MINISTERIO DE INCLUSIÓN, SEGURIDAD SOCIAL Y MIGRACIONES

SECRETARÍA DE ESTADO DE LA SEGURIDAD SOCIAL Y PENSIONES

Gerencia de Informática de la Seguridad Social

ACGISS Electronic Seal certification

Certification policy

V 2.1.3
(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
1.2.2	Amendment to certification profile	04-01-2011
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 reviews.	28-04-2017
2.1	Errata Correction and Seal Profile Modification	19-07-2017
2.1.1	Changes due to internal annual review: errata correction and Ministry name update.	03-08-2018
2.1.2	Annual internal review	31-07-2019
2.1.3	Annual review, 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

Social Security, through its Certification Authority ACGISS, shall issue electronic seal certificates for Social Security Agencies and Entities who request the same.

They consist of qualified certificates of electronic seals, issued in accordance with the requirements established in EU Regulation no. 910/2014.

These certificates are issued as certification of electronic seals for Entities or Administration, in compliance with art. 19 of Royal Decree RD 1671/2009 and the General State Administration's policy on signatures and certificates.

As part of the ACGISS general regulation on certifications, this document covers the specific features of electronic seal 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. Name of document and identification

Document name	Seal Certificates. Certification Policies
Version	2.1.3
Document status	Approved
Issue date	30 October 2020
OID (Internal GISS)	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)
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) Automated actions (1) Electronic seal CP (1-medium level or 2-high level)

1.3. PKI participants

1.3.1. Registration Authorities

Registration of seal certificates should be completed in the Social Security IT Department central offices. The Registration Authority responsible for issuing shall be the GISS Management of Security, Information Security Canter (CSI).

1.3.2. Subscribers and end users

Seal Certificates are destined for different Entities and Bodies within Social Security, covering at least the Subdirectorate-General level.

For the purposes of this Policy, the certificate subscriber and owner shall be considered the Social Security Entity or Body in whose name the certificate is issued.

Likewise, the certificate applicant shall be considered the physical person duly tasked with and accredited to completing the request for a certificate as representative of said Entity or Body.

1.4. Certificate usage

1.4.1. Types and classes of certificates issued

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

The ACGISS issues two types of electronic seal certificates:

- Medium level/substantial certificate: issued on supporting SW for installation and use distributed across Social Security servers and systems requiring authentication or automated signature.
- High level certificate: centrally issued in an HSM and usable through the security platform available at GISS.

1.4.2. Permitted uses for Seal certificates

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

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

1.4.3. Prohibited

Seal certificates shall not be used for purposes other than those specified in this Policy.

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

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

In addition to the general conditions established in the CPS regarding name management, on seal certificates the following fields for administrative identity shall be used under "SubjectAlternativeName":

Type of Certificate **OID 2.16.724.1.3.5.6.1.1 (high level)** **OID 2.16.724.1.3.5.6.2.1 (medium level)**	TYPE OF CERTIFICATE (HIGH OR MEDIUM LEVEL ELECTRONIC SEAL)
Name of subscriber entity **OID 2.16.724.1.3.5.6.1.2 (high level)** **OID 2.16.724.1.3.5.6.2.2 (medium level)**	OFFICIAL NAME OF SUBSCRIBER ENTITY

Subscriber entity NIF tax number	
OID 2.16.724.1.3.5.6.1.3 (high level)	SUBSCRIBER ENTITY NIF TAX NUMBER
OID 2.16.724.1.3.5.6.2.3 (medium level)	

3.2. Initial validation of an identity

The fact that the different Entities or Bodies requesting certification are within the Social Security scope guarantees the latter's capability to authenticate and accredit the identity of subscribers.

3.2.1. Proof of possession of a private key

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 an organisation's identity

Entities or Bodies requesting seal certification are part of the Secretary of State for Social Security. They are entities whose organisation and management are included in the official documentation published in the Official State Gazette (BOE). Before an entity requests a high level electronic seal certificate it should approve the corresponding Resolution, in accordance with the stipulations of art. 19 of Royal Decree RD 1671/2009.

Authentication of the applicant is by way of the tools present for that purpose within Public Administration.

3.3. Identification and authentication of renewal request

This is completed in the same manner as for the initial validation of identity.

3.4. Identification and authentication of revocation request

A request for revocation is prompted by:

- Ex officio by the GISS, due to the causes stipulated in the Certification Practice Statement.
- By a person authorized by the certificate-owning Entity or Body using the corresponding form. The request should be sent to the Registration Authority, with the documentation needed to authenticate said empowerment.

4. OPERATIONAL REQUIREMENTS FOR CERTIFICATES' LIFE CYCLE

4.1. Request for issue of certificate

4.1.1. Who may request a seal certificate

Requests for seal certificate are sent by the Entities or Bodies belonging to the Secretariat of State for Social Security, ranging from the Subdirectorate-general and above.

In accordance with art. 19 of RD 1671/2009, electronic seals shall be created via resolution by the owner from the competent Entity, which shall be published on the main website and shall contain at least the following information as a minimum:

a) Owning body of the seal who shall be the party responsible for its use.

b) General technical features of the relevant signature and certification system.

c) Validation service for verifying the certificate.

d) Actions and procedures in which it may be used.

Lastly, the request for the issuing of a certificate shall be completed by the person empowered to do so in the Resolution by the aforementioned Entity or Body, using the forms available for that purpose.

4.1.2. Registration process and responsibilities

The ACGISS ensures that requests for a certificate are complete, precise, and duly authorised.

The request is completed via a form in which the physical person authorised to carry out said request should provide the details of the headquarters of the certificate-owning Body and those of the aforementioned person. The request shall be signed by this representative and submitted to the GISS Registration Authority. The signature of the application implies that all parties know and accept the conditions of use of the seal certificate.

The Registration Authority shall be responsible for verifying that all the data is correct, before proceeding to apply for the certificate from the ACGISS.

4.2. Processing requests for a certificate

4.2.1. Fulfilling identification and authentication functions

The Registration Authority shall identify the applicant and verify the validity of their empowerment. Authentication of the request arises from validation of the applicant's signature on the form.

The Registration Authority shall verify the accuracy of the data included on the form by consulting relevant official documents and databases.

4.2.2. Approval or rejection of requests

All certificates that do not comply with the requirements established in this policy and the procedures established for them shall be rejected. Forms filled in incorrectly or signed by personnel not empowered to complete said request shall also be rejected.

4.3. Issuing certificates

4.3.1. ACGISS actions during the issuing process

After the Registration Authority has verified the applicant's identity and verified the supporting documentation, it shall send the request to the ACGISS as the Certification Authority to issue the corresponding certificate.

The generation of keys and the issuing of certificates shall take place once the Registration Authority has introduced the data into the registration application.

In the event of high level certificates, the keys are generated within an HSM cryptographic module certified as qualified signature creation devices, from which they cannot be extracted at any time. There will be mechanisms to guarantee this end in accordance with what is specified in the corresponding key management procedure.

In the event of medium level certificates, the keys can be generated by the user or CA. If keys are generated in the CA, they are submitted protected together with the corresponding certificates to the applicant via email with an acknowledgement of receipt. On the other hand, the CA sends (by phone or any other channel) the PIN required for the installation of the certificate to the applicant. The Registration Authority guarantees that it does not keep copies of the private keys of the seal certificates that it issues.

Once the keys are generated, the public keys are sent to the Certification Authority for signature.

The ACGISS generates certificates, securely linking them to the Entity or Body's information, guaranteeing the use of trustworthy products and systems protected against any alteration and the recording of data relevant to the issue.

4.3.2. Notification of issue to the subscriber/owner

The Registration Authority shall notify the subscriber/owner via an email to the applicant.

4.4. Accepting the certificate

4.4.1. Conduct that constitutes acceptance of the certificate

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

4.5. Key pairs and certificate usage

4.5.1. Use by subscribers

Use of seal certificates shall be in accordance with the uses set forth in Law 40/2015 of 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.

4.6. Renewing the certificate without renewing keys

As established in the CPS.

4.7. Renewing certificates and renewing keys

Renewal of certificates shall generally follow the same procedures as specified for their initial issue, by sending the corresponding form.

4.7.1. Circumstances for renewing a certificate with a key changeover

Renewal of certificates may occur due to the following:

- End of certificate validity period.
- Reissue ex officio, by Social Security, due to updating the infrastructure or certificate profiles.

In both cases, a communication shall be sent to the owner sufficiently in advance for them to complete the request for renewal within the stipulated time frame.

4.8. Modifications to certificates

As established in the CPS.

4.9. Revocation and suspension of certificates

4.9.1. Legitimisation for requesting revocation

Requests for revocation of a certificate by the owner shall be completed through a similar procedure to that used for the request for issue: by sending the corresponding form.

Revocation may also occur ex officio by the ACGISS.

4.9.2. Revocation request procedures

To request revocation, the owner should submit the corresponding form to the Registration Authority, signed by an authorised signatory.

The Registration Authority shall verify the information indicated on the form, in accordance with the stipulations set forth previously in this policy.

4.9.3. Maximum time frame for processing revocation requests

The request for revocation shall be dealt with as soon as possible once the Registration Authority has received the corresponding form. A special procedure shall be followed when the revocation arises due to key security being placed at risk outside working 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

High level seal certificates are stored in various HSMs organised in a cluster, thereby guaranteeing proper protection and the recovery of keys when necessary.

For medium level seal certificates, private keys shall not be kept in storage or custody.

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 electronic seal certificates, the following events shall be specifically recorded:

- Seal certificates requests.
- Data relating to issuing, renewing, and revoking seal certificates.
- Changes of the seal certificates policies.
- Seal certificates signature.
- In high level seal certificates, logs relating the access and preparation of HSM and generations of seal's private keys.
- In medium level seal certificates, relevant communications with the person responsible for the certificates.
- Others related to the operation of the infrastructure systems in issuing seal certificates.

6. TECHNICAL SECURITY CONTROLS

6.1. Generating and installing key pairs

6.1.1. Generating key pairs

In the case of high level certificates, keys are securely generated within an HSM cryptographic module certified as a qualified signature creation device. There will be mechanisms defined in the corresponding key management procedure that guarantee that the issuance is carried out correctly.

In the case of medium level certificates, key pairs for seal certificates are generated by the user or the Registration Authority. In the latter case, once the certificate has been created, both the keys and the certificate are sent to the corresponding applicant and any copies of it are deleted.

6.1.2. Delivering private keys to the subscriber

Private keys for high level certificates are not sent to the subscriber, as they instead remain stored within the HSM.

For medium level certificates, if the private key has been generated by the Registration Authority, it is sent to the applicant, together with the public key and the certificate, via email. The password of the same one will be facilitated by the alternative means that is considered more convenient according to the circumstances, either by telephone, in person or by postal mail.

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

For high level certificates, the public key is exported from the HSM and sent via the registration application to the Certification Authority for signature.

For medium level certificates, the public key is sent to the Certification Authority for the certificate to be signed and subsequently this is sent to the applicant.

6.1.4. Key length

Seal certificate keys shall be 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

Content of the fields relating to the permitted key uses, both for high level seal certificates and medium level, is as follows:

KeyUsage	Digital Signature Content Commitment

	KeyEncipherment
ExtendedKeyUsage	Email Protection Client Authentication

6.2. Protecting private keys

6.2.1. Standards for cryptographic modules

For high level certificates, the private key is stored within an HSM that has sufficient security measures for its protection. HSMs are certified FIPS 140-2 level 3 or higher and CC EAL 4+, and as qualified signature creation devices in accordance with the applicable regulations.

6.2.2. Repository for private keys

High level seal certificates are stored within the HSM that generated them.

For medium level certificates, if keys are generated in the Registration Authority, private keys are not stored. Once delivered to the applicant, responsibility for protection of certificate private keys passes to them. Medium level seal certificates shall be installed on servers that are sufficiently protected with access control.

Social Security ensures that private keys are used under the control of their entities.

6.2.3. Private key backups

In the case of high level seal certificates, key backups are portioned in an HSM cluster, replicating the keys in various locations.

The private key of the medium level certificates is not backed up.

6.2.4. Method for activating private keys

Private keys for high level seal certificates are activated through the GISS Security Services Platform, with specific access controls.

Private keys for medium level seal certificates are activated by entering the corresponding operational password in the Social Security applications that use them, by the person responsible for the certificate.

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 prompt for seal certificate keys consists of a password, provided by the Registration Authority to duly authorised persons.

6.4.2. Protecting activation data

Only authorised persons know the password associated with the certificate, which is submitted via independent channel. These persons shall be responsible for the protection of the activation data from that point.

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

7.1.1. High level electronic seal certificate

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 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
1.5. Validity		
1.5.1. Not Before	Start date validity YYMMDDHHMMSSZ	YYMMDDHHMMSSZ
1.5.2. Not After	End date validity YYMMDDHHMMSSZ	YYMMDDHHMMSSZ
1.6. Subject		
1.5.1. Country (C)	ES	ES
1.5.2. Organisation (O)	Subscriber name	"Official name of Entity" E.g.: SECRETARY OF STATE FOR SOCIAL SECURITY
1.5.4. Organisational Unit (OU)	Organisational unit within the service provider, responsible for issuing the certificate.	AUTOMATED ACTION
1.5.5. Organisational Unit (OU)	Type of certificate= "electronic seal"	ELECTRONIC SEAL
1.5.3 Organisational Unit (OU)	Subscriber identification according to DIR3	"DIR3 entity number" E.g.: SE = E04926001
1.5.6. Description	Description of certified use	HIGH LEVEL
1.5.7. Serial Number	Entity unique identity number	"Entity NIF tax number" E.g.: SE = S2819001E
1.5.9. Common Name (CN)	Certificate name	"Name of electronic seal" E.g.: "SOCIAL SECURITY ELECTRONIC SEAL"
1.7. Subject Public Key Info	Certificate public key	(RSA 2048 bits)
2. X.509v3 Extensions		
2.1. Authority Key Identifier		
2.1.1. Key Identifier	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*
2.3. Key Usage		
2.3.1. Digital Signature		"1"
2.3.2. Content Commitment		"1"

2.3.3. Key Encipherment		"1"
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"
2.5. Qualified Certificate Statements		
2.5.1. QcCompliance	Indication of qualified certificate	OID 0.4.0.1862.1.1
2.5.2. QcEuRetentionPeriod	Retention period: 15 years	OID 0.4.0.1862.1.3 =15
2.5.3. QcSSCD	Use of secure signature device	OID 0.4.0.1862.1.4
2.5.4. QcType-eseal	Seal certificate	OID 0.4.0.1862.1.6.2
2.5.5. QcPDS	Location of PDS	OID 0.4.0.1862.1.5 http://www.seg-social.es/ACGISS https://sede.seg-social.gob.es/descarga/ACGISS_PDSSeal.pdf
2.6. Certificate Policies		
2.6.1. Policy Identifier	High level seal certificate in accordance with AGE policy	2.16.724.1.3.5.6.1
2.6.2. Policy Identifier	QCP-l-qscd	0.4.0.194112.1.3
2.6.3. Policy Identifier	OID associated with ACGISS CP	2.16.724.1.4.2.2.1.1.2
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	High level qualified electronic seal certificate. Consult conditions for use at http://www.seg-social.es/ACGISS New CIF of GISS since June 2017: Q2802407C
2.7. Subject Alternative Name		
2.7.2. Directory Name	Administrative identity	
2.7.2.1. Type of certificate	Indicates nature of certificate	2.16.724.1.3.5.6.1.1 = HIGH LEVEL ELECTRONIC SEAL
2.7.2.2. Name of subscriber entity	Subscriber entity of certificate	2.16.724.1.3.5.6.1.2 = "Name of subscriber Entity" E.g.: SECRETARY OF STATE FOR SOCIAL SECURITY
2.7.2.3. Subscriber entity NIF tax number	Subscriber Entity CIF tax number	2.16.724.1.3.5.6.1.3 = "Entity NIF tax number" E.g.: SE = S2819001E
2.8. Issuer Alternative Name	Alternative name of the contact person for the issuing 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

7.1.2. Medium level electronic seal certificate

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 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
1.5. Validity		
1.5.1. Not Before	Start date validity YYMMDDHHMMSSZ	YYMMDDHHMMSSZ
1.5.2. Not After	End date validity YYMMDDHHMMSSZ	YYMMDDHHMMSSZ
1.6. Subject		
1.5.1. Country (C)	ES	ES
1.5.2. Organisation (O)	Subscriber name	"Official name of Entity" E.g.: SECRETARY OF STATE FOR SOCIAL SECURITY
1.5.4. Organisational Unit (OU)	Organisational unit within the service provider, responsible for issuing the certificate.	AUTOMATED ACTION
1.5.5. Organisational Unit (OU)	Type of certificate= "electronic seal"	ELECTRONIC SEAL
1.5.3 Organisational Unit (OU)	Subscriber identification according to DIR3	"DIR3 entity number" E.g.: SE = E04926001
1.5.6. Description	Description of certified use	MEDIUM LEVEL
1.5.7. Serial Number	Entity unique identity number	"Entity NIF tax number" E.g.: SE = S2819001E
1.5.9. Common Name (CN)	Certificate name	"Name of electronic seal" E.g.: "SOCIAL SECURITY ELECTRONIC SEAL"
1.7. Subject Public Key Info	Certificate public key	(RSA 2048 bits)
2. X.509v3 Extensions		

2.1. Authority Key Identifier		
2.1.1. Key Identifier	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*
2.3. Key Usage		
2.3.1. Digital Signature		"1"
2.3.2. Content Commitment		"1"
2.3.3. Key Encipherment		"1"
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"
2.5. Qualified Certificate Statements		
2.5.1. QcCompliance	Indication of qualified certificate	OID 0.4.0.1862.1.1
2.5.2. QcEuRetentionPeriod	Retention period: 15 years	OID 0.4.0.1862.1.3 =15
2.5.3. QcType-eseal	Seal certificate	OID 0.4.0.1862.1.6.2
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_PDSSeal.pdf
2.6. Certificate Policies		
2.6.1. Policy Identifier	Medium level seal certificate in accordance with AGE policy	2.16.724.1.3.5.6.2
2.6.2. Policy Identifier	QCP-l	0.4.0.194112.1.1
2.6.3. Policy Identifier	OID associated with ACGISS CP	2.16.724.1.4.2.2.1.1.1
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	Medium level/substantial qualified electronic seal certificate. Consult conditions for use at http://www.seg-social.es/ACGISS New CIF of GISS since June 2017: Q2802407C
2.7. Subject Alternative Name		
2.7.2. Directory Name	Administrative identity	
2.7.2.1. Type of Certificate	Indicates nature of certificate	2.16.724.1.3.5.6.2.1 = MEDIUM LEVEL ELECTRONIC SEAL
2.7.2.2. Name of subscriber entity	Subscriber entity of certificate	2.16.724.1.3.5.6.2.2 = "Name of subscriber Entity" E.g.: SECRETARY OF STATE FOR SOCIAL SECURITY
2.7.2.3. Subscriber entity NIF tax number	Subscriber Entity CIF tax number	2.16.724.1.3.5.6.2.3 = "Entity NIF tax number"

		E.g.: SE = S2819001E
2.8. Issuer Alternative Name	Alternative name of the contact person for the issuing 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
2.11. Basic Constraints		
2.11.2. Path Length Constraints	A maximum number of steps can be specified.	None

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. Subscribers

Subscribers to seal certificates issued by the ACGISS are obliged to:

a. Supply the ACGISS with the information necessary for making a correct identification.

b. Communicate any changes in the data supplied for the issue of certification during its validity period.

c. Keep diligent custody of private keys.

d. Exercise proper use of the seal certificate, in accordance with the specifications in this Certification Policy.

e. In the case of high-level seal certificates, generate the keys inside an HSM cryptographic module certified as a qualified signature creation device.

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 via its website and 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 seal certificates:

- ETSI EN 319 411-1: requirements applicable to any CP and specific NCP conditions. In addition to this, in the case of high level seal certificates, NCP+ conditions will apply.

  PKI disclosure statement for seal certificates is structured according to annex A of this standard.

- ETSI EN 319 411-2: requirements applicable to any certificate policy and specific QCP-l-qscd conditions (high level seal certificates) or QCP-l conditions (medium level seal certificates).

- ETSI EN 319 412-1, EN 319 412-3 and EN 319 412-5: qualified certificates profiles for legal persons.

9.16. Miscellaneous provisions

As established in the CPS.

9.17. Other provisions

As established in the CPS.