



MINISTERIO  
DE EMPLEO  
Y SEGURIDAD SOCIAL

SUBSECRETARÍA

S.G. DE TECNOLOGÍAS DE LA  
INFORMACIÓN Y COMUNICACIONES

## **Ministry Certification Service Provider Certification Practice Statement**



## Version Control

<b>Identifier</b>	D004
<b>Title</b>	Ministry Certification Service Provider Certification Practice Statement
<b>Version</b>	1.11
<b>Document state</b>	Approved
<b>Approval date</b>	07.04.2017
<b>Expiration date</b>	07.04.2018
<b>OID</b>	1.3.6.1.4.1.27781.2.3.1

## Change Control

<b>Version</b>	<b>Date</b>	<b>Comments</b>
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 TSPM.
1.2	10.09.2010	Header change removing Directory General Services Added sections for art. 21 LFE in section 5.8
1.3	07.04.2011	OCSP certificate OID change. Suppression of OCSP no Check restriction
1.4	16.02.2012	OIDs update
1.5	10.08.2012	Organization Structure update. New document format. Annex C added
1.6	21.03.2014	Added the Public Employee Certificate Centralized and Managed by HSM
1.7	04.07.2014	Annex B removed Annex C is now Annex B with new writing for historic CRLs Identification and Electronic Signature Framework for Public Administrations is remove from References Sections 4.9.3, 6.1.1, and 6.2.1 rewritten
1.8	18.06.2015	SHA-256 added
1.9	18.03.2016	Current legislation updated
1.10	30.05.2016	Minor typos updated SHA-1 references removed
1.11	06.04.2017	Root Certification Authority, SubCA and related URLs added to the document Trusted services updated



## Summary Contents

<b>1</b>	<b>Introduction .....</b>	<b>1</b>
<b>2</b>	<b>Publication and Repository Responsibilities .....</b>	<b>11</b>
<b>3</b>	<b>Identification and Authentication .....</b>	<b>13</b>
<b>4</b>	<b>Certificate Life-Cycle Operational Requirements .....</b>	<b>19</b>
<b>5</b>	<b>Facility, management and operational controls .....</b>	<b>30</b>
<b>6</b>	<b>Technical security controls .....</b>	<b>40</b>
<b>7</b>	<b>Certificate, CRL, and OCSP profiles .....</b>	<b>49</b>
<b>8</b>	<b>Compliance audits and other assessments .....</b>	<b>53</b>
<b>9</b>	<b>Other business and legal matters .....</b>	<b>55</b>
<b>Annex A:</b>	<b>References.....</b>	<b>62</b>





## Table of Contents

<b>1</b>	<b>Introduction .....</b>	<b>1</b>
1.1	Overview .....	1
1.1.1	Relationship between CPSM and other documents .....	1
1.2	Document name and identification .....	1
1.3	PKI Participants .....	2
1.3.1	Certification Authorities .....	2
1.3.2	Registration Authorities .....	4
1.3.3	Validation Authority .....	5
1.3.4	End Users .....	5
1.4	Certificate usage .....	6
1.5	CPSM administration .....	7
1.5.1	Organization administering the document .....	7
1.5.2	Contact person .....	7
1.5.3	CPS administration procedures .....	7
1.6	Definitions and acronyms .....	8
1.6.1	Definitions .....	8
1.6.2	Acronyms .....	9
<b>2</b>	<b>Publication and Repository Responsibilities .....</b>	<b>11</b>
2.1	Repositories .....	11
2.2	Publication of certification information .....	11
2.3	Time for frequency of publication .....	11
2.4	Access controls on repositories .....	11
<b>3</b>	<b>Identification and Authentication .....</b>	<b>13</b>
3.1	Naming .....	13
3.1.1	Types of names .....	13
3.1.2	Administrative Identity and Normalization .....	13
3.1.3	Need for names to be meaningful .....	14
3.1.4	Anonymity or pseudonymity of subscribers .....	15
3.1.5	Rules for interpreting various name forms .....	15
3.1.6	Uniqueness of the names .....	15
3.1.7	Recognition, authentication, and role of trademarks .....	16
3.2	Initial identity validation .....	16
3.2.1	Method to prove possession of private key .....	16
3.2.2	Authentication of organization identity .....	16
3.2.3	Authentication of individual identity .....	17
3.2.4	Non-verified subscriber information .....	18
3.2.5	Criteria for interoperation .....	18
3.3	Identification and authentication for re-key requests .....	18
3.3.1	Identification and authentication requirements for routine re-key .....	18
3.3.2	Identification and authentication requirements for re-key after certificate revocation .....	18
3.4	Identification and authentication for revocation request .....	18
<b>4</b>	<b>Certificate Life-Cycle Operational Requirements .....</b>	<b>19</b>
4.1	Certificate Application .....	19
4.1.1	Who can submit a certificate application .....	19



4.1.2	Enrollment process and responsibilities .....	20
4.2	Certificate application processing .....	20
4.2.1	Specifications for Public Employee Certificates .....	20
4.2.2	Specifications for Electronic Seal Certificates .....	20
4.3	Certificate issuance.....	21
4.3.1	CA actions during certificate issuance .....	21
4.3.2	Notification to subscriber by the CA of issuance of certificate.....	21
4.4	Certificate acceptance.....	22
4.4.1	Conduct constituting certificate acceptance .....	22
4.4.2	Certificate acceptance.....	22
4.4.3	Publication of the certificate by the CA .....	22
4.4.4	Notification of certificated issuance by the CA to other parties.....	23
4.5	Key pair and certificate usage .....	23
4.5.1	General usage requirements .....	23
4.5.2	Usage by subscribers .....	23
4.5.3	Relying party public key and certificate usage.....	24
4.6	Certificate renewal with key pair reused .....	24
4.7	Certificate renewal without key pair reused .....	24
4.8	Certificate modification .....	24
4.9	Certificate revocation and suspension .....	24
4.9.1	Circumstances for revocation .....	25
4.9.2	Who can request revocation .....	26
4.9.3	Procedure for revocation request .....	26
4.9.4	Revocation request grace period.....	27
4.9.5	Time within which CA must process the revocation request .....	27
4.9.6	Revocation checking requirement for relying parties.....	27
4.9.7	CRL issuance frequency .....	27
4.9.8	Maximum latency for CRLs .....	27
4.9.9	On-line revocation/status checking availability .....	27
4.9.10	On-line revocation checking requirements.....	27
4.9.11	Other forms of revocation advertisements available .....	28
4.9.12	Special requirements re key compromise .....	28
4.10	Certificate status services .....	28
4.10.1	Operational characteristics .....	28
4.10.2	Service availability .....	28
4.10.3	Optional features.....	29
4.11	End of subscription.....	29
4.12	Key escrow and recovery .....	29
<b>5</b>	<b>Facility, management and operational controls .....</b>	<b>30</b>
5.1	Physical controls.....	30
5.1.1	Site location and construction .....	30
5.1.2	Physical access .....	30
5.1.3	Power and air conditioning.....	31
5.1.4	Water exposures .....	31
5.1.5	Fire prevention and protection.....	31
5.1.6	Media storage .....	31
5.1.7	Waste disposal .....	31



5.1.8	Off-site backup .....	32
5.2	Procedural controls .....	32
5.2.1	Trusted Roles .....	32
5.2.2	Number of persons required per task .....	33
5.2.3	Identification and authentication for each role .....	33
5.2.4	Roles requiring separation of duties .....	33
5.3	Personnel controls .....	33
5.3.1	Qualifications, experience and clearance requirements .....	33
5.3.2	Background check procedures .....	34
5.3.3	Training requirements .....	34
5.3.4	Retraining frequency and requirements .....	34
5.3.5	Job rotation frequency and sequence .....	34
5.3.6	Sanctions for unauthorized actions .....	34
5.3.7	Independent contractor requirements .....	34
5.3.8	Documentation supplied to personnel .....	34
5.4	Audit Logging Procedures .....	35
5.4.1	Types of events recorded .....	35
5.4.2	Frequency of processing log .....	35
5.4.3	Retention period for audit log .....	36
5.4.4	Protection of audit log .....	36
5.4.5	Audit log backup procedures .....	36
5.4.6	Audit collection system (internal vs external) .....	36
5.4.7	Notification to event-causing subject .....	36
5.4.8	Vulnerability assessments .....	36
5.5	Records archival .....	36
5.5.1	Types of records archived .....	36
5.5.2	Retention period for archive .....	36
5.5.3	Protection of archive .....	37
5.5.4	Archive backup procedures .....	37
5.5.5	Requirements for time-stamping of records .....	37
5.5.6	Archive collections system (internal or external) .....	37
5.5.7	Procedures to obtain and verify archive information .....	37
5.6	Key changeover .....	37
5.7	Compromise and disaster recovery .....	37
5.7.1	Computing resources, software, and/or data are corrupted .....	37
5.7.2	Entity private key compromise procedures .....	37
5.7.3	Entity private key compromise procedures .....	38
5.7.4	Business continuity capabilities after a disaster .....	38
5.8	CA or RA termination .....	38
<b>6</b>	<b>Technical security controls .....</b>	<b>40</b>
6.1	Key pair generation and installation .....	40
6.1.1	Key pair generation .....	40
6.1.2	Private key delivery to the subscriber .....	40
6.1.3	Public key delivery to certificate issuer .....	41
6.1.4	CA public key delivery to relying parties .....	41
6.1.5	Key sizes .....	41
6.1.6	Public key parameters generation and quality checking .....	42



6.1.7	Key usage purposes .....	42
6.2	Private key protection and Cryptographic Module Engineering Controls .....	43
6.2.1	Cryptographic module standards and controls .....	43
6.2.2	Private key (n out of m) multi-person control .....	43
6.2.3	Private key storage on the cryptographic module .....	44
6.2.4	Method of activating private key .....	44
6.2.5	Method of deactivating private key .....	44
6.2.6	Method of destroying private key .....	44
6.3	Custody, copy and recovery of keys .....	45
6.3.1	Policy and practices of storage, copy and recovery of keys .....	45
6.3.2	Private key archival .....	45
6.4	Other aspects on key pair management .....	45
6.4.1	Public key archival .....	45
6.4.2	Certificate operational periods and key pair usage periods .....	45
6.5	Activation data .....	46
6.5.1	Activation data generation and installation .....	46
6.5.2	Activation data protection .....	46
6.6	Computer security controls .....	46
6.6.1	Specific computer security technical requirements .....	46
6.6.2	Computer security rating .....	47
6.7	Life cycle technical controls .....	47
6.7.1	System development controls .....	47
6.7.2	Security management controls .....	47
6.7.3	Life cycle security controls .....	47
6.8	Network security controls .....	48
6.9	Time-stamping .....	48
<b>7</b>	<b>Certificate, CRL, and OCSP profiles .....</b>	<b>49</b>
7.1	Certificate profile .....	49
7.1.1	Version number(s) .....	49
7.1.2	Validity period of certificates .....	49
7.1.3	Certificate extensions .....	49
7.1.4	Algorithm object identifiers .....	51
7.1.5	Name forms .....	52
7.1.6	Certificate Policy Object identifier .....	52
7.1.7	Usage of Policy Constraints extension .....	52
7.1.8	Policy qualifiers syntax and semantics .....	52
7.2	CRL profile .....	52
7.2.1	Version number(s) .....	52
7.2.2	CRL and CRL entry extensions .....	52
<b>8</b>	<b>Compliance audits and other assessments .....</b>	<b>53</b>
8.1	Compliance audits .....	53
8.2	Frequency or circumstances of assessment .....	53
8.3	Identity/qualifications of assessor .....	53
8.4	Assessor's relationship to assessed entity .....	53
8.5	Topics covered by assessment .....	53
8.6	Actions taken as a result of deficiency .....	54
8.7	Communication of results .....	54





<b>9</b>	<b>Other business and legal matters .....</b>	<b>55</b>
9.1	Confidentiality of business information .....	55
9.1.1	Scope of confidential information .....	55
9.1.2	Information not within the scope of confidential information .....	55
9.1.3	Disclosure of suspension and revocation information.....	56
9.1.4	Responsibility to protect confidential information .....	56
9.1.5	Information disclosure by request of the subscriber.....	56
9.2	Privacy of personal information .....	56
9.3	Intellectual Property Rights .....	57
9.3.1	Property of certificates and revocation information .....	57
9.3.2	Property of Certification Policy and Certification Practice Statement.....	57
9.3.3	Property of information concerning to names .....	57
9.3.4	Key property .....	57
9.4	Representations and warranties .....	57
9.4.1	CA representations and warranties .....	57
9.4.2	Representations and warranties of subscribers and other participants .....	58
9.4.3	Limitations of warranties .....	58
9.4.4	Limitations of liability .....	58
9.4.5	Disclaimer of warranties.....	59
9.4.6	Fortuitous event or force majeure.....	59
9.4.7	Governing law .....	59
9.4.8	Clauses of severability, survival, entire agreement and notification .....	60
9.4.9	Applicable law, interpretation and competent jurisdiction.....	60
9.4.10	Dispute resolution procedures .....	61
<b>Annex A:</b>	<b>References.....</b>	<b>62</b>





## 1 Introduction

The Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, commonly known as eIDAS, provides a framework for the Trust Service Providers in connection with European Standards ETSI EN 319 401 (about Trusted Service Providers), ETSI EN 319 411-1 (about common policy requirements for certification authorities), ETSI EN 319 411-2 (about policy requirements for certification authorities issuing qualified certificates).

This document contains the **Certification Practice Statement of the Trusted Service Provider of the Ministry of Employment and Social Security (TSPM / PSCM)**, hereinafter, CPSM.

The CPSM details the obligations the TSPM agrees to comply in relation to technical and organizational security measures, 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 CPSM follows the specifications in RFC 3647 [IETF RFC 3647]. For a correct interpretation, it is recommended to the reader to acquire some general knowledge on PKI, electronic certificates and electronic signature.

The DPCM is published on the URL that appears on the Annex B: Electronic Links (URLs).

### 1.1 Overview

According to this DPCM and each certificate policy, TSPM issues, revokes, and offers information about the validity of the following types of certificates:

Qualified Certificate	Soporte	eIDAS Assurance Level	Purpose
Public Employee	Smart Card	High	Electronic Signature Authentication
Public Employee	HSM	Substantial	Electronic Signature Authentication
Electronic Seal	Container	Substantial	Electronic Signature

The full requirements and specific features for each type of certificate issued by the TSPM are defined in each certificate policy.

#### 1.1.1 Relationship between CPSM and other documents

The CPSM is complemented by documents describing the profiles of certificates.

### 1.2 Document name and identification

The name of this document is **Ministry Certification Service Provider Certification Practice Statement**, whose information appears on the version control of this document (page ii)



The DPCM is published on the URL that appears on the Annex B: Electronic Links (URLs).

### 1.3 PKI Participants

The participants in the certification services that play a role in the TSP are the following:

- The Certification Authority.
- The Registration Authority.
- The Validation Authority.
- The subscribers of the certificates.

#### 1.3.1 Certification Authorities

The *Subdirección General de Tecnologías de Información y las Comunicaciones, SG TIC*, manages the Certification Authority that issues and revokes the certificates in order 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.

There are one Root Certification Authority and some Subordinate Certification Authorities. The data certificate of the Root Certification Authority are the following:

Issuer	CN = AC RAIZ MEYSS 2.5.4.97 = VATES-S2819001E SERIALNUMBER = S2819001E OU = PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS OU = S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES O = MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL L = MADRID C = ES
Subject	CN = AC RAIZ MEYSS 2.5.4.97 = VATES-S2819001E SERIALNUMBER = S2819001E OU = PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS OU = S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES O = MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL L = MADRID C = ES
Serial Number	58 41 50 86
Validity Period	viernes, 02 de diciembre de 2016 11:14:28 domingo, 02 de diciembre de 2046 11:44:28
Hash	sha1 28 56 1D 3F 12 2A B1 F1 16 31 DE AF A3 E0 50 BB 51 FE A4 D2



The data certificate of the Subordinate Certification Authority 1 responsible for issuing the public employee certificates centralized and managed by an HSM and the electronic seal certificates are the following:

Issuer	CN = AC RAIZ MEYSS 2.5.4.97 = VATES-S2819001E SERIALNUMBER = S2819001E OU = PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS OU = S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES O = MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL L = MADRID C = ES
Subject	CN = SUBCA1 MEYSS 2.5.4.97 = VATES-S2819001E SERIALNUMBER = S2819001E OU = PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS OU = S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES O = MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL L = MADRID C = ES
Serial Number	58 41 50 C1
Validity Period	viernes, 02 de diciembre de 2016 12:26:29 martes, 02 de diciembre de 2036 12:56:29
Hash	sha1 E2 CB BC 57 AD 98 42 0C 34 7D A7 C2 57 79 5D C5 FD C5 FD 27

The data certificate of the Subordinate Certification Authority 2 responsible for issuing the public employee certificates in a smart card are the following:

Issuer	CN = AC RAIZ MEYSS 2.5.4.97 = VATES-S2819001E SERIALNUMBER = S2819001E OU = PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS OU = S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES O = MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL L = MADRID C = ES
Subject	CN = SUBCA2 MEYSS 2.5.4.97 = VATES-S2819001E SERIALNUMBER = S2819001E OU = PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS OU = S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES O = MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL L = MADRID C = ES
Serial Number	58 41 50 C2
Validity Period	viernes, 02 de diciembre de 2016 12:52:49 martes, 02 de diciembre de 2036 13:22:49
Hash	sha1 02 1C E9 FB 78 00 CF DD 58 31 BF 89 69 8D 82 5F 4E D2 0D 29



For historic validation reasons, the data certificate of the previous root certificate are the following:

SHA-256:

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	12 1c 2e 70 09 a0 97 a6
Validity Period	jueves, 05 de noviembre de 2009 17:17:45 domingo, 03 de noviembre de 2019 17:17:45
Hash	sha1 0e 9e 4f 47 68 6e b0 37 49 56 a0 6c c7 b0 4d 1a 90 b3 bf 50

SHA-1 previous version:

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

Each type of certificate is described in a document with its certificate policy.

### 1.3.2 Registration Authorities

The Registration Entities assist the TSPM in the functions of identification, registration and authentication of subscribers as well as other tasks related to the management of certificates and the correct assignment to the applicants. 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 Authorities are composed jointly by telematics services that enable the lifecycle management of the certificates and personally attended endpoints dedicated to this purpose.

The Registration Authorities carry out the identification and authentication of the certificate applicants according to the rules of the CPSM and the contract agreement signed with the Certification Authority. In the event that the Registration Authorities belong to the Ministry, it would not be required the signature of any contract 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 Authority may rely on one or more Registration Authorities freely chosen to provide the certification service.

The services offered by the Registration Authorities are available on the Intranet of the Ministry

### **1.3.3 Validation Authority**

The Validation Authorities are responsible for providing information about the validity of electronic certificates issued by a Certification Authority. To provide this information, the Validation Authorities 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 Authority of the TSPM offers its service to any interested party so that they can check the certificate status instantly, safely and trustily.

The access to status validation services is publicly and freely offered. OCSP validation service and the certificate that signs OCSP responses appear in Annex B: **¡Error! No se encuentra el origen de la referencia.**

### **1.3.4 End Users**

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

- Certificate requesters.
- Certificate subscribers.
- The responsible for the certificate.
- The relying parties (certificate verifiers).



#### **1.3.4.1 Certificate Requesters**

Any 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 requester must be an employee of the Ministry.

For electronic seals and OCSP responder and Time Stamping, the request must come from public employees.

#### **1.3.4.2 Certificate Subscribers**

The certificate subscribers are the Public Administrations and the natural or legal persons identified in the *Subject* field of the certificate who ensure the correct use of the key pairs and the associated certificate in accordance with CPSM.

The Electronic Seal certificates identify the associated entity in the *Subject* field (specifically in the *Common Name* attribute).

#### **1.3.4.3 The responsible for the certificate**

The responsible for the certificates, this means the responsible for the custody of the certificates, 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* of the certificate *Subject* field.

For all types of Public Employee certificates issued by the TSPM, the responsible person is the subscriber.

In the case of 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 TSPM.

#### **1.3.4.4 Relying parties**

The certificate verifiers are the entities (including natural and legal persons, Public Administrations and other organizations) that, using a certificate, issued by a Certification Authority operating under the CPSM, verify the integrity of an electronically signed message; identify the message sender; or set up a confidential communication channel with the certificate owner, trusting on the validity of the relationship between the subscriber name and the public key of the certificate provided by the certification authority. Any 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. The 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 defined by the CPSM.





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

Each type of certificate issued by the TSPM with correspondence with the ones defined by [Ley 40/2015] and eIDAS 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 CPs.

## **1.5 CPSM administration**

### **1.5.1 Organization administering the document**

The *Subsecretaría del Ministerio* 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 *Subsecretaría* 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 *Servicio Público de Empleo Estatal* (Public Employment Service) and the units depending of *Secretaría de Estado de la Seguridad Social*.

Therefore, the CEO of the SGTIC is the responsible for the TSPM (including Certification Authorities, Registry and Validation authorities) and therefore the responsible for the definition, review and disclosure of CPSM. There are two assistants to the TSPM responsible, advising and collaborating in the definition, analysis and improvement of TSPM and replacing her in case of prolonged absence, in accordance with applicable law. Both assistants are the Assistants of the SGTIC.

### **1.5.2 Contact person**

Subdirección General de Tecnologías de la Información y las Comunicaciones  
C/ Paseo de la Castellana 63  
28071 – Madrid  
[admin\\_ca@mtin.es](mailto:admin_ca@mtin.es) / [admin\\_ca@meyss.es](mailto:admin_ca@meyss.es)  
Phone Number: +34 91 363 11 88/9 - Fax : +34 91 363 07 73

### **1.5.3 CPS administration procedures**

#### **1.5.3.1 Change Control**

The responsible for the TSPM is the responsible for the approval and deployment of the proposed changes to the CPSM following the Documentation Quality Plan.



The TSPM 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 data 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**

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

<http://ca.empleo.gob.es/meyss/DPCyPoliticass>

#### **1.5.3.3 CPS Approval**

The responsible is the responsible for the approval of the CPSM as stated in the Documentation Quality Plan.

### **1.6 Definitions and acronyms**

#### **1.6.1 Definitions**

The CPSM uses the following definitions:

Authentication	Electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form.
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 containing 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.
Directory	Repository of information that follows the X.500 de ITU-T Standard.
DN	Univocal identification for an item within a X.500 directory.
Electronic signature	Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign
Electronic signature certificate	Electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person
Hash function	Mathematical function that compresses any amount of data into a small fixed datum called a hash value, univocally associated with the initial data, so it is impossible to get two



	different messages that generates the same result after applying the hash function.
Hash or digital footprint	A numeric value resulting from applying a mathematical algorithm against a set of data with the property of being univocally associated with the initial data.
HSM	Hardware Security Module used to store keys and to make cryptographic functions safely.
Identification	Process for recognizing the identity of an applicant or certificate holder.
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.
OTP	One Time Password. Code for a single use that allows authentication for just one time.
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 blocked after repeated introduction of incorrect PIN.
Qualified trusted service provider	Trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body.
RFC	Request For Comments, standard documents emitted by IETF (Internet Engineering Task Force).
Signatory	Natural person who creates an electronic signature
Trusted service provider	Natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider.
Validation	Process of verifying and confirming that an electronic signature or a seal is valid.

### 1.6.2 Acronyms

AAPP	Administraciones Públicas
AGE	Administración General del Estado / Spain Public Administration
RA	Registration Authority
VA	Validation Authority
C	Country
CA	Certification Authority
CDP	CRL Distribution Point
CEC	Certificate Issuance Code
CEN	Comité Européen de Normalisation



CEPCHSM	Public Employee Certificate Centralized and Managed by HSM
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CPSM	Certification Practice Statement of the Ministry
CRL	Certificate Revocation List
CSP	Cryptographic Service Provider
CSR	Certificate Signing Request
CWA	CEN Workshop Agreement
DC	Data Center
DN	Distinguished Name
eIDAS	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
ETSI	European Telecommunications Standard Institute
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
LDAP	Lightweight Directory Access Protocol
LOPD	Law on Protection of Personal Data (Ley Orgánica de Protección de Datos de Carácter Personal)
MINETAD	Ministry of Industry, Energy and Digital Agenda
MINHAP	Ministry of Finance and Public Administration
O	Organization
OU	Organizational Unit
OID	Object Identifier
OCSP	On-line Certificate Status Protocol
PA	Public Administration
PIN	Personal Identification Number
PKCS	Public Key Infrastructure Standards
PKI	Public Key Infrastructure
PKIX	Internet Engineering Task Group
PSCM	TSPM
PUK	PIN UnlocK Code (código o clave de desbloqueo del PIN)
RA	Registration Authority
RFC	Request For Comments
SGTIC	Subdirección General de Tecnologías de la Información y las Comunicaciones
TSL	Trust-service Status List
TSP	Trust Service Provider
TSPM	Trust Service Provider of the Ministry
VA	Validation Authority



## **2 Publication and Repository Responsibilities**

### **2.1 Repositories**

The Certification Authority of the TSPM has a repository of information available 24 hours 7 days a week. In the event of catastrophic system failure beyond the control of TSPM, 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 TSPM holds in its repository the following information:

- The different versions of the CPSM and documents defined therein.
- The CPs for each certificate to develop further requisites within the framework of the CPSM.
- All previous versions of that documentation.
- The certificate revocation lists and other information about revocation status of certificates.

This documentation shall be kept available for a minimum period of fifteen years from the issuance of the certificate. The TSPM 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 TSPM satisfies the initial registration and filing of certain information determined by the technical specifications [ETSI EN 319 411-2] 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 information**

The location of the CPSM is in Annex B:

The locations of the Root Certification Authority Certificate and SubCA Certificates are in Annex B:

The location of the OCSP service is in Annex B:

The location of the CRL publication is in Annex B:

### **2.3 Time for frequency of publication**

The above information, including CPs and CPSM, is published as soon as it is approved. Any change in the CPSM is governed by the provisions of section 1.5.3 of this document.

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

### **2.4 Access controls on repositories**

The TSPM 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 TSPM 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 Naming

#### 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 6818].

#### 3.1.2 Administrative Identity and Normalization

The TSPM uses the normalized naming schema *Identidad Administrativa* proposed by the Spanish administration for each type of certificate and policy. Thus using a common framework, assigning exactly the same name to seals, offices, organizations, jobs 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:

eIDAS Certificates:

- Electronic Seal Certificate for automated administrative procedures (Medium Level)  
*2.16.724.1.3.5.6.2*
- Public Employee Certificate (High Level)  
*2.16.724.1.3.5.7.1*
- CEPCHSM (Medium Level)  
*2.16.724.1.3.5.7.2*

pre-eIDAS Certificates:

- Electronic Seal Certificate for automated administrative procedures (Medium Level)  
*2.16.724.1.3.5.2.2*
- Public Employee Certificate (High Level)  
*2.16.724.1.3.5.3.1*

Certificate	Mandatory “Identidad Administrativa” fields
ELECTRONIC SEAL	<ul style="list-style-type: none"><li>• Type of certificate</li><li>• Name of the subscriber entity</li><li>• NIF of the subscriber entity</li><li>• System or component denomination</li></ul>
PUBLIC EMPLOYEE	<ul style="list-style-type: none"><li>• Type of certificate</li><li>• Name of the entity where is employed</li><li>• NIF of the entity where is employed</li><li>• DNI/NIE of the responsible</li><li>• Given name</li><li>• First surname</li><li>• Second surname</li></ul>



CEPCHSM	<ul style="list-style-type: none"><li>• Type of certificate</li><li>• Name of the entity where is employed</li><li>• NIF of the entity where is employed</li><li>• DNI/NIE of the responsible</li><li>• Given name</li><li>• First surname</li><li>• Second surname</li></ul>
---------	---

Certificate	Optional “Identidad Administrativa” fields
ELECTRONIC SEAL	<ul style="list-style-type: none"><li>• DNI/NIE of the responsible</li><li>• Given name</li><li>• First surname</li><li>• Second surname</li><li>• E-mail address</li></ul>
PUBLIC EMPLOYEE	<ul style="list-style-type: none"><li>• Personal identification number</li><li>• E-mail address</li><li>• Organizational unit</li><li>• Position held</li></ul>
CEPCHSM	<ul style="list-style-type: none"><li>• Personal identification number</li><li>• E-mail address</li><li>• Organizational unit</li><li>• Position held</li></ul>

### 3.1.3 Need for names to be meaningful

The certificate names are understood and interpreted in accordance with the law applicable to the names of natural and legal persons that own 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 Anonymity or pseudonymity of subscribers

Not allowed.

### 3.1.5 Rules for interpreting various name forms

The coding standards for the fields follow the recommendations of [IETF RFC 6818] using UTF-8.

The TSPM 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<sup>1</sup> y CEPCHSM<sup>2</sup>:
  - 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 Seal Certificate for the Automated Administrative Procedures<sup>3</sup>:
  - Description of certificate type.
  - System or component denomination.
  - Name of the subscriber entity.
  - Identification number of the subscriber entity (eg. NIF/CIF).

### 3.1.6 Uniqueness of the names

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

She may also have certificates of the same type issued by different certification authorities.

---

<sup>1</sup> Representation relationship is not admitted for this type of certificate.

<sup>2</sup> Representation relationship is not admitted for this type of certificate..

<sup>3</sup> Representation relationship is not admitted for this type of certificate.



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

### **3.1.7 Recognition, authentication, and role of trademarks**

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

Also, the Certification Authority 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 Authority 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 identity validation**

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

### **3.2.1 Method to prove possession of private key**

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.

In the context of the CEPCHSM, once the public employee has been registered in the system with an advanced level of the registration guarantee and specifically requested the issuance of any of her CEPCHSM with the authentication factors in place, such issuance will start the first time the public employee access the generation process.

The system will inform the public employee that her CEPCHSM is going to be issued. Then the system will generate the corresponding private key and store it safely in the system, ensuring that its use is under the exclusive control of the holder.

The generation of the certificate must be compliant with the requirements that the law establishes regarding the maximum period allowed since the citizen carried out the registration in person.

### **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 individual identity**

This section contains requirements for the verification of the identity of a natural person applicant to a certificate.

#### **3.2.3.1 Required identification elements**

The TSPM uses the following items, reflected in a statement signed by the certificate requester, to prove her identity. 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 TSPM keeps written or electronic evidences 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 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 Authority.

#### **3.2.3.3 Obligation of personal presence**

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

- Public Employee Certificate (high level).
- Public Employee Certificate (medium level) (CEPCHSM)

CEPCHSM allows the possibility of using a qualified electronic certificate.

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

- 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.

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



#### ***3.2.3.4 Relationship of the natural person with any organization***

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

#### **3.2.4 Non-verified subscriber information**

No subscriber information is included in any certificates if it has not been verified.

#### **3.2.5 Criteria for interoperation**

The CPSM does not consider the establishment of trust relationships with external Trust Services Providers (TSP).

### ***3.3 Identification and authentication for re-key requests***

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

#### **3.3.1 Identification and authentication requirements for routine re-key**

By default, the TSPM does not allow periodical renewals of the certificates. In the case of CEPCHSM, certificate renewal is carried out so that the legal requirements regarding the maximum period allowed since the public employee carried out the registration in person are met. Otherwise, to renew the certificate the employee will have to attend in person at the registration office following the established procedures for checking the identity of the employee.

#### **3.3.2 Identification and authentication requirements for re-key after certificate revocation**

By default, the TSPM does not allow certificate renewal after its revocation, as stated in the previous point.

### ***3.4 Identification and authentication for revocation request***

The TSPM authenticates requests and reports relating to revocation of any certificate, verifying that they are from a trusted person.

As such, any request signed with a qualified certificate is valid as well as any request coming from a verified internal email account.



## 4 Certificate Life-Cycle Operational Requirements

### 4.1 Certificate Application

#### 4.1.1 Who can submit a certificate application

There must be a request before the issuance and delivery of any electronic seal or public employee certificate.

##### 4.1.1.1 Requirements for Public Employee Certificates

The request for the issuance of the certificate must be signed by the applicant who is required to prove his identity, according to the provisions of section 3.2 of this document. This entails the delivery of a unique secret code of the certificate and delivery of the signature cryptographic device and associated passwords. This secret code, 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 profile and use of the certificate, including in particular information about the Certification Authority, CPSM, and CPS applicable and their duties, powers and responsibilities.
- Information about the certificate and the cryptographic device.
- Obligations of the certificate subscriber.
- Liability of the certificate subscriber.

These contents may be communicated indirectly by stating the URL where the subscriber may download the CPSM.

##### 4.1.1.2 Requirements for CEPCHSM

The request for the issuance of the certificate must be signed by the applicant who is required to prove his identity, according to the provisions of section 3.2 of this document. This entails either to attend in person to establish the authentication factors that will be used later to generate and download the certificates or to use a qualified electronic certificate to do it by electronic means.

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

- Basic information on the profile and use of the certificate, including in particular information about the Certification Authority, CPSM, and CPs applicable and their duties, powers and responsibilities.
- Information about the certificate.
- Obligations of the certificate subscriber.
- Liability of the certificate subscriber.

These contents may be communicated indirectly by stating the URL where the subscriber may download the CPSM.



#### **4.1.1.3 Requirements for Electronic Seal Certificates**

Any request for these certificates must be made by public employees. The applicant must include her data and the subscriber data. This subscriber must be correctly identified during the delivery of the certificate.

The responsible for the Certification Authority shall authorize the issuance of any electronic seal certificates of electronic seal.

In those cases where the Electronic Seal Certificate includes a public administration entity, its identity must be verified through administrative databases or other equivalent documents.

#### **4.1.2 Enrollment process and responsibilities**

The entity that belongs to the Registration Authority that performs the registry shall ensure that all certificate requests are complete, accurate and properly authorized. Prior to the issuance and delivery of the certificate, the entity shall inform to the subscriber or to the responsible for the certificate about the terms and conditions applicable. Such information shall be communicated in a durable medium, on paper or electronically, and in easily understandable language.

The request shall include 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 TSPM or by an authorised partner.

### **4.2 Certificate application processing**

#### **4.2.1 Specifications for Public Employee Certificates**

In addition to the information appearing in the request, the Certification Authority shall:

- Include 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.
- Ensure the date and time of issue of a certificate.
- Use trustworthy systems and products which are protected against modification and ensure the technical security and, where appropriate, cryptographic of the supporting certification processes.
- Ensure that the certificate is issued by systems using anti-counterfeiting and when the private keys are generated, shall ensure the secrecy of the keys during the process of generating those keys.

#### **4.2.2 Specifications for Electronic Seal Certificates**

Once the request for an electronic seal certificate is received, the Certification Authority shall review the information provided with special emphasis on the identity of the responsible for the certificate and the authorization to its issuance. If any information is not correct, the Certification Authority shall deny the request. If the information in the request is correct, the Certification Authority shall issue the certificate.



## **4.3 Certificate issuance**

### **4.3.1 CA actions during certificate issuance**

The Certification Authority shall:

- Use 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 Authority generates the key pair, the CA shall use a method of certificate generation that is linked safely with the key generation process and shall ensure that the private key is delivered safely to the subscriber or the responsible for the Certificate.
- Protect the confidentiality and integrity of the registration data, especially in the event that they are exchanged with the subscriber or the responsible person for the Certificate.
- Store issued certificates with access permissions and security controls regulated and necessary for this, ensuring the security of communications.
- Not store the private keys associated with the certificates except in the case of CEPCHSM in which the system shall generate at that exact moment the private key and store it safely in the system, ensuring that its use is under the exclusive control of the subscriber.

Additionally the Certification Authority shall:

- Include information on the certificate in compliance with eIDAS and Law 59/2003 (LFE).
- Indicate the date and time the certificate was issued.
- Use a management procedure for the secure signature creation devices ensuring that they are safely delivered to the subscriber or responsible for the certificate.
- Use products protected from tampering, ensuring technical and cryptographic security of the certification processes that they support.
- Use measures against forgery of certificates, and to ensure the secrecy of the keys during the process of generating the same.
- When issuing a certificate in accordance with a request, the CA shall deliver the notifications established in the following section.

### **4.3.2 Notification to subscriber by the CA of issuance of certificate**

The approval of the request for certificates of public employee will be notified implicitly by the issuance and delivery of the certificate.

In the context of a CEPCHSM at the end of the process of generating the certificate, the public employee shall be informed that the certificate is available and can be used from that moment.

Otherwise, the Certification Authority shall notify the requester of the rejection of the request by email, telephone or any other means using the contact data in the request.



## **4.4 Certificate acceptance**

### **4.4.1 Conduct constituting certificate acceptance**

In the case of Public Employee Certificates, the Certification Authority shall provide the subscriber access to the certificate through the application designed for that purpose. This application shall allow the generation of the key pair and shall download the certificate in the cryptographic device. In order to download the certificate, it is mandatory to use the secure code.

In the case of the CEPCHSM, the Certification Authority shall provide the subscriber with access to the certificate through the system designed for that purpose. The system shall inform the public employee about the generation of the key pair, the issuing of the certificate and its storage in the system, ensuring that its use is under the exclusive control of the subscriber. Upon completion of the process of generating the certificate the public employee shall be informed that the certificate is available and could be used from that moment.

In the case of electronic seal certificates, the Certification Authority shall safely deliver the certificate. This delivery will occur after identifying the subscriber or responsible in person. Along with the certificate, some information shall be delivered with the following contents:

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

### **4.4.2 Certificate acceptance**

The cryptographic device storing the certificate (for Public Employee Certificates) shall be accepted by signing the request form by Subscriber or, if applicable, by the person responsible for the certificate.

The Public Employee Certificated shall be accepted by using the computer proceeding to generate and 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 shall be deemed to accept the certificate by the downloading action on that device.

In the case of CEPCHSM a second authentication factor shall be entered for downloading and accepting the certificate. The mere act of issuing the CEPCHSM shall include its implicit acceptance.

For Electronic Seal Certificates, the certificate shall be deemed accepted by signing the request and delivery form by the responsible for the certificate.

### **4.4.3 Publication of the certificate by the CA**

Certificate data identification shall be published in internal repositories, with restricted access.





#### **4.4.4 Notification of certificated issuance by the CA to other parties**

Not applicable.

### **4.5 Key pair and certificate usage**

#### **4.5.1 General usage requirements**

The 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 shall be used only in accordance with applicable law, especially considering the import and export restrictions in each moment.

The *Key Usage* extension shall be 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 programmed, nor can be controlled by the TSPM.

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

The CEPCHSM main goal is the authentication and electronic signature of electronic documents.

#### **4.5.2 Usage by subscribers**

The subscribers shall:

- Comply with the requirements established in this document and in Article 23.1 of the LFE.
- Provide to the Registration Authorities accurate, complete and truthful information regarding the data they request to carry out the registration process.
- Know and accept the conditions of use and restrictions on use of the certificates, in particular those contained in the CPSM that are applicable, as well as the modifications made on them
- Communicate to the competent entity, through the mechanisms enabled for this purpose, any malfunction of the certificate.
- 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 Authority of TSPM 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, she shall:

- 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.



- Do not disclose any authentication factor that allows the use of private keys associated with CEPCHSM.

### **4.5.3 Relying party public key and certificate usage**

Those third parties who trust on the certificates issued by a Certification Authority of the TSPM shall:

- 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 6818] standards.
- Establish trust in the Certification Authority that issued the certificate verifying the certificate chain according to the recommendations of the X.509 v3 and [IETF RFC 6818] standards.
- Use the certificates belonging to types defined in [Ley 40/15] only for those transactions that are subject to that indicated in [Ley 40/2015] or in the CPSM.

### **4.6 Certificate renewal with key pair reused**

In general, TSPM does not allow certificate renewal without key renewal. In the case of the CEPCHSM the certificates renewal within the scope of the CPSM will be carried out by changing the keys.

### **4.7 Certificate renewal without key pair reused**

In general, the procedure applicable to the renewal of the certificate with key renewal involves the application for a new certificate with new keys associated. In the case of CEPCHSM, all renewals, regardless of the cause, will be made changing the keys. In this context it is allowed the renewal with a change in the keys of a certificate because the certificates expired or the password set at the issuance was forgotten.

### **4.8 Certificate modification**

Any certificate modification refers to the case where the attributes of the subscriber or those about the responsible for the certificate, have changed. The TSPM does not allow any modification of certificates.

### **4.9 Certificate revocation and suspension**

The revocation of a certificate is the act by which cancels the validity of a certificate before its expiration date. The effect of the revocation of a certificate is the loss of validity, resulting in the permanent cessation of its effectiveness in accordance with its typical uses and therefore the revocation of a certificate disables the legitimate use of it by the subscriber.

The TSPM does not allow any suspension of certificates.



#### **4.9.1 Circumstances for revocation**

The Certification Authority of the TSPM 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 Authority that issued the certificate, provided that affects the reliability of the certificates issued from this incident.
  - Breach by the Certification Authority, 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.
  - Compromise of the private keys of the public employee for loss, theft, modification, disclosure or revelation of the personal password that allows the activation of those keys, even by any other circumstances, including accidental that indicates the use of the private key by an entity other than the subscriber.
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 for the certificate.
4. Circumstances that affect the subscriber or the responsible for the certificate:
  - Termination of the relationship between the Certification Authority 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 for the Certificate.
  - Breach by the applicant of the certificate of the established requirements in the certificate application.
  - Breach by the subscriber or responsible for 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 Authority 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 Who can request 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 Procedure for revocation request

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

The revocation of a certificate should be sent to the Certification Authority 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 Authority or, where appropriate, to the Registration Entity. Contact details are given in the section 1.5.2 of the CPSM. Subscribers of Public Employees certificates will be able to request the certificates revocation through the application available 24x7. Requests will be processed automatically and certificated revoked immediately.

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 Authority.
- The Certification Authority 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 Authority issuing the certificate will revoke it, publishing its serial number and other identifying information in the CRL. The Certification Authority cannot reactivate the certificate once revoked.

#### **4.9.4 Revocation request grace period**

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

#### **4.9.5 Time within which CA must process the revocation request**

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

#### **4.9.6 Revocation checking requirement for relying parties**

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

The Certification Authority of the TSPM 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 TSPM (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 CRL issuance frequency**

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

The Certification Authority 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 latency for CRLs**

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 On-line revocation/status checking availability**

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

The TSPM 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 TSPM is committed to provide a level of service for these services at least 99%.

#### **4.9.10 On-line revocation checking requirements**

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 TSPM 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.
- The CRL Distribution Point will contain the name of the CRL location.

The location of the CRL is in Annex B:

The location of the historic CRLs is in Annex B:

#### **4.9.10.2 OCSP Protocol**

The TSPM provides certificate status verification via OCSP, according to [IETF RFC 6960] indicating that fact inside the certificates, using the extension *AuthorityInfoAccess* defined in technical specifications [IETF RFC 6818] and [RFC 6960], as follows:

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

The location of the OCSP service is in Annex B:

#### **4.9.11 Other forms of revocation advertisements available**

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

#### **4.9.12 Special requirements re key compromise**

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

### **4.10 Certificate status services**

#### **4.10.1 Operational characteristics**

The CRL can be downloaded from the repository of the Certification Authority 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 TSPM 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 Authority, the CA will make its best to recover the services as soon as possible.

#### **4.10.3 Optional features**

Not stipulated.

#### **4.11 End of subscription**

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 in section 4.9.1.
- 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 Authority.

#### **4.12 Key escrow and recovery**

In the area of CEPCHSM, the private key generated and associated with this certificate shall be kept by the Certification Authority TSPM, taking into account that access to this key will be made by means that guarantee, with a high level of confidence, that only the public employee has the control over it.

In this regard, access to said key can only be made by the subscriber through an application to that effect where the public employee shall be authenticated with user name and password and also must enter his/her second authentication factor. Afterwards when signing, the public employee must enter the PIN that protects the certificate which has to be only known by the public employee and not stored in the systems along with the second authentication factor.

According to the eIDAS, the TSPM (as a trust service provider issuing qualified certificates) when managing electronic signature creation data on behalf of the signatory may duplicate the electronic signature creation data solely in order to make a backup copy of such data provided that the following requirements are met:

- the security of the duplicated data sets is at the same level as for the original datasets;
- the number of sets of duplicated data does not exceed the minimum necessary to ensure continuity of the service.

The TSPM will not duplicate signature creation data for any other purpose.



## **5 Facility, management and operational controls**

### **5.1 Physical controls**

The TSPM 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 TSPM 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 TSPM.
- Fires and floods and other natural disasters.
- Collapse of the structure.
- Failure of support systems (electricity, telecommunications, etc.).

#### **5.1.1 Site location and construction**

The location of the installations allows the presence of security forces in a reasonably short term after an incident is reported to them. The TSPM 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 TSPM establishes multiple levels of access restriction to the different defined perimeters and physical barriers.

For access to the premises of TSPM 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 Authority 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.

All critical operations with certificates are performed in physically secure facilities, with specific levels of security for critical items and protected 24 hours a day, 7 days a week. These systems are isolated from others, so that only authorized personnel can access them.

### **5.1.3 Power and air conditioning**

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

### **5.1.4 Water exposures**

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

### **5.1.5 Fire prevention and protection**

All the facilities and assets of the TSPM have automatic systems for fire detection and firefighting.

Specifically, the cryptographic devices and containers that store the TSPM 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 Off-site backup**

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

## **5.2 Procedural controls**

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

### **5.2.1 Trusted Roles**

The TSPM 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 Authority 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 Authority administrators are as follows:

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

Operators of the Certification Authority 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 Authority 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 Authority and the subscribers.
- Receive and distribute certificates of subscribers.



The Certification Authority 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 required per 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 role**

The TSPM identifies and authenticates the personnel before accessing the corresponding reliable function. All roles of the Certification Authority may be identified using electronic certificates issued by the own Entity of Certification. In particular, HSM administrators and operators are identified and authenticated on the HSM using shared secret techniques in cryptographic cards specific for HSM.

### **5.2.4 Roles requiring separation of duties**

The following tasks are performed at least by two persons:

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

## **5.3 Personnel controls**

### **5.3.1 Qualifications, experience and clearance requirements**

The TSPM 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 TSPM 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 TSPM 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 check procedures**

The TSPM 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 Training requirements**

The TSPM 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 Authority 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 Retraining frequency and requirements**

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

### **5.3.5 Job rotation frequency and sequence**

The TSPM 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 TSPM has a disciplinary system to debug the responsibilities arising from unauthorized actions, which is appropriate to the applicable labour 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 Independent contractor requirements**

The TSPM 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 TSPM facilities.

### **5.3.8 Documentation supplied to personnel**

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



## **5.4 Audit Logging Procedures**

### **5.4.1 Types of events recorded**

The TSPM 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 TSPM keys.
- Changes in certificate issuance policies.
- Attempts to entry and exit of the system.
- Unauthorized attempts to access TSPM 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 its reception, use and uninstallation.
- 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 TSPM 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 TSPM.

### **5.4.2 Frequency of processing log**

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 Retention period for audit log**

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 log**

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 cannot remove or destroy the records of events before the expiration of his storage term.

### **5.4.5 Audit log backup procedures**

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

### **5.4.6 Audit collection system (internal vs external)**

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 Notification to event-causing subject**

When the accumulation system of audit log records an event, it is not necessary to send a notification to whom has caused the event. It is communicated if the result of their action was successful or not, but not that the action has been audited.

### **5.4.8 Vulnerability assessments**

The TSPM 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 analyses are performed daily, monthly and annually in accordance with the Audit Plan or document replacing it from the TSPM.

## **5.5 Records archival**

The TSPM 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 records archived**

The TSPM 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 Retention period for archive**

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



### **5.5.3 Protection of archive**

The TSPM maintains the integrity and confidentiality of the file containing the data included in issued certificates and archives the above statements completely.

### **5.5.4 Archive backup procedures**

The TSPM 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 Requirements for time-stamping of records**

The TSPM 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 Archive collections system (internal or external)**

The TSPM 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 TSPM or external location. In particular, it will be recorded any access or attempt to access audit data.

## **5.6 Key changeover**

Not applicable.

## **5.7 Compromise and disaster recovery**

### **5.7.1 Computing resources, software, and/or data are corrupted**

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 Entity private key compromise procedures**

In the event that the TSPM revokes the Certification Authority 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 Entity private key compromise procedures

The Business Continuity Plan of the TSPM 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 TSPM key are no longer valid. For this, the following steps will be executed:
  - TSPM certificate revocation.
  - Corresponding CRL publishing.
  - Massive Revocation of the Certificates generated by the Certification Authority, proceeding to their elimination by the mechanisms implemented in the system for that purpose.

### 5.7.4 Business continuity capabilities after a disaster

The set of systems that make up the Certification Authority 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 TSPM has a backup or disaster recovery centre, which continues such services in case of a disaster or maintenance of the facilities that house the primary system. The backup centre offers physical security protections detailed in the corresponding Security Plan.

The TSPM 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 TSPM 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 TSPM.

## 5.8 CA or RA termination

The TSPM 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 TSPM will follow these procedures in accordance with art. 21 of the LFE:

- Must notify it to the signatories using electronic certificates issued by the TSPM and applicants for certificates issued in favour 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 TSPM had issued electronic certificates to the public, the TSPM will communicate to MINETAD, 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.
- It will forward to MINETAD, 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 MINETAD 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 as well as the root certificates and their associated private keys.



## 6 Technical security controls

The TSPM 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 Key pair generation and installation

#### 6.1.1 Key pair generation

For the generation of the key root of the hierarchy of the TSPM 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 and [CCEAL4+]. The key pairs for VAs and RAs 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 smart card.
CEPCHSM	Medium	Key generation by the user centralized and managed by HSM. Keys generated by the cryptographic device centralized according to requirements set in certification FIPS 140-2 and accreditation [CCEAL4+].
ELECTRONIC SEAL	Medium	Key generation by the TSPM and delivery in PKCS#12 format (software support). <ul style="list-style-type: none"><li>Key generation using software. It implies that the user uses these keys in secure software container.</li></ul> Key generation by the requester in PKCS#10 format (software support). Delivery of the certificate in PKCS#7 format. <ul style="list-style-type: none"><li>Key generation by the user, using software.</li></ul>

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 of high level the private key is generated directly in the cryptographic device that complies with [CWA 14169].

In the case of CEPCHSM the private key is generated and managed by the HSM so it is never handed over to the subscriber since only access to its use is allowed.



Once the user is registered in the system with an advanced level of the registration guarantee and has specifically requested the issuance of any of his/hers certificates of centralized firm, such issuance will take place the first time the public employee access to the procedure for the certificate generation.

The system will inform the employee that it will issue a certificate of centralized signature. Then the system will generate the corresponding private key and store it safely in the system, ensuring that its use is under the exclusive control of the subscriber.

In the case of certificates headquarters stamp and certificate private key is generated by the Certification and delivered properly protected through a PKCS # 12.

### 6.1.3 Public key delivery to 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 TSPM 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 CA public key delivery to relying parties

The public key of the TSPM 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 TSPM is published in the repository, in the form of self-signed certificate, together with the CPSM ensuring that the key authenticates the TSPM. Users can access the repository to get the public keys of the TSPM.

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 by the AGE, which determines the strength and viability criteria applicable to each certificate policy according to [CCN-STIC-405].

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. Its application is differentiated in a higher and medium level of assurance.

- Root and Subordinate 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 certificates:

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

### 6.1.6 Public key parameters generation and quality checking

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 <sup>(4)</sup>.

CEPCHSM public key is encrypted according to [IETF RFC 5280] and PKCS # 1. The key generation algorithm is RSA.

#### 6.1.6.1 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 accreditation [CC EAL4 +].

#### 6.1.6.2 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 TSPM 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.

### 6.1.7 Key usage purposes

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

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

CERTIFICATE	KEYUSAGE	EXTENDED KEYUSAGE
PUBLIC EMPLOYEE (Authentication, High Level)	Digital Signature	Email Protection Client Authentication SmartCard Logon
PUBLIC EMPLOYEE (Non repudiation, High Level)	Content Commitment	Not Used

<sup>4</sup> The n-th Fermat number is  $F = (2)^{(2^n)} + 1$ .



PUBLIC EMPLOYEE HSM (Authentication Medium Level)	Digital Signature	Client Authentication
PUBLIC EMPLOYEE HSM (Signature Medium Level)	Content Commitment	Not Used
ELECTRONIC SEAL	Digital Signature, Content Commitment, Key Encipherment, Data Encipherment	Email Protection Client Authentication

## **6.2 Private key protection and Cryptographic Module Engineering Controls**

### **6.2.1 Cryptographic module standards and controls**

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

The implementation of each Certification Authority, 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 Authority.

The cryptographic module that protects the private keys associated with CEPCHSM also has accreditations [FIPS 140-2] and accreditation [CCEAL4 +] and the [CWA 14167].

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

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

### **6.2.2 Private key (n out of m) multi-person control**

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

The private key of the TSPM root CA is under multipersonal control. This is activated by the initialization of the Certification Authority 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 Authority.

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

The private key associated with the CEPCHSM is, with a high level of confidence, under the exclusive control of the responsible for the certificate (public employee) and protected by two-factor authentication.



### **6.2.3 Private key storage on the cryptographic module**

Private keys of the TSPM 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 cannot be extracted. These cards were used to enter 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 Method of activating private key**

The private key of the Certification Authority 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.

The activation of the private key associated with CEPCHSM requires that the public employee is authenticated with the user name and password, enters the second authentication factor and the certificate password protection only known by the public employee and not stored in the systems.

### **6.2.5 Method of deactivating private key**

In the case of the certificates of the TSPM 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.

For the CEPCHSM the deactivation of the private key occurs when logging out of the application used for signing.

### **6.2.6 Method of destroying private key**

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.

The private key associated with CEPCHSM is safely destroyed in any process of renewal and revocation as well as the copies made to ensure continuity of service.



## **6.3 Custody, copy and recovery of keys**

### **6.3.1 Policy and practices of storage, copy and recovery of keys**

Private keys of the Certification Authority of TSPM are stored in fireproof areas and protected by dual physical access controls. The custody of the private key set of root Certification Authority, 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 Authority of the TSPM 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 Authority 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 TSPM 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.

For CEPCHSM apply the process described in section 4.12 of the CPSM.

### **6.3.2 Private key archival**

Private keys of the TSPM Certification Entities are filed at the end of its period of operation, permanently. Private keys of other types of certificates are not filed except in the case of CEPCHSM. For these certificates the backup of the private key are stored according with the current legislation.

## **6.4 Other aspects on key pair management**

### **6.4.1 Public key archival**

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

### **6.4.2 Certificate operational periods and key pair usage periods**

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 Activation data generation and installation**

For the establishment of a Certification Authority cryptographic cards must be created, used for recovery and functioning activities. The TSPM Certification Authority 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 are used to carry out any type of operation with the Certification Authority so the operator shall enter the PIN associated to each card. 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 TSPM provides the subscriber a secure signature creation device, device activation data (PIN), are generated securely.

The activation of the private key associated with the CEPCHSM requires that the public employee is authenticated with the username and password and enters the second authentication factor.

### **6.5.2 Activation data protection**

Only authorized personnel, in this case the operators and administrators of the Certification Authority, 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 TSPM 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.

In the case of the key associated with CEPCHSM, the public employee is the only one who knows the personal password of the active directory and has a second authentication factor and is therefore solely responsible for the protection of the activation data of the private key.

## **6.6 Computer security controls**

### **6.6.1 Specific computer security technical requirements**

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

- The TSPM 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 TSPM 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 Computer security rating**

The applications of the certification and registration authority used by the TSPM 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 Life cycle 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 TSPM 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 8.2 of the CPSM

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 Life cycle security controls**

The AGE may require the TSPM 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 TSPM 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 TSPM.
- 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 Time-stamping**

The Keys of the TSPM are generated in secure cryptographic devices, operated by trusted TSPM 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, CRL, and OCSP profiles

### 7.1 Certificate profile

The certificate profiles and extensions supported conform to the definitions given by the AGE.

#### 7.1.1 Version number(s)

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 shown below:

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

#### 7.1.3 Certificate extensions

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

The TSPM 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 TSPM 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 cualificado*) 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 typologies.

CERTIFICATE	MANDATORY FIELDS
ELECTRONIC SEAL	<ul style="list-style-type: none"><li>• <i>Version</i></li><li>• <i>Serial Number</i></li><li>• <i>Issuer Distinguished Name (Country (C), Organization (O), Organizational Unit (OU), Common Name (CN))</i></li><li>• <i>Validity (Not Before, Not After)</i></li><li>• <i>Subject (Country (C), Organization (O), Organizational Unit (OU), OI, Common Name (CN))</i></li></ul>



	<ul style="list-style-type: none"> <li>• <i>Subject Public Key Info</i></li> <li>• <i>Signature Algorithm</i></li> </ul>
PUBLIC EMPLOYEE <sup>5</sup>	<ul style="list-style-type: none"> <li>• <i>Version</i></li> <li>• <i>Serial Number</i></li> <li>• <i>Issuer Distinguished Name (Country (C), Organization (O), Organizational Unit (OU), Common Name (CN))</i></li> <li>• <i>Validity (Not Before, Not After)</i></li> <li>• <i>Subject (Country (C), Organization (O), Organizational Unit (OU), Serial Number, Surname, Given Name, Common Name (CN))</i></li> <li>• <i>Subject Public Key Info</i></li> <li>• <i>Signature Algorithm</i></li> </ul>

CERTIFICATE	RECOMMENDED FIELDS
ELECTRONIC SEAL	<ul style="list-style-type: none"> <li>• <i>Issuer Distinguished Name (Locality, Serial Number, Organization Identifier)</i></li> <li>• <i>Subject (Surname, Given Name, Organization Identifier)</i></li> </ul>
PUBLIC EMPLOYEE <sup>6</sup>	<ul style="list-style-type: none"> <li>• <i>Issuer Distinguished Name (Locality, Serial Number)</i></li> <li>• <i>Subject (Organizational Unit (OU), Organizational Unit (OU), Organization Identifier, Title)</i></li> </ul>

CERTIFICATE	MANDATORY EXTENSIONS
ELECTRONIC SEAL	<ul style="list-style-type: none"> <li>• <i>Authority Key Identifier</i></li> <li>• <i>Subject Key Identifier</i></li> <li>• <i>Key Usage</i></li> <li>• <i>CRLDistributionPoint (distributionPoint)</i></li> <li>• <i>Authority Info Access (Access Method, Access Location del OCSP y del calssuer)</i></li> <li>• <i>Qualified Certificate Statements</i></li> <li>• <i>Certificate Policies (Policy Identifier, Policy Qualifier ID [CPS Pointer, User Notice], EU qualified certificate policy Identifier (sólo si ALTO FIRMA o MEDIO / SUSTANCIAL))</i></li> <li>• <i>Subject Alternative Names (Directory Name)</i></li> </ul>
PUBLIC EMPLOYEE <sup>7</sup>	<ul style="list-style-type: none"> <li>• <i>Authority Key Identifier</i></li> <li>• <i>Subject Key Identifier</i></li> <li>• <i>CRLDistributionPoint (distributionPoint)</i></li> <li>• <i>Authority Info Access (Access Method, Access Location del OCSP y de calssuer)</i></li> <li>• <i>Key Usage</i></li> <li>• <i>Subject Alternative Names (Directory Name= Identidad Administrativa)</i></li> </ul>

<sup>5</sup> CEPCHSM included

<sup>6</sup> CEPCHSM included

<sup>7</sup> CEPCHSM included



CERTIFICATE	RECOMMENDED EXTENSIONS
ELECTRONIC SEAL	<ul style="list-style-type: none"><li>• <i>Issuer Alternative Name</i></li><li>• <i>Subject Alternative Names</i></li></ul>
PUBLIC EMPLOYEE <sup>8</sup>	<ul style="list-style-type: none"><li>• <i>Issuer Alternative Name</i></li><li>• <i>Subject Alternative Names</i></li></ul>

#### 7.1.4 Algorithm object identifiers

The CPSM uses the security scenario called generic safety environment of AGE, which determines the strength and viability criteria applicable to each certificate policy according to Guide [CCN-STIC-405].

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	Length
High and Medium	Root and subordinated CAs	RSA-4096

- End user entities:

Level of Assurance	Entity	Length
Alto	End user certificates	RSA-2048
Medio	End user certificates	RSA-2048

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

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

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}
---------------	--

The TSPM will only certify the public key associated with the cryptographic algorithms identified above and will only use the cryptographic signature algorithms described above

---

<sup>8</sup> CEPCHSM included



for signing certificates, certificate revocation lists and any other element of the Certification Authority.

### **7.1.5 Name forms**

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 and described in CPs.

### **7.1.6 Certificate Policy Object identifier**

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

### **7.1.7 Usage of Policy Constraints extension**

In all certificates issued by the CSPM the extension *policyConstraints* is not obligatory, so it could be an empty sequence.

### **7.1.8 Policy qualifiers syntax and semantics**

They will contain the CPSM URI.

## **7.2 CRL profile**

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

### **7.2.1 Version number(s)**

The CSPM uses only CRL as provided for in [ITU-T X.509] as well as the policy in the technical specification [IETF RFC 6818].

### **7.2.2 CRL and CRL entry extensions**

The CRL will include the following information:

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



## **8 Compliance audits and other assessments**

### **8.1 Compliance audits**

The TSPM conducts regular internal audit to test compliance of security and operational requirements.

### **8.2 Frequency or circumstances of assessment**

According to eIDAS, the CSPM will conduct a compliance audit at least every 24 months by a conformity assessment body, 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 Identity/qualifications of assessor**

The compliance audit will be carried out by a conformity assessment body complying with eIDAS and applicable legislation.

### **8.4 Assessor's relationship to assessed entity**

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

Compliance audits performed by third parties will be carried out by an independent body of TSPM, 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 be operated by 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, she will be always accompanied by staff from SGTIC.

### **8.5 Topics covered by assessment**

The elements to audit will be the following:

- Certification procedures.
- Information systems.
- Protection of Data Centre.
- Documentation of the service.
- Existence of relevant authorizations that empower the operators of those components of the Certification Authority, following the provisions of the CPSM. 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 Authority.
- 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 availability in the machines that conform the Certification Authority as to prevent space overflows.
- Physical backup of the HSM content.
- State of databases systems.
- Adaptation of the CPSM to eIDAS requirements.
- Matching between the procedures and technical controls present in the CPSM with the real and effective measures and controls.

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 taken as a result of deficiency**

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

- The auditor will prepare a report with the results of the audit.
- The auditor shall notify the non-compliance to the parties involved.
- After receiving the report of the compliance audit conducted, the TSPM will discuss with the entity that performed the audit, 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.

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

### **8.7 Communication of results**

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





## **9 Other business and legal matters**

### **9.1 Confidentiality of business information**

#### **9.1.1 Scope of confidential information**

The TSPM 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 TSPM.
- Records of transactions, including full records and the audit records of transactions.
- Records of internal and external audit, created and / or maintained by the TSPM 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 Authority of TSPM.

It is protected the access to the cards of Operation and Management of the cryptographic modules that support the Certification Authority, 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 Information not within the scope of confidential 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 subscriber to a certificate issued by the TSPM.
- The full name of the certificate subscriber and any other circumstance or personal data of the subscriber, in the event that is significant in terms of the purpose of the certificate.
- The email address of the certificate subscriber 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 Responsibility to protect confidential information**

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

### **9.1.5 Information disclosure by request of the subscriber**

The TSPM 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 for the certificate directly to them or others.

## **9.2 Privacy of personal information**

For the service, the TSPM 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 TSPM 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 TSPM collects the data exclusively necessary for the issuance and lifecycle management of the certificate.

The TSPM will not disclose or lease personal information, except as provided in Sections 9.1 of this document, and in section 5.8, upon termination of the Certification Authority.

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 TSPM is the only entity that has intellectual property rights on the certificates it issues. The TSPM 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 CPSM, 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 TSPM.

### **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 Representations and warranties**

### **9.4.1 CA representations and warranties**

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

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

Prior to the issuance and delivery of the certificate to the subscriber, the TSPM 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 TSPM.

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



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

#### **9.4.2 Representations and warranties of subscribers and other participants**

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

- That there are no factual errors in the information contained in the certificates, known or made by the TSPM 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 TSPM 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 certificate for electronic signature, the TSPM 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 LFE.
- That, in the case of generating the private keys of the subscriber their confidentiality is maintained throughout the process.

#### **9.4.3 Limitations of warranties**

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

#### **9.4.4 Limitations of liability**

The TSPM shall only be liable for the issue and delivery of certificates and, for key pairs and secure authentication devices (for authentication, electronic signature, and verification of electronic signatures).

The TSPM may limit its liability by including clauses to the certificate usage that limit the value of transactions for which the certificate can be used.



## **9.4.5 Disclaimer of warranties**

### ***9.4.5.1 Exemption clause of liability with the Subscriber***

The TSPM includes in the document that links it to the subscriber, a clause by which the subscriber agrees to keep the TSPM 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 subscriber 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 TSPM, the Register Authority or any person relying on the certificate.
- The subscriber was negligent in protecting the private key, in the use of a trusting service, or in maintaining right conditions to avoid the compromise, loss, dissemination, modification or non-authorized use of that key.
- The subscriber uses names (surnames, emails, or domain names), or any other certificate information against the intellectual or industrial property rights.

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

In no event shall the TSPM be held liable by any relying party 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:

- Any relying party does not comply with the requirements.
- Any relying party trusted on the certificates under some not recommended circumstances (reckless circumstances).
- Any relying party trusted on the certificates, without any validation status to check if this was revoked or suspended.

## **9.4.6 Fortuitous event or force majeure**

The TSPM shall not be liable in the case of acts of fortuitous event, or force majeure.

## **9.4.7 Governing law**

The provision of trusted services of the PSCM will be governed by the provisions of the Laws of the Kingdom of Spain, in special:

- 59/2003 Law, December 19th, about Electronic Signature (LFE).
- REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS).
- 39/2015 Law, October 1<sup>st</sup>, about Common Administrative Procedure of the Public Administrations.



- 40/2015 Law, October 1<sup>st</sup>, about Legal Framework of the Public Sector.
- 15/1999 Organic Law, December 13<sup>th</sup>, about Personal Data Protection (LOPD).
- Royal Decree 1720/2007, December 21<sup>st</sup>, Regulations to develop and apply the Organic Law 15/1999.
- 56/2007 Law, December 28<sup>th</sup>, Measures to Promote the Information Society.
- Royal Decree 3/2010, January 8<sup>th</sup>, National Security Framework for the Electronic Administration.
- Royal Decree 4/2010, January 8<sup>th</sup>, National Interoperability Framework for the Electronic Administration.
- Royal Decree 1/1996, of April 12<sup>th</sup>, consolidated text for Intellectual Property Law.
- Electronic Signature and Certificates Policy for the AGE.
- Policy description in Law 11/2007, June 22<sup>nd</sup>, associated to the Electronic Signature Policy: certificate profiles in the last available version.
- Order of the Secretary of State for Public Service of July 19<sup>th</sup> 2011 approving the Technical Standard for Interoperability of Electronic Signature and Certificate Policy for the Administration
- Commission Decision of February 25<sup>th</sup> 2011 establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market.

#### **9.4.8 Clauses of severability, survival, entire agreement and notification**

The TSPM 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 TSPM. To this end, it ensures that at least the requirements contained in sections 8, 9.1 y 9.4, 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 Applicable law, interpretation and competent jurisdiction**

The TSPM establishes that regarding the international jurisdiction, all parties submit to the jurisdiction of the courts of Spain.

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



#### **9.4.10 Dispute resolution procedures**

The TSPM will resolve any disputes that may arise concerning the interpretation or applicability of the CPSM.

Any discrepancy situations arising from the use of the certificates issued by the TSPM, shall be resolved by applying the same criteria of competence that in cases of handwritten signed documents.

In cases of dispute arising as a result of the management of certificates between the different TSPs, the CPSM shall be used to resolve any difference of criteria.



## **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.
ETSI EN 319 403	ETSI European Standard 319 403 v2.2.2. Trust Service Provider Conformity Assessment – Requirements for conformity assessment bodies assessing Trust Service Providers.
ETSI EN 319 411-2	ETSI European Standard 319 411-2. Policy requirements for certification authorities issuing qualified certificate
ETSI EN 319 411-3	ETSI European Standard 319 411-3. Policy requirements for Certification Authorities issuing public key certificates. Nota: Excluye los certificados de sitios web basados en los requisitos del CAB Forum.
ETSI EN 319 412-5	ETSI European Standard 319 412-5. Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile.
ETSI EN 319 421	ETSI European Standard 319 421. Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps.
ETSI TS 102 042	ETSI Technical Specification 102 042. Policy requirements for Certification Authorities issuing public key certificates. Note: Includes web site certificates based on CAB Forum requirements.
ETSI TS 102 158	ETSI Technical Specification 102 158. Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates
ETSI TS 102 176-1	ETSI Technical Specification 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 102 176-2. Algorithms and Parameters for Secure Electronic Signatures; Part 2: Secure channel protocols and algorithms for signature creation devices.
ETSI TS 119 412-2	ETSI Technical Specification 119 412-2. Profiles for Trust Service Providers issuing certificates; Part 2: 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 3647	Internet X509 Public Key Infrastructure Certificate Policy and Certification Practice Framework.
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 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 6818	Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
IETF RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP.
ISO 3166-1	Codes for the representation of names of countries and their subdivisions - Part 1: Country codes. Alpha-2 country codes.
ISO 9594-8	Information Technology – Open Systems Interconnection – The Directory: Public-key and Attribute Certificate Frameworks.
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).
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.
Ley 40/2015	40/2015 Law, October 1 <sup>st</sup> , about Legal Framework of the Public Sector.
UTF-8	8-bit Unicode Transformation Format.



## Annex B: Electronic Links (URLs)

Email Organisation Data:

[admin\\_ca@meyss.es](mailto:admin_ca@meyss.es)

CPSM and Certificate Policies:

<http://ca.empleo.gob.es/meyss/DPCyPolíticas>

CRL Root - AC RAIZ MEYSS:

<http://ca.empleo.gob.es/meyss/crl/MEYSSAutoridadRaiz>

<http://ca2.empleo.gob.es/meyss/crl/MEYSSAutoridadRaiz>

CRL - SUBCA1 MEYSS:

<http://ca.empleo.gob.es/meyss/crl/MEYSSSubCA1>

<http://ca2.empleo.gob.es/meyss/crl/MEYSSSubCA1>

CRL - SUBCA2 MEYSS:

<http://ca.empleo.gob.es/meyss/crl/MEYSSSubCA2>

<http://ca2.empleo.gob.es/meyss/crl/MEYSSSubCA2>

OCSP Service Validation Status:

<http://ca.empleo.gob.es/meyss/ocsp>

CA Root certificate, SubCA certificates and OCSP certificate:

<http://ca.empleo.gob.es/meyss/certificados>

The URLs for certification services pre-eIDAS are as follows:

CPSM and Certificate Policies:

<http://ca.mtin.es/mtin/DPCyPolíticas>

OCSP Service Validation Status:

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

Root certificate, OCSP certificate and time stamping certificate:

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

CRL publication:

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

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

Historic CRLs:

Please, send a mail to [admin\\_ca@meyss.es](mailto:admin_ca@meyss.es), stating date of publication and/or serial number.