MINISTERIO DE INCLUSIÓN, SEGURIDAD SOCIAL Y MIGRACIONES

SECRETARÍA DE ESTADO DE LA SEGURIDAD SOCIAL Y PENSIONES

Gerencia de Informática de la Seguridad Social

ACGISS Public Employee Certificates

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 review.	28-04-2017
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	Changes due to the updating of the ministry logo	30-10-2020

Table of Contents

1. INTRODUCTION

1.1. Presentation

Social Security, through its Certification Authority, the ACGISS, shall issue electronic certificates for its employees for the purposes of identification, electronic signature and encryption.

These shall be qualified certificates, in compliance with Law 59/2003 on Electronic Signatures, taking into account the requirements established in EU Regulation no. 910/2014, and issued on a secure cryptographic card provided by Social Security.

These certificates are issued as public employee certificates, in compliance with art. 22 of Royal Decree RD 1671/2009 and the General State Administration policy on signatures and certificates.

As part of the ACGISS general regulation on certifications, this document covers the specific features of public employee certificates. The general terms and conditions for the provision of certification services, not available in this policy, are established in the ACGISS CPS.

The structure of RFC 3647 has been followed in the preparation of this document, including any parts that are specific to this type of certificate.

1.2. Identifying the document

Document name	Employee Certificates. Certification policy
Version	2.0.5
Document status	Approved
Issue date	30 october 2020
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)
Location	http://www.seg-social.es/ACGISS

Internal OID meaning: joint-iso-itu-t (2) country (16) es (724) adm (1) giss (4) infrastructures (2) ACGISSv2 (2) SubCA GISS01 (1) Personnel (2) Public employee CP (1)

1.3. PKI participants

1.3.1. Registration Authorities

The following are considered Registration Authorities:

- Social Security personnel units.
- The GISS Information Security Center, who is responsible for the security tools and components that enable the identification and authentication of users and for the issue of electronic certificates.

1.3.2. Subscribers and end users

Employee certificates are designed so that Social Security workers (civil servants, general service personnel, and temporary personnel) may exercise their functions within the different Social Security departments.

The Secretary of State for Social Security shall be considered the general subscriber to employee certificates. The owner, user and person responsible for the certificates shall be the employees themselves.

1.4. Certificate usage

1.4.1. Types of certificates issued

Employee certificates are issued as personal certificates within the PKI hierarchy, and in accordance with current AGE regulation relating to medium-level public employee electronic certificates.

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 of encryption** **OID** **2.16.724.1.4.2.2.1.2.12**

1.4.2. Typical uses for employee certificates

Employee certificates are certificates for physical persons, issued to workers upon starting their employment within one of the Secretary of State for Social Security's depending Entities, and they are revoked upon cessation of their functions within this same environment.

In accordance with Art. 22 of RD 1671/2009, public employee certificates may only be used as part of the fulfilment of the role occupied, or to link with Public Administrations, when so permitted.

Therefore, these certificates enable users, within the Social Security environment, to access the services needed to exercise the relevant tasks for achieving the purposes of the organisation.

Each key pair shall be used exclusively for the purposes for which it was generated.

1.4.3. Prohibited applications

Employee certificates' scope of action is limited to the Public Administration environment, when so permitted.

In general, certificates and their associated keys shall not be used for purposes different to those specified in the previous section.

1.5. Managing the policy

As established in the CPS.

1.6. Definitions and acronyms

As established in the CPS.

2. REPOSITORIES AND PUBLISHING INFORMATION

As established in the CPS.

Additionally, information relating to the conditions of use and the services relating to this type of certification shall be published on the Social Security Intranet.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Name management

3.1.1. Types of names

Public employee certificates shall be issued in accordance with the AGE policy on signatures and certificates, with regards to the creation and use of certificate fields.

With respect to name management, in addition to the general conditions established in the CPS, the following criteria shall apply for the composition of the CN (Common Name):

- The structure shall be: "NAME" (space) "FIRST SURNAME" (space) "SECOND SURNAME" (space) (space-hyphen-space) "NIF/NIE TAX NUMBER"
- All letters shall appear in capitals and without accents and shall not include more than once space between chains or blank characters at the beginning or end.

- The data used shall be as found in the official Social Security databases.

The following administrative identity fields shall also be used under "Subject Alternative Name":

Type of Certificate **OID 2.16.724.1.3.5.7.2.1**	PUBLIC EMPLOYEE ELECTRONIC CERTIFICATE
Name of subscriber entity **OID 2.16.724.1.3.5.7.2.2**	SECRETARY OF STATE FOR SOCIAL SECURITY
Subscriber entity NIF tax number **OID 2.16.724.1.3.5.7.2.3**	S2819001E
Owner DNI/NIE national identification number **OID 2.16.724.1.3.5.7.2.4**	EMPLOYEE NIF/NIE TAX NUMBER
Owner first name **OID 2.16.724.1.3.5.7.2.6**	EMPLOYEE NAME
Owner first surname **OID 2.16.724.1.3.5.7.2.7**	EMPLOYEE FIRST SURNAME
Owner second surname **OID 2.16.724.1.3.5.7.2.8**	EMPLOYEE SECOND SURNAME

3.2. Initial validation of an identity

3.2.1. Proof of possession of a private key

Key pairs are generated on the cryptographic card supplied by the Registration Authority.

Proof of possession of private keys is obtained from the Certification Authority for the corresponding public keys, together with the certificates, for signature.

3.2.2. Authenticating a physical person's identity

In order to issue public employee certificates, it is always necessary that the physical owner attend one of the Social Security Management Entities' or Common Services' offices.

Authenticating the employee's identity shall be completed in the corresponding personnel unit when starting their job role at one of the Social Security Entities, after prior identification by way of national identity document or equivalent means.

Verification that the owner provides their services within Social Security is guaranteed by the fact that in order to issue the cryptographic employee card, it is necessary to be listed on the personnel register. Incorporation into said register occurs once the corresponding selection process is complete and names have been published in the Official State Gazette (BOE). This register is kept updated in order to detect any changes in the employee's work situation and in particular, if they cease to provide services within the organisation. All amendments to the register are recorded so that it can be consulted at any moment, should it be necessary.

Employee data incorporated into the electronic certificate shall be directly extracted from the personnel register and official Social Security databases in order to guarantee its authenticity.

Authentication of the employee's identity in the certificate management tools and applications is guaranteed by:

- Control of physical access to facilities via cryptographic card, or in the event of card failure, authentication by security staff, guaranteeing their physical presence in the offices.
- Control of subsequent software access to the PC, with a dual factor authentication mechanism: cryptographic card and access PIN.
- Integrated system for managing identities and authorisations to access the different Social Security applications.

3.3. Identification and authentication of requests for renewal

3.3.1. Validation for routine renewal of certificates

Two scenarios are of note:

- Renewal of keys without renewal of the physical card. Identification and authentication shall take place in the relevant personnel unit or by accessing the corresponding system through the GISS identification and authorisation systems, and the use of the current authentication certificate and signature.
- Renewal of keys with renewal of the physical card. The process shall be the same as for the initial issuing of the certificate.

3.4. Identification and authentication of revocation request

A request for revocation is prompted by:

- Ex officio, when a person ceases to provide their services within Social Security, or for other reasons stipulated in the Certification Practice Statement.
- The owner, due to compromise of their keys, or any other cause that requires issuing a new cryptographic card. To request revocation, the owner is required to physically attend the relevant personnel unit or, if this is not possible, use the remote revocation service provided for the purpose. In the event of the latter scenario, the owner shall be subsequently required to physically attend the personnel unit to obtain a new certificate.

4. OPERATIONAL REQUIREMENTS FOR THE LIFE CYCLE OF EMPLOYEE CERTIFICATES

4.1. Request for issue of certificate

4.1.1. Who may request an employee certificate

Applications for the issue of a certificate for a new employee shall be completed by the corresponding personnel unit, via the registration application, after the prior physical attendance of the owner.

Certificates shall be delivered to the public employees (civil servants, general and temporary employees) who provide their services within the scope of the Secretary of State for Social Security.

4.1.2. Registration process and responsibilities

The personnel unit shall be responsible for verifying any information relating to the worker who owns the certificate before requesting its issue using the registration application.

Signature keys are generated on the card and in the presence of the owner, thereby guaranteeing confidentiality of private keys.

In the same way, the applicant shall be provided with the information referred to in article 18 b) of Law 59/2003 before the certificate is issued. These terms and conditions should be signed by the owner.

The ACGISS guarantees that the data present in certificates is correct and complete, and that requests are recorded in the central system.

4.2. Processing requests for a certificate

4.2.1. Fulfilling identification and authentication functions

Requests for employee certificates are initially completed ex officio when a person beings working in Social Security. They are completed in the relevant personnel unit, by a duly authorised public employee. This employee shall be responsible for authenticating the owner and verifying the data necessary for issuing the certificate, in accordance with the corresponding section of this document.

4.2.2. Approval or rejection of requests

Requests are approved by the corresponding personnel units once the previous actions have been performed. Requests are denied if they do not comply with the minimum conditions established for identifying and authenticating the employee's identity.

4.3. Issuing certificates

4.3.1. ACGISS actions during the issuing process

Once the request for public employee certification has been processed according to the particular employee's situation, the certificate shall be issued and the cryptographic card shall be handed over.

In the event that the applicant already possesses a previous employee certificate, the previous certificate shall be revoked before issuing the new one.

The two key pairs are generated on the cryptographic card.

After the keys are generated, the registration application shall send the public keys to the Certification Authority, who will sign it together with the certificate and return them to the owner's card.

Additionally, the ACGISS takes the following aspects into account:

- Generates certificates while securely linking them to the employee's information, as it appears in the personnel register.
- Protects the secrecy and integrity of the registration data.
- Includes the information established in article 11 of Law 59/2003 in the certificate.
- Guarantees the date and time at which a certificate was issued.
- Uses reliable systems and products that are protected against any tampering and that guarantee the technical security and when necessary, cryptography of the certification processes for which they provide support.
- Ensures that the certificate is issued by systems that use protection against forgery.

4.3.2. Notification of issue to the subscriber/owner

The owner is notified of issue once the issuing process is complete, via delivery of the cryptographic card containing the certificate. The card is delivered blocked. This is done to prevent the card’s use before its activation by the user.

4.4. Accepting the certificate

4.4.1. Conduct that constitutes acceptance of the certificate

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

Issuing employee certificates is a requirement of the Secretary of State for Social Security in order to identify employees and facilitate the exercise of their functions. The Secretary of State therefore accepts the terms and conditions of use established in this document.

The certification policy and the summary of conditions of relevant use shall also be published on the Social Security Intranet for consultation by employees.

4.5. Key pair and certificate usage

4.5.1. Use by owners

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

- Authenticating identities.
- Electronic signatures on documents.
- Encrypting data and documents.

The different keys generated shall be used exclusively for their specified purposes and in accordance with the stipulations established in this certification policy.

As previously mentioned, the use of employee certificates shall be limited to the fulfilment of the functions of the role occupied, or to link with other Public Administrations, should this be permitted.

4.6. Renewing the certificate without renewing the keys

As established in the CPS.

4.7. Renewing certificates and renewing keys

4.7.1. Circumstances for renewing a certificate with a key changeover

Renewal of certificates may arise from one of the causes established in the CPS; in particular:

- Loss of or damage to the previous certificate.
- End of certificate validity period. This circumstance shall be communicated to the owner with sufficient notice for them to complete renewal before the end of the validity period.
- Reissue ex officio, by Social Security, due to updating the infrastructure or certificate profiles.

4.7.2. Who may request renewal

When dealing with renewing certificates without renewing the physical cards, and renewal is due to the validity period expiring, or changes to the infrastructure or certificate profiles, the system shall send the employee a notification so that they may initiate the certificate renewal process.

In the event that the certificate needs renewing together with the cryptographic card or that incidents occur in the previous process, the same procedure shall be followed as for the original issue of the certificate.

4.7.3. Processing requests

Before completing a request for a certificate, the employee shall be authenticated, for which the existing GISS systems described in section 2.2.2. shall be used, together with the physical attendance of the employee in a Social Security office. Renewal shall preferably occur via the specific application for the purpose and made available on the Social Security Intranet.

Firstly, the card details and viability of renewal are verified. Next the application shall request the signature on the use of the certificate and then, once the revocation of the previous certification is requested, the request for a new certificate is generated. Lastly, the renewed certificates are stored on the card and the user is informed of their validity.

When card renewal is required, the process followed shall be the same as for the initial issue of the card.

In both cases, all data included in the certificate shall be validated against the personnel register and the Social Security databases in order to guarantee that they are current.

4.7.4. Notification of issue to the subscriber/owner

The procedures indicated ensure communication to the owner once the issuing process has been completed.

4.8. Modifications to certificates

As established in the CPS.

4.9. Revocation and suspension of certificates

4.9.1. Causes for revoking certificates

In addition to the causes for revocation specified in the ACGISS Certification Practice Statement, employee certificates are revoked when the owners cease to provide their services within Social Security.

4.9.2. Legitimisation for requesting revocation

Revocation of employee certificates may be requested by:

- The employee themselves.
- The corresponding personnel unit.
- The ACGISS ex officio.

4.9.3. Revocation request procedures

In order to proceed to request revocation for one of the causes specified in the CPS, the owner should attend the corresponding personnel unit. The applicant accesses the system through the registration application and completes the certificate revocation request.

Ex officio revocation is completed by personnel from the human resources units, also by using the registration application.

When it is not possible for the person to physically attend the units and the established conditions for it are met, revocation shall be completed by using the revocation service made available to employees. It shall be necessary to attend the corresponding personnel unit later to request the issue of a new certificate.

A revoked certificate may not be reused. That is, revocation may not be lifted nor annulled in any other way.

4.9.4. Maximum time frame for processing revocation requests

Revocation requests shall be completed as soon as the public employee has attended the corresponding personnel unit.

The requests that are not made in person shall be processed in the minimum time possible, taking into account the technical limitations of the systems involved. In all cases, requests are guaranteed to be dealt with in a maximum time frame of 24 hours.

4.10. Services for verifying the status of certificates

As established in the CPS.

4.11. Ending the subscription

As established in the CPS.

4.12. Custody and recovery of keys

Custody of the private keys for public employee certificates is not given. For this reason it is therefore not possible to later recover said keys and is instead necessary to initiate a new process for issuing certificates.

5. PHYSICAL SECURITY CONTROLS, MANAGEMENT AND OPERATIONS

As established in the CPS.

5.1. Audit logging procedures

As established in the CPS.

In particular, in the case of public employee certificates, the following events shall be specifically recorded:

- Data relating to issuing, renewing, and revoking employee certificates.
- Changes of the employee certificates policies.
- Employee certificates signature.
- Signature of the conditions of use by the user.

6. OTHERS RELATED TO THE OPERATION OF THE INFRASTRUCTURE SYSTEMS IN ISSUING EMPLOYEE CERTIFICATES.TECHNICAL SECURITY CONTROLS

6.1. Generating and installing key pairs

6.1.1. Generating key pairs

Key pairs are generated internally on the owner's cryptographic card, which has the sufficient security measures in place to protect private keys.

6.1.2. Delivering private keys to the subscriber

Private keys are generated in the presence of the certificate owner, on the cryptographic card, and it is not possible to extract the same. Therefore, there is no delivery of private keys to the owner.

6.1.3. Sending the public key to the issuer of the certificate

Public keys are exported from the card and sent via the registration or renewal applications to the Certification Authority for signature.

6.1.4. Key length

Employee certificate subscriber keys are at least 2.048 bits.

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

6.1.5. Permitted key usage

The content of the fields relating to the permitted uses for keys for both types of certification is as follows:

- Key Usage:

Authentication and signature certificate	
KeyUsage	Digital Signature Content Commitment
Encryption certificate	
KeyUsage	KeyEncipherment DataEncipherment

- Extended Key Usage:

Authentication, signature and encryption certificates	
ExtKeyUsage	Email Protection Client Authentication

6.2. Protecting private keys

6.2.1. Standards for cryptographic modules

Employee certificate private keys are protected by the cryptographic card on which they are found. This card has security mechanisms in place to guarantee the correct custody of the keys.

6.2.2. Repository for private keys

Custody of certificate private keys is by the employee owners themselves.

Private authentication and signature keys are stored on the cryptographic card, making it impossible to extract them from it. Under no circumstance shall it be possible to store the keys in the Certification Authority, Registration Authority or any other element of the PKI infrastructure.

6.2.3. Private key backups

It is not possible to create a security copy of private authentication and signature keys associated with employee certificates, as keys cannot be exported from the card.

6.2.4. Method for activating private keys

The activation of keys and certificates requires the introduction of a personal identification number (PIN) by the owner, which must remain known only to them.

6.2.5. Method for deactivating private keys

Private keys deactivate upon extracting the card from the reader. In addition, when the application that uses the employee certificate terminates the session, it shall be necessary to reintroduce the PIN.

6.3. Other aspects of managing key pairs

As established in the CPS.

6.4. Activation data

6.4.1. Generating and installing activation data

The activation data for employee certificate keys consists of a personal code (PIN) for the card containing them, chosen by the owner when he/she unlocks the card for the first time at his/her workstation. The card is unlocked once the employee is identified and authenticated successfully using the systems of authentication and authorization of the Social Security Ministry.

6.4.2. Protecting activation data

Only the certificate owner knows the personal access code or PIN, and is therefore the only person responsible for protecting the activation data for their private keys.

6.5. IT security controls

As established in the CPS.

6.6. Technical controls on the life cycle

As established in the CPS.

6.7. Network security controls

As established in the CPS.

6.8. Time stamping

As established in the CPS.

7. CERTIFICATE PROFILES

7.1. Certificate profile

FIELD	DESCRIPTION	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 issue.	GISS01
1.4.6. Serial Number	Unique identification number for the certification entity	Q2827003A
1.4.7. Common Name (CN)	Common name of the subordinate CA certificate	SUBCA GISS01
1.5. Validity		
1.5.1. Not Before	Start date validity YYMMDDHHMMSSZ	YYMMDDHHMMSSZ
1.5.2. Not After	End date validity YYMMDDHHMMSSZ	YYMMDDHHMMSSZ
1.6. Subject		
1.6.1. Country (C)	ES	ES
1.6.2. Organisation (O)	"Official" name of the Administration certificate subscriber.	SECRETARY OF STATE FOR SOCIAL SECURITY
1.6.3. Organisational Unit (OU)	Type of Certificate	PUBLIC EMPLOYEE ELECTRONIC CERTIFICATE
1.6.4. Organisational Unit (OU)	Internal subdivision according to certificate category	PERSONNEL
1.6.5. Organisational Unit (OU)	Internal subdivision for administrative purposes	Two digits assigned automatically
1.6.6. Serial Number	Owner NIF/NIE tax number	IDCES-"NIF/NIE"
1.6.7. Surname	First and second surname and DNI national identification number	"FIRST SURNAME" (space) "SECOND SURNAME" (space-hyphen-space) "NIF/NIE TAX NUMBER"
1.6.8. Given Name	First name	"NAME"
1.6.9. Common Name (CN)	Name of the holder	"NAME" (space) "FIRST SURNAME" (space) "SECOND SURNAME" (space) (space-hyphen-space) "NIF/NIE TAX NUMBER"

1.7. Subject Public Key Info	Certificate public key	(RSA 2048 bits)
2. X.509v3 Extensions		
2.1. Authority Key Identifier		
2.1.1. KeyIdentifier	Issuer public key identifier. Identification path	*Automated*
2.1.2. AuthorityCertIssuer	Name of CA corresponding to that key	*Automated*
2.1.3. AuthorityCertSerialNumber	Serial number of CA certificate	*Automated*
2.2. Subject Key Identifier	Subscriber public key identifier	*Automated*
2.5. Qualified Certificate Statements		
2.5.1. QcCompliance	Indication of qualified certificate	OID 0.4.0.1862.1.1
2.5.2. QcEuRetentionPeriod	Retention period	OID 0.4.0.1862.1.3 =15
2.5.3. QcType-esign	Signature certificate	OID 0.4.0.1862.1.6.1
2.5.4. QcPDS	Location of PDS statement	OID 0.4.0.1862.1.5 http://www.seg-social.es/ACGISS https://sede.seg-social.gob.es/descarga/ACGISS_PDSEmployee.pdf
2.6. Certificate Policies		
2.6.1. Policy Identifier	OID indicating medium level public employee certificate according to AGE policy	2.16.724.1.3.5.7.2
2.6.2. Policy Identifier	QCP-n	0.4.0.194112.1.0
2.6.4. Policy Qualifier ID		
2.6.4.1 CPS Pointer	Certification policy URL	http://www.seg-social.es/ACGISS
2.6.4.2 User Notice	Conditions of Use URL	Public employee qualified certificate, medium level. Consult conditions for use at http://www.seg-social.es/ACGISS
2.7. Subject Alternative Name		
2.7.2. Directory Name	Administrative Identity	
2.7.2.1. Type of Certificate	Indicates nature of certificate	2.16.724.1.3.5.7.2.1 = PUBLIC EMPLOYEE ELECTRONIC CERTIFICATE (medium level)
2.7.2.2. Name of subscriber entity	Name of subscriber Entity on which employee depends	2.16.724.1.3.5.7.2.2 = SECRETARY OF STATE FOR SOCIAL SECURITY
2.7.2.3. Subscriber entity CIF tax number	Subscriber Entity CIF tax number	2.16.724.1.3.5.7.2.3 = S2819001E
2.7.2.4. Responsible party DNI/NIE national identification number	Employee NIF/NIE tax number	2.16.724.1.3.5.7.2.4 = "NIF/NIE" TAX NUMBER
2.7.2.6. First name	Employee name	2.16.724.1.3.5.7.2.6 = "NAME"
2.7.2.7. First surname	Employee first surname	2.16.724.1.3.5.7.2.7 = "FIRST SURNAME"
2.7.2.8. Second surname	Employee second surname	2.16.724.1.3.5.7.2.8 = "SECOND SURNAME"
2.8. Issuer Alternative Name	Alternative contact name for issuer entity	
2.8.1. rfc822Name	Contact email address	acgiss.soporte.giss@seg-social.es
2.9. cRLDistributionPoint		
2.9.1. distributionPoint	Distribution point no.1	http://crl.seg-social.gob.es/ac_sub.crl
2.10. Authority Info Access		
2.10.1. Access Method	Online Certificate Status Protocol ID	Id-ad-ocsp
2.10.2. Access Location	OCSP web address	http://ocsp.seg-social.gob.es/

2.10.3. Access Method	Localisation ID for certificate of issuer CA	Id-ad-caIssuers
2.10.4. Access Location	SUBCA certificate access URL	http://www.seg-social.es/ACGISS/Certs/SUBCA_GISS01 http://www.seg-social.es/ACGISS/SUBCA_GISS01
2.11. Basic Constraints		
2.11.2. Path Length Constraints	A maximum number of steps can be specified.	None

3. X.509v3 Extensions (SIGNATURE AND AUTHENTICATION)		
2.3. Key Usage		
2.3.1. Digital Signature		"1"
2.3.2. Content Commitment		"1"
2.3.3. Key Encipherment		"0"
2.3.4. Data Encipherment		"0"
2.3.5. Key Agreement		"0"
2.3.6. Key CertificateSignature		"0"
2.3.7. CRL Signature		"0"
2.4 Extended Key Usage		
2.4.1. Email Protection		"1"
2.4.2. Client Authentication		"1"
2.6. Certificate Policies		
2.6.3. Policy Identifier	OID associated with signature and authentication certification	2.16.724.1.4.2.2.1.2.11

4. X.509v3 Extensions (ENCRYPTED)		
2.3. Key Usage		
2.3.1. Digital Signature		"0"
2.3.2. Content Commitment		"0"
2.3.3. Key Encipherment		"1"
2.3.4. Data Encipherment		"1"
2.3.5. Key Agreement		"0"
2.3.6. Key CertificateSignature		"0"
2.3.7. CRL Signature		"0"
2.4 Extended Key Usage		
2.4.1. Email Protection		"1"
2.4.2. Client Authentication		"0"
2.6. Certificate Policies		
2.6.3. Policy Identifier	OID associated with encryption certificate	2.16.724.1.4.2.2.1.2.12

7.2. Certification revocation list (CRL) profiles

As established in the CPS.

7.3. OCSP profile

As established in the CPS.

8. COMPLIANCE AUDITS

8.1. Frequency of compliance audits

Since they deal with qualified certificates, it shall be necessary to perform at least one assessment of compliance with EU Regulation no. 910/2014 biennially. The provider or the supervising agency may deem it necessary to undertake additional audits to maintain trust in the services provided.

8.2. Identifying and qualifying auditors

As established in the CPS.

8.3. Relation of auditor with the audited entity

As established in the CPS

8.4. Relation of elements subject to audit

As established in the CPS.

8.5. Actions to undertake after a lack of compliance

As established in the CPS.

8.6. Dealing with the audit findings

Since they deal with qualified certificates, the findings of any audits shall be communicated to the supervising agency.

9. COMMERCIAL AND LEGAL REQUIREMENTS

9.1. Charges

As established in the CPS.

9.2. Financial capacity

As established in the CPS.

9.3. Confidentiality

As established in the CPS.

9.4. Personal data protection

As established in the CPS.

9.5. Intellectual property rights

As established in the CPS.

9.6. Obligations and civil liability

As established in the CPS.

9.6.1. Certificate owners

In addition to the general liabilities established in the CPS, owners of ACGISS-issued employee certificates are obliged to do following:

- Immediately advise the department of Human Resources (HR) in their Agency if the user detects any error in the data stored in the personnel databases.
- Also advise the HR department regarding any variation in personal data, in order that it may be corrected in the Confidential Personnel Databases and, if necessary, update the certificates contained on the card.
- Ensure proper use of the certificate, based on the competencies and skills attributed to the task, job role or external personnel in the Social Security service.

9.7. Guarantee disclaimers

As established in the CPS.

9.8. Liability limitations

As established in the CPS.

9.9. Compensation

As established in the CPS.

9.10. Time frame and termination

As established in the CPS.

9.11. Notifications

As established in the CPS.

9.12. Modifications to the policy

9.12.1. Modification procedure

The ACGISS may unilaterally modify this document, assuming that it complies with the procedure established for the purpose, and taking into account the following:

- The modification should be justified from a technical, legal, or commercial standpoint.
- The modification proposed by the ACGISS may not contravene an internal GISS regulation.
- A modifications control exists to guarantee that in each situation the resulting specifications comply with the requirements that the modification intends to fulfil and that prompted the change.
- Any implications that the change of specifications may have on the user are detailed, and the necessity of notifying them regarding said changes is set forth.
- The new regulation should be approved by the GISS following established procedures.

9.12.2. Time frame and mechanisms for notifications

In the event that the modifications made may affect the conditions for the provision of certificates, the ACGISS shall notify the users individually, via its website and/or the Social Security Intranet.

9.12.3. Circumstances in which an OID should be changed

As established in the CPS.

9.13. Conflict resolution

As established in the CPS.

9.14. Governing Law

As established in the CPS.

9.15. Compliance with current legislation

As established in the CPS.

Particularly the following sections of the standards will apply to employee certificates:

- ETSI EN 319 411-1: requirements applicable to any CP and specific NCP conditions. Also PKI disclosure statement for employee certificates is structured according to annex A of this standard.
- ETSI EN 319 411-2: requirements applicable to any certificate policy and specific QCP-n conditions.
- ETSI EN 319 412-1, EN 319 412-2 and EN 319 412-5: qualified certificates profiles for natural persons.

9.16. Miscellaneous provisions

As established in the CPS.

9.17. Other provisions

As established in the CPS.