State Centre for Services of Confidence

The issuer of the qualified time stamps SI-TSA

SI-TRUST

SI-TSA

SI-TSA POLICY

for the issue of qualified time stamps

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

validity: From 1 October 2019

version: 7.1

CP $_{\text{Name}}$: SI-TSA-1

CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.3.1.7

Policy history

Arrangements for the operation of the SI-TSA	
version: 7.1, valid: from 1 October 2019	
SI-TSA policy for the issue of qualified time stamps CP $_{OID}$: 1.3.6.1.4.1.6105.3.1.7 CP $_{Name}$: SI-TSA-1	*Revision of the document*
version: 7.0, valid: from 23 August 2018	
SI-TSA policy for the issue of qualified time stamps CP $_{OID}$: 1.3.6.1.4.1.6105.3.1.7 CP $_{Name}$: SI-TSA-1	*Changes with version 7.0:* • *the data on the IS-TSA-1 and SI-TSA2 certificates are amended.* • *SHA-1 summary algorithm shall be replaced by the SHA-256 algorithm,* • *change data on the time synchronisation server.*
version: 6.0, valid: from 28 May 2018	
SI-TSA policy for the issue of qualified time stamps CP $_{OID}$: 1.3.6.1.4.1.6105.3.1.6 CP $_{Name}$: SI-TSA-1	*Changes with version 6.0:* • *the term "secure time stamp" is replaced by the term "qualified timestamp";* • *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: 5.0, valid: from 7 November 2015	
SI-TSA policy for issuing safe time stamps CP $_{OID}$: 1.3.6.1.4.1.6105.3.1.5 CP $_{Name}$: SI-TSA-1	*Change with version 5.0:* • *use of the new title for CA at the Home Office, now called the National Centre for Services of Confidence.* • *new contact details of the issuer of the SI-TSA.*
amendment to the policy version 4.0, validity: from 21 March 2014	
Amendments to the SI-TDSA for the issue of safe time stamps 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	
Amendments to the SI-TDSA for the issue of safe time stamps 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';* • *it is amended to provide for a guarantee of the value of each legal transaction.*
version: 4.0, valid: from 18 May 2007	
SI-TSA policy for issuing safe time stamps CP $_{OID}$: 1.3.6.1.4.1.6105.3.1.4 CP $_{Name}$: SI-TSA-1	*Change with version 4.0:* • *the identity of the issuer of the SI-TSA is no longer identified in the identity of the issuer of the server certificates, which varies on the occasion of each regular exchange of digital certificates;* • *holders of specific digital certificates issued by the ECS originator can no longer be able to use the SI-TSA service.*
version: 3.0, valid: from 28 February 2006	

SI-TSA policy for issuing safe time stamps CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.3.1.3 CP$_{\text{Name}}$: SI-TSA-1	*Changes with version 3.0:* • *use of the new title for certification service providers at the Centre of the Government for Informatics, newly designated by the Ministry of Public Administration;* • *taking into account the new title for personal qualified digital certificates, the new denomination being 'special qualified digital certificates';* • *holders of specific digital certificates of business operators can no longer use the SI-TSA service.*
version: 2.0, valid: from 10 September 2004	
SI-TSA policy for issuing safe time stamps CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.3.1.2 CP$_{\text{Name}}$: SI-TSA-1	*Change with version 2.0:* • *the use of SI-TSA services is also extended for the purposes of the applications of business entities;* • *Holders of personal qualified digital certificates of SIGEN-CA are able to use the SI-Ts services.*
Version: 1.0, valid: from 10 November 2003	
SI-TSA policy for issuing safe time stamps CP$_{\text{OID}}$: 1.3.6.1.4.1.6105.3.1.1 CP$_{\text{Name}}$: SI-TSA-1	//OR

CONTENT

SUMMARY

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

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

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

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

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

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

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

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

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

Under the SI-TRUST, the issuer of the qualified time stamps of the SI-TSA (hereinafter referred to as “SI-TSA”) shall be operational. *Slovenian Time Age Authority, https://www.si-trust.gov.si/sl/kvalificiran-elektronski-casovni-zig/*, which issues qualified time for public authorities and business operators.

The SI-TSA issuer shall be registered in accordance with the applicable legislation.

The operation policy of the SI-TSA determines the internal operating rules of the issuer defining the purpose, operation and methodology of the time stamps, responsibilities and requirements to be met by all entities.

The present document provides for the operation of the SI-TSA issuer under CP $_{\mathrm{OID}}$ policy: 1.3.6.1.4.1.6105.3.1.7

replacing previous policy versions. All services and newly issued qualified time stamps issued by the ATV issuer are dealt with under the new policy. Qualified stamps issued under previous policies are considered to have a new policy with regard to those provisions which may reasonably be replaced or supplemented by the policy according to which the qualified time stamp was issued.

As the changes brought about by the new policy do not affect the use or management procedures that can change the level of trust, the policy identifier (CP $_{OID}$) will not change.

The qualified time stamps are intended to ensure the existence of a document at a given time, everywhere where it is necessary to prove the time characteristics of transactions and other services in a secure manner, for other needs where a qualified time stamp is required. When we want to stamp in a given application the electronic document (s), we send an “Summary” (HASH) of the document (*s) with a hash* function. This is a series of bit of a specific length that uniquely identifies a document. The issuer shall add time to this summary and sign it together with its private key. It is thus demonstrated that the electronic document existed before the time indicated in the time stamp and, in addition, that it has not changed since the time of stamping.

Notices, instructions, policies and other relevant documents for the use of the services of the ATV issuer are published on the website of the SI-TSA, https://www.si-trust.gov.si/sl/kvalificiran-elektronski-casovni-zig/.

1. INTRODUCTION

1.1. review

(1) The common provisions are defined in the Sectoral Policy for the SI-TRUST (Underset. 1.1) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

(2) Under the SI-TRUST, the issuer of the qualified time stamps of the SI-TSA (hereinafter referred to as "SI-TSA") shall be operational. *Slovenian Time Age Authority, https://www.si-trust.gov.si/sl/kvalificiran-elektronski-casovni-zig/*, which issues qualified time for public authorities and business operators.

(3) The SI-TSA issuer shall be registered in accordance with the applicable legislation.

(4) Following this policy, CP $_{OID}$: 1.3.6.1.4.1.6105.3.1.6 SI-TSA issues qualified electronic time stamps for secure service requirements, managed by the state and other authorities that are considered to be direct spending units of the state budget under the current legislation, and for the needs of the secure services under the responsibility of the business operators, which may be evidenced by a digital certificate SI-TRUST or by any other secure means to be determined by the SI-TSA. The SI-TSA, issued by the issuer of the SI-TSA, shall allocate each issued time stamp to the identifier of the present policy.

(5) The present policy is drafted in line with the recommendations of ETSI TS 102 023 (v.1.2.1) "Electronic Signatures and Infrastructures (ESI); Policy requirements for timedumping authorities' and RFC 3628 'Policy requirements for TimeDumping Authorities' (TSAs) and sets out internal rules for the performance of the issuer defining the purpose, operation and methodology of the time stamps, responsibilities and requirements to be met by all entities.

(6) 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.

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

(8) The SI-TSA shall issue qualified time stamps to within an accuracy of one (1) second or better.

1.2. terms and abbreviations[1]

1.2.1 Terms

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 1.6.1) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

1.2.2 Abbreviations

[1] This subchapter in ETSI TS 102 023 v1.2.1 is not foreseen.

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 1.6.2) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

1.3. Timestamps of the issuer of time stamps

1.3.1 Trust service provider

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 1.3.1) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

1.3.2 issuer of time stamps

(1) The present policy indication of the operation of the SI-TSA shall be: CP $_{\text{OID}}$: 1.3.6.1.4.1.6105.3.1.6

(2) The contact details of the SI-TSA are given below:

Address:	SI-TSA State Centre for Services of Confidence Ministry of Public Administration Tržaška cesta 21 1000 Ljubljana
E-mail:	si-tsa@gov.si
Tel:	01 4788 330
Single contact centre:	080 2002, 01 4788 590 ekc@gov.si
URL:	https://www.si-trust.gov.si

(3) The issuer SIGOV-CA has issued the SI-TASA issuer appropriate digital certificates for two (2) of the issuer server according to a valid SGOV-CA policy. the data of both certificates are given below.

(4) Digital certificate of the first server of the issuer SI-TSA, i.e. an SI-TSA-1 certificate, contains data according to the following table:

Field name	Value for SI-TSA-1 certificate
Version, \ "_blank" *Version*	3 (*meaning version 3*)
ID , Serial Number	*unique internal number of the approved integer number*
Public Key Algorithm, \ "_blank" *Signature Algorthm*	sh256WithRSAEncrConsumption
The issuer of the certificate, \ "_blank" *Issuer*	c = SI, o = Republic of Slovenia, oi = VAT-17659957, cn = SIMGOV-CA
Holder of the certificate , *Subject*	c = SI, o = state authorities, ou = TSA-certificates, cn = SI-TSA-1, serialnumber = 1234773726021
Date of entry into force, Validity: Not Before	*entry into force after GMT*
End of validity, Validity: Not After	*end of validity after GMT*

Public Key Algorithm, \ "_blank" *Public Key Algorthm*	rsacrorryption
Holders of a public key belonging to an appropriate key pair encrypted with the RSA algorithm, \ "_blank" *RSA Public Key*	*2048 bit length key*
The policy of the issuer; \ "_blank" Certificate Policy	*PolicyIdentifier = Policy: set out policies* *[1,1] Policy qualificer Info:* *Policy qualificer Id = CPS* *Qualificer:* *http://www.gov.si/ca/cps/*
Key Usage , *Key Usage*	Digital Signature
To further specify the use (s), *Extended Key Usage*	Time stay g
Key identity (algae. SHA-1): \ "_blank" Subject Key Identifier	*key Identifier,*
Certificate footprint (not part of the certificate)	
The footprint of the MD-5 certificate, Certificate Fingerprint — MD5	*recognisable print of the certificate under MD5*
SHA-1 certificate footprint, Certificate Fingerprint — SHA-1	*recognisable print of the certificate after SHA-1*
SHA-256 certificate footprint, Certificate Fingerprint — SHA-256	*recognisable print of the certificate after SHA-256*
Imprint of base64 (in stamp)	*acknowledgement of the imprint of the certificate in the stamp*

Digital confirmation of the second server for SI-TSA, i.e. an SI-TSA-2 certificate, is given in the table below:

Field name	Value for SI-TSA-2 certificate
Version, \ "_blank" *Version*	3 (*meaning version 3*)
ID , Serial Number	*unique internal number of the approved integer number*
Public Key Algorithm, \ "_blank" *Signature Algorthm*	sh256WithRSAEncrConsumption
The issuer of the certificate, \ "_blank" *Issuer*	c = SI, o = Republic of Slovenia, oi = VAT-17659957, cn = SIMGOV-CA
Holder of the certificate, *Subject*	c = SI, o = state authorities, ou = TSA-certificates, cn = SI-TSA-2, serialnumber = 1234773826026
Date of entry into force, Validity: Not Before	*entry into force after GMT*
End of validity, Validity: Not After	*end of validity after GMT*
Public Key Algorithm, \ "_blank" *Public Key Algorthm*	rsacrorryption

Holders of a public key belonging to an appropriate key pair encrypted with RSA algorithm. *RSA Public Key*	*2048 bit length key*
The policy of the issuer; \ "_blank" Certificate Policy	*PolicyIdentifier = Policy: set out policies* *[1,1] Policy qualificer Info:* *Policy qualificer Id = CPS* *Qualificer:* *Http://www.gov.si/ca/cps/*
Key Usage, *Key Usage*	Digital Signature
To further specify the use (s), *Extended Key Usage*	Time stay g
Key identity (algae. SHA-1): \ "_blank" Subject Key Identifier	*key Identifier,*
Certificate footprint (not part of the certificate)	
The footprint of the MD-5 certificate, Certificate Fingerprint — MD5	*recognisable print of the certificate under MD5*
SHA-1 certificate footprint, Certificate Fingerprint — SHA-1	*recognisable print of the certificate after SHA-1*
SHA-256 certificate footprint, Certificate Fingerprint — SHA-256	*recognisable print of the certificate after SHA-256*
Imprint of base64 (in stamp)	*acknowledgement of the imprint of the certificate in the stamp*

Critical fields are as follows :

- *The intended purpose* (s). *Key Usage*),
- The *extended purpose of the application. Extended Key Usage)*.

1.4. Entities and intended use

1.4.1 Provider of trust and time stamps

(1) The SI-TRUST shall act in accordance with the applicable rules and issue qualified digital certificates and qualified time stamps to which the highest level of protection applies.

(2) The issuer of the qualified time stamps of the SI-TSA. The Slovenian Time Age Authority) shall be operational under the SI-TRUST (https://www.si-trust.gov.si).

1.4.2 Users of qualified time stamps

(1) The users of the qualified time stamps are applications/organisations representing the latter. The issuer of the SI-TSA issues qualified time stamps for national authorities and business operators.

(2) The interrelationship between the organisation and the SI-TSA is governed by this policy and any possible mutual agreement/contract for the use of the time stamping services of the SI-TSA.

1.4.3 Third persons

Third parties are entities relying on the issued time stamps of the SI-TSA.

1.4.4 Intended uses

The SI-TSA services are intended for:

- ensuring the existence of the document at the specified time, by linking the date and time of stamping to 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 time stamp is required.

1.5. compliance with applicable law and other regulations

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 9.14 and 9.15).

2. LIABILITY AND ACCOUNTABILITY

2.1. obligations of the issuer of the time stamps

2.1.1 General

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 9.6.1) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

2.1.2 obligations towards users

(1) The issuer of the SI-TSA or SI-TRUST shall be obliged:

- issue time stamps in accordance with this policy and other regulations and recommendations,
- to ensure the correctness of the qualified timestamp data.

2.2. Obligations of users

Users must:

- provide accurate and complete identity data or other information for the issuer to the issuer,
- at the time of receipt, check it in accordance with the provisions of the SI-TSA issuer,
- if errors or problems arise, immediately inform the SI-TSA;
- take note of this policy and take into account all the provisions on their obligations, responsibilities and restrictions on the use of the timestamp,

- also take into account any other recommendations of the SI-TSA on the reliable use of qualified time stamps;
- Regularly monitor and comply with all notifications and publications of the SI-TSA;
- take care of the archive of electronic documents and the necessary data for verifying the time-stamped documents, in line with the issuer's recommendations;
- comply with this policy and determine the terms of any agreement or agreement and other rules in force, and
- take account of any other rules which are outside the scope of the issuer's jurisdiction and which are laid down elsewhere.

2.3. *Obligations of third parties*

Third parties relying on the time stamps of the SI-TSA must:

- verify the timestamp in accordance with the instructions issued by the SI-TSA;
- if errors or problems arise, immediately inform the SI-TSA;
- take note of this policy and take into account all the provisions on their obligations, responsibilities and restrictions on trust and the use of timestamp;
- also take into account all other recommendations of the SI-TSA on the reliable use of time stamps;
- monitor and comply with all notifications and publications of the SI-TSA;
- take account of any other rules which are outside the scope of the issuer's jurisdiction and which are laid down elsewhere.

2.4. *Liability of the issuer of the time stamps*

(1) The issuer of the SI-TSA or SI-TRUST is responsible:

- that the timestamp issued contains all the prescribed data under this policy and other regulations,
- to carry out all of its obligations referred to above in the sub-area. 2.1 YES/NO.

(2) The issuer of the SI-TSA or SI-TRUST shall not be held liable for direct or indirect damage, losses etc. arising from the use of the time stamps of the issuer of the SI-TSA, if:

- the time stamp was issued as a result of an error, non-authentic data or other defects of the user or any other person governed by public or private law,
- the timestamp service was required following the announcement of the revocation of the digital certificates of the SI-TSA or the ECS originator company.
- was caused by loss/unavailability and unavailability of the infrastructure not covered by the SI-TRUST, including user software and hardware;
- the user did not comply with the provisions of this policy and of mutual agreement/contract and other issuer's recommendations concerning the purpose and method of use of his services
- the user has not complied with other rules in force.

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

(4) The issuer of the SI-TSA/SI-TRUST or the SI-TRUST guarantees the value of each particular legal transaction equipped with a qualified time stamp up to a maximum of EUR 5,000.

2.5. *User liability*

The user shall be liable for any damage resulting from non-compliance with the provisions of this policy, instructions, SI-TSA and other applicable legislation.

2.6. Third-party liability

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 9.6.4) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

2.7. Restrictions on use

(1) Restrictions of use other than those set out in that policy or agreed by mutual agreement or agreement do not.

(2) The use must be in accordance with the legislation in force.

2.8. Price schedule

The fee schedule and the way to charge a time stamping is published on the website of the SI-TSA, https://www.si-trust.gov.si/sl/kvalificiran-elektronski-casovni-zig/.

3. THE SECURITY OF THE ACTION OF THE ISSUER OF THE TIME STAMPS

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 5.1) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

3.1. Procedures and policy statement for the action of the issuer of the time stamps

3.1.1 Statement of the proceedings of the issuer of the time stamps

All the provisions of this heading[2] are set out in the other sections of this policy, provided for by the SI-TRUST policy.

3.1.2 Statement on the policy of the issuer of the time stamps

All the provisions of the SI-TSA operational policy statement[3] are, if not detailed below, given in the other sections of this policy.

Method of use of qualified time stamps

[2] According to ETSI TS 102 023 v.1.2.1., 7.1.1

[3] According to ETSI TS 102 023 v.1.2.1., 7.1.2

The arrangements for the use of the qualified time stamps shall be published by the SI-TSA in its instructions on its website.

Procedure in case of disputes

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 9.13) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

Inspection

The provisions are laid down in the Sectoral Policy for the SI-TRUST (full place. 8).

3.2. Management of the keys of the issuer of the time stamps

3.2.1 Issuer of time stamps keys

(1) The signature key pair and the verification of the qualified time stamps shall be generated in a physically and electronically secure SI-TRUST following a specific process of generating SI-TSA key keys.

(2) Keys generation shall be generated in safe machine cryptographic modules compliant with the NIST FIPS 140-2 level 3.

(3) The GPA issuer's public key has been signed by the originator of the ECS and issued a digital certificate.

(4) Digital confirmation with the public key and the private key of the SI-TASA shall be generated by algorithms and in a manner consistent with the requirements of the SIGOV-CA and in line with the internationally established recommendations.

(5) The detailed specifications for the CIP key are in line with the legislation in force in the SI-TRUST, in line with the legislation in force.

3.2.2 Protection of the private key of the issuer of the time stamps

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 6.2.1) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

3.2.3 Delivery of the stamp of the issuer of the time stamps

(1) The SEC's public key is published and delivered in accordance with the SGOV-CA policy, always in the form of a digital certificate from the SI-TSA.

(2) The features and data on the certificate (s) of the SI-TASA issuer are published on the IS-TSA websites.

3.2.4 Restoration of the public key of the issuer of the time stamps

The validity of the PKI public keys of an issuer of the SI-TSA is determined by the SGOV-CA policy.

3.2.5 End of validity keys of the issuer of the time stamps

(1) The SI-TSA shall ensure that no keys are used after its expiry.

(2) The SI-TSA shall ensure that accumulated keys with valid keys are replaced in a timely manner and in a secure manner.

(3) The procedure for the destruction of the private keys after their expiry shall take place in a safe manner following the provisions of the Interne policy SI-TRUST, in accordance with the provisions of the SI-TRUST. Private keys shall be destroyed so that they cannot be restored.

3.2.6 Management of cryptographic modules for time stamps

(1) The SI-TSA ensures the safety of a mechanical cryptographic module throughout their life cycle.

(2) The detailed arrangements for the handling of the cryptographic module (s) of the SI-TSA are in line with the legislation in force in the SI-TRUST, in line with the legislation in force.

3.3. Time-stamping

3.3.1 Time stamp

(1) The SI-TSA ensures that time stamps are issued in a safe way with point time accuracy of one (1) second or better.

(2) The format of the application for a timestamp and the time stamp itself shall be in accordance with recommendation RFC 3161 “Internet X.509 Public Key Infrastructure — Tim-Stamp Protocol (TSP)”, ETSI standards EN 319 421 and ETSI EN 319 422, as well as the instructions issued by the SI-TSA issuer, which are published on the website of the SI-TSA.

(3) The SI-TSA issuer further supports the possibility of time stamping using the Transport Protocol provided by RFC 3161 in chapter “3.4. Tim-Stamp Protocol via HTTP’, both of which are a request and an answer for a time stamping in XML in accordance with the “Entrust XML” scheme, which is published on the websites of the issuer of the SI-TSA.

(4) The timestamp profile shall contain four (4) data blocks set out in the table below and a more detailed description is given on the websites of the issuer of the SI-TSA:

Data on time stamped data; \ “_blank” *SignedInfo*	*Kananonymisation method*
	Signature algorithm (RSA to encrypt a summary using the SHA-256 algorithm)

	Time stamp data: - *summary algorithm (SHA-256)* - *summary*
	Information on the issuer of the SI-TSA - *summary algorithm (SHA-256)* - *summary that uniquely identifies the issuer of the SI-TSA*
Signature \ “_blank” *SignatureValue*	*Signature*
SI-TSA (TSI). *Keyinfo of TimempAuthority*	*Certificate of base64*
Time stamp, \ “_blank” *TimeStampInfo*	*Policy code under which time stamp is issued*
	Summary of the time-stamped summary message
	A serial number which is unique for each time stamp issued by the SI-TSA
	Time when the time stamp was issued for universal time[4]
	Random generated number included in the time stamp of the option when requested by the user
	Other optional information

3.3.2 Clock synchronisation

(1) The time of the SI-TSA servers shall be coordinated in a safe manner with the time UTC time with the NTP protocol that uses the reference hour of the GPS or the reference oscillator.

(2) The synchronisation of the SI-Ts server hours with the reference time is constantly verified and, in the case of possible exemptions, the SI-Ts are subject to appropriate measures.

3.4. Management and organisation

3.4.1 Protection of infrastructure

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 5.1) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

3.4.2 Access to the infrastructure of the issuer of the time stamps

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 5.1.2) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

[4] universal time, *Universal Time*, marked ‘Z’ at the end of the data, e.g.: 2004-02-16T07: 06: 11.703Z. Universal time is 1 (1) hour in winter, and at an annual time two (2) hours for central European time.

3.4.3 organisational structure of the issuer of the time stamps

Organisation of a trust and trusted service provider

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 5.2.1) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

Number of persons required per task

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 5.2.2) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

Identity of individual applications

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 5.2.3) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

Roles requiring separation of duties

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 5.2.4) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

3.4.4 Personnel controls

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 5.3) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

Qualifications, experience and clearance requirements

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 5.3.1) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

Background check procedures

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 5.3.2) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

Staff training

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 5.3.3) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

Training requirements

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 5.3.4) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

Job rotation frequency and sequence

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 5.3.5) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

Sanctions

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 5.3.6) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

Independent contractor requirements

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 5.3.7) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

Documentation supplied to personnel

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 5.3.8) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

3.4.5 Physical security

Location and structure of the trust service provider

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 5.1.1) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

Physical access to the infrastructure of the trust service provider

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 5.1.2) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

Power and air conditioning

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 5.1.3) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

Water exposures

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 5.1.4) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

Fire prevention and protection

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 5.1.5) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

Media management

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 5.1.6) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

Disposal

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 5.1.7) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

Off-site backup

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 5.1.8) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

3.4.6 Infrastructure management

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 5.1) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

3.4.7 management of access to the infrastructure

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 5.1.2) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

3.4.8 Establishment and maintenance of infrastructure

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 5.1.1) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

3.4.9 Compromising infrastructure safety

The provisions are laid down in the Sectoral Policy for the SI-TRUST (all the subheadings. 5.7) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

3.4.10 Termination of the action of the issuer of the time stamps

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 5.8) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

3.4.11 compliance with applicable law

The provisions are laid down in the Sectoral Policy SI-TRUST (Underset. 9.15) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

3.4.12 System security checks

The provisions are laid down in the Sectoral Policy for the SI-TRUST (all the subheadings. 5.4) FROM THE NORTHERN PART OF CYPRUS TO THE GOVERNMENT-CONTROLLED AREAS DURING THE REPORTING PERIOD.

3.5. Policy management[5]

The provisions are laid down in the Sectoral Policy for the SI-TRUST (full sub-heading. 1.5 and 9.12).

[5] This sub-chapter is not in line with ETSI TS 102 023 v1.2.1 recommendation.