ACGISS Time Stamping

INFORMATION DOCUMENT

(PUBLIC DISCLOSURE STATEMENT – PDS)

Version: 1.1.3

Validity v1: 1 July 2016 – Present day

Last version: 30 October 2020

This document contains the essential information relating to the ACGISS time stamping service in accordance with the directives included in Appendix B of ETSI standard EN 319 421.

1. Complete agreement

This document contains high-level statements regarding the ACGISS time stamping service. It does not replace or cancel the ACGISS Time Stamping Policy document available at http://www.seg-social.es/ACGISS.

2. Contact information

2.1. Organisation responsible

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

2.2. Contact

Name	Social Security IT Department		
E-mail address	acgiss.soporte.giss@seg-social.es		
Address	C/ Doctor Tolosa Latour s/n, 28041 Madrid		
Telephone	91 390 27 03	**Fax**	91 460 40 72

2.3. Contact for revocation processes

Name	Social Security IT Department		
E-mail address	acgiss.soporte.giss@seg-social.es		
Address	C/ Doctor Tolosa Latour s/n, 28041 Madrid		
Telephone	91 390 27 03	**Fax**	91 460 40 72

3. Type of certificate, validation and use

The aim of the time stamping service is to meet the new needs in relation to encryption, signature and signature verification, validation of certificates, time stamping and document storage within the Social Security IT Department (GISS).

The service can be divided into two main functions:

- 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.

Key length for certificates is 2048 bits. RSA signature algorithm and SHA-256 hash algorithms are used to guarantee the security and authenticity of the certificates used.

The time stamp keys are generated and used within HSM cryptographic modules with adequate security measures that guarantee their protection.

3.1. Validation of certificates

Checking the status of certificates can be done via two different methods: via OCSP or by downloading the CRLs. Certificate validation systems are available 24 hours a day, 7 days a week.

Time stamps can be validated using the tools made available to users for verifying electronic signatures on the main Social Security website and on the corporate intranet. The Central State Administration platform @Firma can also be used.

3.2. Subscribers

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

3.3. Community of users and applicability

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

Time stamping services provided by the Social Security TSA are recorded with the national supervisory body as a service provided by the trust service supplier ACGISS, which complies with the technical requirements and obligations specified in current legislation.

4. Limits on usage

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

In general, certificates and their associated keys will not be used for purposes other than those specified in the previous section.

Certificates may not be used after their expiry date or after they have been revoked.

The GISS TSA clock is synchronised with UTC time via its connection with the ROA (Royal Observatory of the Spanish Navy), using on the one hand the SARA network (public sector applications and networks system), with a precision of less than 1 second. This network uses advanced mechanisms to guarantee the reliability, security, capacity, quality 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.

In the event of any loss of synchronisation which prevents the GISS from guaranteeing the time recorded, time stamps will cease to be issued and all parties affected will be informed. Services will be resumed once synchronisation has been correctly restored.

To guarantee the integrity of the information to be sealed, SHA-256 or higher algorithms will be used to generate the hashes of the data on the stamps.

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

All relevant information concerning the functioning of time stamp services will be properly stored for 15 years, in order to comply with current legislation.

5. Subscriber obligations

Subscribers to the time stamping service are obligated to:

- Follow the procedures and directives specified in the certification policy.
- 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 the certification policy.

6. Obligations of third parties relying on the time stamps

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

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

7. Liability limitations

In general, the Provider will 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 will also ensure compliance with the conditions and requirements established in this document, remaining exempt from liability beyond the scope and extent of the time stamp service and, in particular, as regards the content of the stamped documents.

The TSA will 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.

8. Applicable agreements, DPC and PC

The applicable agreements for time stamp service are as follows:

- Specific DPC and PC (OID 2.16.724.1.4.2.2.1.3.1) that regulate issuing conditions and use of certificates and time stamps.
- Policy best-practices-ts-policy (OID 0.4.0.2023.1.1) defined in the ETSI 319 421 standard.
- General conditions on the use of the service included in the certificate information document.

9. Privacy policy

The ACGISS has developed a confidentiality plan, in accordance with the current Spanish legislation on the protection of personal data.

However, it is worth noting that personal data are not used in the provision of time stamp services.

10. Refund policy

Not applicable.

11. Relevant legislation and dispute resolution

11.1. Applicable legislation

The provision of time stamping services is carried out in accordance with the provisions of Regulation (EU) No 910/2014 of the European Parliament and of the Counsel, of 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market.

European standards applicable at the date on which the certification regulations were approved have also been taken into account.

- 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, partially implementing Law 11/2007, of 22 June, on public electronic access to public services.

11.2. Dispute resolution

The ACGISS acts in accordance with the general procedures established for Public Administration. The competent jurisdiction will be the jurisdiction applicable to dispute resolution within Public Administrations.

On the other hand, the corresponding service available at the Social Security website, as well as the internal procedures published in the corporate Intranet, may be used for the resolution of complaints and suggestions.

12. Trust accreditation and compliance audits

GISS is included in the Spanish list of trusted service providers (TSL) https://sede.minetur.gob.es/prestadores/tsl/tsl.pdf

It is also registered with the Ministry of Economy and Business as a trusted supplier of certain electronic services:

http://www.mincotur.gob.es/telecomunicaciones/es-es/servicios/firmaelectronica/paginas/prestadores.aspx

As stipulated in Regulation (EU) No 910/2014, GISS will carry out biennial audits in accordance with that Regulation.