MINISTERIO DE INCLUSIÓN, SEGURIDAD SOCIAL Y MIGRACIONES

SECRETARÍA DE ESTADO DE LA SEGURIDAD SOCIAL Y PENSIONES

Gerencia de Informática de la Seguridad Social

Certification Practice Statement

Certification Authority for the Social Security IT Department (ACGISS)

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
2.0	Full revision due to update of PKI for adoption of eIDAS Regulation	20-06-2016
2.0.1	Revision: errata correction and writing clarifications	22-02-2017
2.0.2	Writing reviews.	31-05-2017
2.0.3	Changes due to the internal annual review, adaptation to the RGPD and the eIDAS audit recommendations.	03-08-2018
2.0.4	Changes due to June 2019 audit	01-08-2019
2.0.5	Changes due to September 2020 audit and Ministry logo update	30-10-2020

Table of Contents

1. INTRODUCTION

1.1. Overview

The Social Security IT Department (henceforth GISS) is a Common Service at the sub-directorate general organisation level, attached to the Secretary of State for Social Security. As part of its functions, it provides information technology services relating to the agencies that form Social Security.

Within the approved adaptation strategy for electronic legislation, with the aim of improving the service provided to citizens and companies, GISS has created a Certification Authority, known as the ACGISS (Certification Authority for the Social Security IT Department), which issues electronic certificates and provides various trust services.

The Public Key Infrastructure (PKI) for the GISS has been designed and is managed in line with the requirements established by EU Regulation no. 910/2014 of the European Parliament and in accordance with Law 59/2003 on Electronic Signatures.

This statement describes the features of the services provided by the ACGISS as a Certification Authority, as well as the practices and procedures used in order to provide said services.

This document has been created in accordance with regulation IETF RFC 3647 (*"Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework"*), making any amendments necessary to facilitate the reading and analysis of the same and to comply with current legislation.

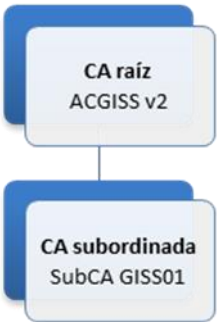
1.2. Document name and identification

Document name	ACGISS. Certification Practice Statement
Version	2.0.5
Document status	Approved
Issue date	03 october 2020
ACGISS OID	2.16.724.1.4.2.2
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)

1.3. PKI participants

1.3.1. Certification Authorities



The PKI general architecture hierarchy is as follows:

- A root Certification Authority that acts as the reference point for trust in the whole system and ultimately guarantees the identity of the provider. It is responsible for issuing certificates for any CA subordinates that are created.
- A subordinate Certification Authority that shall be responsible for issuing the different certificates.

Henceforth, CA will be used when referring to Certification Authorities.

The above-mentioned hierarchy allows risks to be spread, enabling the subordinate CA to manage keys in a swift, online environment, while protecting the root CA key in an offline, secure environment.

1.3.1.1. Root Certification Authority ACGISS v2

The main details of the root CA are as follows:

Subject	CN = ROOT ACGISSv2 SERIALNUMBER = Q2827003A OU = SOCIAL SECURITY IT DEPARTMENT O = CENTRAL TREASURY FOR SOCIAL SECURITY L = MADRID C = ES
OID	2.16.724.1.4.2.2
Serial number	57 62 68 ed
Validity period	From Thursday, 16 June 2016 10:23:07 To Monday, 16 June 2036 10:53:07
Hash (SHA-1)	90 5d 3a 6f b1 49 64 b9 da cf 41 91 a4 1a 0c 0b 6a 2a 02 57
Key length	4096
Signature algorithm	SHA256RSA

1.3.1.2. Subordinate Certification Authorities

Subordinate CAs are intermediate authorities that issue electronic certificates to end users. Currently there is only one Subordinate CA, entitled SubCA GISS01, which issues all end certificates for ACGISS.

Subject	CN = SUBCA GISS01 SERIALNUMBER = Q2827003A OU = GISS01 OU = SOCIAL SECURITY IT DEPARTMENT O = CENTRAL TREASURY FOR SOCIAL SECURITY L = MADRID C = ES
OID	2.16.724.1.4.2.2.1
Serial number	57 62 69 40
Validity period	From Thursday, 16 June 2016 11:51:17 To Monday, 16 June 2031 12:21:17
Hash (SHA-1)	b4 9c 4d ff bb 41 dc 34 8b 1a 97 05 78 5e 59 4d db 9a 9a 45
Key length	4096
Signature algorithm	SHA256RSA

1.3.2. Registration Authorities

Registration Authorities are responsible for the identification and authentication processes for users who request electronic certificates when required by the corresponding certification policies. They process certification requests and provide users with the minimum information necessary.

The units, branches and offices of the Social Security Management Organisms and Common Services designated for this purpose in each specific Certification Policy will act as Registration Authorities.

1.3.3. Subscribers

End users (or certificate holders) are the entities who use the certificates issued by Social Security.

In the case of a PKI that issues certificates for the purposes of Social Security's own functions, end users will generally be internal users from the Secretary of State for Social Security or its collaborators.

A certificate subscriber will be any entity which requests that a certificate be issued for the title holder, who may or may not be the same entity.

A complete list of subscribers and end users for the different types of certificates will be compiled for each Policy.

1.3.4. Relying parties

Relying parties are those who authenticate the certification issued by ACGISS.

1.3.5. Other participants

- Validation Authority (VA)

  This authority is responsible for verifying the status of the certificates issued by Social Security, using the online certificate status protocol OCSP.

- Time Stamp Authority.

  This authority's function is to provide evidence of the date and time on which an operation or transaction takes place electronically, in order to demonstrate that a series of data existed and has not been amended since that point.

  This component service is managed by the Social Security IT Department.

1.4. Certificate usage

1.4.1. Appropriate Certificate uses

The ACGISS issues different types of certificates, basically organised into three groups:

- Automated Action Certificates: for use by Social Security servers and applications.
- Personal Certificates: for personnel who provide services within the Secretary of State for Social Security.
- Certificates associated with Trust Services: related to other trust services provided by the provider, such as validation and time stamp services.

In particular, the ACGISS issues Public Administration certificates, in compliance with the regulations approved by the General State Administration (AGE):

- Public Employee certificates. Issued to Social Security public employees (civil service personnel, other employees and temporary personnel). These certificates have the purpose of providing identification, electronic signature and data encryption, in order to perform the functions of the job post occupied or to relate with other Public Administration Offices, if these offices so accept.
- Electronic Seal Certificates. Issued to Social Security agencies for the purpose of identification and signature of administrative documents within the scope of their functions.

The rest of the certificates issued are basically used internally within Social Security.

The ACGISS reserves the future right to issue new types of certificates and to cease issuing those already in existence.

1.4.2. Prohibited certificate uses

This section lists the applications for which each type of certificate can be used, establishing limits and prohibiting certain applications.

1.4.2.1. Permitted uses for certificates

Certificates issued by the ACGISS shall be used in order to fulfil the legitimate internal functions of the agencies comprising Social Security and its employees. Those corresponding to Public Administration shall be issued in accordance with the stipulations of article 11 of Law 59/2003 of 19 December on electronic signatures, and shall comply with the obligations set within said Law and any current specific regulations within the scope of General State Administration.

The specific use for each of the certificates issued by the ACGISS is detailed in its corresponding Certification Policy.

1.4.2.2. Prohibited applications

In general, certificates shall not be permitted to be used for different ends to those established as valid in this Certification Practice Statement (CPS) or in the existing certification policies.

Certificates issued for the purposes of proof and specified as such in their distinguished name, may not ever be used for any purpose other than the usual uses established.

Additional specific limitations and restrictions on certificate usage shall be established in the specific Certification Policy.

1.5. Policy administration

1.5.1. Organization administering the document

This CPS refers to the GISS Certification Authority version 2 (ACGISS v2).

Documentation relating to the previous architecture, and the certificates issued by it, may be found on the service provider's website. In the case of the CPS, the conditions established up to and including version 1.2 shall apply.

1.5.2. Organising policies and practices

The GISS General Certification Regulation is comprised of the different specific Certification Policies defined for each certificate, and by the Certification Practice Statement.

This document contains the Certification Practice Statement (CPS) by the GISS, as a Trust Service Provider. The general practices and policies established in this document are inherited directly from the existing subordinate CA.

This CPS includes the procedures applicable to the provision of its services, in accordance with the requirements established by the policies it manages and by article 19 of Law 59/2003 of 19 December, on electronic signatures. In particular, it includes the controls for physical and technical security and the commercial and legal features of the provider, as well as general provisions relating to the management of certificates' life cycle.

Every certificate issued will have a corresponding Certification Policy that shall include, in particular, details of the specific identifying and authenticating method and the applicable requirements for its issue, use, and revocation.

1.5.3. Person determining CPS suitability for the policy

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

1.5.4. Contact details for the responsible unit within the organisation

Name	Management of Security, Innovation and Projects (Social Security IT Department)		
E-mail address	acgiss.soporte.giss@seg-social.es buzon.giss-sscc.csi@seg-social.es		
Address	c/ Doctor Tolosa Latour s/n, 28041 Madrid		
Telephone	91 390 27 18	**Fax**	91 390 51 67

1.5.5. CPS Approval procedures

The CPS and Certification Policies are submitted to an annual approval and review process in compliance with internal procedures established for that purpose.

1.6. Definitions and acronyms

1.6.1. Definitions

Activation: the procedure by which the access conditions to a key are unblocked and its use is permitted.

Automated administrative action: Administrative action prompted by a properly programmed IT system, without the need for a physical person to intervene in each individual case. Includes the production of process or procedural resolution actions, as well as simple communication actions.

Authentication: an electronic process that enables electronic identification of a physical or legal person, and the origin and integrity of data kept in electronic format.

Certificate of electronic signature (or electronic certificate, for the purposes of this CPS): an electronic statement linking a signature's authentication data to a physical person and confirming at least the name or pseudonym of that person.

Qualified certificate of electronic signature (or qualified electronic certificate for the purposes of this CPS): a certificate of electronic signature that has been issued by a service provider qualified in trust services and which complies with the requirements established in Appendix I of EU Regulation no. 910/2014.

Electronic Seal Certificate: an electronic statement linking a seal's authentication data to a legal person and confirming the name of that person.

Qualified Electronic Seal Certificate: an electronic seal certificate that has been issued by a service provider qualified in trust services and which complies with the requirements established in Appendix III of EU Regulation no. 910/2014.

Keys (public and private): keys generated by the trust service provider, normally called signature creation data (private key) and signature verification data (public key). They are uniquely linked to each other and belong to a determined person or entity.

Electronic signature creation device: an IT unit or programme configured to be used for creating an electronic signature.

Qualified electronic signature creation device: an electronic signature creation device that complies with the requirements set forth in Appendix II of EU Regulation no. 910/2014.

Electronic seal creation device: an IT unit or programme configured to be used for creating an electronic seal.

Qualified electronic seal creation device: an electronic seal creation device that complies mutatis mutandis with the requirements set forth in Appendix II of EU Regulation no. 910/2014.

Electronic signature: data in electronic format, attached to other electronic data or data logically associated with it, which the signatory uses to sign.

Advanced electronic signature: an electronic signature that complies with the requirements set forth in article 26 of EU Regulation no. 910/2014.

Qualified electronic signature: an advanced electronic signature that is created by a qualified electronic signature creation device and based on a qualified electronic signature.

Hash, fingerprint or digest: a mathematical transaction performed on a set of data of any length; its outcome is a digital fingerprint, of a fixed size, and independent from the size of the original document. It is a method of generating keys that unambiguously represent a document or set of data.

Electronic identification: the process of using a person's identification details in electronic format, which uniquely represent a physical or legal person or a physical person who represents a legal person.

Public Key Infrastructure (PKI): a combination of security hardware, software, policies and procedures that allow execution with a guarantee of cryptographic transactions such as encoding, digital signature and non-rejection of electronic transactions.

Certificate Revocation Lists (CRLs): list of revoked or suspended certificates.

Electronic identification resource: a physical and/or virtual unit containing a person's identification data, which is used for authentication in online services.

Hardware Security Module (HSM): a cryptographic hardware device that generates stores and protects cryptographic keys with a high level of security and tends to support hardware acceleration for cryptographic operations.

OID: a sequence of numbers assigned hierarchically, which allows objects on the network to be identified and which are registered in specialist agencies. In the scope of a trust service provider, this is mainly used to uniquely identify certification policies and practices, as well as various fields on the certificates.

Trust Service Provider: a physical or legal person who provides one or more trust services, either as a qualified or unqualified trust service provider.

Qualified Trust Service Provider: a trust service provider who provides one or various qualified trust services and to whom the supervising agency has awarded qualification

Electronic seal: data in an electronic format, attached to other data in an electronic format, or associated via software to said data, to guarantee its origin and integrity.

Advanced electronic seal: an electronic seal that complies with the requirements set forth in article 36 of EU Regulation no. 910/2014.

Qualified electronic seal: an advanced electronic seal created by a qualified electronic seal creation device and that is based on a qualified electronic seal certificate.

Electronic time stamp: data in electronic format, which links to other data at a specific instance, providing proof that said data existed at that instant.

Qualified electronic time stamp: an electronic time stamp that complies with the requirements established in article 42 of EU Regulation no. 910/2014.

Trust service: electronic service consisting of:

a) the creation, authentication and validation of electronic signatures, electronic seals and electronic time stamps, delivery services for electronic certificates and certificates relating to said services, and

b) the creation, authentication and validation of certificates for authenticating websites, and

c) maintaining signatures, seals and electronic certificates relating to these services;

Qualified trust service: a trust service that complies with the relevant requirements established in EU Regulation no. 910/2014.

Validation: the process of verifying and confirming the validity of electronic signatures and seals.

1.6.2. Acronyms

CA	Certification Authority
ARL	Certification Authority Revocation List
VA	Validation Authority
ACGISS	Certification Authority for the Social Security IT Department
CEN	European Committee for Standardisation

CN	Common Name. (Attribute of an object's DN)
CRL	Certificate Revocation List
CWA	CEN Workshop Agreement
DCCF	Qualified electronic signature creation device
DCCS	Qualified electronic seal creation device
DN	Distinguished Name
CPS	Certification Practice Statement
ETSI	European Telecommunications Standard Institute
FIPS	Federal Information Processing Standard
GISS	Social Security IT Department
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
ISO	International Organisation for Standardisation
LAECSP	Law on Citizens' Electronic Access to Public Services (Law 11/2007)
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
CP	Certification policy
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
RFC	Request for Comments (IETF)
RSA	Rivest-Shimar-Adleman
SHA	Secure Hash Algorithm
SSL	Secure Socket Layer
SUBCA	Subordinate Certification Authority
TSL	Transport Layer Security

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

The GISS has a public information repository on the web page http://www.seg-social.es/ACGISS available 24 hours a day, 7 days a week.

2.1. Publication of certification information

The ACGISS provides public access to the following information:

- Certificates issued by the ACGISS that constitute the PKI chain of trust.
- Certificate revocation lists and other information on certificates' revocation status.
- The general certification regulation, comprising of this CPS and the Certification Policies of the different qualified certificates issued.
- Any other information relating to the services offered that are considered of interest for relying parties.

Any changes to specifications or terms and conditions of service shall be communicated to users via the repository. In all cases, explicit reference shall be made to the changes on the service's main web page.

The ACGISS maintains a record of each published version, so that documents can be consulted after versions have been amended.

2.2. Time or frequency of publication

ACGISS information shall be published once it is available and approved and specifically immediately after any communication is issued regarding the validity of certificates.

Information on certificates' revocation status shall be published in accordance with the stipulations in this document.

Changes to this document are governed by that set forth in the corresponding sections. After 15 days from publication of the new version, reference to the change can be taken off the provider's main web page. Earlier versions of the documentation are retained by the ACGISS for at least 15 years, for consultation by interested parties.

2.3. Access controls on repositories

The ACGISS does not limit read-only access to the information established in the corresponding public section, but it does establish controls to maintain protection of the integrity and authenticity of published information.

The ACGISS uses secure systems for the Repository, so that:

- The authenticity of certificates can be verified.
- Unauthorised persons are unable to alter data.

- Certificates are only accessible in authorised cases and to persons authorised by the signatory.
- Any technical changes that affect the security requirements are detected.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Naming

3.1.1. Types of names

Each certificate contains an X.501 name differentiator in the *Subject* field, including a *Common Name* (CN) component.

In general, certificates contain the following information:

- C - *Country*: ES (corresponds to the country's ISO code; Estado Español).
- O – *Organisation*: Certificate subscriber organisation.
- OU –*Organisational Unit Name*: Name of the type of certificate.
- SN – *Serial Number*: Subscriber tax number and/or the owner of the certificate.
- CN –*Common Name*: The subscriber and/or owner's name in free text.

In the case of qualified certificates issued to physical persons, the following shall also be included:

- *Surname*: Owner surname(s)
- *Given Name*: Owner name

Additional fields can be used, to allow management and identification of the different certificates, which shall be described in the corresponding Certification Policy.

On occasion, the field *Subject Alternative Name* is used, to include information that can be used to identify the user and facilitate interoperability of said identification in the case of Public Administration certificates.

3.1.2. Need for names to be meaningful

The above-mentioned rules guarantee that the names used on certificates are sufficiently meaningful.

The values in the fields shall correspond to official information of the subscriber entities and users, according to their registration in the Social Security databases.

3.1.3. Anonymity or pseudonymity of subscribers

The use of anonymous IDs or pseudonyms shall not be permitted.

3.1.4. Rules for interpreting various name forms

The rules used to interpret certificate distinctive names are found in the standards ISO/IEC 9594– ITU-T X.500, and the applicable section of standard ETSI EN 319 412.

3.1.5. Uniqueness of names

Certificate names shall be unique for each certificate-generating service operated by the ACGISS and for each subscriber.

It shall not be possible to reassign a DN to a certificate once it has been used on another.

3.1.6. Recognition, authentication, and role of trademarks

Since the official information for entities and users kept in the Social Security databases is used, and bearing in mind the existing guarantee that each name is unique, conflicts relating to the names used on certificates is not foreseen.

The above notwithstanding, if a name conflict arises, its resolution shall be in compliance with the stipulations laid out in this document relating to general conflict resolution and the applicable jurisdiction.

3.2. Initial identity validation

3.2.1. Method to prove possession of private key

Root and subordinate CA private keys are generated securely within a Hardware Security Module (HSM), which also provides protection mechanisms for the keys, to avoid them leaving the module.

Regarding final certificates, due to the fact that the generation procedure for the key pair depends on the type of certificate issued, proof of possession of private keys shall be described in each specific Certification Policy.

3.2.2. Authentication of organization identity

Depending on the particular certificate, authentication is specified in the corresponding Certification Policy.

3.2.3. Authentication of individual identity

Subscribers are internal users to the organization, already having their physical address and other means of contact.

Depending on the particular certificate, authentication is specified in the corresponding Certification Policy.

3.2.4. Non-verified subscriber information

Not stipulated.

3.2.5. Validation of authority

In order to verify a physical or legal person's powers of representation, current legislation shall be followed.

3.2.6. Criteria for interoperation

Information used to identify the owners of certificates is based on Spain's official identification mechanisms and is included in certificates in accordance with applicable international standards, thereby guaranteeing interoperability with third parties.

3.3. Identification and authentication for re-key requests

3.3.1. Identification and authentication for routine re-key

This section depends on each specific certificate, and is covered in the corresponding Certification Policy.

3.3.2. Identification and authentication for re-key after revocation

Renewal of certificates after revocation is not possible and a new certificate will need to be issued.

3.4. Identification and authentication for revocation request

This section depends on each specific certificate, and is covered in the corresponding Certification Policy.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. Certificate Application

4.1.1. Who can submit a certificate application

Since the end users to whom certificates are issued depends on the type of certificate being created, this section shall be covered in the specific corresponding Policy.

4.1.2. Enrolment process and responsibilities

In the same way as the above section, the section on the registration process and specific responsibilities shall be covered in the specific Policy for each type of certificate.

4.2. Certificate application processing

4.2.1. Performing identification and authentication functions

Identification and authentication functions shall be fulfilled by the personnel relevant to that task and using existing GISS technological tools.

All specific aspects of identification or authentication of users are subject to the corresponding Policy for each certificate.

4.2.2. Approval or rejection of certificate applications

Terms and conditions for approval or rejection of requests for certificates shall be established in the corresponding Certification Policies.

4.3. Certificate issuance

4.3.1. ACGISS actions during certificate issuance

After approving the request for certification, the ACGISS proceeds to securely issue the certificate and place the certificate at the subscriber's disposal.

The procedures established in this section shall also apply in the case of renewing certificates, since this means issuing a new certificate.

Specific details of ACGISS actions are specified in the corresponding CP.

In each case, the ACGISS:

- Uses a certificate-generating procedure that securely links the certificate to the registration information, including the certified public key.
- Protects the confidentiality and integrity of the registration data.
- Takes the relevant measures against the falsification of certificates.

4.3.2. Notification to subscriber by the CA of issuance of certificate

The ACGISS notifies the subscriber/owner of the issue of the certificate via different means, depending on the type of certificate. Therefore, this process shall also be covered in the specific Certification Policy.

4.4. Certificate acceptance

4.4.1. Conduct constituting certificate acceptance

This section depends on the particular type of certificate and is specified in the corresponding Policy.

4.4.2. Publication of the certificate by the CA

Publication shall be internal within Social Security.

4.4.3. Notification of certificate issuance by the CA to other entities

The GISS shall communicate the issue of any certificates used in services or communications with third party systems whenever necessary for interoperability and to authorise transactions.

4.5. Key pair and certificate usage

4.5.1. Subscriber private key and certificate usage

Subscribers and owners may use keys and certificates for the uses authorised in this present CPS and corresponding PCs. This usage should cease after the validity period has expired or the owner's certificate has been revoked.

In each case, the stipulations in this document shall be binding, in relation to subscriber/owner use of and obligations regarding certificates.

The following purposes for PKI-issued certificates are identified:

- Authentication: Enables the identity of the user to be guaranteed.
- Electronic signature: Allows electronic signature of documents and guarantees their integrity.
- Encryption: Shall be used to guarantee the confidentiality of electronic documents.

4.5.2. Relying party public key and certificate usage

Relying parties who authenticate certificates issued by the PKI are obliged to comply with the conditions of usage established in this document and the corresponding PCs.

4.6. Certificate renewal

Certificates shall not be renewed without renewing keys.

4.7. Certificate re-key

The specific terms and conditions for renewal depend on the particular certificate and are specified in its corresponding Certification Policy.

If the certificate has not been renewed once the validity period expires, it shall become unusable and it will be necessary to issue a new one.

4.7.1. Circumstance for certificate renewal

All certificate renewals are completed with a key changeover.

The validity period for each type of certificate shall be as set forth in the corresponding Certification Policies. Once said period has expired, the certificate shall become unusable and revocation of the same will be necessary, in order to issue a new one.

Certificate renewal is possible in the following cases:

- Certificate renewal due to damage or renewal of support, when relevant, or due to variations in the data recorded on it.
- Certificate renewal due to loss of the aforementioned.
- Renewal due to certification expiry, without support having changed.
- Renewal due to changes in the certification infrastructure or policies; for example, modifications to defined profiles.

4.7.2. Who may request certification of a new public key

Renewal shall be completed as part of the functions of the CA, or voluntarily and at the prompting of the end user, assuming that one of the above scenarios occurs.

In the event that there are specific conditions for each type of certificate, these shall be established in the corresponding Certification Policies.

4.7.3. Processing certificate re-keying requests

In cases where there is a specific procedure for renewal, this shall be established in the corresponding Certification Policy.

4.7.4. Notification of new certificate issuance to subscriber

ACGISS notifies the subscriber/owner of the issue of the certificate via different means, depending on the type of certificate. Therefore, this process is covered in the corresponding Policy.

4.7.5. Conduct constituting acceptance of a re-keyed certificate

The same conditions apply as those for the initial issue of certificate, detailed in the corresponding section.

4.7.6. Publication of the re-keyed certificate by the CA

Publication of certificates shall be internal within Social Security.

4.7.7. Notification of certificate issuance by the CA to other entities

The GISS shall communicate the issue of any certificates used in services or communications with third party systems whenever necessary for interoperability and to authorise transactions.

4.8. Certificate modification

Modification to issued certificates shall not be permitted. Any modification shall necessitate the issue of a new certificate.

4.9. Certificate revocation and suspension

4.9.1. Circumstances for revocation

Revocation results in the loss of validity of an electronic certificate. Causes for said revocation are:

- Expiry of the certificate's validity period.
- Revocation required by the signatory, an authorised third party or the physical person representing the owner.
- Breaching or placing at risk the secrecy of the data used to create the signatory's signature or the trust service provider's data, or the improper use of said data by a third party.
- Legal or administrative ruling that so orders.
- Termination of the legal person for the signatory, or amendment to the custodial or usage conditions for the data used to create the signature that are shown on the certificates issued to a legal person.
- Cessation of activity by the trust service provider, unless management of the electronic certificates issued by it be transferred to another provider.
- Amendment to the data provided in order to obtain the certificate, or a change in the circumstances verified for the purposes of issuing the certificate, with the result that said certificate no longer reflects the true situation.
- Due to renewal or issue of a new certificate that replaces the current one, in which case there is an automatic revocation of the latter.

In addition to these conditions, each certificate may have its own specific revocation conditions detailed in its corresponding Certification Policy.

4.9.2. Who can request revocation

The following may request revocation of a certificate:

- The subscriber or owner in whose name the certificate was issued.
- The Registration Authority who took part in the issuing.
- The ACGISS.

4.9.3. Procedure for revocation request

The procedure depends on each certificate and is specified within the corresponding Certification Policy.

4.9.4. Revocation request grace period

Revocation requests are, within reason, invoked as soon as there is knowledge of cause for revocation, for which reason there is no grace period associated with this process.

4.9.5. Time within which CA must process the revocation request

Revocation requests are dealt with immediately and shall be processed within the minimum time frame possible, according to each type of certificate.

4.9.6. Revocation checking requirement for relying parties

Users should verify the status of any certificates on which they wish to rely.

Ordinary verification procedures regarding the validity of certificates shall be by way of consultation with the Validation Authority, using the OCSP.

4.9.7. CRL issuance frequency

The Root CA issues a List of Revoked CAs (ARL - http://crl.seg-social.gob.es/arl.crl), at least once per year, and in compliance with the frequency established by the ARL itself, and ad hoc, when there is a revocation of a certificate of authority.

The Subordinate CA issues a CRL at least every 24 hours and immediately if there has been a revocation of any certificates issued. The CRL indicates the time scheduled for issuing a new CRL, assuming it is possible to issue one before the time frame indicated on the previous CRL.

4.9.8. Maximum latency for CRLs

CRLs are renewed every 24 hours as a maximum, and they are, within reason, published immediately after being generated due to a revocation, taking into account the technical specifications of the systems used.

4.9.9. On-line revocation/status checking availability

Users may consult the status of certificates issued by the ACGISS via OCSP (http://ocsp.seg-social.gob.es/) through the Validation Authority, which is available 24 hours a day, 7 days a week.

In the event of any error in the verification systems regarding the status of certificates due to causes beyond ACGISS control, the aforementioned shall make every effort to ensure that the service only be inactive for the minimum time possible.

The GISS protects the systems associated with verifying the status of certificates, using the organisational and technical measures described in this document, with the aim of guaranteeing the validity and availability of the information provided. It also guarantees the authenticity and integrity of said information by way of the signature on OCSP responses and the CRLs facilitated to third parties.

Revocation status information is available beyond the validity period of the certificate. It will also be available after termination of TSP in accordance with this policy and in the corresponding termination plan at least through long-term CRLs or other additional mechanisms that are deemed appropriate..

4.9.10. On-line revocation checking requirements

For online verification of the status of certificates, the preferred method shall be the OCSP service, for which software capable of operating said protocol should be available.

There is also a mechanism for public consultation of CRLs via HTTP.

4.9.11. Other forms of revocation advertisements available

Not stipulated.

4.9.12. Special requirements re key compromise

In the event of private keys being compromised, the actions taken shall comply with the specifications established in this document.

Following compromise, certificate is revoked and the use of the subject's private key is immediately and permanently discontinued.

4.9.13. Circumstances for suspension

Not stipulated.

4.10. Certificate status services

Verifying the status of certificates can be done via two different methods: via OCSP or by downloading the CRLs.

4.10.1. Operational characteristics

In order to validate the certificates there is a Validation Authority, to provide information on certificates issued by the ACGISS.

This is an online service implementing the OCSP (Online Certificate Status Protocol), following RFC 2560 and offers a response via HTTP.

CRLs are made available periodically as per the details set forth in this document, via HTTP.

4.10.2. Service availability

The online systems for consulting the status of certificates are available 24 hours a day, 7 days a week.

In the event of a failure of the verification systems regarding the status of certificates due to causes beyond ACGISS control, the aforementioned shall make every effort to ensure that the service only be inactive for the minimum time possible. For this purpose, the systems involved in providing the service and the information relating to the status of certificates are replicated on a central backup, which enables guaranteed continuity of validation services.

4.10.3. Optional features

Not stipulated.

4.11. End of subscription

Termination of the validity of certificates issued by the ACGISS is caused by the following:

- Revocation of the certificate for any of the causes detailed in this document.
- Expiry of the validity period of the certificate.

4.12. Key escrow and recovery

Custody and recovery of keys shall be via the security measures specified in this document and in the corresponding Certification Policy.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1. Physical controls

The ACGISS provides its users with a sufficient level of physical security for the completion of essential tasks relating to the generation and management of certificates.

For this, it establishes controls on its premises, relating to:

- Physical location of facilities and specific conditions of buildings.
- Physical access of authorised personnel.
- Protective measures relating to electronic feeds and the thermal conditions of equipment.
- Protective measures against flood and fire.
- Storage security conditions.
- Procedures for terminating information support.
- Configuring offsite backup.

5.1.1. Site location and construction

The GISS is located on a site with a secured perimeter, which guarantees the security of operations conducted within its buildings. Specifically, it has:

- Control of physical access to the perimeter around the site where its facilities are located.
- Closed circuit television cameras monitoring the whole perimeter, including the restricted access areas.
- Control of access to secure buildings and areas.
- Protection of critical systems in dedicated areas and with additional security controls.
- Systems for protection against disasters and accidents, in compliance with current legislation.

5.1.2. Physical access

The Provider establishes sufficient security levels of access to buildings and perimeters.

Facilities are protected within a secure perimeter, with architectural barriers and sufficient security to detect unauthorised access. There are personnel specifically working to control access to the units within the GISS.

Access to buildings by personnel is through the use of cryptographic cards and through identification for security personnel. All personnel are required to wear their cards in a visible place as a method of identification.

There is an authorisation control system, together with associated procedures, which guarantee that access is only granted to authorised personnel. Non-GISS personnel are continually supervised whilst working in its facilities.

Every access point is registered and filmed by closed circuit television monitors.

In addition, all systems involved in issuing certificates, particularly CAs, and the cryptographic modules containing private keys, are located in one isolated location, protected by an independent control point for authorised persons.

5.1.3. Power and air conditioning

GISS IT equipment is conveniently protected against fluctuations or cuts in electronic supply that could damage or interrupt service.

The facilities have a current stabilisation system and their own generation system for self-sufficiency in order to maintain supply during scheduled shut downs of any of the IT systems.

IT equipment is located in an environment with a guaranteed climate (temperature and humidity) designed to create its optimum working conditions.

5.1.4. Water exposures

The GISS has sufficient detection measures to prevent the equipment or cabling from being exposed to water.

5.1.5. Fire prevention and protection

Every GISS facility and asset has automated detection systems and fire extinguishers.

5.1.6. Media storage and backup

Information storage is completed so as to guarantee both its integrity and confidentiality, should it require it, and complies with the minimum requirements established by current legislation on personal data protection.

The stored data is protected against unauthorised access and is physically protected by the security measures specified in this document.

5.1.7. Waste disposal

Information carriers are destroyed in compliance with GISS internal procedures.

In the event that they contain confidential information, carriers are destroyed using secure methods, in compliance with current legislation on the security of information and personal data protection.

5.1.8. Off-site backup

The GISS has a remote backup centre in which the infrastructure and basic information used in PKI processes is replicated. This centre also has the proper security measures in place.

5.2. Procedural controls

The GISS guarantees that its systems operate securely and has established procedures for the functions that may affect the provision of its services.

Personnel who work for the ACGISS complete the tasks defined in its infrastructure procedures and management, in accordance with GISS security policy.

5.2.1. Trusted roles

The following profiles are of note when managing the PKI:

- Systems administrators: Users authorised to complete tasks relating to installing, configuring and maintaining the PKI systems.
- Systems auditors: Responsible for checking the PKI system traces and logs and completing compliance audits.
- Security officers: Users responsible for defining, verifying, administering and implementing the security policies, standards, and procedures.
- Registration officers: Responsible for the completion of tasks relating to identifying and authenticating applicants for certificates, as well as requests in their name for their issue/revocation.
- Systems operators: Users responsible for completing basic tasks relating to the systems involved in the PKI, including backup and recovery processes.
- Cryptographic Custodians: Users responsible for the custody of the cryptographic material of the PKI.

5.2.2. Number of persons required per task

ACGISS basic PKI functions are supported by more than one person, as part of a plan that guarantees immediate availability in the event of a serious contingency in its facilities.

5.2.3. Identification and authentication for each role

The GISS has implemented various authentication and authorisation systems, for both hardware and software, by which it limits access to the provider's systems and data to personnel authorised for each function.

5.2.4. Roles requiring separation of duties

Work practices in the ACGISS follow the principal that the main administrative and operational tasks in the systems are performed by more than one person, sometimes in different departments, in order to minimise the risk of illicit actions.

In particular, the different profiles involved in managing the PKI, defined in section 5.2.1, are performed by different persons and/or units within the GISS.

5.3. Personnel controls

With regards to personnel controls, the ACGISS takes into account the following aspects:

- Selection of personnel involved in managing the PKI takes place using well-defined procedures, and in accordance with their knowledge and experience.
- Adequate training of personnel is guaranteed, as is the availability of any documentation required for the fulfilment of their functions.
- Personnel involved should respect the usage policies for GISS IT systems as well as all other approved internal regulations relating to information security.
- Mechanisms are in place to require accountability in the event of non-compliance with established regulations.
- Recruitment mechanisms are used, subject to the relevant regulations for entities on public law, with specific requirements and guarantees in the event of non-compliance with agreed terms and conditions.
- It ensures the inexistence of conflicts of interest in the personnel of the organization in trusted roles.
- Personnel are formally appointed to trusted roles by the security management, always requiring the principle of "least privilege" when accessing or when configuring access privileges.

All the personnel controls specified in this document will also apply to contracted external company personnel involved in the administration and operation of these systems.

5.3.1. Qualifications, experience, and clearance requirements

Personnel working at the ACGISS go through a specific selection process and belong to bodies specialising in the development and operation of IT systems.

Personnel from outside companies are classified by occupational categories and should provide proof of their knowledge and experience in aspects relating to their job roles.

All personnel have established functions and are provided with the means and authorisation necessary for those functions.

5.3.2. Background check procedures

Internal personnel should comply with the requirements established in the legislation regarding entry into Administration.

In the event of recruiting externally, the procedures established internally and in the legislation regarding recruitment into Public Administration shall apply.

5.3.3. Training requirements

The GISS commits to training its personnel and requesting training for recruited personnel, with the aim of everyone involved in PKI procedures gaining sufficient qualifications and knowledge.

5.3.4. Retraining frequency and requirements

When necessary, specialist training courses are held, according to the GISS established procedures.

5.3.5. Job rotation frequency and sequence

Not stipulated.

5.3.6. Sanctions for unauthorised actions

Social Security, in its capacity as a public-law Entity, is committed to a disciplinary scheme for all its personnel. It also guarantees that disciplinary clauses be applied to technical support contracts with external companies, so that liability for external workers passes to their company in the event of actionable conduct.

5.3.7. Independent contractor requirements

The provider recruits qualified professionals for the effective execution of functions within the PKI.

The profiles for recruited personnel are specified in the clauses of each company's recruitment documents.

5.3.8. Documentation supplied to personnel

The ACGISS supplies any documentation needed by personnel at any time, in order that said personnel be sufficiently competent in their administrative work within the PKI.

In particular, there are manuals of operation and administration of the main components available to the PKI's trusted roles.

5.4. Audit logging procedures

5.4.1. Types of events recorded

ACGISS keeps track of the most significant security events related to the PKI, including changes relating to the security policy, system start-up and shutdown, system crashes and hardware failures, firewall and router activities, and PKI system access attempts.

Specifically, records are generated concerning any events relating to the life cycle of certificates and the main administrative operations in the PKI systems:

- Operation traces on PKI integrated HW and SW components.
- Data relating to issuing, renewing, and revoking certificates.

5.4.2. Frequency of processing log

Audit records are examined when there are suspicions or when evidence has been gathered from other sources regarding actionable conduct.

Processing audit records consists of reviewing the records, including verifying that they have not been tampered with, a brief inspection of each record entry, and a deeper investigation into any alerts or irregularities in the records. Any actions taken after reviewing the audit shall also be recorded.

5.4.3. Retention period for audit log

Audit records are dealt with in compliance with GISS audit and trace verification procedures.

Information relating to issuing, renewing, and revoking certificates is archived and stored for a minimum period of 15 years.

5.4.4. Protection of audit log

Audit record files are protected against reading, modifications, deletions, and any other type of unauthorised activity, using hardware and software access controls. Access may only be granted to personnel specifically designated for that purpose.

5.4.5. Audit log backup procedures

Backups are completed automatically, in accordance with the GISS policy on security copies.

5.4.6. Audit collection system

The storage system for audit records, located internally in the GISS, is comprised of various record applications, networks, and systems, as well as manually generated data, stored by duly authorised personnel. Management of the whole system is fulfilled in accordance with GISS internal procedures.

5.4.7. Notification to event-causing subject

Automated notification of an event to the event originator is not covered.

5.4.8. Vulnerability assessments

The GISS has general vulnerability assessment systems and services within its systems.

A specific risk analysis methodology is followed, where a risk analysis is performed and periodically reviewed, and a treatment plan is prepared to mitigate the risks detected.

Similarly, risk assessments are conducted to assess the organization's needs and determine the security requirements to be included in the certification policy.

In addition, specific vulnerability assessments can be performed in the event of suspicion relating to any PKI operations.

Any critical vulnerability is addressed within 48 hours after its discovery.

5.5. Records archival

The ACGISS guarantees that all relevant information relating to certificates shall be kept for the appropriate period of time.

5.5.1. Types of records archived

The ACGISS keeps secure records of all the information and documentation relating to certificates generated and the general regulation for certification.

5.5.2. Retention period for archive

Certificates, signed contracts, policies and practices, and information relating to issuing, renewing, and revoking certificates is archived and stored for a minimum period of 15 years.

5.5.3. Protection of archive

In order to protect the archives, the GISS guarantees to:

- Maintain the integrity and confidentiality of archives containing data referring to certificates issued.
- Archive the previously mentioned data, confidentially, and in its entirety.
- Maintain the privacy of the certificate subscriber/owner's registration data.

5.5.4. Archive backup procedures

The ACGISS creates daily backup copies, in accordance with the GISS policy established for this.

In addition, critical information is replicated in the Central Backup, following the procedures and using the general methods indicated by the GISS.

5.5.5. Requirements for time-stamping of records

The IT systems used guarantee the recording of the time ACGISS operations are performed.

The time source used is synchronised with the Royal Institute and Observatory of the Spanish Navy whose periodicity is less than 24 hours. The Royal Institute and Observatory of the Spanish Navy, through the Astronomy Section, has as its mission, the maintenance of a basic unit of Time, legally declared the national standard, and maintains and broadcasts the official "Coordinated Universal Time", considered for all purposes to be the base for the official time of Spain.

5.5.6. Archive collection system

The archive system is internal within the ACGISS and operates in accordance with established procedures.

5.5.7. Procedures to obtain and verify archive information

Only personnel authorised by the GISS have access to the data archive, which is guaranteed by the existence of various hard and software access controls.

5.6. Key changeover

Renewing CA keys means the renewal of the certificate.

The procedures for providing new keys from the Certification Authorities shall be the same as for providing the current public key, including the publication and communication of the new keys on the Provider's information repository.

5.7. Compromise and disaster recovery

5.7.1. Incident and compromise handling procedures

In its continuity plan, the Provider establishes procedures applicable for managing incidents and, in particular, compromises to key security.

Incident reporting and response procedures are employed in such a way that damage from security incidents and malfunctions are minimized.

Detection of incidents, particularly any relating to the life cycle of certificates and the access controls to systems and services, as well as security copies of information and data, shall be performed in accordance with the stipulations set forth in this document.

In addition, the GISS has internal communications and technical incident resolution mechanisms and procedures in place, produced in its systems and services.

Specifically, procedures are in place to respond quickly to incidents and notify the appropriate parties of any breach of security within 24 hours of being identified.

If the loss of integrity affects to a natural or legal person, the notification is performed as soon as possible from detection.

5.7.2. Computing resources, software, and/or data are corrupted

If corruption of resources, applications, or data should occur, the ACGISS shall initiate the necessary procedures to ensure that the system returns to its normal functioning state.

The GISS has various different recovery and restoration procedures available for its systems, including a backup centre that replicates the PKI architecture and its associated data.

5.7.3. Entity private key compromise procedures

The GISS's continuity plan considers the compromise or suspicion of compromise of the Provider's key to be a disaster.

In the event of a CA's private key being compromised, the ACGISS:

- Shall inform all subscribers and users of the compromise, as well as the supervising agency.
- Shall indicate that any certificates and information submitted regarding revocation status using said key are no longer valid.
- Shall revoke the CA certificate and publish the corresponding revocation lists. In this regard, it will study the best alternative to transfer revocation services to a third party, signing the necessary agreements where appropriate, to ensure compliance with its obligations regarding certificate status verification services.
- Shall plan the generation of new certificates for the CAs, as well as the issue of new certificates to users.
- Shall re-establish service as quickly as possible.
- Shall investigate the causes of the compromise and shall take the appropriate measures to avoid a repeat incident.

In the event of a compromise of one of the algorithms used for generating certificates, the provider shall inform users and plan the issue of new certificates with adequate algorithms.

5.7.4. Business continuity capabilities after a disaster

The ACGISS develops, maintains, and if necessary, executes contingency and continuity plans in the event of a disaster at its facilities, whether it be due to natural or intentional causes, which indicate how to restore the IT system's services.

The GISS replicates the PKI databases and systems in its backup centre. The databases used by the Provider for disaster recovery are synchronised with the production databases, within the time limits specified in the established procedures. The ACGISS disaster recovery equipment has the adequate physical security measures in place.

The ACGISS is capable of restoring the majority of PKI operations reasonably immediately, and at least within 24 hours of the disaster. As a minimum it will be able to perform the following actions:

- Revoke certificates.
- Publish revocation information.

5.8. CA or RA termination

The ACGISS ensures that possible interruptions to subscribers and third parties due to cessation of services by the ACGISS are minimal and, in particular, it ensures continuous maintenance of the records required to provide evidence of certification for legal proceedings.

Before terminating its activity as a Trust Service Provider, the GISS shall perform the following actions:

- It shall inform all subscribers and users, as well as the supervising agency, at least 2 months before terminating its activity.
- It shall also inform the above-mentioned stakeholders of certificates, advising of any transfer of liability for the archives.
- It shall, when necessary, perform the relevant tasks for transferring liability for maintenance of registration information and the events logs archives for the periods of time indicated to the subscriber and the verifiers, respectively.
- It shall destroy ACGISS private keys, or shall withdraw them from use.
- It shall guarantee the continuity of the systems for consulting the status of issued certificates for an appropriate period (15 years), in order to ensure their correct validation after termination of the service. At least it will be possible to consult the status of the certificates by means of a long-term CRL according to the established termination plan. In this regard, if GISS cannot maintain our own systems, GISS will study the possibility of transferring these services to a third party, signing the necessary agreements, to ensure compliance with these obligations.

6. TECHNICAL SECURITY CONTROLS

The ACGISS uses reliable systems and products that are protected against any tampering and that guarantee the technical security and cryptography of the certification processes for which they provide support.

6.1. Key pair generation and installation

6.1.1. Key pair generation

CA root certificate key pairs are generated inside an HSM (hardware security module) which complies with the necessary requirements for their protection. Generation is performed within GISS facilities, using the hard and software security measures established in this document.

CA keys are generated according to a defined key-generation procedure that details the roles involved and the functions performed. Said ceremony is completed in front of an auditor who guarantees that the actions have been undertaken in compliance with the procedure.

CA key pair generation procedure and the subsequent public key certification are performed under simultaneous control of at least two trusted employees, and always keeping this minimum number of personnel authorized to perform this function.

CA keys are stored in various partitions within the HSMs, and each has its own access control. For the root CA private key, an independent partition shall be used which is kept offline.

The installation and recovery of the CA's key pairs require simultaneous control of at least two trusted employees.

The time scale for CA key pairs established in the certificates depends on the security of the cryptographic algorithms and mechanisms used. The ACGISS guarantees that before they expire, new certificates shall be generated, according to the procedures established in this CPS. This shall be completed within the appropriate period of time to allow users and third parties to be aware of the change and avoid interruptions to operations.

Certificate keys shall be generated according to the stipulations set forth in the corresponding Policies.

6.1.2. Private key delivery to subscriber

The private key shall be sent to the owner in compliance with the stipulations set forth in the Certification Policy.

6.1.3. Public key delivery to certificate issuer

The process for sending the public key shall be in compliance with the stipulations set forth in the Certification Policy for each type of certificate.

6.1.4. CA public key delivery to relying parties

ACGISS CA public keys are communicated to the certificate verifiers and the supervising agency, ensuring the integrity of the key and the authenticity of its origin.

These Certification Authority public keys are also published in the public Repository, as auto-signed certificates.

6.1.5. Key sizes

ACGISS Certification Authority keys are at least 4.096 bits. Keys for end certificates issued shall be at least 2.048 bits.

RSA signature algorithm and SHA-2 hash algorithm are used to guarantee the security and authenticity of the certificates issued.

6.1.6. Public key parameters generation and quality checking

The parameters for public keys are generated in compliance with PKCS#1. The quality of the generation parameters is guaranteed by the systems and tools used when administering the certificates.

6.1.7. Key usage purposes

In the fields "*Key Usage"* and "*Extended Key Usage*" on the certificates, the ACGISS details the permitted uses for the corresponding private keys.

For CAs, the permitted uses include:

- Key Certificate Signature.

- CRL Signature.

6.2. Private Key protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic module standards and controls

Cryptographic hardware (HSM) is used, certified FIPS 140-2 Level 3 or higher, and CC EAL 4+.

Standards applicable to the cryptographic modules used in end certificates are detailed in the corresponding Certification Policy.

Existing QSCD certification status is monitored until the end of the validity period of the certificate, and appropriate measures are taken in case of modification of this status.

6.2.2. Private Key (n out of m) multi-person control

ACGISS private keys, both physically and logically, are under multi-person control to prevent one sole person from having access to them.

6.2.3. Private key escrow

ACGISS private keys are generated in cryptographic modules with strict security measures, and are stored in fireproof spaces and protected by physical access controls that guarantee only authorised personnel may gain access.

HSMs are subject to adequate security controls during transportation and storage, and they are operated within a secure environment, following operation and maintenance procedures that guarantee their proper performance over time.

6.2.4. Private key backup

For business continuity reasons, backups of the ACGISS private keys exist in secure tokens, stored in units separate from their usual storage location, and under strict access controls and procedures. In addition, generated keys are replicated in various HSMs connected in a cluster and securely synchronised, thereby minimising the possibility of losing private keys.

6.2.5. Private key archival

Not stipulated.

6.2.6. Private key transfer into or from a cryptographic module

ACGISS private keys are directly generated in the cryptographic module and do not need to be introduced into it. Any subsequent transfer shall be performed between cryptographic modules or from the backup tokens, ensuring in each case that the process is secure.

6.2.7. Private key storage on cryptographic module

Private keys are generated directly in the cryptographic modules, in partitions specifically created for the purpose which have the necessary security measures in place to guarantee their protection.

6.2.8. Method of activating private key

CA private keys are activated by way of SW operations performed by authorised roles.

6.2.9. Method of deactivating private key

Private keys may be deactivated by way of the CA's SW, by the roles specified in the corresponding operational procedures.

6.2.10. Method of destroying private key

Private keys are destroyed following a procedure that prevents their theft, modification, unauthorised exposure or unauthorised usage.

All copies of CA keys will be destroyed at the end of their life cycle.

6.2.11. Cryptographic Module Rating

ACGISS cryptographic modules comply with the security requirements necessary to guarantee the protection of PKI keys, in accordance with international regulations and standards, as previously established in this document.

6.3. Other aspects of key pair management

6.3.1. Public key archival

The ACGISS archives its public keys in accordance with the stipulations set forth in this document.

6.3.2. Certificate operational periods and key pair usage periods

Usage terms for keys are determined by the duration of the certificate. Once said period has expired they may no longer be used.

6.4. Activation data

6.4.1. Activation data generation and installation

Generating the data for activating the CA private keys is performed as indicated previously in this document, following the procedure established for the CA key generation ceremony. Passwords and access codes are generated according to the minimum requirements established to ensure a sufficient level of protection.

The generation of activation data for final certificates shall depend on each type of certificate, and therefore shall be specified in the corresponding Certification Policy.

6.4.2. Activation data protection

The activation data for ACGISS private keys is only known by authorised personnel. The access codes change periodically in order to increase their protection.

For end certificates, the activation data protection is specified in the corresponding Policy.

6.4.3. Other aspects of activation data

No additional stipulations.

6.5. Computer security controls

The ACGISS guarantees the use of adequate security controls to protect the PKI systems and data.

6.5.1. Specific computer security technical requirements

It is guaranteed that systems access is limited to duly authorised individuals. In particular:

- The GISS maintains a security policy and various associated technical standards in order to adequately manage its IT systems. The GISS ensures that at least one biennial review of the security regulations is carried out or when substantial legal or technical changes are detected that affect them.
- The GISS uses secure networks and components, adequately managed and monitored.
- The ACGISS guarantees effective administration of the level of access granted to users to maintain the system's security, including managing user accounts, performing audits and modifying or denying access as appropriate.

  The ACGISS guarantees that access to IT systems and applications is restricted in accordance with the stipulations set forth in the policy on access control, and that the systems contain sufficient security controls to implement the established segregation of functions. To this end, it has its own systems for managing identities and authorising systems access.

  In particular, access controls are enforced on attempts to add or delete certificates and modify other associated information.

- Organisation personnel are identified and authorised before using critical applications relating to the life cycle of certificates.
- Personnel are responsible for the actions performed when exercising their functions and may justify their activities, for example by using an events log.
- Security and monitoring systems enable rapid detection, registration and response against irregular or unauthorised attempts to access resources.
- Access to the public repositories for ACGISS information includes an access control point for modifications or deletion of data.
- The GISS guarantees to have sufficient measures in place to guarantee the integrity and continuity of processes and data in the event of contingencies.
- The ACGISS uses certified HW and SW products with sufficient guarantees for the completion of their functions.
- Specifically, there are defined security controls related to protection against malicious software, media management, deterioration and application security updates and patches.

6.5.2. Computer security rating

The processes for managing the security of the PKI support infrastructure are evaluated by the GISS in order to detect possible weaknesses, by way of performing internal and external audits, and establishing the necessary security controls.

In addition, the GISS uses various product and process certifications in the provision of its services, which guarantee an adequate level of IT security.

6.6. Life cycle technical controls

6.6.1. Systems development controls

A security requirements assessment is performed by a GISS specialist centre during the design and requirement specification stages for components used at the ACGISS. Developments are rolled out following the existing internal regulation guaranteeing their quality and that they are fit for their approved purpose.

Change control procedures are established for new versions, updates and emergency patches of said components.

There are various independent environments for systems development, pre-production and production, with specific procedures and requirements for development within them.

6.6.2. Security management controls

The ACGISS keeps an inventory of its IT assets and performs security controls on them in accordance with the necessity for protection established in the relevant internal regulation.

In order to protect them from being withdrawn without authorization, there is an exhaustive control of entry and exit of material and information.

Systems configuration is audited periodically, at least annually, in accordance with the established stipulations set for the corresponding section in this document.

Capacity needs are monitored, and procedures shall be planned to guarantee sufficient availability of software and storage of IT assets.

6.6.3. Life cycle security controls

Security controls exist across the life cycle of the systems that may impact the security of the PKI.

6.7. Network security controls

It is guaranteed that access to the different ACGISS networks is limited to duly authorised individuals. In particular:

- Controls are implemented by way of firewalls, to protect the internal network from external domains accessible by third parties. The firewalls are configured to prevent access and protocols that are unnecessary for ACGISS operations.
- Network management mechanisms and procedures are used to guarantee the security of GISS operations.
- Sensitive data is protected when it is exchanged across non-secure networks.
- It is guaranteed that local network components are located in secure environments, as is regular control of their configurations.
- In particular, CA systems are kept in a secure area with specific security controls to protect systems and communications between components.
- Security controls related to network segregation and security communications apply, with areas with different levels of security.
- There is access control to specific PKI networks through dedicated VLANs.
- A redundant external network connection is available to ensure the availability of services.
- Penetration tests are carried out periodically, recording the evidences of each penetration.

6.8. Time-stamping

The time source used for time stamping ACGISS operations is synchronised with the Royal Institute and Observatory of the Spanish Navy, using the NTP protocol.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. Certificate profile

Certificates shall comply with the stipulations set forth in the standards applicable to each type of certificate and shall follow the format X.509 v3.

This point shall be detailed in the corresponding Certification Policy.

7.2. CRL profile

Certification revocation lists comply with the relevant standards and specifically, with profile X.509 v2.

The main fields of CRLs are:

- CRL version.
- Issuing organisation identification.
- Date of issue of the CRL and its next update.
- CRL number.
- Serial number of the revoked certificate.
- Date of revocation.
- Reason for revoking the certificate.

7.3. OCSP profile

The services offered by the ACGISS comply with RFC 6960 (*Internet X.509 Public Key Infrastructure Online Certificate Status Protocol – OCSP*). OCSP certificates shall use standard X.509 version 3.

7.4. Other

Specific information relating to the practices and profiles for certificates used for date stamping are established in the specific certification policy by the TSA (Time Stamp Authority).

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The ACGISS shall perform regular compliance audits to verify that, once underway, it complies with the security and operational requirements specified in this CPS, each certificates' Certification Policy and the relevant legislation.

8.1. Frequency or circumstances of assessment

Biennial compliance audits should be performed on PKI qualified services, in accordance with the stipulations of EU Regulation no. 910/2014.

However, as many intermediary internal and external audits deemed necessary shall be performed for verifying the functionality of the PKI.

8.2. Identity/qualifications of assessor

The ACGISS has an audit department which shall be responsible for performing whatever internal audits it deems appropriate.

In order to perform external audits, the ACGISS shall select an external independent auditor, who should demonstrate sufficient experience in IT security, IT systems security, and compliance audits on Providers and related elements, as well as be accredited to do so.

8.3. Assessor's relationship to assessed entity

External audits shall be performed by independent auditors from the GISS.

Internal audits shall be performed by a independent department from those who perform ACGISS administration and operations.

8.4. Topics covered by assessment

The minimum elements subject to audit shall be as follows:

- Certification Authority processes and related elements.
- IT systems involved in ACGISS activities.
- Physical protection of the affected elements.
- Documentation relating to the provision of trust services.

8.5. Actions taken as a result of deficiency

Once the completed compliance audit report has been received, the ACGISS shall discuss any deficiencies found with the entity that performed the audit and shall develop and execute a corrective plan to resolve them.

If the audited ACGISS is unable to develop or execute said plan, or if the deficiencies found signify an immediate threat to the security or the integrity of the system, one of the following actions shall be taken:

- Revocation of the ACGISS key, as described in this CPS.
- Termination of the ACGISS service, as described in this CPS.

8.6. Communication of results

The audit team shall communicate the conclusions of the audit with all interested parties.

Audit reports confirming compliance with the technical and security requirements established by the standard on qualified certificates shall be communicated to the supervising agency.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

There are no charges established for the provider's services.

9.2. Financial responsibility

9.2.1. Insurance coverage

The ACGISS has a sufficient level of coverage for public liability, under the terms covered in article 20.2 of Law 59/2003, of 19 December.

9.2.2. Other assets

No additional stipulations.

9.3. Confidentiality of business information

9.3.1. Scope of confidential information

The following information is kept confidential or restricted by the ACGISS:

- Business information supplied by providers and other persons with whom the ACGISS has an obligation of secrecy, established legally or by agreement.
- Records of transactions and audits of transactions.
- Records of internal and external audits created and/or kept by the ACGISS and its auditors.
- Business continuity and emergency plans.
- Security plans for relevant systems.
- Documentation on operations and other operational plans.

9.3.2. Information not within the scope of confidential information

The following information is of a non-confidential nature:

- The ACGISS Certification Practice Statement.
- The Certification Policies of recognised certificates issued by the ACGISS.
- Any other information identified as "Public" or published in the Provider's Repository.

9.3.3. Responsibility to protect confidential information

The ACGISS is responsible for establishing the appropriate measures for protecting confidential information.

These measures include the appropriate clauses on confidential information in relevant legal documents.

9.4. Privacy of personal information

9.4.1. Privacy plan

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 divulge or hand over this personal data except for in foreseen cases or when it is legally obligated.

9.4.2. Information treated as private

In compliance with the stipulations set in article 4 of (EU) Regulation 2016/679, personal information is considered to be any information about an identified or identifiable natural person, an identifiable natural person being any person whose identity can be determined, directly or indirectly.

Personal information that does not have to be included in certificates or in the indicated mechanism for verifying certificate status is considered private, personal information.

The following data is always considered private information:

- Requests for certificates, approved or denied, as well as other personal information obtained to issue and maintain certificates, except for the information indicated in the corresponding section.
- Private keys generated or stored by the ACGISS.
- Any other information identified as "Private information".

Confidential information in accordance with the data protection regulations is protected from loss, destruction, damage, falsification, and illicit or unauthorised processing.

9.4.3. Information not deemed private

Information included in certificates and in the aforementioned mechanism for the verification of certificate status is not considered private, in accordance with the provisions of article 17.2 of Law 59/2003 of 19 December, on electronic signatures.

In all cases, the following information is not considered to be confidential:

- Certificates containing the public key.
- The name and surnames of the certificate subscriber, as well as any other circumstances or personal data relating to the owner, assuming that they are significant with regards to the end purpose of the certificate, in accordance with the corresponding policy.
- The uses detailed in the certificate.
- The validity period of the certificate, as well as the certificate issue date and expiry date.
- The certificate serial number.
- The different statuses and situations of the certificate and the date each started, in particular: pending generation and/or delivery, valid, revoked, suspended or expired, and the reason for each change of status.
- The Certification Revocation Lists (CRLs), as well as all other information regarding the revocation status.

9.4.4. Responsibility to protect private information

The Social Security guarantees, as a minimum, compliance with its legal obligations and therefore shall respond to claims for damages that it may cause in the execution of its daily activities, in the event of non-compliance, for the present purposes, with the obligations covered in the applicable regulations for the protection of personal data.

The Social Security establishes a procedure for communicating, managing and responding to incidents relating to personal data.

The Social Security introduces methods for identifying and authenticating, such as the necessary control for personnel access to personal data and managing the personal data carriers and backups.

9.4.5. Notice and consent to use private information

The provision of consent for the processing of personal data is done in accordance with what is established in the applicable personal data protection regulations.

9.4.6. Disclosure pursuant to judicial or administrative process

The ACGISS only divulges confidential information in legally foreseen circumstances.

In particular, the ACGISS is obliged to reveal the identity of signatories when so requested by legal entities in the exercise of their legal functions, and under the conditions set forth in the data protection regulations, when required.

9.4.7. Other information disclosure circumstances

In its confidentiality policy, described in this document, the ACGISS includes any other scenarios where it may be permitted to divulge subscriber information directly to the subscriber themselves or to third parties.

9.5. Intellectual property rights

9.5.1. Ownership of certificates and revocation information

The ACGISS, the Social Services Management Entities and Common Services are the only entities that are entitled to intellectual property rights over the certificates they issue.

9.5.2. Ownership of certification policies and CPS

The ACGISS, the Social Services Management Entities and Common Services are the only entities that are entitled to the intellectual property rights over the Certification Practice Statement, its corresponding Certification Policies and any other document relating to the services offered.

9.5.3. Ownership of the information relating to names

The subscriber or owner is the owner of the certificate Distinguished Name, without prejudice to third party rights.

9.5.4. Ownership of keys

Key pairs are the property of those responsible for the certificates. When a key is divided into parts, all parts of the key are the property of the party responsible for the key.

9.6. Representations and warranties

9.6.1. ACGISS representations and warranties

The ACGISS shall respond to claims for damages it causes to any person while executing their activities, in the event of non-compliance with the obligations set forth in Law 59/2003, article 22.

In particular, it shall be liable for:

- Issuing certificates in compliance with the approved Policies and the relevant standards.
- Revoking certificates under the terms covered in the CPS.
- Maintaining, free of charge, verification systems for certificate statuses.
- Using reliable and certified systems and products, with the adequate protective measures in place, guaranteeing the security of the certification processes.

- Keeping the information on the provider's public repository updated.
- Communicating any changes to the CPS and Certification Policies, according to the established procedures and terms and conditions.
- Protecting ACGISS private keys, as detailed in this document.
- Properly retaining and archiving information generated during the time period in which they are legally demandable.
- Responding to claims for damages caused in the exercise of its activity, in accordance with the stipulations of Law 59/2003 of 19 December.
- Collaborating on internal and external audit processes.
- Respecting the procedures established for the cessation of its activity.

9.6.2. RA representations and warranties

The ACGISS may delegate some functions to the Registration Authority, who shall be responsible for aspects attributed by the Provider.

Registration Authorities are obliged to do the following:

- Respect the terms and conditions established in the CPS and specific Certification Policies.
- Verify the identity of certificate subscribers.
- Verify the information supplied by subscribers, before issuing certificates.
- Inform the subscriber and users about their obligations and the minimum information relating to the provider.
- Transmit and deliver certificates in accordance with the stipulations detailed in the corresponding policies.
- Archive the documentation generated during the course of exercising its functions.

9.6.3. Subscriber representations and warranties

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 that make up part of certificate life cycle.
- Communicate any modification to the data once it has been supplied.
- Understand and accept the terms and conditions of issue and use of certificates.
- Use certificates and their keys in accordance with the conditions and uses established in the CPS 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, exposure or unauthorised usage.
- Inform the GISS of any certificate malfunction.

- Observe the procedures established in the relevant policies, regarding any change in the circumstances that conferred the right to issue certificates, such as cessation of service provision in the organisation.

9.6.4. Relying party representations and warranties

Third parties who accept certificates issued by the ACGISS should:

- 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 in them and in the relevant certification policies.

9.7. Disclaimers of warranties

Not stipulated.

9.8. Limitations of liability

9.8.1. Provider's liability limitations

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

In particular, it shall not be liable for damages caused by the signatory or bona fide third parties, due to non-compliance with the obligations established in this document for subscribers, owners and third parties who accept their certificates.

9.8.2. Acts of God and force majeure

Not stipulated.

9.9. Indemnities

Not stipulated.

9.10. Term and termination

9.10.1. Term

The CPS and Certification Policies shall become valid from the moment of approval by the GISS and their publication on the Provider's web page, and shall remain valid until new versions are approved.

9.10.2. Termination

The CPS and Certification Policies shall be replaced by any new versions approved for certificates issued from that point onwards.

9.10.3. Effects of termination and survival

The obligations and restrictions established in this CPS and the corresponding Certification Policies shall continue to exist after their replacement by a new version for any certificates previously issued.

9.11. Individual notices and communications with participants

The ACGISS has established notification mechanisms between parties for the corresponding policies and relevant internal procedures.

In addition, it shall publish any significant notifications that may affect the services provided on its web page.

9.12. Amendments

9.12.1. Procedure for amendment

The ACGISS may unilaterally modify this document, assuming it complies with the following procedures:

- The modification should be justified from a technical, legal, or commercial standpoint.
- The modification proposed by the ACGISS may not contravene any of the certification policies established by it.
- 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 ACGISS, according to the procedure established for it.

9.12.2. Notification mechanism and period

In the event that the modifications made may affect the acceptability of certificates, the ACGISS shall notify the users via its website and shall make the new version of the CPS public.

9.12.3. Circumstances under which OID must be changed

OIDs established at the ACGISS shall be modified by regulatory necessity, or in the event of new certificate versions being issued, which implies the application of new certification practices different to the previous ones. New OIDs shall require internal approval.

9.13. Dispute resolution provisions

9.13.1. Extrajudicial conflict resolution

In its legal documentation with subscribers, the ACGISS establishes procedures for mediating and resolving relevant conflicts, both by agreement and legal means, and it adheres to the general procedures established for Public Administration.

On the other hand, the corresponding mailbox 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.

9.13.2. Competent jurisdiction

The competent jurisdiction shall be jurisdiction applicable to conflict resolution within Public Administrations.

9.14. Governing law

With regards to the legislative framework, the following regulations are noteworthy:

- EU Regulation no. 910/2014 of the European Parliament and of the Council of 23 July 2014, regarding electronic identification and trust services for electronic transactions in the domestic market.
- 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, which partially implements Law 11/2007 of 22 June, on Citizens' Electronic Access to Public Services.
- 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).
- Organic Law 3/2018 of December 6, Protection of Personal Data and guarantee of digital rights.

- Royal Legislative Decree 1/1996, of 12 April, approving the Consolidated Text of the Law on Intellectual Property.

Additionally, all the regulations related to the administrative procedures referred to in this document, as well as those relating to the rights and obligations of the personnel who render their services in the Administration, will apply.

In addition, European standards have been taken into account, among which the following should be noted:

- ETSI EN 319 401: General policy requirements for TSPs supporting electronic signatures.
- ETSI EN 319 411: Policy and security requirements for TSPs issuing certificates.
- ETSI EN 319 412: Profiles for TSPs issuing certificates.
- ETSI EN 319 421: Policy and security requirements for TSPs issuing time-stamps.
- ISO/IEC 9595: Information technology -- Open Systems Interconnection -- Common management information service (X.500).
- RCF 3647 - Internet X. 509 Public Key Infrastructure Certificate Policy.
- RFC 3739 - Internet X.509 Public Key Infrastructure: Qualified Certificates Profile.
- RFC 5280 - Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL).
- RFC 6960 - Online Certificate Status Protocol - OCSP.

9.15. Compliance with applicable law

The ACGISS declares its compliance with current regulations.

9.16. Miscellaneous provisions

Not stipulated.

9.17. Other provisions

9.17.1. Organisational aspects

The GISS units responsible for generating and revoking certificates are responsible for the provision of services free from any type of pressure that may place into doubt the trust of the services provided.

These units are properly identified within the organisational structure.

Also, it is guaranteed that there is no discrimination of any kind in the provision of ACGISS certification services.

Services are provided by GISS without subcontracting or outsourcing any of them.

9.17.2. Tests

The provider shall provide relying parties with the means to test its qualified certificates.

All test certificates shall be correctly identified as such in their distinguished name and shall be used solely for this purpose.

9.17.3. Disabled persons access

Social Security has the proper mechanisms and procedures in place to facilitate access to services for disabled persons.

9.17.4. Terms and conditions

Terms and conditions relating to the certification issued by the ACGISS shall be published on the Social Security Intranet, in addition to the website of the service provider in the case of qualified certificates.