ACGISS Public Employee Certificates

INFORMATION DOCUMENT

(PUBLIC DISCLOSURE STATEMENT – PDS)

Version: 1.1.

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

Employee certificates are issued as qualified personal certificates within the PKI ACGISS v2 hierarchy, and in accordance with current AGE regulations relating to public employee electronic certificates.

These certificates are intended for Social Security workers (civil servants, contract and temporary personnel) who carry out their functions within the different Social Security departments.

The different applicable certification policies are identified below:

OID (Internal GISS)	2.16.724.1.4.2.2.1.2.1*
OID (AGE policy)	2.16.724.1.3.5.7.2
OID (ETSI EN 319 411-2)	0.4.0.194112.1.0 (QCP-n)

Each electronic certificate consists of two key pairs, one for authentication and signature and the other for encrypting the data, identified with different OIDs:

- **Authentication and signature certification OID 2.16.724.1.4.2.2.1.2.11**
- **Encryption certification OID 2.16.724.1.4.2.2.1.2.12**

Meaning of internal OID: joint-iso-itu-t (2) country (16) es (724) adm (1) giss (4) infrastructures (2) ACGISSv2 (2) SubCA GISS01 (1) Personal (2) Public employee CP (1)

The keys of the employee 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

Employee certificates are certificates for natural persons, issued to workers on starting their employment within one of the Social Security Department's dependent Bodies, and they are revoked on ceasing their functions within that same environment.

Employee certificates assist Social Security workers by enabling them to complete the following tasks in carrying out their functions:

- Authenticating identities.
- Electronic signing of documents.
- Encrypting data and documents.

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

In accordance with Art. 22 of RD 1671/2009, public employee certificates may only be used in carrying out the functions of the position held or in dealings with Public Administrations, where they allow it.

Therefore, these certificates enable users, within the Social Security environment, to access the services needed to perform the tasks assigned to them for the purposes of the organisation.

3. Limits on certificate usage

Acceptance of the certificate occurs at the point when the owner signs the subscription agreement.

The scope of action of employee certificates is limited to dealings with Public Administrations, where they allow it.

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.

Certificates will be revoked when employees cease to work for the Social Security department.

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.

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 2.16.724.1.4.2.2.1.2.1*) 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 employee.

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.

The owner consents to the exclusive internal publication of their certificate for the purposes of fulfilling the organisation's own functions.

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, employee 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.