ACGISS Electronic Seal Certificates

INFORMATION DOCUMENT

(PUBLIC DISCLOSURE STATEMENT – PDS)

Version: 1.1.4

Validity v1: 1 July 2016 – Present day

Last revision: 30 October 2020

This document contains essential information regarding ACGISS certification services in accordance with the directives included in Appendix A of Standard ETSI EN 319 411-1.

1. Contact information

1.1. Organisation responsible

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

1.2. 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

1.3. 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

2. Type of certificate, validation and use

2.1. Type of certificate

Electronic seal certificates are issued as automated action certificates within the PKI ACGISSv2 hierarchy and in accordance with the current AGE regulations relating to electronic certificates for electronic seals of administrative bodies.

The ACGISS issues two types of electronic seal certificates:

- Medium/significant level certificate: issued on SW medium for installation and use distributed across Social Security servers and systems requiring authentication or automated signature.
- High level certificate: centrally issued in an HSM certified as a qualified signature creation device and usable through the security platform available in the GISS.

Seal certificates are intended for different Entities and Bodies within the Social Security system, of at least Subdirectorate-General level, which will be regarded as the subscribers or owners of the certificates.

The different applicable certification policies are identified below:

OID (Internal GISS v2)	2.16.724.1.4.2.2.1.1.1 (medium level) 2.16.724.1.4.2.2.1.1.2 (high level)
OID (AGE policy)	2.16.724.1.3.5.6.2 (medium level) 2.16.724.1.3.5.6.1 (high level)
OID (ETSI EN 319 411-2)	0.4.0.194112.1.1 (QCP-l) (medium level) 0.4.0.194112.1.3 (QCP-l-qscd) (high level)

Meaning of OID: joint-iso-itu-t (2) country (16) es (724) adm (1) giss (4) infrastructures (2) ACGISSv2 (2) SubCA GISS01 (1) Automated Action (1) Electronic seal CP (1-medium level or 2-high level)

The keys of the seal certificates are at least 2,048 bits and RSA signature algorithms and SHA-256 hash algorithms are used.

2.2. 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.

2.3. Certificate usage

Electronic seal certificates will be used to guarantee the identification and authentication of the owning Entity or Body's exercise of their competences in automated administrative actions.

In particular, use of seal certificates will comply with the uses established in Law 40/2015, on the Public Sector legal Regime, RD 1671/2009 and other applicable regulations.

In general, electronic seals may be used for performing the following actions:

- Authenticating the identity of the owning Entity or Body.

- Electronic signature of documents in the exercise of their functions.
- Encryption of data and documents in the exercise of their functions.

3. Limits on certificate usage

The seal certificate is considered accepted as soon as the notification that issue has been successfully completed is received by the applicant, unless a contradictory communication of rejection or data modification is received within a time frame of 5 working days.

Each seal certificate will be used exclusively by the owner and for the purposes for which it was issued.

The different keys generated will be used exclusively for their specified purposes and in accordance with the provisions of their certification policy.

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

4. Subscriber obligations

Certificate subscribers/owners are obliged to do the following:

- Supply the Registration Authorities with exact, complete and true information relating to the data requested in the processes forming the certificate life cycle.
- Communicate any changes to the data after it has been supplied.
- Understand and accept the terms and conditions of issue and use of the certificates established in the DPC and respective policies.
- Not use certificates after their validity period has expired or they have been revoked.
- Protect private keys, taking proper precautions to avoid their loss, disclosure or unauthorised usage.
- Inform the GISS of any certificate malfunction and any compromise of keys.
- In the case of high-level seal certificates, generate the keys in HSM certificated as qualified signature creation devices

5. Third party obligation to verify certificate status

Third parties who accept certificates issued by the ACGISS must:

- Assume liability for the proper verification of the validity and revocation status of the certificates.
- Assume liability for the proper verification of the electronic signatures used on the ACGISS certificates.
- Understand the liabilities arising from acceptance of the certificates.
- Limit acceptance of the certificates to the permitted uses established on them and in the relevant certification policies.

6. Liability limitations

The ACGISS limits its liability under the terms of article 23 of Law 59/2003.

The provision of certification services will be performed in accordance with the provisions of the applicable certification regulations, using tools and practices to guarantee the security of the certificates issued.

The ACGISS will not be liable for harm or loss caused by the signatory or third parties acting in good faith, due to non-compliance with the obligations established in the DPC and PC for subscribers, owners and third parties who accept their certificates.

In addition, the ACGISS has a sufficient level of cover for public liability, under the terms set out in article 20.2 of Law 59/2003, of 19 December.

7. Applicable agreements, DPC and PC

The applicable agreements for public employee certification are as follows:

- Specific DPC and PC (OID 2.16.724.1.4.2.2.1.1.1 (medium level) and 2.16.724.1.4.2.2.1.1.2 (high level)) that regulate issuing conditions and use of certificates.
- General conditions of service incorporated into the certificate information document or PDS.
- Contract for issuing certificates signed by the applicant.

8. Privacy policy

Personal data are collected and processed according to the protection plans approved in the Social Security in accordance with what is established in the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (RGPD).

The Provider does not disclose or transfer this personal data, except in the cases provided or when legally required.

Registration information and information relating to certificate generation is stored for at least 15 years, in accordance with the provisions of the DPC.

9. Refund policy

Not applicable.

10. Relevant legislation and dispute resolution

10.1. Applicable legislation

The provision of certification services is performed in accordance with the provisions of Regulation (EU) No 910/2014 of the European Parliament and Counsel of 23 July 2014, on electronic identification and trust services, and Law 59/2003, of 19 December, on Electronic Signatures.

In addition, seal certificates are issued and used in accordance with the provisions of Law 40/2015, of 1 October, on the public sector legal regime, and in the AGE policy on signatures and certificates.

The European standards relevant at the date of approving the certification regulations have also been taken into account.

10.2. 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.

11. 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 as a qualified service provider with the Ministry of Economy and Business:

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.