Trust Service Authority of Slovenia
SI-PASS-CA issuer of qualified certificates for
Authentication and e-Signature Service

SI-TRUST
SI-PASS-CA

SI-PASS-CA POLICY DISCLOSURE STATEMENT

for qualified certificates for Authentication and e-Signature Service

Summary of the public part of internal rules of the Trust Service Authority of Slovenia

validity: since 28 June 2016
version: 1.0

CP_{Name}: SI-PASS-CA

- **Policy for qualified certificates for natural persons for a qualified electronic signature**
  CP_{OID}: 1.3.6.1.4.1.6105.7.1.1
- **Policy for qualified certificates for natural persons**
  CP_{OID}: 1.3.6.1.4.1.6105.7.2.1
- **Policy for normalized certificates for natural persons**
  CP_{OID}: 1.3.6.1.4.1.6105.7.3.1

1. Information on the trust service provider[1]

Contact information of the Trust Service Authority of Slovenia or Certification Authority at the Ministry of Public Administration:

Address:	Republic of Slovenia Trust Service Authority of Slovenia Ministry of Public Administration Tržaška cesta 21 SI-1000 Ljubljana Slovenia
Telephone:	+386 1 4788 330
Website:	http://www.ca.gov.si
Tag:	State-institutions

Contact information of SI-PASS-CA issuer:

Address:	SI-PASS-CA Trust Service Authority of Slovenia Ministry of Public Administration Tržaška cesta 21 SI-1000 Ljubljana Slovenia
E-mail:	si-pass-ca@gov.si
Telephone:	+386 1 4788 330
Website:	http://www.si-pass-ca.gov.si
Emergency telephone number for revocations (24 hours all days in the year):	+386 1 4788 777
Technical support centre:	080 2002, +386 1 4788 590 ekc@gov.si

2. Certificates, their acquisition and use

2.1. Types of certificates[2]

According to the certificate policy, SI-PASS-CA is issuing the following certificates for the needs of SI-PASS Authentication and e-Signature Service:

- Qualified certificates for natural persons for a qualified electronic signature,
- Qualified certificates for natural persons and
- Normalized certificates for natural persons.

Policy label is CP_{Name}: SI-PASS-CA, identification labels of the SI-PASS-CA policy vary according to the certificate type:

- CP_{OID}: 1.3.6.1.4.1.6105.7.1.1 for qualified certificates for natural persons for a qualified electronic signature,
- CP_{OID}: 1.3.6.1.4.1.6105.7.2.1 for qualified certificates for natural persons and
- CP_{OID}: 1.3.6.1.4.1.6105.7.3.1 for normalized certificates for natural persons.

[1] Policy SI-PASS-CA, Sec. 1.3.1
[2] Policy SI-PASS-CA, Sec. 1.1, 1.2

Each certificate contains a relevant policy identifier in the form of CP_{OID} tag.

2.2. Acquisition of certificates[3]

Prospective holders of certificates are always natural persons.

The application for the acquisition of the certificate is submitted electronically on SI-PASS user pages, based on the application in the SI-PASS service.

For the acquisition of the certificate for natural persons for a qualified electronic signature, the prospective holder of the certificate can log in to the SI-PASS service in one of the following ways:
- With a one-time password smsPASS,
- With a qualified certificate on a secure signature creation device,
- By electronic identification means of level of assurance “high” in accordance with eIDAS.

For the acquisition of a qualified certificate for natural persons, the prospective holder of the certificate can log in to the SI-PASS service in one of the following ways:
- With a qualified certificate,
- By electronic identification means of level of assurance “medium” in accordance with eIDAS.

For the acquisition of a normalised certificate for natural persons, the prospective holder of the certificate can log in to the SI-PASS service in one of the other ways of log-in supported by the SI-PASS service.

The application for the acquisition of the certificate is granted automatically based on a successfully carried out procedure for acquiring the certificate.

In the event of an approved application, the SI-PASS-CA certificate will be immediately issued after the approval of the application.

Certificates are issued exclusively on the infrastructure of the Certification Authority at MPA.

2.3. Use of certificates and keys[4]

Private key of the holder and his or her certificate are safely stored on the infrastructure of the SI-PASS-CA issuer.

Before using the certificate, the holder must appropriately log in to the SI-PASS service and enter the password which protects his or her private key.

The holder of a qualified certificate for natural persons for a qualified electronic signature can log in the SI-PASS service in one of the following ways:
- With a one-time password smsPASS,
- With a qualified certificate on a secure signature creation device,
- By electronic identification means of level of assurance “high” in accordance with eIDAS.

The holder of a qualified certificate for natural persons can log in to the SI-PASS service in one of the following ways:
- With a qualified certificate,
- By electronic identification means of level of assurance “medium” in accordance with eIDAS.

[3] Policy of SI-PASS-CA, Sect. 4.1, 4.2, 4.3
[4] Policy of SI-PASS-CA, Sect. 4.5

The holder a normalized certificate for natural persons can log in to the SI-PASS service in one of the other ways of log-in supported by the SI-PASS service.

3. Limitations of use[5]

SI-PASS-CA certificates can be used for:
- Verification of digitally signed electronic data,
- Services or applications which require the use of qualified certificates of the Certification Authority at MPA.

Private key of the holder and his or her certificate are safely stored on the infrastructure of the SI-PASS-CA issuer.

Logs of recorded events in relation to the keys and certificates are stored at least seven (7) years after the expiry of the certificate, to which the log entry applies.

Other logs of recorded data are stored at least seven (7) years after the actual event.

Logs of recorded events from the previous paragraph which include personal data are kept in accordance with the applicable legislation.

4. Duties and responsibilities of the holder[6]

The holder or prospective holder of a certificate is regarding the protection of his private key required to:
- Make sure that the login method used in the SI-PASS service is not at risk,
- Protect his or her private key with a suitable password in accordance with the SI-PASS-CA recommendation, so only the holder can access it,
- Carefully protect the password for the protection of the private key,
- After the expiry or revocation of the certificate act in accordance with the SI-PASS-CA recommendations.

The holder must protect his or her private key against unauthorized use.

The holder or prospective holder of the certificate is required to:
- Familiarize themselves with this policy before the certificate is issued,
- Comply with the policy and other applicable regulation,
- If, after submitting the application for the acquisition of a one-time password smsPASS, the holder does not receive a notification from the SI-PASS-CA issuer via e-mail or post to his or her address of residence, he or she must contact the authorized persons of the SI-PASS-CA issuer,
- After receiving the certificate, verify all the information and in case of any problems or errors immediately notify SI-PASS-CA or request the certificate to be revoked,
- Monitor all SI-PASS-CA notifications and act accordingly,
- Update all needed software and hardware according to the notifications to work safely with the certificates,
- Immediately send all changes regarding the certificates to SI-PASS-CA,
- Demand revocation of the certificate, if the private keys have been compromised in such a way that it effects the reliability of usage, or there is a risk of abuse,
- Use the certificate for the purpose specified in the certificate (see subsection 7.1) and the manner stipulated by the SI-PASS-CA policy,
- Take care for the originally signed documents and their archive.

[5] Policy SI-PASS-CA, Sect. 1.1, 4.5, 5.4.3
[6] Policy SI-PASS-CA, Sect. 4.5.1, 9.6.3

The holder is responsible for:

- Damage caused in the event of misuse of the certificate from the application of revocation to revocation,
- Any damage caused directly or indirectly, caused by the holder because the certificate was abused or used in an unauthorized way,
- Any other damage arising from failure to comply with the provisions of this policy and other SI-PASS-CA notifications as well as regulations in force.

5. Requirements for the Certificate Revocation List verification for third parties[7]

Third parties which rely on the certificate must, before use, check the latest published Certificate Revocation List.

Due to the credibility and wholesomeness it is necessary to always check the credibility of this list, which is digitally signed by SI-PASS-CA.

Third parties must carry out a complete verification process of the trust chain in accordance with the RFC 5280 for every certificate they use.

If the third party cannot verify the certificate status in the Certificate Revocation List, it can decline the use of the certificate or regardless consciously accept and use the certificate.

The Certificate Revocation List is updated:

- After every certificate revocation,
- Once daily, if there are no new entries or changes in the Certificate Revocation List, namely around twenty-four hours (24) after the last update.

The Online Certificate Status Protocol (OCSP) is supported in accordance with the recommendation RFC 2560 »X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP«.

6. Disclaimers and Limitation of Liability[8]

Certification Authority at MPA is not liable for any damages caused by:

- Improper or insufficient protection of passwords, revealing confidential data to third parties and irresponsible treatment by the holder,
- Abuse or intrusion in the information system of certificate holder and thus enabling access to the certificate to unauthorised persons,
- Failure or malfunctioning of the information infrastructure of the certificate holder or third parties,
- Failure to verify data and validity of the certificate,
- Failure to verify the validity period of the certificate,
- Treatment of the certificate holder or third parties in opposition to the notifications of the SI-PASS-CA issuer, policy and other regulations,
- Enabled use or misuse of the holder's certificate to unauthorised persons,
- The use of an issued certificate with false and unauthentic information or other actions by the holder,
- The use of certificates and the validity of certificates upon changes of the information in the certificate or the names of the holders,

[7] Policy SI-PASS-CA, sect. 4.9.6, 4.9.7, 4.9.9
[8] Policy SI-PASS-CA, sect. 9.7, 9.8

- Infrastructure failure not under the management of the Certification Authority at MPA,
- Information signed using the certificate,
- Conduct of holders when using certificates, even in the case if the holder or the third party complied with all the provisions of this policy, notifications of the SI-PASS-CA issuer and other applicable regulations,
- Use and reliability of hardware and software of the certificate holder.

SI-PASS-CA issuer or the Certification Authority at MPA guarantees the value of an individual legal transaction regarding the type of the certificate to the value of:
- For qualified certificates for qualified electronic signature up to EUR 5.000 and
- For qualified certificates up to EUR 1.000.

7. Policy and Applicable Legislation[9]

The reference document is the SI-PASS-CA Policy for qualified certificates for Authentication and e-Signature Service.

The label of the policy is CP_{Name}: SI-PASS-CA, identification marks of the policy SI-PASS-CA vary on the certificate type:
- CP_{OID}: 1.3.6.1.4.1.6105.7.1.1 for qualified certificates for natural persons for a qualified electronic signature,
- CP_{OID}: 1.3.6.1.4.1.6105.7.2.1 for qualified certificates for natural persons and
- CP_{OID}: 1.3.6.1.4.1.6105.7.3.1 for normalized certificates for natural persons.

The Certification Authority at MPA and the SI-PASS-CA issuer operate in accordance with:
- Electronic Commerce and Electronic Signature Act,
- eIDAS Regulation,
- European directives,
- Personal Data Protection Act,
- Classified Information Act,
- ETSI recommendations regarding qualified certificates and trust services,
- RFC recommendations regarding X.509 certificates,
- And other valid regulations and recommendations.

8. Protection of personal data and storage period

8.1. Protection of personal data[10]

All personal and classified data of the certificate holders, vital for certificate management services, are handled by the SI-PASS-CA issuer in accordance with the applicable legislation.

Protected data are all data acquired by the SI-PASS-CA issuer either in submitted applications or in relevant registers to prove the identity of the holder.

There is no other unprotected personal data, except those listed in the certificate and Certificate Revocation List.

The Certification Authority at MPA is responsible in accordance with the Personal Information Protection Act (Official Gazette of RS, No. 94/07 – official consolidated text) and other applicable legislation related to the protection of personal information.

[9] Policy SI-PASS-CA, sect. 1.2, 9.14
[10] Policy SI-PASS-CA, sect. 9.4

The holder authorises the Certification Authority at MPA or the SI-PASS-CA issuer for the use of personal data on his or her application form for the acquisition of the certificate or later in writing.

The Certification Authority at MPA does not provide other information on certificate holders than those stated in the certificate, unless some specific information is required for specific services or applications in relation to the certificate and the holder authorised the Certification Authority at MPA for it (see previous sub-section), or at the request of a competent court or administrative authority.

Information is provided also without written consent, if required by law or applicable regulations.

8.2. Storage period[11]

Archived data related to the keys and certificates are stored at least seven (7) years after the expiry of the certificate to which the data relates.

Other archived data is stored at least seven (7) years after their creation.

Archived data from the previous paragraph containing personal data are kept in accordance with applicable legislation.

9. Reimbursement of costs[12]

Management costs of the certificates are calculated according to the price list published on http://www.si-pass-ca.gov.si/cenik.php. Reimbursement of costs to the holder is not stipulated.

10. Procedures in the case of dispute[13]

Parties will endeavour to amicably settle disputes, but if this would not be possible, the disputes will be resolved by the competent court in Ljubljana. Parties agree to settle disputes solely with the use of regulations of the Republic of Slovenia.

11. Compliance with applicable legislation[14]

Conformity assessment of the Certification Authority at MPA or SI-PASS-CA issuer is carried out by the competent inspection service in accordance with applicable regulation and directives.

The frequency of the inspection is under the responsibility of the inspection service, which is liable in accordance with the current legislation.

Implementation of ZEPEP provisions by the Certification Authority at MPA is in accordance to ZEPEP controlled by the competent inspection service in accordance with applicable legislation for inspection.

Internal conformity assessment is carried out by the internal auditor and other authorised persons of the Certification Authority at MPA.

Inspection service is an authority liable in accordance with the applicable legislation.

[11] Policy SI-PASS-CA, sect. 5.5.2
[12] Policy SI-PASS-CA, sect. 9.1
[13] Policy SI-PASS-CA, sect. 9.13
[14] Policy SI-PASS-CA, sect. 9.15, 8

Areas of conformity assessment are stipulated with the applicable legislation and regulations.

In case of any defects or errors the SI-PASS-CA issuer or the Certification Authority at MPA will make efforts to their elimination as soon as possible.

The Certification Authority at MPA will publish a summary of the conclusions of the inspection on their webpages.