MINISTERIO
DE INCLUSIÓN, SEGURIDAD SOCIAL
Y MIGRACIONES

SECRETARÍA DE ESTADO
DE LA SEGURIDAD SOCIAL
Y PENSIONES

Gerencia de Informática
de la Seguridad Social

Time stamping by ACGISS

Certification policy

V 2.0.5
(October 2020)

Social Security IT
Department
c/ Doctor Tolosa Latour s/n
28041 Madrid

Change control

Version	Observations	Date
1.0	Original version	10-12-2009
1.1	OIDs assigned	15-12-2009
1.2	Amendment to internal branches of GISS OIDs	02-02-2010
1.2.1	Amendment to certification profile	07-04-2010
2.0	Full revision due to update of PKI for adoption of eIDAS Regulation	20-06-2016
2.0.1	Review: error correction and writing clarifications	22-02-2017
2.0.2	Writing revisions	31-05-2017
2.0.3	Changes due to internal annual review: errata correction and Ministry name update.	03-08-2018
2.0.4	Annual internal review	31-07-2019
2.0.5	Review of documentation in accordance with ETSI standards, update of the Ministry's Logo and changes derived from the eIDAS 2020 audit	30-10-2020

Table of Contents

1. INTRODUCTION

1.1. Presentation

As Provider of Trust Services, the Social Security IT Department (GISS) issues qualified certificates and also offers time stamping services whose objective is to demonstrate that a series of data has existed and has not been modified since a determined point in time.

This document covers the policy and statement of practices for the GISS Time Stamping Authority (TSA), and includes the obligations and liabilities for all implicated parties, such as technical details and terms and conditions of use for the service.

In order to guarantee the reliability of said service, this policy is based on X.509 v3 cryptography of public keys and certificates issued by the GISS Certification Authority (ACGISS), and will therefore ultimately be subject to the stipulations set forth in its Certification Practice Statement (CPS).

From the point of view of current legislation, the service is recorded as one of the services provided by the ACGISS, on the Ministry of Energy, Tourism and Digital Agenda website.

In order to prepare this document, standard EN 319 421 has been followed, incorporating the requirements and conditions of current legislation and international standards, which may be consulted in the references section of this document.

1.2. Name of document and identification

Document name	ACGISS Time Stamping. Certification policies and practices
Version	2.0.5
Document status	Approved
Issue date	30 October 2020
OID (Internal GISS)	2.16.724.1.4.2.2.1.3.1
Location	http://www.seg-social.es/ACGISS

OID meaning: joint-iso-itu-t (2) country (16) es (724) adm (1) giss (4) infrastructures (2) ACGISSv2 (2) SubCA GISS01 (1) Trust Services (3) TSA policy (1)

2. DEFINITIONS AND ACRONYMS

2.1. Definitions

Time Stamp Authority (TSA): Authority belonging to a Trust Services Provider, which provides confirmation of prior existence of specific electronic documentation at a given time.

Security services platform: Social Security IT Department (GISS) infrastructure, which includes functions relating to electronic signature, custody of documents and time stamping.

Time stamp policy: Consists of a series of regulations indicating the applicability of a time stamp on a particular community or application, with common security requirements.

Electronic time stamp: data in electronic format which links with other data at a specific instance, providing proof that said data existed at that instant;

Qualified electronic time stamp: an electronic time stamp that complies with the requirements established in article 42 of EU Regulation no. 910/2014.

Relying party for time stamps: Person or entity who voluntarily authenticates the time stamp and the electronic certificate used for its signature, as a method of accrediting the authenticity and integrity of the signed document

Coordinated Universal Time (UTC): Also known as *civilian time*, it is the time in the zone of reference by which all other zones in the world are calculated.

2.2. Acronyms

ACGISS	Certification Authority for the Social Security IT Department
ASN	Abstract Syntax Notation
CPS	Certification Practice Statement
FIPS	Federal Information Processing Standards
GISS	Social Security IT Department
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
ISO	International Organisation for Standardisation
OID	Object Identifier
RFC	Request for comment
TSA	Time-Stamping Authority
TSP	Time-Stamping Protocol
TSS	Time-Stamping Service
TST	Time-Stamp Token
TSU	Time-Stamping Unit
UTC	Coordinated Universal Time

3. GENERAL CONCEPTS

3.1. Time stamping service

The time stamping service (TSS) is integrated into the Security Services Platform, whose mission is to fulfil needs regarding encryption, verification of signatures, validation of certificates, time stamping, and custody of documents within the Social Security IT Department (GISS) scope.

Two main functions within the service are worth noting:

- Provision of the time stamping service, corresponding to the generation of stamps.
- Service management for time stamping, including monitoring and service control functions, to ensure that operations are performed as specified by the TSA.

Time stamping functionality is provided via HTTP and in ASN1 format, in compliance with standard RFC 3161 of the IETF.

3.2. Time stamp authority

The TSA is an authority trusted by users (subscribers and relying parties) to issue time stamps.

GISS, as a trust services provider, constitutes the Time Stamp Authority within the scope of the Secretary of State for Social Security, providing the necessary infrastructure to guarantee the security and accuracy of the service under the requirements set forth in current legislation.

As a TSA, it is liable for all actions relating to the provision of the time stamping service, and ensures compliance with the stipulations set forth in this document.

3.3. Subscribers

Subscribers to this service belong to the Management Organisms and Commons Services within the scope of the Secretary of State for Social Security.

3.4. Community of users and applicability

Service users shall mainly be specific applications/systems or clients within the scope of the Secretary of State for Social Security. The TSA shall be used via the GISS Security Services Platform.

Time stamping services provided by the Social Security TSA are recorded in the supervising agency as a service provided by the ACGISS certification services provider, which complies with the technical requirements and obligations specified in the current legislation.

3.5. Limitations of use

The area of activity for time stamp certificates and services is limited to specific applications/systems or clients within the scope of the Social Security Department.

TSA services are generally used for checking for the existence of a data at a given time, mainly carried out in processes of document signing and data exchanges with other entities.

The services will be used in accordance with what is established in this document and in the internal procedures that are applicable.

3.6. Service availability

TSA services are available 24 hours a day, 7 days a week, except for contingencies or maintenance operations.

In the event of a failure of TSA systems, GISS shall make every effort to ensure that the service only be inactive for the minimum time possible. For this purpose, systems involved in providing the service are replicated and balanced, which enables guaranteed continuity of services.

4. POLICIES AND PRACTICES

4.1. Introduction

Time stamp practices detail the implementation of the controls necessary for complying with the time stamp policy and guaranteeing the reliability and trustworthiness of the service.

In addition to the conditions specified in this section, the general mechanisms and procedures in the ACGISS CPS shall apply, as well as the different regulations within the GISS scope.

4.2. Obligations and responsibilities

4.2.1. TSA obligations

4.2.1.1. *General*

The Social Security IT Department (GISS), as Trust Services Provider and Time Stamp Authority, shall be obliged to:

- Follow the procedures and directives specified in this policy document and the ACGISS CPS.
- Protect private keys used for issuing time stamps, in a way that ensures their confidentiality and integrity.

- Use reliable products and systems that guarantee the security of the time stamp processes to whom they provide support.
- Maintain and calibrate the time reference used, in order to guarantee the hour and date included in the stamps issued.
- Issue time stamps with content and accuracy as required by current legislation.
- Retain all information and documentation relating to the time stamping service.
- Publish and maintain this Policy document and the Time Stamp Practice Statement, as well as any other relevant information for service users.
- Facilitate a validation service for time stamps, in order for relying parties to verify their validity.
- As a service provider, respond to claims for damages caused, in accordance with the specifications set forth in Law 59/2003 on Electronic Signatures.

4.2.1.2. TSA obligations to its subscribers

The TSA commits to providing the service according to the specified terms and conditions, in particular, those relating to its availability and accuracy.

It shall be responsible for guaranteeing continuity of service, and therefore should plan any necessary technical maintenance shutdowns sufficiently in advance and advise subscribers of this through the available means.

It also commits to:

- Issue time stamps in accordance with the information provided by subscribers, and free from data entry errors.
- Issue time stamps in compliance with current regulations, including the minimum content that may be required at any time.
- Publish this document and facilitate any other information that may be relevant to the subscriber.
- Keep time stamps information, in accordance with the stipulations of the applicable legislation.

4.2.2. Subscriber obligations

Subscribers to the time stamping service are obligated to:

- Follow the procedures and directives specified in this document.
- Comply with published terms and conditions.
- Identify and authenticate themselves in accordance with the specific requirements.
- Verify the time stamp electronic signature, including verifying the validity of the certificates used.
- Use time stamps within the limits and scope described in this policy.

Moreover, Social Security uses custody processes to re-stamp data objects periodically and avoid obsolescence of algorithms. These can be used by all subscribers of the service. Also subscribers may carry out additional re-signing processes if they deem it convenient.

4.2.3. *Relying party obligations for time stamps*

Relying parties for time stamps issued by GISS are obliged to:

- Follow the procedures and directives specified in this document.
- Verify the time stamp electronic signature, including verifying the validity of the certificates used.
- Accept time stamps within the limits and scope described in this policy.

4.2.4. *Liabilities*

In general, the Provider shall respond to claims for damages caused to any person in the exercise of their activity, if it does not comply with the obligations imposed by Law 59/2003 on Electronic Signatures.

It shall also ensure compliance with the conditions and requirements established in this present document, remaining exempt from liability beyond the scope and reach of the time stamp service and, in particular, with regards to the content of the stamped documents.

The TSA shall not be liable if any of the following situations arise:

- If the limits established by GISS regarding possible uses are breached, or they are not used in compliance with the conditions established and communicated to the service subscriber.
- If the subscriber or relying parties for the stamps do not verify their electronic signature, including the validity of the certificate used.

4.3. Terms and conditions for use of service

By way of this document, which shall be published on the provider website, the TSA facilitates access to the terms and conditions of use relating to the time stamping service, for its subscribers and relying parties.

Additionally, it shall make information available about how to verify the time stamp, so that it and any existing limitation on the time period may be considered sufficiently trustworthy.

5. TSA MANAGEMENT AND OPERATION

5.1. Organisational structure

The Time Stamp Authority is included within the ACGISS certification hierarchy.

All information relating to the provision of GISS certification services is available on the Provider website and, in particular, in the CPS.

5.2. Personnel security

As specified in the CPS.

5.3. Asset classification and management

As specified in the CPS

5.4. Managing systems access

Access to the TSA system should be limited to duly authorised persons. Controls exist in order to prevent unauthorised access to the internal network, TSA functions and information managed it manages.

Procedures exist to manage existing user profiles on the GISS security platform and in particular, in the time stamp module, granting the necessary privileges to each and controlling the operations they perform by way of audit trails and events logs.

5.5. Managing the life cycles of keys

5.5.1. Generating TSA keys

The TSA ensures that keys used for time stamp signatures are generated in a ceremony under controlled circumstances and in a physically secured environment, within an HSM cryptographic module certified with FIPS 140-2 level 3 and CC EAL 4+.

Key length for certificates is 2048 bits.

RSA signature algorithm and SHA-256 hash algorithm are used to guarantee the security and authenticity of the certificates used.

The initial lifetime of TSU’s keys and certificates will be 5 years.

5.5.2. Protecting private keys

The TSA commits to protect private keys, in order for them to maintain their confidentiality and integrity. In particular, private keys shall be kept and used within a cryptographic module that complies with the requirements specified in the previous section, at least, under multi-person control, and ensuring that keys are never extracted from said cryptographic module.

5.5.3. Distributing the TSA public key

The TSA public key shall be available on the Social Security website in an electronic certificate, auto-signed by the ACGISS.

Any additional information relating to consulting the validity of the certificate may be consulted in the ACGISS CPS.

5.5.4. Regenerating the TSA key

Regeneration of the TSA key is prompted, among other causes, by expiration of the certificate, or when a possible key compromise is detected.

Issue of a new certificate shall be communicated to service users when necessary.

5.5.5. Backup of the TSA key

TSU’s private keys are backed up, copied, stored and retrieved only by personnel in trusted roles using, at least, dual control in a physically secured environment.

Personnel and procedures for these functions and security measures applied to copies will be those established in CPS.

5.5.6. End of life cycle for the TSA key

The TSA guarantees that keys shall not be used beyond their validity period. The GISS has established internal procedures that ensure the renewal of keys before their expiration date. This prevents that TST are generated with a private key that has already expired.

It shall also be ensured that private keys are securely destroyed, preventing any possible recovery of them.

5.5.7. Managing the cryptographic modules used for signing time stamps

The TSA shall monitor and ensure that the cryptographic hardware used to sign the TST functions correctly and take the necessary measures to prevent tampering.

Installation, activation and possible duplication of keys within the cryptographic module shall only be performed by the personnel authorised to do so, with each action duly recorded.

The TSA guarantees that private signature keys kept within these modules shall be deleted according to existing security procedures before the modules be withdrawn.

In addition, all aspects of HSM management established in the DPC will apply

5.6. Time stamping

5.6.1. Time stamping

The TSA commits to ensuring that the generation of the TST be performed securely and with the correct time reference.

In addition to the unique identifier incorporated in each TST, an identifier of this corporate time stamping policy will be included in the time stamp response, so that the conditions and guidelines applicable to time stamps can be known. Likewise, a reference to policy 0.4.0.2023.1.1 corresponding to the best-practices-ts-policy defined in the ETSI 319 421 standard is incorporated into the TST time tokens.

Likewise, the time value used shall be synchronised with UTC time, with the accuracy specified in the applicable legislation. In the event of a loss of synchronization that prevents the GISS guarantee this value, the issuance of time stamps will be stopped and all affected parties will be informed. The TSA services will be resumed after the synchronization between the TSA clock and the UTC time has been successfully reestablished.

Time stamps shall be signed with a key exclusively generated for these purposes, using the security measures necessary for guaranteeing its validity, as defined in the ACGISS CPS.

TSA systems shall reject any attempt to issue time-stamps if the signing private key has expired.

The time stamping service uses SHA-256 or higher algorithms to generate the hashes of the data to be stamped.

RFC 3161 “Time Stamp Protocol” shall be followed, with the restrictions set forth in regulation ETSI TS 101 861 “Time Stamping Profile”. Time stamps shall be completed via HTTP, using ASN1 notation.

5.6.2. Synchronising with UTC

The main mission of the Royal Observatory of the Spanish Navy is to maintain the basic unit of Time in Spain, and officially maintain and broadcast the Coordinated Universal Time scale (UTC (ROA)), considered for all purposes to be the base for the official time of Spain (R. D. 23 October 1992, no. 1308/1992).

The GISS TSA clock is synchronised with UTC time via connection with the ROA (Royal Observatory of the Spanish Navy), through on the one hand the SARA network (System of Applications and Networks for Administrations) with a precision of less than 1 second. This network has advanced mechanisms to guarantee reliability, security, capacity, quality of service and interoperability of the services provided. On the other hand, in order to minimize the chances of loss of synchronism, an alternative channel of direct synchronization with ROA via the Internet is also configured.

Clocks should be kept calibrated in order to ensure the precision declared and there are mechanisms to protect them from any risk that may arise due to a change in time beyond said calibration.

The TSA also ensures that, in the event of any difference greater than the given threshold between a timestamp’s time and the UTC time, all interested parties are adequately informed. Calculation of time complies with the stipulations set forth in the NTP (Network Time Protocol) and BIPM (International Bureau of Weights and Measures) recommendations.

5.7. Physical security

As established in the CPS.

5.8. Security management

As established in the CPS.

Also, TSA systems have additional mechanisms for quality and security management appropriate for the time-stamping services.

5.9. Network security

As established in the CPS.

5.10. Incident management

As established in the CPS.

5.11. Evidence management

As established in the CPS.

5.12. Business continuity management

As established in the CPS.

In addition to this, there are specific contingence procedures for TSA systems, which guarantee operations recovery in less than 24 hours and response to TSU's private signing keys compromise and loss of synchronization of TSA.

In the event of a TSU's private key being compromised, at least ACGISS:

- Shall inform all subscribers and users of the compromise.
- Shall revoke the TSA certificate and publish the corresponding revocation list.
- Shall plan the generation of new TSA certificate in order to avoid loss of service, if there are not security problems.
- Shall investigate the causes of the compromise and shall take the appropriate measures to avoid a repeat incident.

In the event of a loss of synchronization, at least ACGISS:

- Shall stop emitting time stamps.
- Shall inform all subscribers and users of the loss of synchronization.
- Shall re-establish service as quickly as possible.

5.13. Cessation of the TSA

In the event of cessation of its services, the TSA ensures minimum impact on subscribers and relying parties for the stamps, in particular, guaranteeing maintenance of the information required to verify the correction of time stamps.

The TSA shall perform the following actions sufficiently in advance:

- Inform all subscribers and relying parties of everything relating to the cessation of activity.

- Communicate all existing mechanisms for maintaining events logs and audit trails necessary to demonstrate the proper functioning of the TSA for a reasonable period.
- Uphold its obligations to make the public key or its certificates available to relying parties for a reasonable period.
- TSA shall revoke the TSU's certificates.
- Destroy all private keys, including security copies, preventing their recovery.

In addition, advise the supervision agency of the cessation of services and the mechanisms it shall make available to users to verify the validity of time stamps issued.

5.13.1. Deployment and maintenance of trust systems

The TSA uses trustworthy systems and products that are sufficiently protected against modifications and alterations, when the risk analysis determines it based on their level of criticality.

The technical controls for the life cycle of the systems involved shall be established in the CPS.

5.13.2. Commitment of TSA services

The TSA guarantees that if a security event occurs during the time stamp services, including the compromise of its private key or loss of calibration with the UTC, it shall inform subscribers and relying parties for the stamps via the available methods for the same.

5.13.3. Record of information relating to time stamp services

All relevant information concerning the functioning of the timestamp services will be kept to allow TSA's service restoration and, in particular, to provide any evidence necessary for legal proceedings. These actions will be in operation for 15 years to comply with current legislation.

The types of events and information recorded shall be documented. Events relating to key management, and the synchronisation and calibration of clocks, among other events, shall be included.

All recorded information and events shall be sufficiently protected to prevent tampering and to maintain the required confidentiality.

5.14. Conformity or compliance

This policy is designed to comply with the requirements for the issuing of qualified time stamps, issued taking into account the requirements established in the EU Regulation no. 910/2014.

TSTs shall include the identifier of the time stamp policy, in order to guarantee the trustworthiness of the time stamps issued. The TSA commits to comply with the obligations and implement the controls specified in this policy.

6. TECHNICAL FEATURES OF THE SERVICE

6.1. Time stamp certificate profile summary

FIELD	CONTENT	VALUES
1. X.509V1		
1.1. Version	V3	2
1.2. Serial Number	Unique identifier no.	*Automated*
1.3. Signature Algorithm	Type of algorithm. OID 2.16.840.1.101.3.4.2	SHA256RSA
1.4. Issuer Distinguished Name		
1.4.1. Country (C)	ES	ES
1.4.2. Organisation (O)	Provider official trade name	GENERAL TREASURY FOR SOCIAL SECURITY
1.4.3 Organisational Unit (OU)	Organisational unit responsible for issue	SOCIAL SECURITY IT DEPARTMENT
1.4.4. Locality (L)	Location	MADRID
1.4.5. Organisational Unit (OU)	Organisational unit within the service provider, responsible for issuing the certificate.	GISS01
1.4.6. Serial Number	Unique identification number for the certification entity	Q2827003A
1.4.8. Common Name (CN)	Common name of the subordinate CA certificate	SUBCA GISS01
1.6. Subject		
1.5.1. Country (C)	ES	ES
1.5.2. Organisation (O)	Subscriber name	SECRETARY OF STATE FOR SOCIAL SECURITY
1.5.5. Organisational Unit (OU)	Organisational unit within the service provider, responsible for issuing the certificate.	TRUST SERVICES
1.5.6. Serial Number	Entity unique identity number	S2819001E
1.5.7. Common Name (CN)	Certificate name	TSA TIME STAMP AUTHORITY
1.6 Subject Public Key Info	Encrypted public key for stamp	(RSA 2048 bits)
2. X.509v3 Extensions		
2.3. Key Usage		
2.3.1. Digital Signature		"1"
2.3.2. Content Commitment		"1"
2.4 Extended Key Usage		
2.4.1. Date stamp	1.3.6.1.5.5.7.3.8	"1"
2.5. Qualified Certificate Statements	Qualified certificate policy (OID 0.4.0.1862.1.1)	
2.6. Certificate Policies	OID associated with ACGISS CP and policy URL	2.16.724.1.4.2.2.1.3.1
2.7. Subject Alternative Name	Contact email address	acgiss.soporte.giss@seg-social.es
2.8. Issuer Alternative Name	Contact email address	ACGISS.Soporte@seg-social.es
2.9. cRLDistributionPoint	Distribution point no.1	http://crl.seg-social.gob.es/ac_sub.crl
2.10. Authority Info Access	OCSP web address SUBCA certificate access URL	http://ocsp.seg-social.gob.es/ http://www.seg-social.es/ACGISS/Certs/SUBCA_GISS01

6.2. Process for requesting and issuing a time stamp

6.2.1. Process for issuing a time stamp

The steps necessary to generate a time stamp are as follows:

- The client calculates the hash of the document to stamp.
- The client then sends a request for a time stamp to a specific URL, following RFC 3161 protocol, including the hash of the document to be stamped.
- The TSA receives the application and assesses whether it is complete and correct.
- If the result is correct, the TSA signs the request, generating a time stamp (including the document hash, the date and time obtained from a trustworthy source and the TSA electronic signature).
- The time stamp is returned to the client.
- The client should validate the stamp signature and duly save it.
- The TSA maintains a record of stamps issued for future verification.

6.2.2. Format for requests and responses

Clients should send their applications via HTTP, creating a *time-stamping request* in ASN1 format, to the following URL:

http://host:port/tspTSA/inputRequestTSA[1]

The format of the request is defined in RFC3161, and it should follow the ASN1 structure, defined as:

```
TimeStampReq: = SEQUENCE {
      Version             INTEGER {v1 (1)},
      MessageImprint      ,
      reqPolicy           TSAPolicyId        OPTIONAL,
      nonce        INTEGER                   OPTIONAL,
      certReq             BOOLEAN                   DEFAULT FALSE,
      extensions          [0] IMPLICIT Extensions   OPTIONAL}

MessageImprint: = SEQUENCE {
      hashAlgorithm       AlgorithmIdentifier,
      hashedMessage       OCTET STRING }
```

The format of the response is as follows:

```
TimeStampResp: = SEQUENCE {
      Status              PKIStatusInfo,
```

[1] The request to obtain the time stamp is sent through the Security Services Platform, for which it is necessary a previous user registration.

```
      timeStampToken                 OPTIONAL
}

PKIStatusInfo: = SEQUENCE {
      status PKIStatus,
      statusString PKIFreeText OPTIONAL,
      failInfo PKIFailureInfo OPTIONAL
}

PKIStatus: = INTEGER {
      granted (0),
      grantedWithMods (1)
      rejection (2),
      waiting (3),
      revocationWarning (4),
      revocationNotification (5)
}

PKIFailureInfo: = BIT STRING {
      badAlg (0),
      badRequest (2),
      badDataFormat (5),
      timeNotAvailable (14),
      unacceptedPolicy (15),
      unacceptedExtension (16),
      addInfoNotAvailable (17)
      systemFailure (25)
}

TimeStampToken: = ContentInfo
      -- contentType is id-signedData as defined in [CMS]
      -- content is SignedData as defined in([CMS])
      -- eContentType within SignedData is id-ct-TSTInfo
      -- eContent within SignedData is TSTInfo

id-ct-TSTInfo OBJECT IDENTIFIER: = {iso(1) member-body(2)
us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) ct(1) 4}

TSTInfo: = SEQUENCE {
      Version            INTEGER {v1 (1)},
      policy             TSAPolicyId,
      messageImprint     MessageImprint,
      serialNumber       INTEGER,
      genTime            GeneralizedTime,
      accuracy           Accuracy                 OPTIONAL,
      ordering           BOOLEAN                  DEFAULT FALSE,
      nonce        INTEGER                  OPTIONAL,
      tsa                [0]GeneralName           OPTIONAL,
      extensions         [1]IMPLICIT Extensions   OPTIONAL }
```

7. REFERENCES

Relevant legislation:

- EU Regulation no. 910/2014 of the European Parliament and of the Council of 23 July 2014, regarding electronic identification and trust services for electronic transactions in the domestic market.
- Law 59/2003 of 19 December, on Electronic Signatures.
- Law 39/2015 of 1 October, on Common Administrative Procedure for Public Administrations.
- Law 40/2015 of 1 October, on the public sector legal regime.
- Royal Decree 1671/2009 of 6 November, which partially implements Law 11/2007 of 22 June, on Citizens' Electronic Access to Public Services.

The following standards regarding time stamps have been taken into account in their preparation:

- ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
- ETSI EN 319 422 Profiles for TSP Providing Time-stamping Services.
- RFC 3268 "Requirements for time-stamping authorities"
- RFC 3161 "Internet X.509 Public Key Infrastructure – Time Stamp Protocol (TSP)"