MINISTERIO
DE EMPLEO
Y SEGURIDAD SOCIAL

SUBSECRETARÍA

S.G. DE TECNOLOGÍAS DE LA
INFORMACIÓN Y
COMUNICACIONES

Certification Service Provider of the Ministry of Employment and Social Security
Certification Practices Statement

sgtic@meyss.es

C/ AGUSTÍN DE BETHENCOURT, 4
28071 MADRID
TEL: 91 363.11.88
FAX: 91 363.07.73

Version Control

Identifier	D003
Title	Certification Service Provider of the Ministry of Employment and Social Security Certification Practices Statement
Responsible	SG de Tecnologías de la Información y las Comunicaciones Ministerio de Empleo y Seguridad Social
Version	1.5
Date	10.08.2012
	1.3.6.1.4.1.27781.2.3.1

Version History

Version	Date	Comments
1.0	05.11.2009	Final Document
1.1	29.03.2010	ISO/IANA number changes for MPR and OID changes in the certificates issued by CSPM.
1.2	10.09.2010	Heading Change, suppression of DG de Servicios Added LFE art. 21 in paragraph 5.8
1.3	07.04.2011	OCSP certifícate OID change. Suppression of OCSP no Check restriction
1.4	16.02.2012	OID update
1.5	10.08.2012	Organization Structure actualization. New document format. Annex C added.

Brief contents

Contents

1 Introduction

This document contains the **Declaration of Certification Practices of the Certification Service Provider of the Ministry of Employment and Social Security (CSPM)**, hereinafter, CPSM.

The CPSM is available electronically in an easy and free way. The CPSM is drafted in accordance with the specifications in RFC 3647 [IETF RFC 3647]. The CPSM assumes that the reader is familiar with the concepts of PKI, certificate and and electronic signature, otherwise it is recommended to the reader to acquire the knowledge of these concepts before going on to read this document.

In compliance with article 19 of Law 59/2003, of 19 December, on Electronic Signature (LFE), the CPSM details the obligations the CSPM agrees to comply in relation to measures of technical and organizational security, the conditions for the application, issuance, use, suspension and termination of the term of electronic certificates, management of creation data and verification of electronic signatures and electronic certificates, the certificate profiles and mechanisms of information on its validity.

The CSPM determines the suitability of the CPSM regarding Certification Policy of the AGE and the certificate profiles published and admitted under the scheme identification and electronic signature of the AAPP.

In the event that the PSCM is unable to provide the services under the conditions set forth in this CPSM, it will not give any service until express authorization of operation by the responsible body after examining the actual conditions of operation.

1.1 Presentation

1.1.1 Levels of assurance

Based on the two levels of assurance established for the various certificates issued under the LAECSP and the different modes of electronic signatures contained in the LFE, the CSPM issues its certificates as shown below:

- Medium level of assurance: Systems with advanced electronic signature based on qualified electronic certificate.
- High level of assurance: Systems with qualified electronic signature.

All certificates include implicitly in each defined profile, the corresponding assurance level with a unique identifier: the object identifier *Administrative Identity*.

1.1.2 Types and classification of certificates

According to the LFE and the LAECSP there is a typology of certification services for the purpose of issuing electronic certificates for different applications and different end users.

Below is a description of the types of certificates that are defined and relevant for CSPM to indicate the correct use of the same.

- The Public Employee Certificate is the certificate provided for in Article 19 of the LAECSP, for those in the service of the Administration.
- The Electronic Office Certificate is the certificate provided for in Article 17 of the LAECSP.

- The Certificate of Electronic Seal for Automated Actuation is the certificate provided for in Article 18 of the LAECSP, also called electronic seal certificate of Public Administration, body or public entity.

In the scope of the CPSM and specific documentation for each certificate, the CSPM issues the following types of certificates:

- Public Employee Certificates, high level, supported on a secure signature creation device according to Article 24 of the LFE (cryptographic card or USB token).
- Electronic Office Certificates, medium level, supported on a software container (on a secure application server).
- Electronic Seal Certificates, medium level, supported on a software container (on a secure application server).

Out of the scope of the LAECSP, the CSPM additionally issues the following types of certificates:

- The OCSP responder certificate is the certificate that allows signing the responses emitted by the OCSP server.
- The Time Stamp Certificate TSA is the certificate that allows signing time references.
- The Software Signature Certificate is the certificate that allows signing software code and executable modules.

Each type of certificate issued carries a degree of confidence associated with different levels of assurance under which they are issued, due to technical and safety requirements that are associated with these levels.

The specifics relating to each type of certificate issued by the CSPM are regulated in specific documentation for each certificate type.

1.1.3 Relationship between CPSM and other documents

The CPSM includes all the procedures detailed in the Certification Policy of AGE to be met by certification bodies, subscribers and other users of certificates. The CPSM is complemented by documents describing the profiles of certificates.

1.2 Name and identification of the document

1.2.1 Identification of this document

This document name is **Certification Service Provider of the Ministry of Employment and Social Security. Certification Practices Statement**, CPSM with the following information:

- Document version	1.5
- Document status	Final
- Emission date	June 30th 2012
- Expiration date	NA

- OID	1.3.6.1.4.1.27781.2.3.1

Internet address of this document is listed in Annex C.

1.2.2 Identification of certificate types

Each type of certificate has his own *OID*, as indicated below, and is included inside the certificate in the *PolicyIdentifier* field.

Each *OID* is univocal and is not used to identify different types, policies or versions of issued certificates.

- Public employee certificate:
  - High level (non repudiation certificate): *[1.3.6.1.4.1.27781.2.4.4.1.3]*
  - High level (authentication certificate): *[1.3.6.1.4.1.27781.2.4.4.2.3]*
- Electronic Office certificate:
  - Medium level: *[1.3.6.1.4.1.27781.2.4.2.2.2]*
- Electronic Seal certificate:
  - Medium level: *[1.3.6.1.4.1.27781.2.4.3.2.3]*
- OCSP Responder certificate: *[1.3.6.1.4.1.27781.2.4.33.1.2]*
- Time Stamp certificate: *[1.3.6.1.4.1.27781.2.4.34.1.2]*
- Software Signature certificate: *[1.3.6.1.4.1.27781.2.4.32.1.2]*

1.3 Participants in the certification services

The CPSM regulates a community of users who must obtain certificates according to the LAECSP, the LFE and the corresponding administrative regulation.

The next paragraphs identify both the components of the Certification Service Provider as the community of entities involved in the management and maintenance of the certificates and the keys.

1.3.1 Certification services provider

A Certification Services Provider (CSP) is a natural or legal person who issues certificates or provides other services related to electronic signatures, according to the LFE. A CSP generates electronic certificates by the operation of certification bodies of his ownership that electronically sign the certificates.

Within the CSPM, according to the system of certification of AGE, these providers offer services:

- Accreditation Entity, provider that admits, supervises and accredits Certification Entities.
- Certification Entity, provider that issues certificates.
- Registration Entity, provider that registers users.
- Validation Entity, provider that verifies certificates and signatures.
- Time Stamping Entity, provider that issues time stamps.

1.3.1.1 Accreditation Entity

Accreditation functions in the CSPM are attributed to the Undersecretary of the Ministry, which supports, accredits and monitors certification bodies.

1.3.1.2 Certification Entity

The *Subdirección General de Tecnologías de Información y las Comunicaciones, SGTIC,* handles the CSPM components to ensure the correct matching of key pairs of the subscribers with the identity they represent. This linkage of key pairs with identity occurs through X.509 v3 certificates as described in the CPSM and profiles of certificates.

The Certification Entity is composed in a unique and exclusive way, by the root CA whose certificate data are shown below:

Issuer	CN = AC1 RAIZ MTIN SERIALNUMBER = S2819001E OU = PRESTADOR DE SERVICIOS DE CERTIFICACION MTIN OU = SUBDIRECCION GENERAL DE PROCESO DE DATOS O = MINISTERIO DE TRABAJO E INMIGRACION L = MADRID C = ES
Subject	CN = AC1 RAIZ MTIN SERIALNUMBER = S2819001E OU = PRESTADOR DE SERVICIOS DE CERTIFICACION MTIN OU = SUBDIRECCION GENERAL DE PROCESO DE DATOS O = MINISTERIO DE TRABAJO E INMIGRACION L = MADRID C = ES
Serial Number	05 0b 41 5e 82 7b
Validity Period	jueves, 05 de noviembre de 2009 17:17:45 domingo, 03 de noviembre de 2019 17:17:45
Hash	sha1 6a d2 3b 9d c4 8e 37 5f 85 9a d9 ca b5 85 32 5c 23 89 40 71
Signature Algorithm	sha1RSA

Each type of certificate is described in a document with the certificate profile.

1.3.1.3 Registration Entities

The Registration Entities assist the CSPM in the functions of identification and authentication of subscribers as well as other tasks related to the management of certificates. They have as its primary mission to ensure that the information contained in the certificate application is complete and truthful. The tasks they perform are:

- Identification y authentication of the identity of the persons that apply for or receive a certificate.
- Delivery of the secure signature creation devices to the certificate subscriber or to the responsible.
- Approval of the certificate generation.
- Archiving of documents relating to the certification services or shipment of the same for its archive.

The Registration Entities are composed jointly by telematics services that enable the lifecycle management of certificates and personally attended posts dedicated to this purpose.

The Registration Authorities perform the identification of the certificate applicants according to the rules of the CPSM and the agreement signed with the Certification Entity. In the event that the Registration Entities belong to the Ministry, it would not be required the signature of any agreement and the relationship between them is governed by the CPSM and the Certification Policies that apply. The Registration Authorities responsible for managing certificate requests are defined for each type of certificate.

The Certification Entity may rely on one or more Registration Entities freely chosen to provide the certification service.

The services offered by the Registration Entities for Public Employee certificates are on the Intranet of the Ministry.

1.3.1.4 Validation Entities

The Validation Entities are responsible for providing information about the validity of digital certificates issued by a Certification Entity. To provide this information, Validation Entities use the services from the list of trusted entities (TSL), which maintains the list of certification services supported by all the Public Administrations.

The Validation Entity of the CSPM serves users so that they can check the certificate status instantly, safely and reliably.

Access to status validation services is offered publicly. The location of the OCSP validation service and the certificate of the OCSP service is in Annex C.

1.3.1.5 Time Stamping Entities

The Time Stamping Entity provides cryptographic evidences of existence at a particular time, the one shown in the time stamp.

Access to time stamping services for electronic signature is offered to all the applications of the Ministry.

The Time Stamping Entity of the Ministry provides service as determined by [ETSI TS 102 023] and the additional requirements set by AGE to adapt this standard to Spanish legislation and improve quality levels.

The location of the time stamp certificate is in Annex C.

1.3.2 End Users

End users are the persons or entities that own and use the electronic certificates issued by the CSPM certification authorities. There are different end user types:

- Certificate requester.
- Certificate subscriber.
- Certificate responsible.
- Certificate verifier.

1.3.2.1 Certificate requester

A certificate is requested by a person in his own name, on behalf of an institution or on behalf of another legal or natural person.

In the case of certificates of Public Employees, the applicant must be an employee of the public body.

For Electronic Office certificates, electronic seal, OCSP responder and Time Stamping, the request must come from public employees.

The certificate request Signature Software will be made by a public employee belonging to the unit will proceed to the signing of this software.

1.3.2.2 Certificate subscriber

Certificate subscribers are the Public Administrations and the natural or legal persons identified in the Subject field of the certificate and that ensure they use the key and the certificate in accordance with CPSM.

In the Electronic Office certificates and the Electronic Seal certificates, the Subject field (specifically in the Common Name attribute) also identifies the server or device to which they are associated.

1.3.2.3 Certificate responsible

Certificate responsible, that means responsible of the custody of the certifícate, is the natural person identified as such in the object "*Identidad Administrativa*" inside the *SubjectAltName* extension. Additionally, the responsible may be identified in the fields *Given Name* and *Surname* inside the certificate *Subject*.

In the case of Public Employee certificates, the responsible person is the subscriber of the same.

In the case of Electronic Office and Electronic Seal certificates, the responsible will be a public employee.

In the case of OCSP responder certificate, the responsible will be the responsible of the Validation Entity.

In the case of Tim Stamp certificate, the responsible will be the responsible of the Time Stamping Entity.

In the case of Software signing certificates, the responsible will be the responsible of the Unit that requested the certificate to sign the software.

1.3.2.4 Certificate verifiers

Verifiers are the entities (including natural and legal persons, Public Administrations and other organizations) who, using a Public Employee certificate, issued by a Certification Authority operating under the CPSM, verifies the integrity of an electronically signed message or identifies the message sender or sets up a confidential communication channel with the certificate owner, trusting on the validity of the relationship between the suscriptor name and the public key of the certificate provided by the certification authority. A verifier will use the information contained in the certificate to determine the certificate usage in a particular case.

1.4 Certificate usage

The certificates issued under the CPSM shall be used only in the defined transactions inside the permitted systems and applications. Issuance of the Public Employee certificates under the CPSM obliges the subscriber to the acceptance and use thereof in the terms expressed in the CPSM.

It is emphasized that falls outside the scope of the CPSM to ensure the technological feasibility of applications that make use of any of the certificate profiles defined by the CPSM.

It is not allowed in any way the use of any of these certificates outside the scope described in the DPCM, what could cause immediate revocation of the certificates by the misuse of the same

Each type of certificate issued by the PSCM with correspondence with the ones defined by LAECSP will be delimited in its use by the provisions of the law. The remaining types shall conform to the specifications in the certificate or in their profile documents.

1.5 CPSM Administration

1.5.1 Organization that administers the document

The *Undersecretary* of the Ministry holds regular representation of the ministry and the direction of their common services, as well as the exercise of the powers referred to in Article 15, of 14 April, the Organisation and Functioning of the AGE, and in particular , coordination and management of human, financial, technological and material resources of the department..

The SGTIC (former Subdirección General de Proceso de Datos) depends on the Undersecretary and is responsible for the promotion and coordination of IT policy of the ministry and its agencies, coordination of eGovernment in the department, planning and management of information systems necessary for the performance of services, the management and administration of telephone and data communications networks for central services, interprovincial and abroad, the administration of the ministry's web presence, advice and assistance in information and communication technologies, supervision on information and communication technologies in autonomous bodies attached to the Ministry, except Public Employment Service and the units depending of the Social Security..

Therefore, the responsible of the CSPM (including certification, Registration, Validation and Time Stamping entities) is the SGTIC responsible and therefore the definition, review and disclosure of CPSM. There are two assistants to the CSPM responsible, advising and collaborating in the definition, analysis and improvement of CSPM and replacing him in case of prolonged absence, in accordance with applicable law. Both assistants are the Assistants of the SGTIC.

1.5.2 Contact data

Subdirección General de Tecnologías de la Información y las Comunicaciones
C/ Agustín de Bethencourt, 4
28003 - Madrid
ca@meyss.es

Telephone: 91 363 11 88/9 – Fax: 91 363 07 73

1.5.3 Document management procedure

1.5.3.1 Procedure for change specification

It is for the CSPM responsible the approval and application of the proposed changes to the CPSM.

The CSPM will review the CPSM at least once a year. Errors, updates, suggestions or improvements on this document will be communicated to the organization whose contact details appear in section 1.5.2. All communications should include a description of the change, its justification and the information of the person requesting the modification.

All approved changes in the CPSM will be disseminated to all interested parties as specified in the following section.

1.5.3.2 Publication procedures

The CSPM will publish all information it deems appropriate regarding the services offered (including CPSM) in a repository accessible to all users. The location of the current CPSM is published in:

http://ca.mtin.es/mtin/DPCyPoliticas

1.5.3.3 Procedure for approval of the CPSM and external policies

The CPSM has been approved by the head of CSPM after verifying that this document complies with the requirements of the Certification Policy of AGE.

No External Policies implementation is stipulated in the CPSM, being the only valid reference the Certification Policy of AGE.

1.6 Definitions and acronyms

1.6.1 Definitions

En el ámbito de la DPCM se utilizan las siguientes definiciones:

C	Country: Distinguished Name attribute for an object within a X.500 directory structure.
CN	Common name: Distinguished Name attribute for an object within a X.500 directory structure.
CSR	Certificate Signing Request, dataset containig a public key plus the electronic signature using the associated private key, sent to the Certification Authority for the issuance of an electronic certificate containing this public key.
DN	Univocal identification for an item within a X.500 directory.
HSM	Hardware Security Module used to store keys and to make cryptographic functions safely.
O	Organization: Distinguished Name attribute for an object within X.500 directory structure.
OCSP	On line Certificate Status Protocol: This protocol allows checking the revocation status of an electronic certificate.

OU	Organizational Unit: Distinguished Name attribute for an object within a X.500 directory structure.
PIN	Personal Identification Number: Password that protects access to a cryptographic card.
PKCS	Public Key Cryptography Standards is a set of standards defined by RSA Laboratories and internationally accepted.
PKIX	Workgroup inside IETF established to develop the specifications related with PKI and Internet.
PUK	Password used to unblock a cryptographic card bloqued after repeated introduction of incorrect PIN.
RFC	Request For Comments, standard documents emitted by IETF(Internet Engineering Task Force).

1.6.2 Acronyms

AAPP	Public Administrations
AGE	AGeneral Administration of the State
AR	Register Entity, also known as Register Authority
AV	Validation Entity, also known as Validation Authority
C	Country.
CA	Certification Authority.
CDP	CRL Distribution Point.
CEC	Certificate Emision Code.
CEN	Comité Européen de Normalisation
CN	Common Name
CP	Certificate Policy
CPD	Data Processing Centre
CPS	Certification Practice Statement
CPSM	Certification Practice Statement of the Ministry
CRL	Certificate Revocation List
CSP	Cryptographic Service Provider
CSPM	Cryptographic Service Provider of the Ministry
CSR	Certificate Signing Request
CWA	CEN Workshop Agreement
DN	Distinguished Name
DPC	Declaración de Prácticas de Certificación (see CPS)
DPCM	Declaración de Prácticas de Certificación del Ministerio (see CPSM)
ETSI	European Telecommunications Standard Institute
FIPS	Federal Information Processing Standard
GTP	Permanent Work Group
HSM	Hardware Security Module
IETF	Internet Engineering Task Force (Internet standardization body)
ITU-T	International Telecommunication Union -Telecommunication Standardization Sector
LAECSP	Law 11/2007 of June 22nd, on electronic access of citizens to Public Services (Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos).
LDAP	Lightweight Directory Access Protocol
LFE	Law 59/2003 of December 19th on Electronic Signature (Ley 59/2003 de

	19 de diciembre de Firma Electrónica).
LOPD	Law on Protection of Personal Data (Ley Orgánica de Protección de Datos de Carácter Personal)
MINETUR	Ministry of Industry, Energy and Tourism
MINHAP	Ministry of Finance and Public Administration
O	Organization
OU	Organizational Unit
OID	Object IDentifier
OCSP	On-line Certificate Status Protocol
PIN	Personal Identification Number
PKCS	Public Key Infrastructure Standards
PKI	Public Key Infrastructure
PKIX	Workgroup inside IETF (Internet Engineering Task Group)
PSC	Prestador de Servicios de Certificación (see CSP)
PSCM	Prestador de Servicios de Certificación del Ministerio (see CSPM)
PUK	PIN UnlocK Code
RA	Registration Authority
RFC	Request For Comments
SGTIC	Subdirección General de Tecnologías de la Información y las Comunicaciones
TSL	Trusted Service List
VA	Validation Authority

2 Information publication and Certificate repository

2.1 Repository of information and certificates

The Certification Entity of the CSPM has a repository of information available 24 hours 7 days a week. In the event of catastrophic system failure beyond the control of CSPM, this commits to make best efforts to make the service becomes available again in the period specified in section 5.7.4 of this document.

The CSPM holds in its repository the following information:

- Different versions of the CPSM and documents defined therein.
- The general certification policy of the AGE and certificate profiles dictated by the CSPM to develop further requisites within the framework of the CPSM.
- All previous versions of that documentation indicating the periods in which they were applied.
- The certificate revocation lists and other information of revocation status of certificates.

This documentation shall be kept available for a minimum period of fifteen years from the issuance of the certificate. The CSPM satisfies the initial registration and filing of appropriate information to the duration of the different types of documents and electronic files used by the AGE, which stipulates minimum periods for each type of document and file.

The CSPM satisfies the initial registration and filing of certain information determined by the technical specifications [ETSI TS 101 456] and [ETSI TS 102 042].

In any case, supporting evidence proving the acceptance of the certificate will be kept permanently, such documentary evidence will not be destroyed at any time.

2.2 Publication of Certification Entity information

The location of the CPSM is in Annex C.

The location of the Certification Entity root certificate is in Annex C C.

The location of the OCSP service is in Annex C.

The location of the CRL publication is in Annex C.

2.3 Publication frequency

The above information, including profiles and CPSM, is published as soon as it is available. Changes in CPSM are governed by the provisions of section 1.5 of this document.

The information of certificate revocation status is published in accordance with sections 4.9.7 and 4.9.9 of this document.

2.4 Access control

The CSPM does not restrict read access to the information set out in Section 2.2, but establishes controls to prevent unauthorized persons from adding, modifying or deleting records of the information repository, protecting also the integrity and authenticity of revocation status information.

The CSPM uses reliable systems for information repository so that:

- Only authorized persons can make entries and changes.
- Authenticity of information can be checked for.
- Any technical change affecting the safety requirements can be detected.

3 Identification and authentication

3.1 Management of names

3.1.1 Types of names

All certificates contain a distinguished name (DN) of the person and / or organization identified in the certificate, as defined in accordance with the provisions of the Recommendation [ITU-T X.501] and contained in the Subject field, including a component Common Name. All certificates issued comply also with the standard [IETF RFC 3280].

3.1.2 Administrative Identity and Normalization

The CSPM uses the normalized naming schema Administrative Identity proposed by the Spanish administration for every type of certificate and profile. Thus using a common framework, assigning exactly the same name to seals, offices, organizations, posts and units, etc. for the entire State Public Administration.

The Administrative Identity object has the ISO/IANA number 2.16.724.1.3.5.X.X, provided by the Spanish administration as a base to identify it, thus establishing a worldwide univocal identifier. For each certificate the value is:

- Electronic Office certificate (Medium level)

  2.16.724.1.3.5.1.2

- Electronic Seal certificate for automated administrative procedures (Medium level)

  2.16.724.1.3.5.2.2

- Public Employee (High level)

  2.16.724.1.3.5.3.1

Certificate	Mandatory "Administrative Identity" fields
ELECTRONIC OFFICE	• Type of certificate • Name of the subscriber entity • NIF of the subscriber entity • Descriptive name of the Electronic Office • Domain name or IP address
ELECTRONIC SEAL	• Type of certificate • Name of the subscriber entity • NIF of the subscriber entity • System or component denomination
PUBLIC EMPLOYEE	• Type of certificate • Name of the entity where is employed • NIF of the entity where is employed • DNI/NIE of the responsible • Given name • First surname • Second surname

Certificate	Optional "Administrative Identity" fields
ELECTRONIC OFFICE	• None
ELECTRONIC SEAL	• DNI/NIE of the responsible • Given name • First surname • Second surname • E-mail address
PUBLIC EMPLOYEE	• Personal identification number • E-mail address • Organizational unit • Position held

3.1.3 Meaning of the names

The certificate names are understood and interpreted in accordance with the law applicable to the names of natural and legal persons owners of the certificates.

The names on the certificates are treated according to the following rules:

- Names are encoded as they appear in the documentation. It may be chosen to use only uppercase letters for encoding.
- Tildes can be removed, to ensure the highest technical compatibility.
- Redundant blank characters between strings can be removed, as duplicates or those located at the beginning or end of strings, provided this will not make it difficult to interpret the information.
- Names can be adjusted and reduced, in order to ensure compliance with length limits applicable to each certificate field.

And specifically, for certificates of public employee, the following applies:

- It must indicate the name, as described in the DNI / NIE.
- It must indicate the first and second surname, separated only by a space, as described by the DNI / NIE. In the absence of the second surname, it will be left blank (no characters).
- It must indicate the number of DNI / NIE, along with the letter of control, as described in the DNI / NIE.
- It includes a mandatory symbol or character that separates the name and surnames of the ID number.
- It includes the literal *DNI* before DNI / NIE number.
- It includes a literal *AUTENTICACION* (authentication), *FIRMA* (non repudiation) or *CIFRADO* (encryption) that identifies the type of certificate. This identifier will always be at the end of the CN and in brackets. For certificates with medium level of assurance, if multiple profiles are grouped in a single certificate, this option is not included.

3.1.4 Use of anonymous and pseudonyms

They are not allowed.

3.1.5 Interpretation of name formats

The coding standards for the fields follow the recommendations of [IETF RFC 3280] and [IETF RFC 4630], using UTF-8.

The CSPM provides an extraction method for each of the individual data which, together, uniquely determine the identity of the owner and / or custodian of the electronic certificate. Specifically, for each type of certificate issued, the data provided will be:

- Public Employee Certificate[1]:
  - Description of certificate type.
  - Name of the subscriber.
  - First surname of the subscriber.
  - Second surname of the subscriber(optional in case of foreigners).
  - Personal identification number (e.g. DNI / NIE ...).
  - Name of the entity where the subscriber is employed.
  - Identification number of the entity where the subscriber is employed (e.g. NIF / CIF).
  - Destination unit to which the employee is assigned.
  - Title or job.
  - Email address.
- Electronic Office Certificate[2]:
  - Description of certificate type.
  - Descriptive name of the Electronic Office.
  - Domain name or IP address.
  - Name of the subscriber entity.
  - Identification number of the subscriber entity (eg. NIF/CIF).
- Electronic Seal Certificate[3]:
  - Description of certificate type.
  - System or component denomination.
  - Name of the subscriber entity.
  - Identification number of the subscriber entity (eg. NIF/CIF).

Additionally, in the types of certificates with correspondence in the reference document [EIFEBI], interpret the fields completed in the certificates as described in that document.

[1] Representation relationship is not admitted for this type of certificate.
[2] Representation relationship is not admitted for this type of certificate.
[3] Representation relationship is not admitted for this type of certificate.

3.1.6 Unicity of names

The names of the subscribers of certificates are unique for each certificate generation service operated by a Certification Entity and for each type of certificate, that is, a person may have different types of certificates issued by the same Certificate Authority.

He can also have certificates of the same type issued by different certification entities.

A subscriber name that is already in use, cannot be reassigned to a different subscriber.

3.1.7 Resolution of conflicts related to names

Certificate requesters will not include in the application any information that may involve a breach by the subscriber in the rights of third parties.

The Certification Entity does not determine that a certificate applicant is entitled to the name that appears in a certificate request.

Also, the Certification Entity does not act as an arbitrator or mediator, or any other way to resolve any dispute concerning the ownership of names of people or organizations, domain names or trade names.

The Certification Entity reserves the right to refuse a license application because of name conflict.

The name conflicts of certificate responsible, when they are identified in the certificate with his own name, will be solved by the addition, in the distinguished name, of the DNI number of the responsible or any other identification data assigned by the subscriber.

3.2 Initial validation of the identity

This section establishes the requirements for identification and authentication procedures that are used during the registration of certificate subscribers and responsibles, conducted prior to the issuance and delivery of the same.

3.2.1 Private key proof of possession

This section describes the methods used to prove the possession of the private key corresponding to the public key being certified.

The method of proof of possession of the private key is PKCS # 10 or the reliable procedure of delivery and acceptance of the secure signature creation device and the corresponding procedure of certificate download or other cryptographic proof or an equivalent procedure.

3.2.2 Authentication of organization identity

In all types of certificates issued to Public Administrations is necessary to identify the public administration, body or public entity. Therefore:

- No accrediting documentation is required for the existence of public administration, body or public entity.
- It is required the identity documentation of the responsible person acting on behalf of the Public Administration, body or public entity.

3.2.3 Authentication of the identity of an applicant

This section contains requirements for the verification of the identity of a natural identified in a certificate.

3.2.3.1 Required identification elements

The CSPM uses the following items, reflected in a statement signed by the certificate requester, to prove the identity of the same. For personal identification of the certificate holder, it will be requested:

- DNI, NIE or Passport to access the first name, the first and second surnames.
- The name of the entity to which the employee is assigned, where appropriate.

The CSPM keeps written or electronic prove of such identification including at least:

- The identity of the person making the identification.
- A signed statement from the person who performs the authentication to ensure that the subscriber identification has been performed as specified in the CPSM.
- The date of verification.

At the time of signing this declaration, the user accepts the terms of use of certificates and submits to the provisions of CPSM with regard to the conditions of use thereof.

3.2.3.2 Validation of the identification elements

The validation of the identification data in the certificate request is checked by contrasting the application information with the documentation provided, electronically or on physical media, by the corresponding Registration Entity.

3.2.3.3 Necessity of personal presence

Direct physical presence of the applicant is mandatory to obtain the following types of certificates:

- Public Employee Certificate (high level).

It is allowed identification without physical presence, based on administrative databases or existing certificates, for the following types of certificates:

- Electronic Office Certificate (medium level).
- Electronic Seal Certificate (medium level).

Thus, methods based on indirect physical presence are used, since the physical identity validation has occurred previously and ministry records are constantly kept updated.

It is guaranteed in any case, the delivery and acceptance of the certificate by the subscriber or by the responsible person of the certificate.

3.2.3.4 Relationship of the natural person with an organization

The relationship of the natural person with the Administration is done by checking official documents that ensure this linkage, such as BOE or takeover document or equivalent.

3.2.4 Subscriber's information not verified

No subscriber information is included in the certificates if it is not verified.

3.3 Identification and authentication of renewal requests

The certificates that have been revoked will not be renewed in any case, being necessary to proceed to a new application and validation of identity, in accordance with the provisions of Section 3.2.

3.3.1 Validation for periodical renewals

The CSPM does not allow periodical renewals of the certificates.

3.3.2 Validation for certificate renewal after revocation

The CSPM does not allow certificate renewal after its revocation.

3.4 Identification and authentication of revocation requests

The CSPM authenticates requests and reports relating to revocation of a certificate, verifying that come from an authorized person.

It is generally considered as sufficiently authenticated a revocation request signed with qualified certificates or equivalent. In the case of applications for personal certificate revocation, it is verified that the request comes from an internal email account of the ministry.

3.5 Authentication of a suspension request

The CSPM does not allow certificate suspension.

4 Operational requirements in the certificate lifecycle

4.1 Certificate issuance request

4.1.1 Legitimacy to request the issuance

Prior to the issuance and delivery of an Electronic Office, Electronic Seal or Public Employee certificate, there is a prior request made ex parte.

4.1.1.1 Specifications for Public Employee Certificates

The application for issuance of the certificate must be signed by the applicant who is required to prove his identity, according to the provisions of section 3.1 of this document. This entails the delivery of a unique secret code of the certificate (CEC) and delivery of the signature cryptographic device and associated passwords. The CEC, along with other authentication data, allows the generation of key pairs and the certificate download in the signature cryptographic device.

Along with the application, information is delivered with the following contents:

- Basic information on the type and use of the certificate, including in particular information about the Certification Entity and CPS applicable and their duties, powers and responsibilities.
- Information about the certificate and cryptographic device.
- Obligations of the certificate holder.
- Liability of the certificate holder.

These contents may be communicated indirectly indicating the URL where you can download the CPSM.

Estos contenidos podrán comunicarse de forma indirecta indicando la URL en la que puede descargarse la DPCM.

4.1.1.2 Specifications for Electronic Seal Certificates

The request must come from public employees. The applicant must include his data and those of the responsible person of the Certificate in the request for issuance of the certificate, being imperative the identification of the responsible person when collecting the certificate.

The head of the Certification Entity authorize the issuance of certificates of electronic seal after the resolution of the Undersecretary of the Ministry or the competent governmental headline published in the electronic office concerned.

In cases where the Certificate of Electronic Seal incorporates a body, proof of its identity must be done through administrative databases or other equivalent documents.

4.1.1.3 Specifications for Electronic Office Certificates

The request must come from public employees. The applicant must include his data and those of the responsible person of the Certificate in the request for issuance of the certificate, being imperative:

- Approval of the request by the management of the Certification Entity

- Identification of the person responsible for the safe delivery of the certificate.

4.1.2 Registry Procedure: responsibilities

The entity making the registry ensures that certificate applications are complete, accurate and properly authorized. Prior to the issuance and delivery of the certificate, the entity informs to the subscriber or to the responsible of the certificate of the terms and conditions applicable to the certificate. Such information is communicated in a durable medium, on paper or electronically, and in easily understandable language.

The application is accompanied by supporting documentation of identity and other circumstances of the applicant and the subscriber, in accordance with the provisions of Sections 3.2.2 and 3.2.3 of this document.

Registration functions may be performed by the CSPM or by an explicitly designated partner.

4.2 Processing the application

4.2.1 Specifications for Public Employee Certificates

In addition to the information contained in the application, the Certification Entity:

- Includes in the certificate the information provided for in Article 11 of Law 59/2003 (LFE), in accordance with the provisions of Section 7 of the CPSM.
- Ensures the date and time of issue of a certificate.
- Uses trustworthy systems and products which are protected against modification and ensure the technical security and, where appropriate, cryptographic of the certification processes that they support.
- Ensures that the certificate is issued by systems using anti-counterfeiting and when the Certification Entity generates private keys, ensures secrecy of the keys during the process of generating those keys.

4.2.2 Specifications for Electronic Office and Seal Certificates

Upon receipt of the application for a Certificate of Electronic Office / Seal, the Certification Entity reviews the information provided with special emphasis on the identity of the responsible of the certificate and the authorization to issue the same. If the information is incorrect, the Certification Entity denies the request. If the data are correct, the Certification Entity shall issue the certificate.

4.3 Certificate Issuance

4.3.1 Actions of the Certification Entity in the issuance procedure

The Certification Entity:

- Uses a procedure of download and generation of certificates that safely links the certificate to the registration information, including the certified public key.
- When the Certification Entity generates the key pair, uses a method of certificate generation that is linked safely with the key generation process and ensures that the

private key is delivered safely to the subscriber or the responsible person of the Certificate.

- Protects the confidentiality and integrity of the registration data, especially in the event that they are exchanged with the subscriber or the responsible person of the Certificate.
- Stores issued certificates with access permissions and security controls regulated and necessary for this, ensuring the security of communications.
- Does not store the private keys associated to the certificates.

Additionally the Certification Entity:

- Includes information on the certificate provided for in Article 11.2 of Law 59/2003 (LFE).
- Indicates the date and time the certificate was issued.
- Uses a management procedure for the secure signature creation devices that ensures that they are safely delivered to the subscriber or responsible person of the Certificate.
- Uses products protected from tampering, ensuring technical and cryptographic security of the certification processes that they support.
- Uses measures against forgery of certificates, and to ensure the secrecy of the keys during the process of generating the same.

4.3.2 Notification of issuance to subscriber

The approval of the application for certificates of public employee is communicated trough secure delivery of the certificate.

Otherwise, the Certification Entity notifies the applicant of the rejection of the application by mail, telephone or other means using the contact as reflected in the application.

4.4 Delivery and acceptance of the certificate

4.4.1 Responsibilities of the Certification Entity

In the case of Public Employee Certificates, the Certification Entity provides the subscriber access to the certificate through the application designed for this purpose that allows the generation of the key pair and download the certificate in the cryptographic device. To download the certificate is mandatory to use the CEC.

In the case of certificates or Electronic Seal or Electronic Office, the Certification Entity safely delivers the certificate. This delivery will occur after identifying the subscriber or responsible in person. Along with the certificate, information is delivered with the following contents:

- Basic information on the type and use of the certificate, including in particular information about the Certification Entity and CPS applicable and their duties, powers and responsibilities.
- Information about the certificate and cryptographic device, in case it exists.
- Obligations of the certificate holder.
- Liability of the certificate holder.

4.4.2 Certificate acceptance

The cryptographic device to house the certificate (if the certificate uses this) is accepted by signing the delivery form by Subscriber or, if applicable, by the person responsible of the certificate.

Certificates for Public Employee are considered accepted using a telematic mechanism to download the certificate. In the case of certificates whose key pair is generated in a secure signature creation device under sole control of the user, the user is deemed to accept the certificate by the downloading action on said device.

For Electronic Seal Certificates or Electronic Office Certificates, the certificate is deemed accepted by signing the delivery form by the responsible of the certificate.

4.4.3 Certificate publication

The identification data of the certificates are published in the internal repository without the prior consent of those responsible.

4.4.4 Notification of issuance to third parties

Not applicable.

4.5 Usage of the key pair and the certificate

4.5.1 General usage requirements

Certificates shall be used in accordance with its own function and purpose established, without being usable in other functions and other purposes. Similarly, the certificates will be used only in accordance with applicable law, especially considering the import and export restrictions in each moment.

The *Key Usage* extension is used to set technical limits to the uses that can be given to a private key corresponding to a public key listed in a certificate X.509 v3. However, it should be noted that the effectiveness of limitations based on extensions of certificates depends on occasion of the operation of software applications that have not been made, nor can be controlled by the CSPM Certification Entities.

Public Employee Certificates are used to create a secure electronic signature that meets the requirements of Article 24 of the LFE, the CPSM and the corresponding additional conditions.

4.5.2 Usage by the subscribers

Subscribers must:

- Protect their private keys at all times, as provided herein. In particular, subscriber of a certificate must be especially diligent in the custody of his secure signature creation device, in order to prevent unauthorized use.
- Report in due time, to the Certification Entity of CSPM which furnished the certificate, the suspected key compromise or loss. This notification shall be made directly or indirectly by the mechanisms provided in the CPSM.

If the subscriber generates its own keys, he must:

- Create, where appropriate, the keys within the secure signature creation device using an algorithm recognized as acceptable for electronic signature.
- Use algorithms and key lengths recognized as acceptable for qualified electronic signature.

4.5.3 Usage by a third party that relies on the certificates

It is the obligation of those third parties who rely on the certificates issued by a Certification Entity of the CSPM:

- Use the certificates for the purposes for which they were issued, as detailed in the certificate information (eg, defined in the extension Key Usage and Extended Key Usage).
- Check that each certificate being used is valid as defined in X.509 v3 and [IETF RFC 3280] standards.
- Establish trust in the Certification Entity that issued the certificate verifying the certificate chain according to the recommendations of the X.509 v3 and [IETF RFC 3280] standards.
- Use the certificates belonging to types defined in the LAECSP only for those transactions that are subject to that indicated in the LAECSP or CPSM.

4.6 Certificate renewal without key renewal

The CSPM does not allow certificate renewal without key renewal.

4.7 Certificate renewal with key renewal

The procedure applicable to the renewal of the certificate with key renewal involves the application for a new certificate with new keys associated.

4.8 Certificate modification

The Certificate Modification refers to the case where the attributes of the subscriber or those of the responsible of the certificate, not forming part of the unicity control provided for by the CPSM have changed. The CSPM does not allow modification of certificates.

4.9 Certificate revocation and suspension

The CSPM does not allow suspension of certificates.

4.9.1 Reasons for certificate revocation

A certification Entity of the CSPM will revoke a certificate for any of the following causes:

1. Circumstances that affect the information contained in the certificate:
    - Modification of any information contained in the certificate.
    - Discovery that any of the information provided in the certificate application is incorrect, as well as the alteration or change in circumstances verified for the issuance of the certificate.
    - Discovery that any of the information contained in the certificate is incorrect.
2. Circumstances that affect the security of the key or the certificate.
    - Compromise of the private key or infrastructure or systems of Certification Entity that issued the certificate, provided that affects the reliability of the certificates issued from this incident.
    - Breach by the Certification Entity, of the requirements of the certificate management procedures established in the CPSM.
    - Compromise or suspected compromise of the security of the key or of the subscriber's certificate or of the responsible person.
    - Access or unauthorized use, by a third party, of the subscriber's private key.
    - Irregular use of the certificate by the subscriber or the person responsible, or lack of diligence in the custody of the private.
3. Circumstances that affect the security of the cryptographic device:
    - Compromise or suspected compromise of the security of the cryptographic device.
    - Loss or damage of the cryptographic device.
    - Non authorized Access by third party to the activation data of the subscriber or responsible of the certificate.
4. Circumstances that affect the subscriber or the responsible of the certificate:
    - Termination of the relationship between the Certification Entity and the certificate subscriber or responsible.
    - Modification or termination of the underlying legal relationship or what caused the issuance of the certificate to the subscriber or responsible person of the Certificate.
    - Breach by the applicant of the certificate of the established requirements in the certificate application.
    - Breach by the subscriber or responsible of the certificate obligations, liabilities and guarantees established in the legal instrument or CPSM.
    - The death or supervening incapacity of the certificate subscriber or responsible.
    - Subscriber application for certificate revocation in accordance with the provisions of section 3.4 of the CPSM.
5. Other circumstances:

- The termination of the Certifying Entity service, in accordance with the provisions of section 5.8 of the CPSM.
- Other justified reasons.

The legal instrument that binds the Certification Entity with the Subscriber states that the Subscriber should request the revocation of the certificate in case of having knowledge of any of the circumstances listed above.

4.9.2 Legitimacy to request the revocation

Revocation request of a certificate can be made by:

- The subscriber in whose name the certificate was issued.
- A legally authorized representative by the responsible or the subscriber of the certificate.
- The Registration Entity that requested the issuance of the certificate.
- Anyone with knowledge of one or more of the causes for revocation, as indicated in paragraph 4.9.1.

4.9.3 Procedures for revocation request

To request the revocation of certificates, the Certification Entity takes into account the following rules.

The revocation of a certificate should be sent to the Certification Entity or, where appropriate, to the Registration Entity that approved the application for certification, providing the following information:

- Date of revocation request.
- Subscriber Identity.
- Detailed reason for the revocation request.
- Name and title of the person requesting the revocation.
- Contact details of the person requesting the revocation.

Where immediate revocation of the certificate is required, an email will be sent to the Certification Entity or, where appropriate, to the Registration Entity. Contact details will be given in the appropriate section of the CPSM. It will be possible for subscribers to electronically revoke certificates.

The request will be authenticated by the recipient, according to the requirements of the relevant section of the CPSM, prior to the revocation. The revocation request will be processed upon receipt.

- In the event that the recipient of the application is the Registration Entity, once authenticated the request, will issue a request for revocation of the certificate to the Certification Entity.
- The Certification Entity prior to revocation must verify the authenticity of the request. It Is at its discretion to carry out verification measures of the reasons for revocation. If the revocation request is valid in form and sufficient reasons, the Certification Entity issuing the certificate will revoke it, publishing its serial

number and other identifying information in the CRL. The Certification Entity cannot reactivate the certificate once revoked.

4.9.4 Term for revocation request

Revocation requests shall be sent as soon as the cause of revocation is known.

4.9.5 Maximum delay for revocation request processing

Revocation request will be processed in the shortest time possible, always within the working hours of the Certification Entity.

4.9.6 Obligation to consult the certificate revocation information

The verifier shall check the status of those certificates on which he wish to trust.

The Certification Entity of the CSPM shall make available to verifiers a service of certificate status information based on the OCSP protocol and, at least, another way to access and download the certificate revocation lists (CRL). These methods will be operational for all existing platforms at no extra cost.

The services of certificate revocation status verification offered by the CSPM (supported in the area of AGE) will not necessarily require the signature of any agreement by the Public Administration to use them.

4.9.7 Frequency of CRL emission

In each certificate is specified the address of the corresponding CRL, using the *cRLDistributionPoints* extension.

The Certification Entity shall issue a CRL daily even when there are no changes or updates, to ensure the validity of published information. In the published CRL it will be indicated the scheduled time for the issuance of a new CRL.

4.9.8 Maximum delay on CRL publication

The state change of the validity of a certificate will be indicated in a CRL in less than five minutes elapsed from the occurrence of such change.

4.9.9 Availability of certificate revocation status services

Verifiers may retrieve certificates published in the Repository of the Certification Entity, through OCSP or CRL.

The CSPM ensures a level of service, ensuring the availability of all the certification services that offers, in particular those of certificate validity status information.

The information services of the state of the validity of the certificates are available 24 hours a day 7 days a week, 365 days a year. The CSPM is committed to provide a level of service for these services at least 99%.

4.9.10 Obligation to consult the certificate revocation status services

The verifier shall check the status of those certificates on which he wish to trust.

If for any reason it was not possible to obtain information on the status of a certificate, the system that needs to use it will reject its use or, based on the risk, the degree of responsibility and the consequences that could occur, use it without guaranteeing its authenticity in the terms and standards set out in the CPSM.

The CSPM will indicate in its certificates the mechanisms with open public access to its certificate status information services through the following methods:

4.9.10.1 CRL Emission

The CRL issuance is made in full mode, indicating that fact inside the certificates by the use of *Distribution Points* extension of the CRL (cRLDistributionPoints) defined in IETF Technical Specification 32801, as follows:

- It will include at least one distribution point CRL, two distribution points could be included, pointing to separate servers.
- Said CRL Distribution Point will contain the name of the CRL location.

The location of the CRL is in Annex C.

The location of the historic CRLs is in Annex C.

4.9.10.2 OCSP Protocol

The CSPM provides certificate status verification via OCSP, indicating that fact inside the certificates, using the extension *AuthorityInfoAccess* defined in technical specifications [IETF RFC 5280] and [RFC 2560], as follows:

- Access description will be included, indicating the OID reserved for OCSP service access and the URL where the OSCP server is located.

The location of the OCSP service is in Annex C.

4.9.11 Other ways for certificate revocation information

The CSPM has no other ways of information about certificate revocation.

4.9.12 Special requirements in case of private key compromise

The compromise of the private key of a Certification Entity of the CSPM will be notified to all the participants through official media or general broadcast.

4.10 Services for certificate revocation status checking

4.10.1 Operational characteristics of the services

The CRL can be downloaded from the repository of the Certification Entity and will be installed by the verifiers. Verifiers may also check the status using OCSP.

4.10.2 Service availability

The information services of the state of the validity of the certificates are available 24 hours a day 7 days a week, 365 days a year. The CSPM is committed to provide a level of service for these services at least 99%.

In case of failure of systems checking certificate status for reasons beyond the control of the Certification Entity, it will try to have this service unavailable the shortest time.

4.10.3 Other characteristics

Not stipulated.

4.11 Finalization of certificates validity

The extinction of the validity of a certificate occurs in the following cases:

- Early revocation of the certificate for any of the reasons set out in this document.
- Expiration of the validity of the certificate.

If there is no request for certificate renewal, termination of its validity shall mean that the termination of the relationship between the subscriber and the Certification Entity.

5 Controls of physical security, management and operations

5.1 Physycal security controls

The CSPM has facilities that protect physically the provision of the services of certificate generation and revocation management caused by unauthorized access to systems or data. Cryptographic modules are protected against loss and unauthorized use.

The CSPM has physical and environmental security controls to protect the the resources of the facilities where the equipment used for the provision of the indicated services are located. Physical protection is achieved through the creation of clearly defined security perimeters around the indicated services.

Physical and environmental security policy applies to the provision of the services listed below and establishes requirements for the following contingencies, which are documented in the CPSM succinctly:

- Burglary and unauthorized entry.
- Unauthorized output of equipment, information, media and applications relating to components used for the services of the CSPM.
- Fires and floods and other natural disasters.
- Collapse of the structure.
- Failure of support systems (electricity, telecommunications, etc.).

5.1.1 Location and construction of the installations

The location of the installations allows the presence of security forces in a reasonably short term after an incident is reported to them. The CSPM has at its disposal security personnel of the Ministry at the premises.

The quality and strength of the materials of construction of the facility ensures adequate levels of protection against intrusion attempts by force.

5.1.2 Physical access

The CPSM delegates physical access controls in the Security Area of the Ministry and in the SGTIC.

The CSPM establishes multiple levels of access restriction to the different defined perimeters and physical barriers.

For access to the premises of CSPM where processes related to the life cycle of the certificate are carried out, it is required prior authorization, identification at the time of access and registration thereof, including filming for CCTV and archiving.
The identification at the access control system is performed by the recognition of some individual's biometric parameter, except for escorted visits.

Cryptographic key generation of the Certification Entity and its storage was performed in specific units for these purposes and requires dual access and permanence (at least two people simultaneously).

In any case, machines and platforms listed in the CPSM and corresponding to certification systems are conveniently labelled for identification and placed in the data centre under the applicable safety criteria for the unit referred above.

The possession and custody of the keys to access the cabinets that house the system platforms is exclusive to SGTIC staff.

The complete system of root CA is the responsibility of the Undersecretary of the Ministry and is located in its facilities of security.

5.1.3 Electricity and air conditioning

The computers of the CSPM are adequately protected from fluctuations or power failures that could harm them or disrupt service.

The facility has a system of stabilization of the current, as well as its own generator with sufficient autonomy to maintain the power supply as long as required to complete an orderly shutdown of all systems.

The computers of the CSPM are located in an environment that ensures climate (temperature and humidity) suitable for optimal working conditions.

5.1.4 Exposure to water

The CSPM possesses flooding detection systems in place to protect the equipment and assets for this eventuality.

5.1.5 Fire alarm and protection

All the facilities and assets of the CSPM have automatic systems for fire detection and fire fighting.

Specifically, the cryptographic devices and containers that store the CSPM keys, have a specific and additional system to the rest of the installation for fire protection.

5.1.6 Media storage

The storage of information media is performed in a way that ensures both confidentiality and integrity, according to the classification of the information set. To this end it has fireproof cabinets. Access to these media, including for disposal, is restricted to persons specifically authorized.

5.1.7 Waste disposal

The removal of media, both magnetic and paper, is performed by mechanisms that guarantee the impossibility of recovering the information. In the case of magnetic media, will be formatting, permanently erased, or physical destruction of the media. For paper documents, it is subjected to a physical treatment of destruction.

5.1.8 Backup outside the facilities

The CSPM monthly stores a backup of information systems, in offices physically separated from those in which the systems are.

5.2 Procedure controls

Staff at the service of the CSPM performs administrative and management procedures in accordance with the provisions of the CPSM.

5.2.1 Reliable functions

The CSPM identifies in its security policy, functions or roles with the condition of reliable. The reliable functions include:

- Personnel responsible for security.
- System Administrators.
- System Operators.
- System Auditors.

The reliable functions identified, and their associated responsibilities are documented and succinctly described herein.

Administrators of the Certification Entity will be solely and exclusively personnel of the SGTIC designated for that purpose, and they cannot, in any way, assume simultaneously roles that are defined as exclusive. The main functions of the Certification Entity administrators are as follows:

- Life cycle management of key pairs of the CSPM.
- Supervision of the initialization of the elements that make up the Certification Authority.

Operators of the Certification Entity will be solely and exclusively personnel of the SGTIC designated for that purpose, and they cannot, in any way, assume simultaneously roles that are defined as exclusive. The main functions of the Certification Entity operators are as follows:

- The generation and revocation of certificates.
- Performing backups of their operation data.
- The functions related to the maintenance of its operations, such as the publication of the CRL and the maintenance of the root CA.
- The management of cryptographic hardware modules.

Registry operators will be personnel the Undersecretary. Registry operators perform and have responsibility for the proper execution of the following actions:

- Verify the identity with the mechanisms and procedures allowed in the CPSM.
- To record correctly the identity of subscribers after verification.
- Brokering communication requests and responses between the Certification Entity and the subscribers.
- Receive and distribute certificates of subscribers.

The Certification Entity may be operated by third party personnel contracted for this purpose for reasons of support and maintenance and approved by the head of the SGTIC.

Any operation on the entity must be authorized in advance and in writing stating an official belonging to SGTIC that has to ensure reliable operation.

The personnel responsible for security has as its main task to ensure the implementation of the actions necessary for compliance with the security measures described in this document.

System auditors will evaluate the degree of compliance with the requirements of the certification operation established in the CPSM.

5.2.2 Number of persons by task

There is a separation of sensitive functions, as well as granting of least privilege where possible. To determine the sensitivity of the function, the following elements are taken into account:

- Duties associated with the function.
- Access level.
- Function monitoring.
- Training and awareness.
- Skills needed.

5.2.3 Identification and authentication for each function

The CSPM identifies and authenticates the personnel before accessing the corresponding reliable function. All roles of the Certification Entity may be identified using electronic certificates issued by the own Entity of Certification.

5.2.4 Roles requiring dual presence

The following tasks are performed at least by two persons:

- Management of cryptographic equipment.
- Generation of certificates of the Certification Entity.

5.3 Personnel controls

5.3.1 Requirements on background, qualifications, experience and authorization

The CSPM employs personnel qualified and with the necessary experience to provide the services offered in the field of electronic signature and the adequate procedures of security and management. This requirement applies to CSPM management staff, especially regarding safety procedures. The qualification and experience are complemented by appropriate learning and training.

The personnel in reliable positions is free of personal interests that conflict with the development of the role that has been entrusted.

The CSPM will not assign to any reliable or management position to a person who is not suitable for the job, especially for having been convicted of crime or offense concerning their suitability for the job.

5.3.2 Background verification procedure

The CSPM will contrast or request the relevant factors that demonstrate the accuracy of the information contained in the curricula of the people hired referred to in the previous paragraph.

5.3.3 Qualification requirements

The PSCM will train personnel occupying management and reliable positions, until they reach the necessary qualifications, in accordance with section 5.3.1 of the CPSM.

Training should include the following contents:

- Principles and mechanisms of security of the Certification Entity as well as the user environment of the person to be formed.
- Versions of systems and applications in use.
- Tasks to be performed by the person.
- Management and processing of security incidents and commitments.
- Procedures for business continuity and emergency.

5.3.4 Requirements and frequency of knowledge update

The CSPM will perform an update on staff training at least every two years.

5.3.5 Sequence and frequency of personnel rotation

The CSPM may determine methods of job turnover for service provision in shifts, in order to meet the needs of the service 24x7.

5.3.6 Sanctions for unauthorized actions

The CSPM has a disciplinary system to debug the responsibilities arising from unauthorized actions, which is appropriate to the applicable labor legislation and, in particular, coordinated with the disciplinary system of the collective agreement or other regulation that is applicable to staff. Disciplinary actions include suspension or firing of the person responsible for the harmful action.

5.3.7 Requirements for external professional recruitment

The CSPM may hire external professionals occasionally for any function, even for a reliable place, in which case they must submit to the same controls as the other employees.

In the event that the professional does not need to undergo such checks, he will be constantly accompanied by authorized personnel, when in CSPM facilities.

5.3.8 Delivery of documentation to personnel

The CSPM provides the documentation strictly required by its personnel at all times, in order to be sufficiently competent.

5.4 Security audit procedures

5.4.1 Types of registered events

The CSPM keeps registry of, at least, the following safety-related events from the entity:

- Power on and off of the systems
- Start and completion of the implementation of the certification authority or the central registration authority.
- Attempts to create, delete, change passwords and user permissions within the system.
- Generation and changes in CSPM keys.
- Changes in certificate issuance policies.
- Attempts to entry and exit of the system.
- Unauthorized attempts to access CSPM network.
- Unauthorized attempts to access the system files.
- Writing and failed attempts to write in the certificate repository.
- Events related to the lifecycle of the certificate, such as application, issuance, revocation and renewal of a certificate.
- Events related to the life cycle of the cryptographic module, including reception, use and uninstallation of the same .
- Other events collected by the Log systems of the certification authority or registration authority, including system administration tasks.
- Other events collected by the Database log systems.
- Other events collected by the cryptographic modules log system.

The CSPM stores, manually or electronically, the following information:

- The key generation ceremony.
- Physical access logs.
- Maintenance and configuration changes of the systems.
- Changes in personnel.
- Reports of security incidents.
- Records of the destruction of material containing key information, activation data or personal information.
- Possession of activation data for operations with the private key of CSPM.

5.4.2 Processing frequency of audit records

Audit records are reviewed at least once a week in search of unusual or suspicious activity.

Processing audit records is done by reviewing records, verifying that they have not been tampered, a brief inspection of all log entries and further investigation of any alerts or irregularities in the logs.

The actions taken after the audit review are also documented.

5.4.3 Conservation period of audit records

Audit records are stored on the premises for at least two months after processing and thereafter archived in accordance with section 5.5.2 of the CPSM.

5.4.4 Protection of audit records

Log files, both manual and electronic, are protected from readings, modifications, deletions or any other unauthorized handling with controls using logical and physical access.

The entity that carries out the processing of the audit logs has no capacity to modify the records. There are procedures to ensure that they can not remove or destroy the records of events before the expiration of his storage term.

5.4.5 Backup procedures

At least two incremental backup copies of audit logs are generated daily and full backups weekly.

5.4.6 Cumulative system of audit records

The accumulation system of audit log consists of the application and network logs and the records of the operating system, in addition to manually generated data that is stored by authorized personnel.

5.4.7 Audit event notification to event originator

Cuando el sistema de acumulación de registros de auditoría registra un evento, no es preciso enviar una notificación al que causó el evento. Se comunica si el resultado de su acción ha tenido éxito o no, pero no que se ha auditado la acción.

5.4.8 Vulnerability analysis

The CSPM controls any attempted violation of the integrity of the certificates management system, including equipment that supports it, physical locations and personnel assigned to its operations.

Vulnerability analysis are performed, reviewed and revised through an examination of these monitored events. These analyzes are performed daily, monthly and annually in accordance with the Audit Plan or document replacing it from the CSPM.

5.5 Information archiving

The CSPM ensures that all information relating to certificates is maintained for a period of time appropriate, as set out in section 5.5.2 of the CPSM.

5.5.1 Types of registered events

The CSPM stores all events that occur during the life cycle of a certificate and record the operations performed by the system in the process of these events.

5.5.2 Conservation period of records

The CSPM archives the records specified in the previous section of this document without loss over a period of 15 years minimum.

5.5.3 Archive protection

The CSPM:

- Maintains the integrity and confidentiality of the file containing the data included in issued certificates.
- Archive the above statements completely.

5.5.4 Backup procedures

The CSPM performs daily incremental backups of its electronic documents. Also conducts weekly full backups.

Additionally, records are kept on paper in a place outside the premises of the provider itself for data recovery cases in accordance with section 5.7 of the CPSM.

5.5.5 Time stamp requirements

The CSPM issues the certificates and CRLs with reliable information of date and time. This date and time information is not signed electronically.

The servers that issue certificates and CRLs are synchronized every hour with an external server, which in turn is synchronized with the time server of the Ministry of Public Administration.

5.5.6 Archival system localization

The CSPM has a maintenance system of archival data outside its own premises.

5.5.7 Procedures to obtain and verify archive information

Only authorized personnel have access to archived data, whether in the same premises of CSPM or external location. In particular, it will be recorded any access or attempt to access audit data.

5.6 Renewal of Certification Entity key

Not applicable.

5.7 Key compromise and disaster recovery

5.7.1 Corruption of resources, applications or data

When there is an event of corruption of resources, applications or data, the necessary arrangements will be taken, in accordance with the Security Plan and Business Continuity Plan, to return the system to normal operation.

5.7.2 Revocation of Certification Entity public key

In the event that the CSPM revokes its Certification Entity for any of the reasons stated in the CPSM, it will perform the following:

- Inform of that fact by publishing a CRL.
- Make every effort to report the revocation to all subscribers as well as to third parties who rely on these certificates.
- Where appropriate, notify the competent body of the AGE.

5.7.3 Compromise of Certification Entity private key

The Business Continuity Plan of the CSPM considers the compromise or suspected compromise of its private key as a disaster. In case of compromise, it will carry out at least the following actions:

- Make every effort to inform the compromise to all subscribers and verifiers.
- Indicate that certificates and revocation status information that have been delivered using the CSPM key are no longer valid. For this, the following steps will be executed:
    - CSPM certificate revocation.
    - Corresponding CRL publishing.
    - Massive Revocation of the Certificates generated by the Certification Entity, proceeding to their elimination by the mechanisms implemented in the system for that purpose.

5.7.4 Disaster on installations

The set of systems that make up the Certification Entity is deployed in conditions of high availability and redundancy in each and every one of the components that comprise it. This will ensure the continuity of services against the fall of any of its components.

Additionally, the CSPM has a backup or disaster recovery center, which continues such services in case of a disaster or maintenance of the facilities that house the primary system.

The backup center offers physical security protections detailed in the corresponding Security Plan.

The CSPM develops, maintains, tests and, if necessary, will execute its Business Continuity Plan. This plan sets out how to restore the services of the information systems in the event of a disaster on the premises.

The CSPM is able to restore normal operation of services of revocation within 24 hours of the disaster, being able to run at least the following actions:

- Where applicable, certificate revocation.
- Publication of revocation information.

The backup database used is synchronized with the production database, within the time limits specified in the Business Continuity Plan of the CSPM.

5.8 Service termination

The CSPM will minimize potential disruptions to subscribers and third parties as a result of the termination of its services as a provider and, in particular, will ensure continued maintenance of records required to provide evidence of certificates issued and other services offered, in case of civil or criminal investigation. Before stop operating, the CSPM will follow these procedures in accordance with art. 21 of the LFE:

- Must notify it to the signatories using electronic certificates issued by the CSPM and applicants for certificates issued in favor of legal persons, and may transfer, with their express consent, the management of the ones that are still valid on the date on which cessation occurs to another certification service provider that assume them or otherwise terminate its validity. This communication will take place with a minimum advance of two months before the effective end of the activity and inform, if any, on the characteristics of the proposed provider to the transfer of management of certificates.
- In the event that the CSPM had issued electronic certificates to the public, the CSPM will communicate to MINETUR, with the time indicated in the previous point, the cessation of its activity and the destination it will give to its certificates, specifying, where appropriate , if it is transferring the management and to whom or terminate its validity. It will also notify any other relevant circumstances that may prevent the continuation of its activity. In particular, communicate, upon becoming aware of it, the opening of any bankruptcy proceedings against it.
- The CSPM will forward to MINETUR, prior to termination of its activity, the information on electronic certificates whose validity has been extinct, for it to take over custody for the purposes of the provisions of Article 20.1.f LFE. The MINETUR will keep publicly accessible a specific consultation service where bearing an indication on these certificates for a period deemed sufficient in terms of searches made to the same.
- Execute the necessary tasks to ensure the obligations of maintenance of the registration information and event log files for the respective periods, as indicated to subscriber and third parties who rely on the certificates.

- Destroy its private keys.

6 Technical security controls

The CSPM uses trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the certification processes that they support.

6.1 Generation and installation of the key pair

6.1.1 Key pair generation

For the generation of the key root of the hierarchy of the CSPM a procedure was conducted according to the key ceremony inside the high security perimeter, specifically designed for this task.

Key pairs of the root certification authority were generated in a cryptographic module with FIPS 140-2 level 2 and 3. The key pairs for Validation Entities, time stamping and registration authorities were generated on secure servers.

The key pairs of the remaining certificates are generated according to the following table:

CERTIFICATE	LEVEL	GENERATION METHOD
PUBLIC EMPLOYEE	High	Key generation by the user inside cryptographic card.
ELECTRONIC OFFICE	Medium	Key generation by the CSPM and delivery in PKCS#12 format (software support). • Key generation using software. It implies that the user uses these keys in secure software container. Key generation by the requester in PKCS#10 format (software support). Delivery of the certificate in PKCS#7 format. • Key generation by the user, using software.
ELECTRONIC SEAL	Medium	Key generation by the CSPM and delivery in PKCS#12 format (software support). • Key generation using software. It implies that the user uses these keys in secure software container. Key generation by the requester in PKCS#10 format (software support). Delivery of the certificate in PKCS#7 format. • Key generation by the user, using software.

The secure devices can be cryptographic cards, cryptographic USB tokens, or any other type of device, in particular cryptographic modules (HSM), which comply with the safety requirements established by current regulations for secure devices.

6.1.2 Private key delivery to the subscriber

In the case of Public Employee Certificates the private key is generated directly in the cryptographic device that complies with [CWA 14169].

In the case of Certificates with software support:

- If the certificate private key is generated by the Certification Body, is delivered properly protected through a PKCS # 12.
- If not, the generation is done by the subscriber, not existing therefore subsequent delivery of the key.

6.1.3 Public key delivery to the certificate issuer

The public keys of Public Employee Certified are generated by certificate issuer itself, obtaining a copy of the same at that moment.

The method of transmission of the public key to the CSPM is the standard format PKCS # 10, another cryptographically equivalent test or any other method approved by the AGE. No private key escrow is made in any case.

6.1.4 Distribution of the Certification Service Provider public key

The public key of the CSPM must be communicated to third parties that rely on the certificates, ensuring the integrity of the key and authenticating its origin. The public key of the CSPM is published in the repository, in the form of self-signed certificate, together with the CPSM ensuring that the key authenticates the CSPM. Users can access the repository to get the public keys of the CSPM.

Relying parties should establish additional measures to verify the validity of the self-signed certificate, verifying the certificate digital fingerprint.

Additionally, in applications S / MIME, the data message may contain a certificate chain, thus being distributed to users.

6.1.5 Key sizes

The CPSM uses the security scenario defined in [EIFE], which determines the strength and viability criteria applicable to each certificate profile. The two levels of assurance contained in the CPSM are considered within this scenario.

The specifications listed below follow technical specification [ETSI TS 102 176-1]. Different cryptographic requirements are considered for the issuing authorities and institutions or final certificates. His application is differentiated in a higher and medium level of assurance.

- Issuing authorities:

Assurance level	Entity	Algorithm and minimum length
High	Root CA	RSA-4096
High	Subordinate CA	RSA-2048
Medium	Root CA	RSA-2048

Medium	Subordinate CA	RSA-2048

- Final entities:

Assurance level	Entity	Algorithm and minimum length
High	Final certificates	RSA-2048
Medium	Final certificates	RSA-1024

6.1.6 Generation of public key parameters

The public key parameters are generated in accordance with PKCS # 1, using as the second public key argument, FERMAT 4, ie, the 4 th Fermat number ([4]).

6.1.7 Quality test of public key parameters

The quality of the parameters is guaranteed, for the Root Certification Authority keys, by the cryptographic module accredited [FIPS 140-2] Level 2 and 3, and with ongoing accreditation [CC EAL4 +].

6.1.8 Key generation in software or hardware systems

The random numbers necessary for generation of keys associated with high level certificates are generated in cryptographic devices, either cryptographic cards or HSM modules. The keys associated with the certificates of CSPM are generated in cryptographic hardware modules that meet the agreed security certification levels.

The keys associated with the Public Employee Certificates are generated in cryptographic devices that meet the agreed security certification levels.

Key generation for the other types of certificates is done by computer applications.

6.1.9 Key usage

Certificate extensions *KeyUsage* and *Extended KeyUsage* indicate the permitted uses of the corresponding private keys and associated certificates.

The key usages permitted by CPSM are normalized following the proposal made by AGE under the LFE and the LAECSP, according to the type and profile of each certificate.

Additionally, the level of insurance under which a certificate is issued, determines the permitted use of the keys as follows:

[4] The n-th Fermat number is F = (2)^(2^n)+1.

CERTIFICATE	KEYUSAGE	EXTENDED KEYUSAGE
PUBLIC EMPLOYEE (Authentication, High Level)	Digital Signature	Email Protection, Client Authentication
PUBLIC EMPLOYEE (Non repudiation, High Level)	Content Commitment	Not Used
ELECTRONIC OFICE	Digital Signature, Key Encipherment	Server Authentication
ELECTRONIC SEAL	Digital Signature, Content Commitment, Key Encipherment, Data Encipherment	Email Protection, Client Authentication

This normalizes the use of keys, setting the following conditions:

- Strict compliance with the recommendations of [ETSI TS 102 280] for certificates that are issued to natural persons in safe device (Certificates of Public Employees) and obliges to implement a model based on three separate certificates.
- For all other certificates, the key usage and, where appropriate, extended key usage, will be assigned according to RFC standards applicable. This option is applicable for certificates that are not issued to natural persons (Electronic Office and Electronic Seal).

6.2 Private key protection

6.2.1 Standards for cryptographic modules

The module in use to generate root CA private keys and sign the certificates, is accredited [FIPS 140-2] Level 2 and 3 and ongoing accreditation [CCEAL4 +].

The implementation of each Certification Entity, considering that cryptographic security modules (HSM) are used, includes the following tasks:

- Initializing the HSM module status.
- Creation of the cards for Administrator and Operator.
- Generation of the keys of the Certification Entity.

For cryptographic cards approval [CCEAL4 +] applies, meeting the requirements of Article 24 of LFE as secure signature device creation.

All secure signature creation devices described here (HSM and cryptographic cards):

- Provide the highest levels of security for issuing and storage of electronic certificates, meeting the technical specification [CWA 14167], parts 1 and 2.
- Provide the highest guarantees as secure signature creation devices, fulfilling the protection profiles established in the technical specification [CWA 14169].

All components mentioned above support the PKCS # 11 standard and, in the case of cryptographic cards, Microsoft CSP.

6.2.2 Control by more than one person of the private key

Access to the operation of the private key of the Certification Entity is subject to a secure authentication process, being further guarded by secure cryptographic devices (HSM).

The private key of the CSPM root CA is under multipersonal control. This is activated by the initialization of the Certification Entity software by the minimum combination of operators of the corresponding AC. This is the only method of activation of said private key. Requires two operators, out of a total of five, to activate and use the private key of the root certification entity.

The custody of the private keys of other certificates is done by the holders themselves. Access to private key is protected by a PIN. In this case access will be made by a single person: The certificate responsible person.

6.2.3 Private key storage in the cryptographic module

Private keys of the CSPM Root Certification Authority were generated directly in the cryptographic modules during key generation ceremony being stored in encrypted files with fragmented keys and smart cards which can not be extracted. These cards were used to introduce the private key in the cryptographic module.

For Certificates of Public Employees, the keys were generated directly and locally by the cryptographic device.

6.2.4 Private key activation method

The private key of the Certification Entity is activated by running the startup procedure for secure cryptographic module by the persons listed in section 6.2.2.

The private key of each subscriber is activated by entering the PIN on the cryptographic device or signature software.

6.2.5 Private key deactivation method

In the case of the certificates of the CSPM Root Certification Authority, disabling the private key occurs by removing the persons listed in section 6.2.2 its operator or administrator cards as appropriate.

For certificates stored in cards considered secure signature creation device, when it is removed from the reader device or when the application that uses the session ends, it is necessary to enter again the PIN.

6.2.6 Private key destruction method

Private keys are destroyed so as to prevent theft, modification, unauthorized disclosure or unauthorized use.

For Cryptographic Modules (HSM), the keys will be erased by the process of setting factory mode, which ensures total and safe reset of the key. In the CPSM it is excluded any other method than those that implements the module.

In the case of cryptographic cards, the keys are removed by wiping the device using the device management application.

6.3 Custody, copy and recovery of keys

6.3.1 Policy and practices of custody, copy and recovery of keys

Private keys of the Certification Entity of CSPM are stored in fireproof areas and protected by dual physical access controls. The custody of the private key set of root certification entity, generated and contained in the cryptographic module takes place in SGTIC physically and logically. Access requires a multiple authentication process based on cryptographic card.

The custody of the private key set of other components such as time stamping or validation takes place in SGTIC physically and logically. Access requires an authentication process.

The custody of the private key for the other types of certificates, regardless of the supporting device, it is the responsibility of the subscriber accessing the same via PIN or secure password.

The private key of the root certification entity of the CSPM has a backup copy stored in a separate area from where it usually is located and must be retrieved, if necessary, by personnel subject to the trusted personnel policy. The personnel shall be expressly authorized for such purposes. At all times there is a hardware backup copy of the keys of the Root Certification Entity being reviewed every year. When keys are stored in a dedicated processing hardware module, the appropriate controls are provided so that they can never leave the device.

Security controls to be applied to of the CSPM backups are of equal or higher level than those usually applied to the keys in use.

In the case of other certificates, under any circumstances the private keys used for non-repudiation services are stored by third parties: only subscribers will guard the only copy of this key in cryptographic module or equivalent. Only in cases where exists the recovery service of private key, for purposes other than non-repudiation, these keys can be stored.

6.3.2 Private key archival

Private keys of the CSPM Certification Entities are archived at the end of its period of operation, permanently. Private keys of other types of certificates are not archived.

6.4 Other aspects on key pair management

6.4.1 Public key archival

The CSPM archives its public keys, according to the provisions of section 5.5 of the CPSM.

6.4.2 Usage period of public and private keys

Periods of use of the keys are determined by the duration of the certificate, after which they cannot continue to be used.

6.5 Activation data

6.5.1 Generation and installation of the activation data

For the establishment of a Certification Entity cryptographic cards must be created, used for recovery and functioning activities. The CSPM Certification Entity operates with two types of roles, each one with its corresponding cryptographic cards:

- The administrator card set. These cards will be needed to restore the state of the HSM if a disaster occurs or if you want to move the keys to another module.
- The operator card set. These cards will be used to protect the keys of the Certification Entity. There must be a minimum of operators present and they must indicate the PIN of their respective cards to perform any operation with the Certification Entity, whether or not involving the use of keys.

If one or more cards are lost or damaged, or the administrator forgets his PIN or are no longer usable for any reason, the whole set of cards must be re-generated as soon as possible using all security cards.

When the CSPM provides the subscriber a secure signature creation device, device activation data (PIN), are generated securely.

6.5.2 Protection of the activation data

Only authorized personnel, in this case the operators and administrators of the Certification Entity, possess the cryptographic cards that have activation capability for the Certification Entities and know the PIN and passwords to access the activation data.

When the CSPM facilitates to the subscriber the secure signature creation device, the Subscriber is solely responsible for creating data activation of the same. No subscriber should disseminate for any reason, nor store in any support, the activation PIN of his personal cryptographic card or equivalent activation data.

6.6 Informatics security controls

6.6.1 Specific technical requirements on informatics security

It is guaranteed that access to the systems is limited to duly authorized persons. Particularly:

- The CSPM ensures effective management of the access level of users (operators, administrators, and anyone with direct access to the system) to maintain system security, including user account management, auditing of modifications or denied access.
- The CSPM ensures that access to information systems and applications is restricted according to the provisions of the access control policy and that systems provide adequate security controls to implement segregation of duties identified in the practices of the provider, including the separation of management functions of the

security systems and operators. Specifically, the use of system utility programs is restricted and tightly controlled.

- The personnel of the provider is identified and recognized before using critical applications related to the life cycle of the certificate.
- The personnel of the provider is responsible and can justify their activities, for example using an event log.
- It must be avoided the possibility of disclosing sensitive data due to reusing storage objects (eg deleted files) that are accessible to unauthorized users.
- The safety and monitoring systems allow rapid detection, recording and action against irregular or unauthorized access attempts to its resources (e.g. by intrusion detection system, monitoring and alarm).
- Access to public repositories of information of the provider (for example, certificates or revocation status information) has an access control for modification or deletion of data.

6.6.2 Evaluation of the informatics security level

The applications of the certification and registration authority used by the CSPM are reliable and should accredit this condition, for example, by a product certification against an appropriate protection profile according to [ISO 15408], or equivalent.

6.7 Lifecycle technical controls

6.7.1 System development controls

Special attention will be paid to safety requirements during the phases of design and specification of requirements of any component used in applications of Certification and Registration, to ensure that systems are safe.

Change control procedures are used for new releases, updates and patches, emergency of such components.

6.7.2 Security management controls

The CSPM maintains an inventory of all information assets and makes a classification of them according to their protection needs, consistent with the risk analysis carried out.

The system configuration is audited periodically, in accordance with the provisions of section 9.2 of the DPCM

It is kept track of the capacity requirements and procedures are planned to ensure the availability and storage media for information assets.

6.7.3 Evaluation of the lifecycle security level

The AGE may require the CSPM to undergo independent evaluations, audits and, where appropriate, safety certifications of the lifecycle of the provider products.

6.8 Network security controls

Access to the different networks of the CSPM is limited to individuals duly authorized. Particularly:

- There are controls to protect the internal network from external domains accessible by third parties. Firewalls are configured to prevent access and protocols that are not required for the operation of the CSPM.
- Sensitive data are protected when exchanged over unsecured networks (including as such the registration data of the subscriber).
- Local network components are located in secure environments and their settings are audited periodically.

6.9 Security controls of cryptographic modules

The Keys of the CSPM are generated in secure cryptographic devices, operated by trusted CSPM personnel in a safe environment and under dual control (at least two people simultaneously). These devices comply with the cryptographic security standards which have been indicated in the previous sections.

The key generation algorithms are accepted for the use of the key to which it is intended for the different types of certificates defined.

7 Certificate and CRL profiles

7.1 Certificate profile

The certificate profiles and extensions supported conform to the definitions in the document [EIFEBI]. Additionally, the certificates are in conformity with the standards specified in the corresponding additional conditions.

7.1.1 Version number

Only certificates based on version 3 of Recommendation ITU-T X.509 are allowed.

7.1.2 Validity period of certificates

The validity period of the issued certificates is standardized in line with the policy of use of certificate signing algorithms applied by the AGE, as shown below:

CERTIFICATE	LEVEL	VALIDITY PERIOD
PUBLIC EMPLOYEE	High / Medium	Three year
ELECTRONIC OFFICE	Medium	Three year
ELECTRONIC SEAL	Medium	Three year

7.1.3 Fields and extensions of certificates

All OID used to identify the different fields of the certificates are unique worldwide.

The CSPM does not issue certificates that contain proprietary extensions marked as critical. In any case, the AGE may ignore the content of proprietary extensions that are not marked as critical.

The CSPM provides the syntax and semantic processing of the fields or extensions contained in certificates:

- The same field or extension is not used to set different semantic definitions in the same type of certificate.
- There will be a method of extraction of each of the individual data which, together, uniquely determine the content of all the fields and extensions of the certificate.
- The method of extraction and semantic interpretation of information does not depend on the content of any other field.

Qualified certificates issued under the CPSM include express statement that they are issued as such (with the term "*certificado reconocido*") within *CertificatePolicies* extension of the certificate or by using specific extensions (OID 1.3.6.1.5.5.7.1.3)

Below are extensions and fields of the certificates for use in the CPSM for the different tipologies.

CERTIFICATE	MANDATORY FIELDS
PUBLIC EMPLOYEE	• *Version* • *Serial Number* • *Issuer Distinguished Name (Country (C), Organization (O), Organizational Unit (OU), Common Name (CN))* • *Validdity (Not Before, Not After)* • *Subject (Country (C), Organization (O), Organizational Unit (OU), Serial Number, Common Name (CN))* • *Subject Public Key Info* • *Signature Algorithm*
ELECTRONIC OFFICE	• *Version* • *Serial Number* • *Issuer Distinguished Name (Country (C), Organization (O), Organizational Unit (OU), Common Name (CN))* • *Validity (Not Before, Not After)* • *Subject (Country (C), Organization (O), Organizational Unit (OU), Serial Number, Common Name (CN))* • *Subject Public Key Info* • *Signature Algorithm*
ELECTRONIC SEAL	• *Version* • *Serial Number* • *Issuer Distinguished Name (Country (C), Organization (O), Organizational Unit (OU), Common Name (CN))* • *Validity (Not Before, Not After)* • *Subject (Country (C), Organization (O), Organizational Unit (OU), Serial Number, Common Name (CN))* • *Subject Public Key Info* • *Signature Algorithm*

CERTIFICATE	RECOMMENDED FIELDS
PUBLIC EMPLOYEE	• *Issuer Distinguished Name (Locality (L))* • *Subject (Title, Surname, Given Name)*
ELECTRONIC OFFICE	• *Issuer Distinguished Name (Locality (L))*
ELECTRONIC SEAL	• *Issuer Distinguished Name (Locality (L))* • *Subject (Surname, Given Name)*

CERTIFICATE	MANDATORY EXTENSIONS
PUBLIC EMPLOYEE	• *Authority Key Identifier* • *Subject Key Identifier* • *cRLDistributionPoint (distributionPoint, distributionPoint)* • *Authority Info Access (Access Method, Access Location)* • *Key Usage* • *NON REPUDIATION HIGH LEVEL: Key Usage (Content Commitment)* • *AUTHENTICATION HIGH LEVEL: Key Usage (Digital Signature)* • *ENCIPHERMENT HIGH LEVEL: Key Usage (Key Encipherment, Data Encipherment)* • *NON REPUDIATION, AUTHENTICATION AND ENCIPHERMENT MEDIUM LEVEL: Key Usage (Digital Signature, Content Commitment, Key Encipherment, Data Encipherment)* • *Extended Key Usage* • *AUTHENTICATION HIGH LEVEL: Extended Key Usage (Email Protection, Client Authentication)* • *ENCIPHERMENT HIGH LEVEL: Extended Key Usage (Email Protection, Client Authentication)* • *NON REPUDIATION, AUTHENTICATION AND ENCIPHERMENT MEDIUM LEVEL: Extended Key Usage (Email Protection, Client Authentication)* • *Qualified Certificate Statements* • *HIGH LEVEL: Qualified Certificate Statements (QcCompliance, QcEuRetentionPeriod, QcSSCD)* • *MEDIUM LEVEL: Qualified Certificate Statements (QcCompliance, QcEuRetentionPeriod)* • *Certificate Policies (Policy Identifier, Policy Qualifier ID [DPC Pointer, User Notice])* • *Subject Alternative Names (Directory Name= Identidad Administrativa)*
ELECTRONIC OFFICE	• *Authority Key Identifier* • *Subject Key Identifier* • *Key Usage (Digital Signature, Key Encipherment)* • *cRLDistributionPoint (distributionPoint, distributionPoint)* • *Authority Info Access (Access Method, Access Location)* • *Extended Key Usage (Server Authentication)* • *Qualified Certificate Statements* • *HIGH LEVEL: Qualified Certificate Statements (QcCompliance, QcEuRetentionPeriod, QcSSCD)* • *MEDIUM LEVEL: Qualified Certificate Statements (QcCompliance, QcEuRetentionPeriod)* • *Certificate Policies (Policy Identifier, Policy Qualifier ID [DPC Pointer, User Notice])* • *Subject Alternative Names (Directory Name= Identidad Administrativa)*
ELECTRONIC SEAL	• *Authority Key Identifier* • *Subject Key Identifier* • *Key Usage (Digital Signature, Content Commitment, Key Encipherment, Data Encipherment)* • *Extended Key Usage (Email Protection, Client Authentication)* • *cRLDistributionPoint (distributionPoint, distributionPoint)* • *Authority Info Access (Access Method, Access Location)* • *Qualified Certificate Statements* • *HIGH LEVEL: Qualified Certificate Statements (QcCompliance, QcEuRetentionPeriod, QcSSCD)*

	• *MEDIUM LEVEL: Qualified Certificate Statements (QcCompliance, QcEuRetentionPeriod)* • *Certificate Policies (Policy Identifier, Policy Qualifier ID [DPC Pointer, User Notice])* • *Subject Alternative Names (Directory Name= Identidad Administrativa)*

CERTIFICATE	RECOMMENDED EXTENSIONS
PUBLIC EMPLOYEE	• *Authority Key Identifier (Key Identifier, AuthorityCertIssuer, AuthorityCertSerialNumber)* • *Issuer Alternative Name (rfc822Name)* • *Key Usage* • *NON REPUDIATION HIGH LEVEL: Key Usage (Digital Signature, Key Encipherment, Data Encipherment, Key Agreement, Key Certificate Signeture, CRL Signature)* • *AUTHENTICATION HIGH LEVEL: Key Usage (Content Commitment, Key Encipherment, Data Encipherment, Key Agreement, Key Certificate Signature, CRL Signature)* • *ENCIPHERMENT HIGH LEVEL: Key Usage (Digital Signature, Content Commitment, Key Agreement, Key Certificate Signature, CRL Signature)* • *NON REPUDIATION, AUTHENTICATION AND ENCIPHERMENT MEDIUM LEVEL: Key Usage (Key Agreement, Key Certificate Signature, CRL Signature)* • *Subject Alternative Names (rfc822Name, User Principal Name (UPN))*
ELECTRONIC OFFICE	• *Authority Key Identifier (Key Identifier, AuthorityCertIssuer, AuthorityCertSerialNumber)* • *Key Usage (Content Commitment, Data Encipherment, Key Agreement, Key Certificate Signature, CRL Signature)* • *Issuer Alternative Name (rfc822Name)* • *Subject Alternative Names (rfc822Name)*
ELECTRONIC SEAL	• *Authority Key Identifier (Key Identifier, AuthorityCertIssuer, AuthorityCertSerialNumber)* • *Key Usage (Key Agreement, Key Certificate Signature, CRL Signature)* • *Issuer Alternative Name (rfc822Name)* • *Subject Alternative Names (rfc822Name)*

7.1.4 Algorithms OID

The CPSM uses the security scenario called generic safety environment of AGE, which determines the strength and viability criteria applicable to each certificate profile. The two levels of assurance contained herein are considered within this scenario.

The specifications listed below follow the technical specification [ETSI TS 102 176-1]. Different cryptographic requirements are set for the issuing authorities and institutions or final certificates. There are also differences between high level of assurance and medium:

- Root Authority:

Level of assurance	Entity	Algorithm and minimum length		Observations
		Alg	Minimum length	
High and Medium	Root and subordinated CAs	SHA-1	RSA-2048	• SHA-256 and dual generations are contemplated to ensure continuity • RSA 4096 is also admitted

- Final Entities:

Level of assurance	Entity	Algorithm and minimum length		Observations
		Alg	Minimum length	
High	Final certificates	SHA-1	RSA-2048	• SHA-256 and dual generations are contemplated to ensure continuity
Medium	Final certificates	SHA-1	RSA-1024	• RSA 2048 length o higer are recomended

These specifications will be used for the period 2008 to 2009. These requirements will be reviewed and establish new updates to take effect from 2010.

The signatures of the certificates issued under the CPSM are identified with the following OID:

sha1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

Also, the certificates shall contain the following OID to identify algorithms of the issued public keys:

rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}

El PSCM sólo certificará las claves públicas asociadas con los algoritmos criptográficos identificados anteriormente y sólo utilizará los algoritmos criptográficos de firma descritos anteriormente para firmar certificados, listas de certificados revocados y cualquier otro elemento de la Entidad de Certificación.

7.1.5 Name formats

The composition of names for user certificates whose type is defined in the CPSM is that described in paragraphs 3.1.2 and 3.1.3. For this purpose, use will be made of the fields *Subject* and *SubjectAlternativeName* according to the normalized scheme proposed by the AGE:

Mandatory values (see 7.1.3):

- *Subject* field(*Country* (C), *Organization* (O), *Organizational Unit* (OU), *Serial Number*, *Common Name* (CN))
- *SubjectAlternativeName* field(*Directory Name = Identidad Administrativa*)

Optional values (see 7.1.3):

- *Subject* field(*Organizational Unit* (OU), *Title*, *Surname*, *Given Name*)
- *SubjectAlternativeName* field(*rfc822Name*)

7.1.6 OID in the *policyConstraints* extension

Issued certificates will use OID to identify his type as defined in section 1.2.2.

7.1.7 Use of the *policyConstraints* extension

In all certificates issued by the CSPM shall appear the extension *policyConstraints* and it cannot be an empty sequence.

7.1.8 Syntax and semantics of policy qualifiers

It will contain the CPSM URI.

7.2 CRL profile

The profile of the CRL is in accordance with the standards specified in the corresponding additional conditions.

7.2.1 Version number

The PSCM uses only CRL as provided for in [ITU-T X.509] as well as the profile in the technical specification [IETF RFC 5280].

7.2.2 CRL and extensions

The CRL will include the following information:

- The version field, code assigned to version 2.
- The callsign field of the next update of the complete CRL, containing the scheduled date of the next issue of the CRL.

8 Compliance audit and other controls

8.1 Compliance audits

The CSPM conducts regular internal audit to test compliance of security and operational requirements necessary to meet certification services policy of the AGE.

8.2 Frequency of compliance audit

The CSPM will conduct a compliance audit annually, in addition to internal audits that can perform at their own discretion and at any time, because of a suspected breach of any security measure or a key compromise.

8.3 Identification and qualification of the auditor

The compliance audit will be carried out by the internal audit department CSPM, if it exists, or external personnel specialized in conducting audit checks selected by the contractual formula of application at the CSPM. The hired independent auditor must demonstrate experience in information security, information systems security and compliance auditing services for public key certification.

8.4 Relationship between auditor and audited Entity

The auditor will not belong in any case to the personnel in charge of the operation of the Certification Entity. Also the auditor, in case of being external, will not belong to the teams that have participated in the implementation of the architecture of CSPM.

Compliance audits performed by third parties will be carried out by an independent body of CSPM, which should have no conflict of interest that impairs his ability to perform audit services.

The auditor will require access to the system with the specific role of auditor. On inspection tasks the auditor wants to perform in relation to the cryptographic modules, these will always operated SGTIC staff, providing the required information.

The auditor will never be allowed under any circumstances to the physical handling of the same, nor will be given access to machines that support the platform. In case of audit of levels of physical security, he will be always accompanied by staff from SGTIC.

8.5 List of elements under audit

Audited elements are the following:

- Certification procedures.
- Information systems.
- Protection of data Processing Centre.
- Documentation of the service.
- Existence of relevant authorizations that empower the operators of those components that make up the Certification Entity, following the provisions of the DPCM. Verification of the non compliance with this circumstances is a very serious fault.

- Effective measures to secure access to the administration and roles of the various components that make up the Certification Entity.
- Effective Segregation of the roles established in the CPSM.
- Control and monitoring of the software versions and correct updating thereof, proceeding to the strict checking of operational software and official versions supported by the platform.
- Contingency procedures.
- Space availabylity in the machines that conform the Certification Entity as to prevent space overflows.
- Physical backup of the HSM content.
- State of databases systems.
- Adaptation of the CPSM to the Certification Policy of the AGE.
- Matching between the procedures and technical controls present in the CPSM with the real and effective measures.

In a generic manner, together with the critical aspects identified above shall be audited in line with best practices defined in [ISO27001] or equivalent.

8.6 Actions to be taken as a result of a lack of conformity

When an auditor finds a deficiency in the operation of the Certification Entity or the procedures stipulated in the CPSM, the following actions will be carried out:

- The auditor will prepare a report with the results of his audit.
- The auditor shall notify the deficiency to the parties involved.
- After receiving the report of the compliance audit conducted, the CSPM will discuss with the entity that performed the audit and the AGE, the deficiencies found and develop and implement a corrective plan to solve such deficiencies.
- Once the deficiencies are corrected, the auditor will verify the implementation and effectiveness of the solutions adopted.

In case of detecting that the anomaly is related to a bad practice of platform use by a operator, will determine whether to set him aside until further operational integration into the platform.

If the CSPM is unable to develop and / or implement such a plan or if the deficiencies pose an immediate threat to the security or integrity of the system, one of the following actions will be taken:

- Revoke the CSPM key, as described in section 5.7.2 of this document.
- Terminate the CSPM service, as described in section 5.8 of this document.

8.7 Treatment of audit reports

The CSPM will deliver the reports of the audit results to the appropriate entity within the AGE to, within 15 days after completion of the audit.

9 Legal requisites

9.1 Confidenciality

9.1.1 Type of information to be protected

The CSPM considers the following information as sensitive and therefore boasts the necessary protective measures in terms of access and treatment:

- Applications for certificates, approved or disapproved, and any other personal information collected for the issuance and maintenance of certificates, except the information indicated in the section below.
- Private keys generated or stored by the CSPM.
- Records of transactions, including full records and the audit records of transactions.
- Records of internal and external audit, created and / or maintained by the CSPM and their auditors.
- Emergency and business continuity plans .
- Security policy and plans.
- Documentation of operations and other operational plans, as archives, monitoring and similar.
- Any other information identified as sensitive.

It is protected by the physical means present in the SGTIC the cryptographic information that conform access to the Certification Entity of CSPM.

It is protected the access to the cards of Operation and Management of the cryptographic modules that support the Certification Entity, as well as the serial numbers and activation of the cryptographic hardware devices.

Access passwords to the different roles present in the platform Are protected and should not be disseminated in any case between members of incompatible profiles nor between members of the same group.

9.1.2 Non sensitive information

The following information is considered non sensitive, and so is recognized by the affected:

- Certificates issued or in process of issuance.
- Linkage of the holder to a certificate issued by the CSPM.
- The full name of the certificate holder and any other circumstance or personal data of the holder, in the event that is significant in terms of the purpose of the certificate.
- The email address of the certificate holder or email as appropriate.
- The uses outlined in the certificate.
- The period of validity of the certificate, and the date of issue of the certificate and the expiration date.
- The serial number of the certificate.

- The different states or conditions of the certificate and the date of the beginning of each of them, namely: pending generation and / or delivery, valid, revoked, suspended or expired and the reason that caused the change of state.
- The certificate revocation lists (CRLs), and the remaining revocation status information.
- The information contained in the repositories of certificates.
- Any other information that is not indicated in the preceding section of this document.

9.1.3 Disclosure of suspension and revocation information

See above section.

9.1.4 Legal disclosure of information

The CSPM only will disclose the information identified as sensitive in cases provided by law to do so. Specifically, records that support the reliability of the data contained in the certificate will be disclosed if required to provide evidence of the proper issuance and lifecycle management of the certificate in case of legal proceedings, even without the consent of the subscriber the certificate.

The CSPM indicates these circumstances in the privacy policy under Section 9.2 of this document.

9.1.5 Information disclosure by request of the holder

The CSPM includes in the privacy policy under Section 9.2 of this document, requirements to permit the disclosure of subscriber information and, where appropriate, of the responsible person of the certificate directly to them or others.

9.2 Personal data protection

For the service, the CSPM collects and stores certain information, including personal data. Such information is collected directly from those affected, with their explicit consent or in cases where the law allows collecting information, without consent of the affected.

The CSPM develops a privacy policy, according to the Organic Law 15/99 of 13 December on the Protection of Personal Data (LOPD), and documents, in the CPSM, the safety aspects and procedures corresponding to the document of security as defined in Royal Decree 1720/2007 of 21 December, approving the Regulations implementing the LOPD. The CPSM is considered as Document of Security.

The CSPM collects the data exclusively necessary for the issuance and lifecycle management of the certificate.

The CSPM will not disclose or lease personal information, except as provided in Sections 9.1.2 to 9.1.5 of this document, and in section 5.8, upon termination of the Certification Entity.

Confidential information in accordance with the LOPD is protected from loss, destruction, damage, forgery and unauthorized or unlawful processing, in accordance with the requirements established by Royal Decree 1720/2007.

9.3 Intellectual Property Rights

9.3.1 Property of certificates and revocation information

The CSPM is the only entity that has intellectual property rights on the certificates it issues.

The CSPM grants nonexclusive license to reproduce and distribute the certificates, free of charge, provided that the reproduction is full and does not alter any element of the certificate, and is necessary in relation to electronic signatures and / or encryption systems within the scope of the DPCM, as defined in section 1.4.

The same rules are applicable to the use of certificate revocation information.

9.3.2 Property of Certification Policy and Certification Practice Statement

The AGE is the only entity that has the rights of intellectual property on the certification policies of the AGE.

The CPSM is exclusive property of the CSPM.

9.3.3 Property of information concerning to names

The subscriber retains all rights, if it exists, on the brand, product or trade name contained in the certificate.

Subscriber is the owner of the certificate's distinguished name, consisting of the information specified in section 3.1 of the CPSM.

9.3.4 Key property

Key pairs are the property of the subscribers of certificates. When a key is split into parts, all parts of the key are owned by the owner of the key.

9.4 Obligations and liability

9.4.1 Model of obligations for the certification service provider

The CSPM guarantees, under its own responsibility, that meets all the established requirements for each type of certificate issued.

The CSPM is the only entity responsible for the performance of the procedures in the CPSM, even when part or all of the operations to be outsourced externally.

The CSPM provides its services of certification in accordance to the DPCM, which details its functions, operating procedures and safety measures.

Prior to the issuance and delivery of the certificate to the subscriber, the CSPM informs him about the terms, conditions and limitations on the use of the certificate, its price - case of having it - and limitations of use.

This requirement is met by an informative text of the applicable certificate policy, in plain language, long lasting, published in the Information Repository of the CSPM.

The CSPM links the subscribers and third parties who rely on the certificates through proper legal instruments.

The CSPM assumes other obligations directly incorporated in the certificate or incorporated by reference.

9.4.2 Guarantees to subscribers and third parties who rely on the certificates

The CSPM, establishes and rejects guarantees, and establishes the limitations of liability. The CSPM ensures to the subscriber:

- That there are no factual errors in the information contained in the certificates, known or made by the CSPM and, where appropriate, by the registrar.
- That there are no factual errors in the information contained in the certificates, due to lack of diligence in the management of the certificate application or its creation.
- That the certificates meet all the material requirements established in the CPSM.
- That the revocation services and use of the Repository meet all material requirements established in the CPSM.

The CSPM ensures to the third parties who rely on the certificates:

- That the information contained or incorporated by reference in the certificate is correct, except where noted otherwise.
- In the case of certificates published in the Repository, that the certificate has been issued to the subscriber identified in it and that the certificate has been accepted in accordance with section 4.4 of the CPSM.
- That the approval of the certificate application and the issuance of the certificate have met all the material requirements established in the CPSM.
- The speed and security in the provision of services, especially the services of revocation and Repository.

Additionally, when issuing a non repudiation certificate, the CSPM ensures to the subscriber and to the third party relying on the certificate:

- The certificate contains the information that must contain a qualified certificate, in accordance with article 11 of Law 59/2003, of 19 December (LFE).
- That, in the case of generating the private keys of the subscriber their confidentiality is maintained throughout the process.

9.4.3 Rejection of other guarantees

The CSPM rejects any other warranties not legally required, other than those referred to in section 9.4.2.

9.4.4 Limitation of liability

The CSPM limits its liability to the issuance and management of certificates and, where appropriate, of subscriber key pairs and cryptographic devices supplied by the CSPM (authentication, signature and signature verification).

The CSPM can limit its liability by including the certificate usage limits and limits of the value of transactions for which the certificate can be used.

9.4.5 Disclaimer clauses

9.4.5.1 Exemption clause of liability with the Subscriber

The CSPM includes in the document that links it to the subscriber, a clause by which the subscriber agrees to keep the CSPM harmless from any act or omission that results in damage, injury or loss, expenses of any kind , including judicial and legal representation that may be incurred by the publication and use of the certificate, under any of the following causes:

- Falsehood or misrepresentation made by the user of the certificate.
- Error of the user of the certificate when providing data on the application, if in the act or omission mediated intent or neglect respect to CSPM, the Register Entity or any person relying on the certificate.
- Neglect in protecting the private key in the use of a reliable system or in maintaining the necessary precautions to prevent the compromise, loss, disclosure, modification or unauthorized use of the key.
- Employment by the subscriber of a name (including common names, email address and domain names), or other information in the certificate, that infringes intellectual or industrial property of others.

9.4.5.2 Exemption clause of liability with third parties relying on the certificate

The third party relying on the certificate agrees to keep the CSPM harmless from any act or omission that results in damage, injury or loss, expenses of any kind , including judicial and legal representation that may be incurred by the publication and use of the certificate, under any of the following causes:

- Failure to observe obligations of the third parties that rely on a certificate.
- Reckless trust in a certificate, under the circumstances.
- Lack of checking the status of a certificate, to determine that is not suspended or revoked.

9.4.6 Fortuitous event or force majeure

The CSPM shall be exempt from any responsibility for the effects that may arise from fortuitous causes or force majeure.

9.4.7 Applicable law

The law applicable to the provision of services, including policy and certification practices, is the Spanish law, especially:

- Law 11/2007 of June 22nd, on electronic access of citizens to Public Services (LAECSP).
- Law 59/2003 of December 19th on Electronic Signature (LFE).
- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
- Law 6/1997, of 14 april, on Organization and Operation of the AGE.

9.4.8 Clauses of Severability, survival, entire agreement and notification

The CSPM establishes in the general conditions of issue and use of certificates, clauses of severability, survival, entire agreement and notification:

- Under the severability clause, the invalidity of a clause does not affect the rest of the CPSM.
- Under the survival clause, certain rules still in force after completion of the provision of services by the CSPM. To this end, it ensures that at least the requirements contained in sections 9.4 Obligations and responsibilities, 8 Compliance Audit and 9.1 Confidentiality, continue in force after termination of services.
- Under the entire agreement clause means that the CPSM contains the complete will and all agreements between the parties.
- Under the notification clause in the CPSM establishes the procedure by which the parties mutually facts are reported.

9.4.9 Competent jurisdiction clause

The CSPM stipulates that international jurisdiction is for the Spanish judges.

The territorial and functional jurisdiction is determined under the rules of private international law and applicable rules of procedural law.

9.4.10 Conflict resolution

The CSPM will resolve any disputes that may arise concerning the interpretation or applicability of the CPSM to the Certification Policy.

The discrepancy situations arising from the use of the certificates issued by the CSPM, be resolved by applying the same criteria of competence that in cases of signed documents produced manually.

In cases of dispute arising as a result of the management of certificates between the different entities of certification service providers accredited or approved, it will be as established in the CPSM.

Annex A: References

CCEAL4+	Common Criteria Evaluation Assurance Level (EAL) 4+.
CCN-STIC-405	Security guide for IT. Algorithms and parameters for secure electronic signature.
CWA 14167	CEN-CWA 14167: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signature.
CWA 14169	CEN-CWA 14169: Secure Signature-Creation Devices "EAL 4+", establishes a protection profile for secure signature creation devices of the law 59/2003 of 19 December 2003 on electronic signatures and the European directive.
EIFE	Public Administrations scheme for identification and electronic signature. (Esquema de identificación y firma electrónica de las Administraciones Públicas)
EIFEBI	Public Administrations scheme for identification and electronic signature. Part I: Profiles for electronic certificates.
EIFEBIII	Public Administrations scheme for identification and electronic signature. Part III: Proposals for additional general conditions in the AGE
ETSI TS 101 456	ETSI Technical Specification TS 101 456. Policy requirements for certification authorities issuing qualified certificates.
ETSI TS 101 862	ETSI Technical Specification TS 101 862. Qualified Certificate Profile.
ETSI TS 102 023	ETSI Technical Specification TS 102 023. Policy requirements for time-stamping authorities.
ETSI TS 102 042	ETSI Technical Specification TS 102 042. Policy requirements for certification authorities issuing public key certificates.
ETSI TS 102 176-1	ETSI Technical Specification TS 102 176-1. Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms.
ETSI TS 102 176-2	ETSI Technical Specification TS 102 176-2. Algorithms and Parameters for Secure Electronic Signatures; Part 2: Secure channel protocols and algorithms for signature creation devices.
ETSI TS 102 280	ETSI Technical Specification TS 102 023. X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons.
FIPS 140-2	Federal Information Processing Standards (FIPS) 140-2, Security Requirements for Cryptographic Modules.
IETF RFC 2560	X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol–OCSP.
IETF RFC 3279	Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile.
IETF RFC 3280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
IETF RFC 3647	Internet X509 Public Key Infrastructure Certificate Policy and Certification Practice Framework.
IETF RFC 3739	Internet X.509 Public Key Infrastructure Qualified Certificates Profile.
IETF RFC 4055	Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate

	Revocation List (CRL) Profile.
IETF RFC 4325	Internet X.509 Public Key Infrastructure Authority Information. Access Certificate Revocation List (CRL) Extension.
IETF RFC 4491	Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile.
IETF RFC 4630	Update to Directory String Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
ISO 3166-1	Codes for the representation of names of countries and their subdivisions – Part 1: Country codes. Alpha-2 country codes.
ISO 15048	Common Criteria for Information Technology Security Evaluation (CC/ISO 15408).
ISO 27001	ISO/IEC 27001 (Information technology - Security techniques - Information security management systems - Requirements).
ISO 9594-8	Information Technology - Open Systems Interconnection - The Directory: Public-key and Attribute Certificate Frameworks.
ITU-T X.501	ITU-T Recommendation X.501 TC2 (08/1997) | ISO/IEC 9594-2:1998.
ITU-T X.509	ITU-T Recommendation X.509 (2005): Information Technology – Open Systems Interconnection - The Directory: Authentication Framework.
UTF-8	8-bit Unicode Transformation Format.

Annex B: Admission Scheme for Certification Service Providers

The CSPM exposes that knows and meets the requirements and additional conditions set out in the document [EIFEBIII].

The CSPM is registered in the list of certification service providers published on the Website of Ministry of Industry, Energy and Tourism (MINETUR) [EIFEBIII].

The CSPM has voluntarily applied the procedures for admission and processing of applications under the scheme of particular conditions of certification of the AAPP (evaluation and admission procedure of CSP and certificates in the administration), assuming the costs of the proceedings, for evaluation, audit and other provided. This scheme complements the already applied by the MINETUR for monitoring and supervision of providers subject to the LFE [EIFEBIII].

The CSPM meets the technical and operational criteria developed and maintained by the Permanent Working Group comprising representatives of the Ministry of Finance and Public Administration (MINHAP) and MINETUR, henceforth, GTP, in addition to the obligations of the LFE, necessary for providers seeking admission as CSP for the administration [EIFEBIII].

- The condition of admitted CSP, and the recognition of the activity performed is collected by the GTP and published both in the list of certification service providers in the website of the MINETUR as in other portals or electronic offices of the Administration.
- It appears in the list of allowed electronic certificates within the scope of relations with and within the State Public Administration, for purposes of implementation and verification of electronic signatures in electronic documents issued or received in this area, maintained centrally by the GTP.
-

The CSPM is prepared to pass no periodic external reviews carried out only by the GTP (or external personnel designated for that purpose), proving their reliability as CSP admitted by the Administration:

- The GTP is responsible for auditing the compliance with additional general conditions by the admitted certification service providers. This process is carried out to complement the powers of inspection and control of MINETUR.
- The GTP is responsible for supervising and controlling that profiles defining each existing certificate accurately reflect the same structure of the certificates generated by the CSP.
- The GTP may require to the providers the provision of the documentation appropriate for the development of its auditing and monitoring functions, as well as the new check of compliance with additional conditions, being obliged to assist them in any way necessary for it .
- The provider that seriously obstructs or prevents auditing and monitoring of compliance with additional conditions, or fails to fulfill them, will lost the right of admission of its certificates by the AGE. Additionally, the GTP shall notify the

certification body of the provider's activity for the purposes of the review, in the appropriate sense, of said certification.

Annex C: Links (URL)

CPSM and certifícate profiles:

http://ca.mtin.es/mtin/DPCyPoliticas

OCSP Service:

http://ca.mtin.es/mtin/ocsp

Root certificate, OCSP certifícate and Time Stamp certificate:

http://ca.mtin.es/mtin/certificados

CRL publication:

http://ca.mtin.es/mtin/crl/MTINAutoridadRaiz

http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz

Historic CRL:

http://ca.mtin.es/mtin/crlHistoricas