or hardware. The SIGOV-CA never holds a private key. The public key shall be sent to the ICA, which shall issue the certificate, of which the public key shall form an integral part. The online certificate and associated keys shall be stored with the holder or on the holder’s smart card and only the certificate shall be published 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/authentication key pair consists of the holder's software or hardware. The SIGOV-CA never holds a private signature key. The public key for the authentication of the signature shall be sent to the SIRGOV-CA issuing the signature verification certificate, of which the public key for the authentication of the signature forms an integral part. The certificate for signature verification shall be stored with the holder or on the holder's smart card.
- The decryption/encryption keys pair shall be made at the side of the issuer SIGOV-CA. the private decryption key shall be stored on the holder's software or hardware. For the purposes of possible access (decryption) to relevant encrypted data, 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 securely stored in the SIRGOV-CA archives, and the ECS shall issue a 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 SIGOV-CA retains the necessary information on the holder and the organisation for the purpose of electronic commerce, in accordance with the rules in force.

The holder must carefully protect the private keys, his digital certificate and a smart card, and comply with the policy, the information provided by the ICA, and the applicable legislation.

1. INTRODUCTION

1.1. Review

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

(2) Under the SI-TRUST, the issuer of the SIGOV-CA is operational. *Slovenian governmental certification authority)*, https://www.si-trust.gov.si/sl/digitalna-potrdila/drzavni-organi/, which issues digital certificates for public authorities and other authorities that are regarded under the current legislation as direct spending units of the general government budget (hereinafter 'the *organisations*'). The present document sets out the policy of the issuer of SIGOV-CA for all types of digital certificates for the needs of direct spending units of the general government budget.

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

(4) In the context of the present policy, the SIGOV-CA policy issues the following digital certificates:

- special qualified digital certificates for organisations working in organisations,
- special qualified digital certificates for employees of organisations through the mandatory use of smart cards;
- special qualified digital certificates for employees with the general title of the organisation (s).
- special qualified digital certificates for employees with the general title of an organisation or an organisational unit with the mandatory use of smart cards;
- online qualified digital certificates for organisations working in organisations,
- online qualified digital certificates for employees in organisations through the mandatory use of smart cards;
- online qualified digital certificates for employees with the general title of the organisation/organisational unit,
- online qualified digital certificates for employees with the general title of an organisation or an organisational unit with the mandatory use of smart cards;
- online qualified digital certificates for website authentication managed by organisations;
- online qualified digital certificates for organisations' electronic seals
- online qualified digital certificates for organisations' electronic seals with the mandatory use of smart cards;
- online normalised digital certificates for organisations managed by organisations,
- online normalised digital certificates to sign code for the organisation;
- Normalised digital certificates for qualified time stamps issuers[1];
- Normalised digital certificates for systems for continuous validation of digital certificates[2].

(5) The SIRGOV-CA certificate (hereinafter referred to as ' *certificates*') may be used for the purpose of:

- 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 special and online certification for employees and for employees with a general title, on the basis of Policy according to CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.1.2.9, CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.1.4.9, CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.1.6.9, CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.1.8.9 and CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.1.15.9 It is mandatory to use smart cards and for the

[1] The certificates for the issuer of the time stamps shall, where not otherwise stated, be treated as special qualified digital certificates.

[2] Certificates for systems for continuous validation of digital certificates shall, where not otherwise stated, be treated as online qualified digital certificates.

other it should take into account the recommendations of the issuer SIGOV-CA for the protection of private keys or the use of secure cryptographic modules.

(7) The present policy is drawn up in accordance with Recommendation RFC 3647 " Internet X.509 Public Key Infrastructure Certificate and Certification Practices Framework", which provides for the internal rules of the issuer of SIGOV-CA, defining the purpose, operation and methodology of the digital certification management and certification methodology, the responsibility of the SI-TRUST and the requirements to be met by holders of the digital certificates of the ECS, third parties relying on digital certificates, and other entities that, in accordance with the regulations, use the services of the ECS Issuer.

(8) Mutual relations may also be implemented on the basis of a written agreement between the organisations and the SI-TRUST or between third parties relying on the certificates of the issuer SIGOV-CA 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 SIGOV-CA policy for qualified digital certificates for public authorities (hereinafter referred to as *SIMGOV-CA policy*).

(2) This policy code is CP $_{\text{Name}}$: SID-CA and SGOV-CA policy identification codes vary according to the type of certificate:

- CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.1.1.9 for online qualified digital certificates for employees,
- CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.1.2.9 for online qualified digital certificates for employees with the mandatory use of smart cards;
- CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.1.3.9 for special qualified digital certificates for employees,
- CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.1.4.9 for special qualified digital certificates for employees with the mandatory use of smart cards,
- CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.1.5.9 for online qualified digital certificates for employees with a general title,
- CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.1.6.9 for online qualified digital certificates for employees with a general title by making use of smart cards mandatory;
- CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.1.7.9 for special qualified digital certificates for employees with a general title,
- CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.1.8.9 for special qualified digital certificates for employees with a general title by mandatory use of smart cards,
- CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.1.9.9 for online normalised digital certificates for servers,
- CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.1.10.9 for Online normalised digital certificates for code signature,
- CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.1.11.9 for normalised digital certificates for the issuers of qualified time stamps (hereinafter referred to as *TSA*; *Time Stamp Authority*),
- CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.1.12.9 for normalised digital certificates for validation systems of digital certificates (hereinafter referred to as *OCSP*) *"Online Certificate Status Protocol*",
- CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.1.13.9 for online qualified digital certificates for website authentication,
- CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.1.14.9 for online qualified digital certificates for electronic seal;
- CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.1.15.9 for online qualified digital certificates for the mandatory use of smart cards for electronic seal.

(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) In the context of the SI-TRUST, the issuer of qualified digital certificates shall operate.

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

Address:	REPLY — CA State Centre for Services of Confidence Ministry of Public Administration Tržaška cesta 21 1000 Ljubljana
E-mail:	sigov-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 SIGOV-CA shall perform the following tasks:

- issuance of a qualified and normalised digital certificate;
- sets out and publishes its policy of action;
- sets out and publishes forms for claims for its 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;
- it shall ensure the smooth operation of its services in accordance with this policy and with other regulations,
- inform its users;
- he/she is responsible for the functioning of his or her application.
- take over the digital certificates for future holders, for which the use of smart cards is mandatory; and
- it provides all other services in line with policy and other regulations.

(5) Upon initiation of its production operations, the ECS issuer has formed its own digital certificate, which is intended to certify the certificates issued by the SIGOV-CA to the holders or issuers of qualified time stamps.

Certificate No 1 SGOV-CA shall contain the following information[3]:

Field names	Value or importance
Certificate (s) of the underlying (s) in the certificate	
Version \ "_blank" *Version*	3
ID, *Serial Number*	3A5C 701A
Signature algorithm, \ "_blank" *Signature Algorthm*	sh1WithRSAEncrConsumption
Issuing body, \ "_blank" *Issuer*	c = SI, o = stan-institutions, ou = sivis-ca

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

Holder, *Subject*	c = SI, o = stan-institutions, ou = sivis-ca
Date of entry into force, *Validity: Not Before*	Jan 10 13: 52: 52 2001 GMT
End of validity, *Validity: Not After*	Jan 10 14: 22: 52 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	
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" Hash *Key Identifier*	1EF8 D453 6BB3 8306 E904 0657 02F9 A5BFS C658 3C72
The identifier of the holder's key; OID 2.5. *29.14,* \ *"_blank" Subject Key Identifier*	1EF8 D453 6BB3 8306 E904 0657 02F9 A5BFS C658 3C72
Certificate footprint (not part of the certificate)	
The footprint of the MD-5 certificate, \ "_blank" *Certificate Fingerprint — MD5*	739D D35F C63C 95FE C6ED 89E5 8208 DD89
SHA-1 certificate footprint, *Certificate Fingerprint — SH* A-1	7FB9 E2C9 95C9 7A93 9F9E81A0 7AEA 9B4D 7046 3496
SHA-256 certificate footprint, *Certificate Fingerprint — SH* A-256	74CB 3A4E A791 AFB0 A2D1 A0B1 3301 B3B0BE E5 0E5AD79 C1A 6A2F 66 3C6E4F 7EE484 A

(6) Five (5) years before the date of expiry of the first own digital certificate, the issuer SIGOV-CA was able to form a second own digital certificate, which is intended to certify the certificates issued by the SIGOV-CA to the holders or issuers of qualified time stamps from 11.1.2016 onwards.

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

Field names	Value or importance
Certificate (s) of the underlying (s) in the certificate	
Version \ "_blank" *Version*	3
ID, *Serial Number*	BD1A 837C 0000 0000 567B C70E
Signature algorithm, \ "_blank" *Signature Algorthm*	sh256WithRSAEncrConsumption
Issuing body, \ "_blank" *Issuer*	c = SI, o = Republic of Slovenia, oi = VAT-17659957, cn = SIMGOV-CA
Holder, *Subject*	c = SI, o = Republic of Slovenia, oi = VAT-17659957, cn = SIMGOV-CA
Date of entry into force, *Validity: Not Before*	DEC 24 09: 51: 06 2015 GMT

End of validity, *Validity: Not After*	DEC 24 10: 21: 06 2035 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	
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*	465E 40E5 53ED FEFE
The identifier of the holder’s key; OID 2.5. *29.14,* *\ “_blank” Subject Key Identifier*	465E 40E5 53ED FEFE
Certificate footprint (not part of the certificate)	
SHA-1 certificate footprint, *Certificate Fingerprint — SH* A-1	4357 B45E 9FF9 0BDA BA78 B532 2B0 656F D1B7 BA58
SHA-256 certificate footprint, *Certificate Fingerprint — SH* A-256	64DC 4058 1A84 B6F2 93C1 AFFF 63F8 E14A 99B7 EA4 1D1F DB38 65CA BAA2 FA01 B610

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

Field names	Value or importance
Certificate (s) of the underlying (s) in the certificate	
Version \ “_blank” *Version*	3
ID, *Serial Number*	B16D D0EA
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 = stan-institutions, ou = sivis-ca
Date of entry into force, *Validity: Not Before*	May 24 12: 09: 58 2016 GMT
End of validity, *Validity: Not After*	Jan 8 23: 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*	1EF8 D453 6BB3 8306 E904 0657 02F9 A5BFS C658 3C72
Certificate footprint (not part of the certificate)	
SHA-1 certificate footprint, *Certificate Fingerprint — SH* A-1	B55 8376 2AFC AB05 2FC5 C06E 70FF E767 A06A D9E1
SHA-256 certificate footprint, *Certificate Fingerprint — SH* A-256	BE73 A04F 7A02 AEE2 D35C 3ADB 7AEF A2FA 2FF3 334D 920A 4FFD 24FFD CD D751 FDAA 4C1D

Field names	Value or importance
Certificate (s) of the underlying (s) in the certificate	
Version \ "_blank" *Version*	3
ID, *Serial Number*	A0E3 6B67 0000 0000 571D D0E9
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 = SIMGOV-CA
Date of entry into force, *Validity: Not Before*	May 24 12: 03: 18 2016 GMT

End of validity, *Validity: Not After*	DEC 22 23: 00: 00 2035 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*	465E 40E5 53ED FEFE
Certificate footprint (not part of the certificate)	
SHA-1 certificate footprint, *Certificate Fingerprint — SH* A-1	02D9 7F2A 66F6 8B06 1C5D FC6F F6A4 05B4 8F7D 50E4
SHA-256 certificate footprint, *Certificate Fingerprint — SH* A-256	9863 73DA59F D093 84B0 A47C 8E31 55AB 7424 ECDA 5DDB2 E2A4 3FBD 7591 434E

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 performing the functions of the TSI TRUST and must comply 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,
- transmission of requests and other data in a secure manner to SGOV-CA.

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

(4) The issuer SIGOV-CA has set up his/her application service at your headquarters (see below. 1.3.1) and this information is published on the Internet.

1.3.3 Certificate holders

(1) The subject is subject to a digital certificate (Subscriber) *for* holders of certificates who are employed by the organisation or who carry out work for this organisation (*subject*).

(2) By signing a certificate application, the President 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 a certificate for information systems, the signature of the code, the website and the electronic seals, the holder of such certificate shall have the authority authorised by the head, in the case of a certificate for the issuer of qualified time stamps and a system for continuous validity of the digital certificates, to be certified by the head of the organisation or by the authorised person. 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,
- the heads and the authorised persons of the organisation of the qualified time stamps; and
- the heads or authorised persons of organisations of systems for continuous validation of the validity of the digital certificates.

(4) A mutually agreed written agreement may be concluded between the organisation and the certifying authority and the SI-TRUST, as the case may be.

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 on-line ECS certificates issued in the context of the present policy can 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*).

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 in cases* of certificates for website authentication, code signature, TSA and OCSP systems in addition to the *Extended Key Application* field. *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) The issuer TSA and OCSP shall only be awarded one key pair, namely the digital signature key pair/authentication.

(5) 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
Web to sign code [4]	digital signature/authentication pair (certificate for signature verification)	- Signature key - Signature authentication key	signature/authentication enforceable software codes
website authentication[4]	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
certificate for TSA[5]	digital signature/authentication pair (certificate for signature verification)	- Signature key - Signature authentication key	signature/authentication the time stamps
OCSP[4] certificate	digital signature/authentication pair (certificate for signature verification)	- Signature key - Signature authentication key	signature/authentication OCSP responses

1.4.2 Unauthorised use of certificates and keys

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

1.5. Policy management

1.5.1 Policy Manager

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

1.5.2 Contact persons

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

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

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

1.5.4 Procedure for the adoption of a new policy

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

[5] The purpose of using a certificate to sign the code, the issuers TSA or OCSP systems is further limited to the authentication of an executable programme code, qualified timestamp or OCSP responses.

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 of the issuer SIGOV-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 SIMGOV-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 functioning of the issuer of SIGOV-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 ICA AGREED, is not a publicly available document.

(5) Online server certificates do not display records of certificates and valid digital certificates.

(6) 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, where certificates are kept, is accessible to the public on *the* x500.gov.si server protocol.

(3) They shall also be accessible through the website SIGOV-CA under the HTTPS protocol:

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

(4) The SI-TRUST or ICA SHALL ensure the authorised and safe addition, modification or deletion of data in the public directory of certificates in accordance with the SI-TRUST policy.

3. IDENTITY AND AUTHENTICITY

3.1. naming

3.1.1 name (s) of name (s)

(1) Each certificate shall contain, in accordance with recommendation RFC 5280, the holder and the issuer information in the form of a discriminatory name established as UTF8String or PrintableString according to RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Ref. resolution List (CRL)" and standard X.501.

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

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

(4) 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;
- for the issuers of qualified time stamps, the name of the issuer,
- for systems for verifying the validity of the digital certificates, the name of the system.

(5) Each distinguishing name shall also include a serial number to be determined by the ICA GOV-CA[6] (see below). 3.1.5).

[6] The issuer of the SIGOV-CA certificate shall not contain the serial number.

(6) The Distinguished Name is, according to the type of identity or certificates, according to the following rules:[7]

Type of certificate	Field name	Distinguished Name[8]

certificate of issuer SIGOV-CA	issuing body, *issued*	c = SI,
		o = Republic of Slovenia, oi = VAT-17659957, cn = SIMGOV-CA

special certificates for employees	Holder, Subject	c = SI,
		o = state authorities,
		MA = certification,
		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,
		o = state authorities,
		MA = certification,
		CN =,
		GN = < Name >,
		SurName = < Surname >
		SN = serial number >

online employee certificates	Holder, Subject	c = SI,
		o = state authorities,
		MA = website certificates,
		CN = < name >,
		GN = < Name >,
		SurName = < Surname >
		SN = serial number >

online certificates for employees with the general title of the organisation (s)	Holder, Subject	C = SI,
		O = state authorities,
		MA = website certificates,
		CN =,
		GN = < Name >,
		SurName = < Surname >
		SN = serial number >

online certificates for information systems	Holder, Subject	C = SI,
		O = state authorities,
		MA = systems,
		CN =,
		SN = serial number >

online certification for the signature of the code	Holder, Subject	C = SI,
		O = state authorities,
		MA = Design,
		CN =,
		SN = serial number >

web certificates for website authentication	Holder, Subject	C = SI,
		O = state authorities,
		MA = servers,

[7] The rules for the production of discriminatory names for other types of certificate shall be determined and published by the ECS.

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

		L = < Place of Organisation >,
		BC = < type of organisation >,
		JUR = level of registration >,
		CN =,
		SN = serial number >

online certificates for electronic seals	Holder, Subject	C = SI,
		O = state authorities,
		MA = esals,
		CN =,
		SN = serial number >

certificates for the issuers of qualified time stamps	Holder, Subject	C = SI,
		O = state authorities,
		MA = TSA-certificates,
		CN =,
		SN = serial number >

certificates for systems for verifying the validity of digital certificates	Holder, Subject	C = SI,
		O = state authorities,
		MA = ocdor-certificates,
		CN =,
		SN = serial number >

3.1.2 requirement to make sense of names

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

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

3.1.3 Use of anonymous names or pseudonyms

Not foreseen.

3.1.4 Rules for the interpretation of names

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

3.1.5 uniqueness of names

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

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

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

Serial number	Importance	Value
1 rd place	label for certificate issued by SIGOV-CA	1

2-8 City	unique number of holder	//OR	
9 — 10 rd place	label for special certificate	employed	20
		employed by common title	22
		issuer of TSA	26
	tag for web certificate	employed	14
		employed by common title	18
		information system	10
		signature of the code	19
		OCSP system	11
		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 possession of the private key to which the public key in the certificate belongs is 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 kept by the ECS.

3.2.2 Identification of organisations

(1) In order to obtain the accuracy of the information, the head of the organisation shall, by his signature, be guaranteed by the head of the organisation.

(2) The issuer of SIGOVS-CA verifies the accuracy of the data on the organisation and its Head in the official records or in the official records.

(3) In the case of online authentication certificates for websites, the issuer of a SIGOV-CA shall verify the ownership of, or control over, the online domain in the basic and all additional names of the websites, in one of the following ways:

- the issuer SIGOV-CA sends a unique tag message to the email addresses “admin”, “administrator”, “Webmaster”, “choster” 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 SIGOV-CA sends a 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 ECS issuer 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.

(4) In the case of online authentication certificates, the issuer of a SIGOV-CA website shall check the credentials of the CAA for the online domain of an initial and all additional names of websites and allow 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) The organisation shall verify, for its employed persons, their identity, under the terms of the SIGOV-CA, that the head of organisation guarantees:

- 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 the SIGOV-CA shall check the identity of the holders in the relevant registers.

(3) The e-mail address of the owner of SIGOV-CA shall be checked by the subscriber holder in the central e-mail address of the national authorities.

3.2.4 Non-verified initial verification data

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

- General titles;
- information systems,
- signature of the code,
- TSA; and
- OCSP systems; 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

By signing the application for an acquisition, the organisation or the head of the organisation shall guarantee that he/she wants a specific person who is employed or performing tasks for that organisation, to obtain a certificate either for himself or for the information system, the signature of the code, a website, an electronic seal, the issuer of the TSA or the OCSP system with which that person will operate.

3.2.6 criteria for interoperation

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

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

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

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

3.3.1 Identity and credibility in the event of renewal

(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) Application for revocation of a certificate by the holder, as appropriate, shall be submitted by the holder:

- 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 revocation by telephone, the holder of the SIGOV-CA hotline number must indicate 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 the certificate for information systems, the signature of the code, the authentication of the websites and the electronic seals, the holder of such certificate shall be authorised by the holder of such certificate, in the case of a certificate for the issuer of qualified time stamps and a system for continuous validity of the digital certificates, and by the head of the organisation or, as the case may be, the head of the authorising officer. 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 President must duly complete and sign the application for the certificate.

(2) Access requests shall be made available through the application services or other authorised persons of the issuer SIGOV-CA and on the website of SIMGOV-CA.

(3) In order to obtain a certificate, the prospective holder and the head shall be required to:

- complete the certificate request with real and correct data;
- provide it in a secure manner with the application service,
- to carry out the acceptance of the certificate in a secure manner on the instructions of the ICA, in the event that the prospective holder himself bears the digital certificate.

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 head of an organisation where the prospective holder of the certificate is employed shall guarantee the identity of the prospective holder of the certificate, which he has verified in accordance with the legislation in force.

(2) The issuer of the ECS 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 valid documents.

4.2.2 Approval/rejection of the application

(1) Before submitting a request, the ECS issuer shall inform the President and the prospective holder of any necessary documentation 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

(1) It shall transmit to the prospective holder of the digital certificate the future holder of the digital certificate, using the smart card, together with the digital certificate and the instructions for handling in a secure manner, at the latest within ten (10) days of the approval of the request.

(2) In the absence of a mandatory use of a smartcard authorisation, the SIMGOV-CA shall transmit to the prospective holder of the digital certificate the reference number 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) Certificates shall be issued exclusively on the SI-TRUST infrastructure.

(2) The ECS issued DAT certificate shall be published in a public directory and on the Internet (see below). 4.4.2).

4.3.1.1 Notification procedure of the issuer SIGOV-CA with the mandatory use of a smartcard

In the case of an approved request, the consent of the prospective holder of the certificate to the prospective holder of the certificate shall be transmitted by the contact person of the organisation requesting the holder of the certificate to the holder of the certificate, the smart card with the digital certificate, and the pre-set password for access to the digital certificate by means of a postal code marked "Personal" to the address of his/her organisation.

4.3.1.2 Procedure for the issuer of SIGOV-CA, without mandatory use of a smartcard

In the case of an approved CVCA application, the prospective holder of the certificate shall forward to the prospective holder the reference number and the authorisation code along the following two separate routes: the reference number by e-mail and the authorisation code by means of a postal item, exceptionally, may be handed over by the authorising officer SIGOV-CA in person. Both information will need to be taken over by the prospective holder to take over the digital certificate.

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 expiry date of the certificate issued by the issuer and/or the key issuer shall inform the holder of the notification by e-mail.

4.4. Certificate acceptance

4.4.1 Certificate acceptance procedure

4.4.1.1 Certificate acceptance procedure with mandatory use of a smartcard

(1) In the case of an approved third-party CA request, the prospective keeper shall take possession of a qualified digital certificate using a smart card for a prospective owner on its infrastructure. The SIGOV-CA shall then forward the smart card with a digital certificate taken over by a contact person of the organisation requesting the certificate to the future holder.

(2) A pre-set password for access to a digital certificate is provided to the holder by means of a postal code marked "Personal" to the address of his/her organisation.

(3) The details of the procedure are set out in the SI-TRUST policy.

(4) As soon as the holder has accepted the smart card on which the certificate has been taken over, the holder must check the information contained in the certificate. If the issuer of the SIGOV-CA fails to inform the ICA of any errors without undue delay, it shall be considered to agree to the terms of the arrangement and to agree to the terms and conditions of operation and the assumption of liabilities and responsibilities.

4.4.1.2 Acceptance procedure without mandatory use of a smartcard

(1) To take over a certificate, the prospective holder needs a reference number and an authorisation code issued by the SIGOV-CA. 4.3YES/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/drzavni-organi/. 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. If the issuer fails to inform the ICA of any errors, it is considered to agree with the contents of the ECS and to agree to the terms 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 period of acceptance for the new sixty (60), otherwise the reservation of the certificate shall be cancelled by the ECS.

(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 keys and the certificate in a manner consistent with the notices and recommendations of the SGOV-CA,
- private keys and any other confidential information shall be protected by means of a suitable password in accordance with the recommendations of SGOV-CA or in any other way such that it is accessible only to the holder,
- carefully protect passwords to protect private keys;
- upon expiry of the certificate, the certificate shall be handled in accordance with the notifying CA.

(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 generation of new key pairs and the extension of the validity of the special certificate shall automatically be carried out using the secure protocol of the PKI-CMP certificate at the first use of the holder's certificate with direct access to the SIRGOV-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 11.1.2016 and signed with Certificate No 1 of the SIGOV-CA issuer 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:

- the password for access to private keys is forgotten and does not have the possibility to unlock a smart card,
- 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 11.1.2016 and signed with Certificate No 1 of the SIGOV-CA issuer shall be allowed only for the purpose of accessing the history keys of the decryption keys following prior agreement with the issuer — CA. the procedure may only be carried out until the expiry date of certificate No 1 of the ECS SGOV-CA until 10.1.2021.

4.7.2 Who can ask for the key to be regenerated

Regeneration may be requested by the holder of the certificate to the holder.

4.7.3 process for key recovery

4.7.3.1 Procedure for certificates with mandatory smart card usage

(1) The renewal of the certificate keys shall be carried out on the basis of a completed recovery request from the holder of the certificate and the head to be delivered to the reply to the CA.

(2) As for issuing a new certificate, the holder shall receive a smart card with a digital certificate which has been regenerated on his infrastructure on the basis of a regeneration request for the holder, by the issuer of the ECS.

(3) Certificate for authentication of a signature issued for a regeneration process shall contain the same distinguishing name as the original certificate.

(4) The SIGOV-CA is provided to the holder by a smart card holder together with a regenerated digital certificate

(s) and instructions for handling in a safe manner no later than ten (10) days after processing of the request for regeneration (Podstl. 4.7.1).

4.7.3.2 Procedure for certificates without mandatory use of a smart card

(1) The renewal of the certificate keys shall be carried out on the basis of a completed recovery request from the holder of the certificate and the head to be delivered to the reply to the CA.

(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 ECS 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. Upon request of the titular holder, it shall be possible to prolong the regeneration time for the new sixty (60), otherwise the validation of the certificate shall be cancelled by the SIGNATE-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 acquisition 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. 4.4.1YES/NO.

4.7.6 Publication of a renewed certificate

The procedure is the same as for the first acquisition of the certificate, see below. 4.4.2YES/NO.

4.7.7 Issue notice to other entities

The procedure is the same as for the first acquisition of the certificate, see below. 4.4.3YES/NO.

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 head of the organisation in the event 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 ECS issuer shall revoke the certificate even without the request of the holder or the head of the organisation as soon as it becomes aware of:

[9] According to the recommendation of RFC 3647, this sub-chapter also includes a procedure for the service of suspension not provided by the ECS publisher.

- 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 SIGOV-CA has ceased to be issuing 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.

4.9.2 Who may request cancellation

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

(2) Revocation of the certificate may also be requested by the head of the organisation.

4.9.3 Cancellation procedure

(1) Revocation may be requested by the holder:

- personal time in the application service,
- Electronically by e-mail twenty four (24) hours a day, all days in a year, if the possibility of misuse or unreliability of the certificate is otherwise in business time,
- The frequency of 24 (24) hours per day for all days of the year in the case of an abuse or unreliability of the certificate, otherwise in business hours.

(2) Revocation may be requested by the head of the organisation:

- face-to-face in business time,
- Electronically by e-mail twenty four (24) hours a day, every day of the year in the case of misuse of the certificate, otherwise in business hours.

(3) If the operation of the SI-TRUST is, due to unforeseen events, significantly reduced, the holder or the head of the organisation may only request cancellation personally 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 head of the organisation must send an electronic message to the SIGOVCA by means of a revocation request, which must be digitally signed with a trusted certificate for its authentication. At the same time, the issuer of the request for cancellation shall notify the SIGOV-CA by telephone using the hotline 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 in the corresponding application for certification as a password for revocation of the certificate or otherwise securely passed on to the SGOV-CA. without a revocation password, the holder may not override the certificate by telephone.

(5) The holder and the President shall be informed by e-mail of the date and time of the cancellation, the issuer of the cancellation request and the reasons for the revocation.

(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

A cancellation request should be requested without delay in the event of an abuse or unreliability, etc., of urgency, or otherwise on the first working day of business time (see 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.

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

4.9.11 Other means of access to certificate status

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

4.9.12 Other requirements for private key abuse

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

4.9.13 Grounds for suspension

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

4.9.14 Who may request the suspension

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

4.9.15 Procedure for the suspension

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

4.9.16 time of suspension

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

4.10. Verification of the status of certificates

4.10.1 Access for verification

The register of invalidated certificates is published in a public directory on *the* server x500.gov.si and on https://www.si-trust.gov.si/sl/podpora-uporabnikom/digitalna-potrdila-sigov-ca/, on-line verification of the status of the certificate is available at http://ocsp.sigov-ca.gov.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. Termination of the relationship between the trust service holder and the trust service provider

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 SIGOV-CA shall keep the history of the decryption keys and detect a copy of them only in exceptional cases, where they 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 SIGOV-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 11.1.2016 and signed with Certificate No 1 of the ECS issuer can only be carried out until the expiry date of certificate No 1 of the issuer SIGOV-CA until 10.1.2021.

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:

- on the basis of a request for the detection of a copy of the decryption keys for access to data that are encrypted and accessible with the decryption key of the holder,
- 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 President shall complete the request for the detection of the copy of the decryption keys and transmit it in a secure manner to the SIGOV-CA.

(2) Reply to CA before 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 and trusted service provider

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

5.2.2 Number of persons required per task

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

5.2.3 Identity of individual applications

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

5.2.4 Roles requiring separation of duties

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

5.3. Personnel controls

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

5.3.1 Qualifications, experience and clearance requirements

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

5.3.2 Background check procedures

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

5.3.3 Staff training

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

5.3.4 Training requirements

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

5.3.5 Job rotation frequency and sequence

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

5.3.6 Sanctions

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

5.3.7 independent contractor requirements

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

5.3.8 Documentation supplied to personnel

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

5.4. System security checks

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

5.4.1 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 the event of renewal of a certificate issued by the issuer of SIGOV-CA, the procedure shall be published on the website of SIMGOV-CA.

5.7. *Compromise and disaster recovery*

5.7.1 Incident and compromise handling

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

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

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

5.7.3 Entity private key compromise procedures

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

5.7.4 compromise and disaster recovery

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

5.8. *Extinction of the issuer*

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

6. TECHNICAL SAFETY REQUIREMENTS

6.1. *Key generation and positioning*

6.1.1 Key generation

(1) The generating of the issuer master key pair for signature and authentication is the formal and controlled procedure with the installation of the SIRGOV-CA software, of which a separate record is kept (document "Holder of the process of generating keys of the SiGOV-C-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 changes in the authorisation procedure, or significant changes to the settings of the SIGOV-CA information system, which are carried out when the system is set up, shall be documented in a separate record, or in the relevant journal.

(4) The backup module shall be used for generating the issuer pair key pair (see below). 6.2.1).

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

Certificate type	Certificate	The key is generated
specifically for employees and employees with a general title by mandatory use of a smart card	digital signature key pair (certificate for signature verification)	using a holder's smart card on the issuer's infrastructure
	pair of decryption/encryption keys (encryption certificate)	With regard to the issuer SIGOV-CA
specifically for employees and employees with a general title without the mandatory use of a smart card	digital signature key pair (certificate for signature verification)	at the holder
	pair of decryption/encryption keys (encryption certificate)	With regard to the issuer SIGOV-CA
online for employees and for employees with a general title through the mandatory use of a smart card	digital signature key pair/authentication and decryption/encryption	using a holder's smart card on the issuer's infrastructure
online for electronic stamps with mandatory smart card usage	digital signature key pair (certificate for signature verification)	using a holder's smart card on the issuer's infrastructure
online for information systems and website authentication and for employees and employees with a common title without the use of a smart card	digital signature key pair/authentication and decryption/encryption	at the holder
certificate to sign the code and for electronic seals without using a smartcard	digital signature key pair (certificate for signature verification)	at the holder
certificate for TSA	digital signature key pair (certificate for signature verification)	with TSA
OCSP certificate	digital signature key pair (certificate for signature verification)	in OCSP

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

in particular through the mandatory use of a smart card	digital signature/authentication pair (certificate for signature verification)	private signing key	No transfer is made in the process of generating a digital certificate[11]; a smart card with a digital certificate and a private key is received by the holder via a contact person of his/her organisation.
	decryption/encryption pair (encryption certificate)	private decryption key	when generating the digital confirmation, the transfer from the issuer to the holder's smart card after PKI-CMP; a smart card with a digital certificate and a private key is received by the holder via a contact person of his/her organisation.
especially without the mandatory use of a smart card	digital signature/authentication pair (certificate for signature verification)	private signing key	no transfer
	decryption/encryption pair (encryption certificate)	private decryption key	transfer from issuer to holder through PKI-CMP
online with mandatory smart card usage	digital signature/authentication and decryption/encryption	private key	No transfer is made in the process of generating a digital certificate[12]; a smart card with a digital certificate and a private key is received by the holder via a contact person of his/her organisation.
online without the mandatory use of a smart card	digital signature/authentication and decryption/encryption	private key	no transfer

6.1.3 delivery of the certificate to the issuer of the certificates[13]

In the procedure of acceptance of the certificate, holders shall deliver their public key to the signature of the ECS issuer 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 (see sub-items). 2.1).

(2) The certificate with the public key of the issuer of SIGOV-CA is accessible to the holder or to third parties:

- In the public directory *x500.gov.si* on the LDAP protocol (see below. 2.3),
- in the form of PEM at https://www.si-trust.gov.si/assets/si-trust-root/povezovalni-podrejeni/sigovca-1/sigov-ca.xcert.pem or https://www.si-trust.gov.si/assets/si-trust-root/povezovalni-podrejeni/sigovca-2/sigov-ca2.xcert.pem
- for certificates without use of a smart card using a PKI-CMP protocol for special certificates and PKCS # 7 for online certificates.

6.1.5 Key length

[11] The key shall be generated using the holder's smart card on the issuer's SiGOV-CA infrastructure.

[12] The key shall be generated using the holder's smart card on the issuer's SiGOV-CA infrastructure.

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

Certificate	RSA key length [bit]
certificate of issuer SIGOV-CA	3072
certificate for: • employed • employees with a general title • information systems • signature of the code • OCSP systems • website authentication • electronic seals	2048[14]
certificate to TSA	2048

6.1.6 Generating and quality of public key parameters

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 SIGOV-CA detects copies of the private key for decryption for special certificates which have been found out of the rat. 6.1.1A key on the side of the issuer SGOV-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 SIGOV-CA provides a backup of its private key. Details are set out in the SI-TRUST internal policy.

[14] Value means the prescribed minimum length.

(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 premises.

6.2.5 Private key archiving

The SIGOV-CA shall archive copies of the private keys for the decryption of specific certificates (in accordance with the provisions laid down in the sub-account. 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 carried over from the site where they are created, i.e. the ECS issuer — CA, under the PKI-CMP protocol:

- to the holder of certificates without mandatory use of a smart card,
- the holder's smart card in certificates with the mandatory use of a smartcard.

(3) The other private keys of the holders shall be composed of:

- in the case of a certificate holder without using a smartcard,
- using the holder's smart card on the issuer of SIGOV-CA on the certificates by using a smartcard.

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

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
certificate for TSA	digital signature key pair (certificate for signature verification)	private key	3 years
		public Key	5 years
OCSP certificate	digital signature key pair (certificate for signature verification)	private key	3 years
		public Key	3 years
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

6.4. Access passwords

6.4.1 Password generation

(1) The authorised person (s) of the ECS shall use the strong passwords to allow the ECS private key to 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, shall be generated on the SIRGOV-CA page.

(3) The certificate, with the mandatory use of a smart card, is protected by a pre-set password at the reception of the certificate. The pre-set password must be changed by the holder before the first use of the certificate.

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

(5) The SAGOV-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 certificated originator's person for access to the private key of a SIMGOV-CA shall be stored in accordance with the SI-TRUST policy.

(2) Activation data for certification shall be secured in a secure manner by the ECS issuer.

(3) In the case of certificates without the mandatory use of a SIMGOV-CA card, the prospective holder of the certificate shall forward to the future holder of the certificate a reference number and an authorisation code along two separate routes:

- reference number by e-mail,
- author's code, with postal item,
- however, they shall also, exceptionally, be handed over in person.

(4) 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.

(5) In the case of certificates with the mandatory use of a SIMGOV-CA smart card, the prospective holder shall forward to the future holder of the certificate a smart card with a digital certificate and a pre-set password on two separate routes:

- a smart card with a dig certificate through a contact person of its organisation,
- a pre-set with a postal code marked "Personal" to the address of his/her organisation.

(6) The pre-set password must be changed by the holder before the first use of the certificate.

(7) The ECS recommends that the password for access to the private key is not stored or stored in a safe place and that only the holder has access to it.

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

6.4.3 Other aspects of passwords

Not prescribed.

6.5. Safety requirements for issuing computer equipment by the issuer

6.5.1 Specific technical safety requirements

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

6.5.2 Level of security protection

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

6.6. Issuer's life cycle technical control

6.6.1 Control of the evolution of the system

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

6.6.2 Managing safety

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

6.6.3 Life cycle control

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

6.7. Network security controls

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

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

6.8. Time-stamping

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

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

7.1. Certificate Profile

(1) Based on this policy, we issue and address the following types of certificate for organisations' needs in this section[15]:

- special certificates for employees,
- special vouchers for employees with the mandatory use of smart cards;
- online certificates for employees,
- online certification for employees with the mandatory use of smart cards;

[15] The certificate of the issuer SIGOV-CA is set out in detail in a separate document. 1.3.1YES/NO.

- special certificates for employees with the general title of the organisation or organisational unit,
- special certificates for employees with the general title of an organisation or an organisational unit with the mandatory use of smart cards;
- online certificates for employees with the general title of the organisation or organisational unit,
- online certificates for employees with the general title of an organisation or an organisational unit with the mandatory use of smart cards;
- online certificates for information systems,
- online certification for the signature of the code,
- online certificates for website authentication,
- online certificates for electronic seals;
- online certificates for electronic seals with the mandatory use of smart cards;
- certificates for TSA issuers; and
- certificate for OCSP systems.

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

(3) The issuer SIGOV-CA certificate is followed by standard *X.509.*

7.1.1 Certificate version

All certificates issued by the issuer SIGOV-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 SIRGOV-CA certificate

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

7.1.2.2 Certificate Profile for Holders

(1) 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
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 = SIMGOV-CA
The period of validity, \ "_blank" *Disability*	Not Before: <*Entry into force post-GMT* > Not After: <*End of validity after GMT* > *In format*< LLMMDUDummssZ >

Holder, \ "_blank" *Subject*	*the distinguishing name of the holder, 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*	*e-mail address, see below. 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.sigov-ca.gov.si/crl/sigov-ca2.crl
	URL: ldap://x500.gov.si/cn=SIGOV-CA
	OI = VATSI-17659957,
	o = the Republic of Slovenia,
	c = SI? certificateRequationList
	c = SI,
	o = the Republic of Slovenia,
	OI = VATSI-17659957,
	CN = SIMGOV-CA,
	CN = CRL < serial *number of the register, see below. 7.2.2* >

Access to information on the issuer, OID 1.3.6.1.5.5.7.1.1, \ "_blank" *Authority Information Access*	Access Method: OCSP (OID 1.3.6.1.5.5.7.48.1) Access Location: URL = http://ocsp.sigov-ca.gov.si Access Method: CaIssuer (OID 1.3.6.1.5.5.7.48.2) Access Location: URL = http://www.sigov-ca.gov.si/crt/sigov-ca2-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*	465E 40E5 53ED FEFE
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 qualificer Info: policy qualificer Id = CPS qualificer: http://www.ca.gov.si/cps/
Qualified certificate identifier, OID 1.3.6.1.5.5.7.1.3, QcStatements *statement*	*depending on the type of certificate, see below. 7.1.2.2.1 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*

(2) Under the same information on title, organisation data, the electronic address may only be held by the holder with the same type of certificate.

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 *extended use of the key, 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 by mandatory smart card usage	employed by mandatory use of a smart card	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: 1.3.6.1.4.1.6105.1.4.9	Policy: 1.3.6.1.4.1.6105.1.8.9	Policy: 1.3.6.1.4.1.6105.1.3.9	Policy: 1.3.6.1.4.1.6105.1.7.9
Qualified certificate identifier, OID 1.3.6.1.5.5.7.1.3, QcStatements *statement*	//OR	//OR	//OR	//OR

(3) The values of the fields for the *purpose of use, the extended use objective, 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 by mandatory smart card usage	employed by mandatory use of a smart card	employed	employed by common title	issuer of TSA
Key Usage, *Key Usage*	Digital Signature, ContenPurpose ment				Digital Signature
The extended use of the key, *Extended Key Usage*	//OR				Time stay g
The policies under which the	Policy: 1.3.6.1.4.1.6105.1.4.	Policy: 1.3.6.1.4.1.6105.1.8	Policy: 1.3.6.1.4.1.6105.1.3	Policy: 1.3.6.1.4.1.6105.1.7	Policy: 1.3.6.1.4.1.6105.1.1

certificate (OID) has been issued and which also indicate that it is a qualified certificate, *Certificate Policies*	9 0.4.0.194112.1.2	.9 0.4.0.194112.1.2	.9 0.4.0.194112.1.0	.9 0.4.0.194112.1.0	1.9
Qualified certificate identifier, OID 1.3.6.1.5.5.7.1.3, QcStatements *statement*	QcCompliance statement QcSSCD statement QcType: eSign PdsLocation: https://www.ca.gov.si/cps/sigovca_pds_en.pdf https://www.ca.gov.si/cps/sigovca_pds_sl.pdf	QcCompliance statement QcSSCD statement QcType: eSign PdsLocation: https://www.ca.gov.si/cps/sigovca_pds_en.pdf https://www.ca.gov.si/cps/sigovca_pds_sl.pdf	QcCompliance statement QcType: eSign PdsLocation: https://www.ca.gov.si/cps/sigovca_pds_en.pdf https://www.ca.gov.si/cps/sigovca_pds_sl.pdf	QcCompliance statement QcType: eSign PdsLocation: https://www.ca.gov.si/cps/sigovca_pds_en.pdf https://www.ca.gov.si/cps/sigovca_pds_sl.pdf	

(4) The fields identified as Critical are *the* following:

- *Key Usage Key Message (* s) for all types of special certificates;
- The *extended application of* the *key*. *Extended Key Message* for TSA.

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. 7.1.2YES/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 by mandatory smart card usage	employed by mandatory use of a smart card	employed	employed by common title
Key Usage, *Key Usage*	Digital Signature, Key Encipherment, 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: 1.3.6.1.4.1.6105.1.2.9 0.4.0.194112.1.2	Policy: 1.3.6.1.4.1.6105.1.6.9 0.4.0.194112.1.2	Policy: 1.3.6.1.4.1.6105.1.1.9 0.4.0.194112.1.0	Policy: 1.3.6.1.4.1.6105.1.5.9 0.4.0.194112.1.0
Qualified certificate	QcCompliance statement	QcCompliance statement	QcCompliance statement	QcCompliance statement

identifier, OID 1.3.6.1.5.5.7.1.3, QcStatements *statement*	QcSSCD statement QcType: eSign PdsLocation: https://www.ca.gov.si/cps/sigovca_pds_en.pdf https://www.ca.gov.si/cps/sigovca_pds_sl.pdf	QcSSCD statement QcType: eSign PdsLoation: https://www.ca.gov.si/cps/sigovca_pds_en.pdf https://www.ca.gov.si/cps/sigovca_pds_sl.pdf	QcType: eSign PdsLocation: https://www.ca.gov.si/cps/sigovca_pds_en.pdf https://www.ca.gov.si/cps/sigovca_pds_sl.pdf	QcType: eSign PdsLocation: https://www.ca.gov.si/cps/sigovca_pds_en.pdf https://www.ca.gov.si/cps/sigovca_pds_sl.pdf

Field name	Online certificate value		
	website authentication	electronic seal with mandatory smart card application	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	//OR
The policies under which the certificate (OID) has been issued and which also indicate that it is a qualified certificate, *Certificate Policies*	Policy: 1.3.6.1.4.1.6105.1.13.9 0.4.0.194112.1.4	Policy: 1.3.6.1.4.1.6105.1.15.9 0.4.0.194112.1.3	Policy: 1. 3.6.1.4.1.6105.1.14.9 0.4.0.194112.1.1
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/sigovca_pd_en.pdf https://www.ca.gov.si/cps/sigovca_pd_en.pdf	QcCompliance statement QcSSCD statement QcType: onesal PdsLocation: https://www.ca.gov.si/cps/sigovca_pd_en.pdf https://www.ca.gov.si/cps/sigovca_pd_en.pdf	QcCompliance statement QcType: onesal PdsLocation: https://www.ca.gov.si/cps/sigovca_pd_en.pdf https://www.ca.gov.si/cps/sigovca_pd_en.pdf

Field name	Online certificate value		
	information system	signature of the code	OCSP system
Key Usage, *Key Usage*	Digital Signature, Key Encipherment	Digital Signature	
The extended use of the key, *Extended Key Usage*		Code Signing	OCSP Signing
The policies under which the certificate (OID) has been issued and which also indicate that it is a qualified certificate, *Certificate Policies*	Policy: 1.3.6.1.4.1.6105.1.9.9	Policy: 1.3.6.1.4.1.6105.1.10.9	Policy: 1.3.6.1.4.1.6105.1.12.9
Qualified certificate identifier, OID 1.3.6.1.5.5.7.1.3, QcStatements	//OR	//OR	//OR

statement			

(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 SIGOV-CA reserves the right to refuse the application for a certificate 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 1 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 *lien SGOV-CA write-down*
The distinguishing name of the issuer; \ “_blank” *Issuer*	c = SI, o = Republic of Slovenia, oi = VAT-17659957, cn = SIMGOV-CA
Time of issue of the CRL, thisUpdate	Last Update: *Time of release after GMT* >
Time of issue for the next CRL, NextUpdate	Next Update: <*Time of next issue after GMT* >
identity identifiers withdrawn and revocation time, vokedCertificate	Serial Number: <*ID of cancelled dig certificates* > Revoation Date: <*Time of revocation after GMT* >
Signature algorithm, \ “_blank” *Signature Algorthm*	sh256WithRSAEncrConsumption
Extensions of X.509v2 CRL	
Key of the issuer key; \ “_blank” *Authority Key Identifier* *(OID 2.5.29.35)*	*authority Key Identifier*
Individual Register Number (CRL1, CRL2,....), \ “_blank” *CRLnumber* *(OID 2.5.29.20)*	*individual Register serial number*
Issuer’s alternative name Issues erAltName *(OID 2.5.28.18)*	*not used*

List of changes DeltaCRLindicator (*OID 2.5.29.27)*	*not used*
Publication of the list of amendments issuingDistributionPoint *(OID 2.5.29.28)*	*not used*

(2) Invalidated digital certificates, the validity of which has expired, remain published in a single register and are only published in the full register until the expiration date.

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

(4) The register of invalidated digital certificates is made publicly available in the repository (see below. 2.1).

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

Publication of the CRL		Access to CRL
individual registers	C = SI, o = Republic of Slovenia, oi = VAT-17659957, cn = SIMGOV-CA, cn = CRL < *serial number* of the register >	- Ldap://x500.gov.si/cn=CRL< *register serial number* >, cn = SIMGOV-CA, oi = VAT-17659957, o = Republic of Slovenia, c = SI
full Register	C = SI, o = the Republic of Slovenia, oi = VAT-17659957, cn = SIMGOV-CA (*in the field "CertificationRevocationList")*	- http://www.sigov- ca.gov.si/crl/sigov-ca2.crl - Ldap://x500.gov.si/cn= SGOV-CA, oi = VATS-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.sigov-ca.gov.si.

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

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/drzavni-organi/.

9.1.2 Access price for certificates

Access to the directory issued by the issuer of SIGOV-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 a certificate withdrawn by the issuer of SIGOV-CA is free of charge.

9.1.4 Prices of other services

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

9.1.5 Reimbursement of expenses

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

9.2. Financial responsibility

9.2.1 Insurance coverage

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

9.2.2 Other cover

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

9.2.3 Holders' insurance

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

9.3. Protection of commercial information

9.3.1 protected data

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

9.3.2 Non-safeguarded data

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

9.3.3 Liability with regard to the protection of commercial information

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

9.4. Protection of personal data

9.4.1 Privacy plan

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

9.4.2 Protected personal data

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

9.4.3 Personal data not protected

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

9.4.4 Responsibility for the protection of personal data

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

9.4.5 Power of attorney concerning the use of personal data

The holder or the head of organisation shall authorise the SI-TRUST or issuer of the ECS to use the 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 information on the holders of certificates other than those stated in the certificate, unless specific data are specifically required for the implementation of the specific certification service (s) and the SI-TRUST holds the holder or the head of the organisation empowered to do so (see previous subchapter) or at the request of a 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 SIRGOV-CA services,
- check claims,
- to deliver the necessary documentation to the holders or future holders and organisations,

- forward requests and other information in a secure manner to SIGOV-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 possible arrangement between the organisation and the SI-TRUST before issuing the certificate,
- comply with the policy and identify possible arrangements between the organisation and the SI-TRUST and other applicable regulations;
- if, after the submission of the application for a certificate or other service from the issuer, the ECS has not received the e-mail notification specified in the request, it must be addressed to the authorising officer of the issuer SIGOV-CA,
- upon receipt of a certificate or after acceptance of the certificate, check the information in the certificate and, in the event of any errors or problems, immediately inform the SIRGOV-CA or request the revocation of the certificate,
- follow up on and comply with the notifications and comply with the notifying CA.
- duly updated, in accordance with the notifications, the necessary hardware and software for safe work with certificates,
- all changes linked to the certificate shall be notified without delay to SIGOV-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. 7.1And according to the arrangements laid down in the SIMGOV-CA policy,
- provide the original signed documents and archive of these documents.

(2) The head of organisation shall be:

- 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 up all notifications to the 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;
- any changes concerning the holder and the organisations linked to the holder’s certificate shall be notified without delay to the SIGOV-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 notifications to the SIGOV-CA and the 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 obligations and responsibilities 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 SIGOV-CA/SI-TRUST, respectively, guarantees the value of each transaction by type of certificate to the value of:

- for the mandatory use of smart cards, up to a maximum amount of EUR 5,000, and
- For certificates without the use of smart cards, up to a maximum amount of EUR 1,000.

9.9. Redress

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

9.10. policy validity

9.10.1 Duration

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

9.10.2 End of the policy period

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

9.10.3 Effect of the policy expiry

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

9.11. Communication between entities

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

9.12. amendment of a document

9.12.1 procedure for the application of amendments

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

9.12.2 Validity and publication of amendments

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

9.12.3 Change of the policy identification code

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

9.13. procedure in case of disputes

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

9.14. applicable legislation

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

9.15. compliance with applicable law

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

9.16. General provisions

9.16.1 Comprehensive deal

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

9.16.2 Assignment of rights

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

9.16.3 Independence identified by

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

9.16.4 Receivables

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

9.16.5 Force majeure

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

9.17. Miscellaneous provisions

9.17.1 understanding

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

9.17.2 Conflicting provisions

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

9.17.3 Derogation from the provisions of

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

9.17.4 Cross verification

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