MINISTERIO DE TRABAJO
Y ECONOMÍA SOCIAL

SUBSECRETARÍA

S.G. DE TECNOLOGÍAS DE LA
INFORMACIÓN Y COMUNICACIONES

Ministry Trust Service Provider
Certification Practice Statement

sgtic@meyss.es
EA0041850

PASEO DE LA CASTELLANA 63
28071 MADRID
TEL: 91 363.11.88
FAX: 91 363.07.73

Version Control

Identifier	D004
Title	Ministry Trust Service Provider Certification Practice Statement
Version	07
Document state	Approved
Approval date	20201026
OID	1.3.6.1.4.1.27781.2.3.1

Change Control

Version	Date	Comments
1.0	20091105	Final Document.
1.1	20100329	ISO/IANA number changes for MPR and OID changes in the certificates issued by TSPM.
1.2	20100910	Header change removing Directory General Services. Added sections for art. 21 LFE in section 5.8.
1.3	20110407	OCSP Certificate OID change. Suppression of OCSP no Check restriction.
1.4	20120216	OIDs update.
1.5	20120810	Organization Structure update. New document format. Annex C added.
1.6	20140321	Added the Public Employee Certificate Centralized and Managed by HSM.
1.7	20140704	Annex B removed. Annex C is now Annex B with new writing for historic CRLs. Identification and Electronic Signature Framework for Public Administrations is removed from References. Sections 4.9.3, 6.1.1, and 6.2.1 rewritten.
1.8	20150618	SHA-256 added.
1.9	20160318	Current legislation updated.
1.10	20160530	Minor typos updated. SHA-1 references removed.
1.11	20170406	Root Certification Authority, SubCA and related URLs added to the document. Trusted services updated.
02	20170612	Updates corresponding to Observation Report and Preassessment Audit. Added section 1.7.
03	20170727	Updates in sentences with “shall” term. Spanish Supervisory Body replaces MINETAD. Use of term “TSPM Director” instead of “TSPM Responsible”. and instead of “responsible for the TSPM”. Non-discrimination clause updated in section 1.7. ULR landing page added for terms and conditions in section 1.7 Rewriting of section 6.2.2 and 6.5.1.

04	20180727	Use of *trust service provider* term instead of *certification service provider* term. Ministry name updated. Date format adapted to ISO 8601: YYYYMMDD. Privacy and data protection clause updated. Change in the name of the National Supervisory Body. Trusted roles section rewritten. The term *employees* has been replaced by the term *staff* in the Security Policy section. Reference to public procurement law updated. GDPR reference added. Audit results communication updated. Typos corrected on sections 1.3.2, 2.1, 3.1.5, 5.1.1, and 5.5.7.
05	20190727	DIR3 code updated. Expiration date removed from version control. Accessibility explicitly included in the general conditions of the TSPM services (1.7) and in the applicable law (9.4.7). Some acronyms and definitions removed and updated. Security policy and interested parties for the security policy updated in section 1.7.1. Updated to one year the periodicity of the risk analysis and evaluation (1.7.2). The signature policy used by the TSPM is added in the new section 1.7.3. Section 4.9.9 is updated to improve the practices of the certificate status verification service Section 6.6 updated to indicate how the TSPM operates against the loss of QSCD condition. Update of references to LOPDGDD (Annex A).
06	20200601	DIR3 code updated. Updated text about certificate requesters and subjects (1.3.4.1 and 1.3.4.2) to improve readability. Ministry name updated. Updated TSPM organization (1.5). Updated 4.9 section with publishing revocation information about revoked and expired certificates, about key compromise or service termination, and about the period needed. Some aspects in the section rewritten to improve readability. Remove 6.3 title in order to make CPS structure fully compliant with RFC 3647. Network security controls updated (6.7).
07	20201026	Information about signature and public key algorithms for root and subordinate certificates is added in *1.3.1 Certification Entity*. Updated section 1.7.3 Signature Policy of the PSCM with the algorithms and signature parameters used.

		Section 4.4.2 Conduct that constitutes acceptance of the certificate is aligned with the terms and conditions document of the electronic seal certificate. Information on certifications of the products used in the different services, such as QSCD or HSM, is expanded in section 6.2.1 Cryptographic module standards. Renamed section 7.2 Profile of the list of revoked certificates to the one more adjusted to RFC 7.2 CRL Profile. Added section 7.3 OCSP profile aligned with the structure defined in RFC 3647. Restructured section 9 Legal requirements in full to align with the RFC and sections 9.1, 9.2, 9.9, 9.10, 9.12, 9.16 and 9.17 are added. Section 9.17 Other stipulations contains the information about the PSCM test certificates.

Summary Contents

Table of Contents

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 Labour and Social Economy (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 CPSM is published on the URL that appears on the Annex B: Electronic Links (URLs).

1.1 Overview

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

Qualified Certificate	Device	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 Trust Service Provider Certification Practice Statement**, whose information appears on the version control of this document (page ii)

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

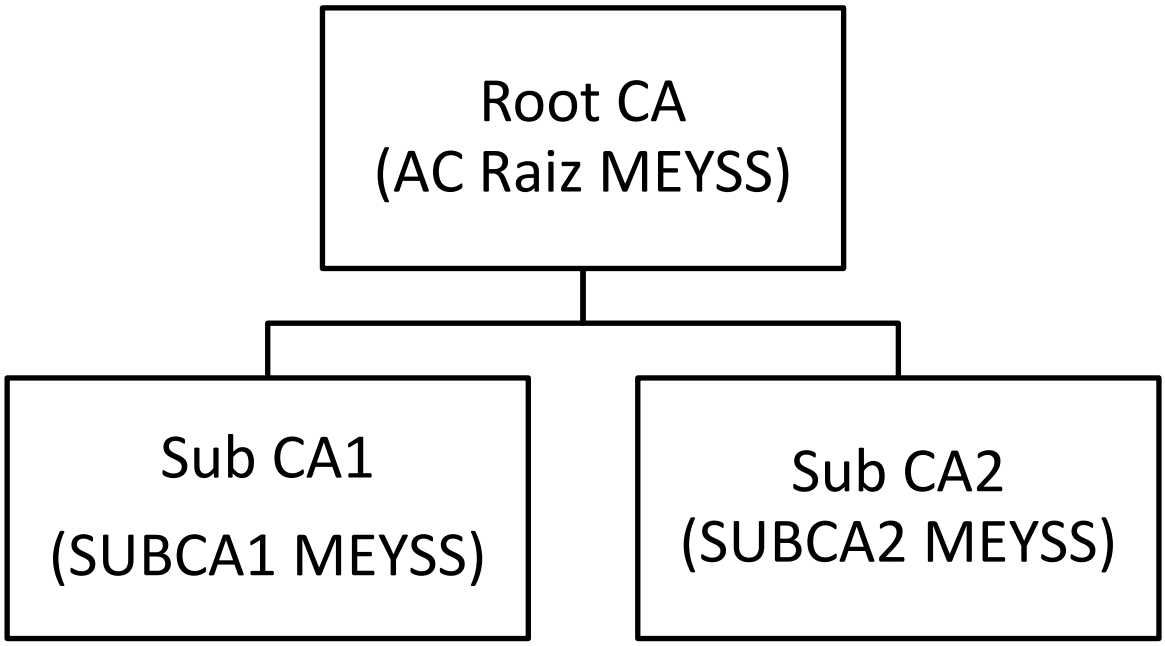
1.3 PKI Participants

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 end users.

1.3.1 Certification Authorities

There are one Root Certification Authority and some Subordinate Certification Authorities according to this scheme.



Root CA = Root Authority

SubCA1 = SubCA Authority for issuing:

- electronic seal certificates
- CEPCHSM (remote public employee certificates).

SubCA2 = SubCA Authority for issuing public employee certificates on smart card (QSCD).

OIDs for any kind of issued certificate appears on the following table:

Certificate type	OID	Qualified	CA
Remote public employee certificate (CEPCHSM)	1.3.6.1.4.1.27781.2.5.4.7.1	QCP-n	SUBCA1 MEYSS
Electronic seal certificate	1.3.6.1.4.1.27781.2.5.3.2.1	QCP-l	SUBCA1 MEYSS
Public Employee Certificate for signing (high level assurance)	1.3.6.1.4.1.27781.2.5.4.1.1	QCP-n-qscd	SUBCA2 MEYSS
Public Employee Certificate for authentication (high level assurance)	1.3.6.1.4.1.27781.2.5.4.2.1		SUBCA2 MEYSS

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 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 and 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 its responsible (custodian).
- 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:

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 (custodian).
- 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 a public employee.

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 (subjects) 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.

In case of public employee certificates, the subject shall be a public employee and she will be the same as the person who made the request.

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

To avoid any conflicts of interests, the subscriber and the TSPM organization entity are separate entities.

1.3.4.3 The responsible for the certificate

The responsible for the certificate, 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 is a public employee.

In the case of OCSP responder certificate, the responsible is the responsible of the TSPM.

1.3.4.4 Relying parties

The certificate verifiers (relying parties) 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 uses the information contained in the certificate to determine the certificate usage in any particular case.

1.4 Certificate usage

The certificates issued under the CPSM are 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 are delimited in its use by the provisions of the law. The remaining types 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 63, 40/2015 Law of October 1st , about 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*) reports to the *Subsecretaría* and exercises for the central, interprovincial and foreign services of the Department and for the attached autonomous bodies, with the exception of the Public State Employment Service (*Servicio Público de Empleo, SEPE*), the functions of planning, creation, development, modification and management of the information systems needed for the operation of services, management and administration of the telephone and data communication networks, and of the associated security and confidentiality systems, administration of the Ministry's Internet presence, conducting audits of the Information Systems in matters of quality and security, in accordance with the regulations on ICT security, ensuring the principles of impartiality and independence that must govern this activity, and the promotion and coordination of the information policy and digital administration of the Ministry and its autonomous bodies.

Therefore, the CEO of the SGTIC is the TSPM Director (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 Director, 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, Spain
admin_ca@mtin.es / admin_ca@meyss.es
Phone Number: +34 91 363 11 88/9 - Fax: +34 91 363 07 73

1.5.3 CPSM administration procedures

1.5.3.1 Change Control

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

The security officer of the TSPM reviews the CPSM annually or should a significant change happened in that period. Errors, updates, suggestions or improvements on this document shall be communicated to the organization whose contact data appear in section 1.5.2. All

communications shall include a description of the change, its justification and the information of the person requesting the modification.

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

1.5.3.2 Publication

The TSPM publishes 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/DPCyPoliticas

1.5.3.3 CPSM Approval

The TSPM security officer requests the approval of the CPSM to the TSPM Director who approves the document (or not) as stated in the TSPM 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.
QSCD	Qualified Signature Creation Device that is certified and approved for being used to generate Qualified Electronic Signatures (QES).
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.
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.
GDPR	General Data Protection Regulatory.
HSM	Hardware Security Module.
IETF	Internet Engineering Task Force.
LDAP	Lightweight Directory Access Protocol.
LOPDGDD	Law on Protection of Personal Data (Ley Orgánica de Protección de Datos de Carácter Personal).
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.
PSCM	TSPM
QSCD	Qualified Signature Creation Device.
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.

1.7 General conditions of the certification services

The legal nature of the TSPM as a public body is free from any commercial, financial and other pressure that might adversely affect trustworthy in the services provided. Its organizational structure ensures impartiality in making decisions regarding the establishment, provisioning and maintenance and suspension of the certification services, and in particular the certificates generation and revocation operations.

The TSPM outsources partially certain activities, such as the development, deployment, monitoring and deployment of some computer systems. These activities are carried out according with the TSPM Certification Policies and Practices and the contracts/agreements signed with entities that perform such activities following the Public Sector Procurement Law [Law 9/2017].

The CPSM and Certification Policies collect general obligations and responsibilities of the involved parties in the various certification services for their use inside the limits and the related application framework, always in the competence field of each of those parties. The foregoing is understood without the prejudice of the specialities that may exist in the contracts, agreements or enforcement agreements.

The TSPM states that all the practices of its trust services are operated always under the principle of non-discrimination for reasons of race, sex, religion, creed, nationality, disability or any other personal or social circumstance.

Where feasible, trust services provided by the TSPM and end-user products used in the provision of those services are made accessible for persons with disabilities.

The TSPM publishes the general terms and conditions of its services in the URL https://ca.empleo.gob.es/es/CA_MEYSS/declaracion.htm. Any relevant change is notified via the public repository (see section 2.1) by publishing an announcement in the home page plus the old version and the new version. After 30 days, the old version is removed but is retained by the TSPM for at least 15 years and may be consulted by interested parties with justifiable cause.

1.7.1 Security Policy

The TSPM defines a security policy which is approved by the TSPM Director. This security policy sets out the TSPM approach to managing its information security as well as the trust services provided.

The TSPM publishes and communicates this security policy to its staff on the Intranet of the department.

This security policy is reviewed and revised on an annual basis or if there has been any significant event affecting the TSPM.

Any change to the security policy is communicated to subscribers and third parties (relying parties, assessment and supervisory bodies, subcontractors, etc.), where applicable.

1.7.2 Risk Analysis

As stated in the information security policy, the TSPM follows a specific risk analysis methodology (MAGERIT) to carry out a risk assessment to identify, analyse and evaluate trust service risks taking into account business and technical issues.

According to the results, the TSPM selects the appropriate risk treatment measures ensuring that the level of security is commensurate to the degree of risk. The TSPM determines all security requirements and operational procedures that are necessary to implement the risk treatment measures chosen and documents them in the CPSM.

The TSPM Director approves the risk assessment and accepts the residual risk identified.

This risk assessment is reviewed and revised on an annual basis or if there has been any significant change or event affecting the TSPM.

1.7.3 TSPM Signature Policy

The TSPM provides all its trust services in accordance with the requirements established by the AGE Signature and Certificate Policy. Under this directive, the TSPM follow the signature formats CAdES (extension of the signed file *.csig*), XAdES (extension of the

signed file *.xsig*) and PAdES (extension of the signed file identical to the original PDF format, in general, *.pdf*).

Following the current version of the signature policy, RSA algorithms are used for signatures with SHA-256 hashes.

2 Publication and Repository Responsibilities

2.1 Repositories

The TSPM has a public information repository on http://ca.empleo.gob.es available 24 hours a day, 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 available again in the period specified in section 5.7.4 of this document.

The TSPM repository:

- guarantees on line information availability. Hard copies may be provided if needed
- facilitates the use of a free, fast and secure service by which relying parties can consult the registry of certificates issued
- maintains an updated directory of certificates which lists all certificates issued and whether they are valid or if their validity period has been suspended or expired
- also issues Certificate Revocation Lists (CRLs) and real-time certificate verification services, using Online Certificate Status Protocol (OCSP) in URLs stated in Annex B

This documentation is kept available for a minimum period of 15 years from the issuance of the certificate.

TSPM revocation and validation services are available 24 hours a day, 7 days a week except for the minimum time required for maintenance operations and for solving severe incidents.

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 has been 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.

TSPM notifies users of changes in specifications or in the terms and conditions of services via the TSPM website. There is an announcement of changes in the home page and both versions of the document are published. After 30 days, the previous version is removed, but is retained by TSPM for at least 15 years and may be consulted by interested parties with justifiable cause.

2.4 Access controls on repositories

The TSPM allows public read-only access to the information published in its Repository. However, controls are put in place to keep unauthorized individuals from adding, changing or deleting the registers provided by this service to protect the integrity and authenticity of the documents and certificates status so that their content is not compromised.

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	• Type of certificate • Name of the subscriber entity • NIF of the subscriber entity • System or component denomination
PUBLIC EMPLOYEE	• Type of certificate • Name of the entity where is employed • NIF of the entity where is employed • DNI/NIE of the responsible • Given name • First surname • Second surname
CEPCHSM	• Type of certificate

	• Name of the entity where is employed • NIF of the entity where is employed • DNI/NIE of the responsible • Given name • First surname • Second surname

Certificate	Optional "Identidad Administrativa" fields
ELECTRONIC SEAL	• DNI/NIE of the responsible • Given name • First surname • Second surname • E-mail address
PUBLIC EMPLOYEE	• Personal identification number • E-mail address • Organizational unit • Position held
CEPCHSM	• Personal identification number • E-mail address • Organizational unit • Position held

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 does 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 is 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 is always located 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 are:

- Public Employee Certificate[1] and CEPCHSM[2]:
  - 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[3]:
  - 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.

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

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

3.1.7 Recognition, authentication, and role of trademarks

Certificate requesters do 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.

Any name conflicts with the certificate subscribers who are identified in the certificate with their first names, are 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 starts the first time the public employee access the generation process.

The system informs the public employee that her CEPCHSM is going to be issued. Then the system generates 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 is 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 are not 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 has got 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 are 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 authorizes 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 ensures that all certificate requests are complete, accurate and properly authorized. Prior to the issuance and delivery of the certificate, the entity informs to the subscriber or to the responsible for the certificate about the terms and conditions applicable. Such information is communicated in a durable medium, on paper or electronically, and in easily understandable language.

The request includes 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:

- Includes in the certificate the information provided for in Article 11 of Law 59/2003 (LFE), in accordance with the provisions of Section 7 of the CPSM.
- Ensures the date and time of issue of a certificate.
- Uses trustworthy systems and products which are protected against modification and ensure the technical security and, where appropriate, cryptographic of the supporting certification processes.
- Ensures that the certificate is issued by systems using anti-counterfeiting and when the private keys are generated, it ensures 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 reviews 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 denies the request. If the information in the request is correct, the Certification Authority issues the certificate.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The Certification Authority:

- Uses a procedure for 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 uses a method of certificate generation that is linked safely with the key generation process and ensures that the private key is delivered safely to the subscriber or the responsible for the Certificate.
- Protects the confidentiality and integrity of the registration data, especially in the event that they are exchanged with the subscriber or the responsible person for the Certificate.
- Stores issued certificates with access permissions and security controls regulated and necessary for this, ensuring the security of communications.
- Does not store the private keys associated with the certificates except in the case of CEPCHSM in which the system generates at that exact moment the private key and stores it safely in the system, ensuring that its use is under the exclusive control of the subscriber.

Additionally the Certification Authority:

- Includes information on the certificate in compliance with eIDAS and Spanish regulation on electronic signature.
- Indicates the date and time the certificate was issued.
- Uses a management procedure for the secure signature creation devices ensuring that they are safely delivered to the subscriber or responsible for the certificate.
- Uses products protected from tampering, ensuring technical and cryptographic security of the certification processes that they support.
- Uses measures against forgery of certificates, and to ensure the secrecy of the keys during the process of generating the same.
- When issuing a certificate in accordance with a request, the CA delivers 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 is 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 is informed that the certificate is available and can be used from that moment.

Otherwise, the Certification Authority notifies the requester about 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 provides the subscriber access to the certificate through the application designed for that purpose. This application allows the generation of the key pair and downloads 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 provides the subscriber with access to the certificate through the system designed for that purpose. The system informs 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 is informed that the certificate is available and can be used from that moment.

In the case of electronic seal certificates, the Certification Authority safely delivers the certificate. This delivery occurs after identifying the subscriber or responsible in person. Along with the certificate, some information is 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) is accepted by signing the request form by Subscriber or, if applicable, by the person responsible for the certificate.

The Public Employee Certificated is 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 is deemed to accept the certificate by the downloading action on that device.

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

For Electronic Seal Certificates, the certificate is deemed accepted by signing the request and terms and conditions, and by receiving the certificate signed containing the private key whose pair is the public key attached to the request.

4.4.3 Publication of the certificate by the CA

Certificate data identification are 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 are used in accordance with its own function and purpose established, without being usable in other functions and other purposes. Similarly, the certificates are used only in accordance with applicable law, especially considering the import and export restrictions in each moment.

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

The Public Employee Certificates is 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:

- 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:

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

- 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 is 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, are 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 revokes 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 of obligations, liabilities and guarantees established in the legal instruments, terms of use or CPSM.
   - The use of the certificate to enable criminal activities.
   - 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 is 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 employee certificates are able to request their certificate revocation through the online application available 24x7. Requests are processed automatically and the certificates are 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 is processed upon receipt.

- In the event that the recipient of the application is the Registration Entity, once authenticated the request, issues 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 revokes it, publishing its serial number and other identifying information in the CRL as well as in the OCSP service. The Certification Authority cannot reactivate the certificate once revoked.

4.9.4 Revocation request grace period

As regards the period in which the Certification authority solves the revocation request, the TSPM proceeds to the immediate revocation of the certificate at the time of verifying the requester identity.

4.9.5 Time within which CA must process the revocation request

The time used for the provision of revocation services is synchronized with UTC at least every 24 hours.

The maximum delay between receipt of a revocation request and the decision to change its status information is 24 hours.

4.9.6 Revocation checking requirement for relying parties

Each relying party shall check the status of those certificates on which it is going to trust.

The Certification Authority of the TSPM makes available to verifiers a service of certificate status information based on the OCSP protocol and, at least, another way to access by downloading the certificate revocation lists (CRL). The services for certificate revocation status verification offered by the TSPM are free of charge.

4.9.7 CRL issuance frequency

Each certificate issued specifies the address of the corresponding CRL, using the *cRLDistributionPoints* extension.

The Certificate Revocation Lists (CRL) of the final entity are released at least every 24 hours, or when a revocation occurs and has a validation period of 24 hours.

4.9.8 Maximum latency for CRLs

The state change of the validity of a certificate is indicated in a CRL in less than 5 minutes elapsed from the occurrence of such change. This means that the maximum delay between the confirmation of the revocation of a certificate to become effective and the actual change of the status information of this certificate is 5 minutes.

4.9.9 On-line revocation/status checking availability

The TSPM provides any relying party with certificate status information about the certificates issued. The certificate status information is publicly, automated and internationally available free of charge at any time and even after the validity period of the certificate. Both OCSP service and CRL are supported.

The TSPM ensures a level of service, ensuring the availability of all the certification services that offers, in special services related to certificate status information. The TSPM guarantees the integrity and authenticity of the certificate status information.

The service is available on-line 24 hours per day, 7 days a week. Upon system failure, the Business Continuity Plan shall be launched in order to solve the incident as soon as possible and ensure that the service is available.

4.9.10 On-line revocation checking requirements

The verifier checks the status of those certificates on which it 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 should reject its use or, based on the risk, the degree of responsibility and the consequences that could occur, for using it without guaranteeing its authenticity in the terms and standards set out in the CPSM.

The TSPM indicates 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 (it contains the full list of revoked certificates), indicating that fact inside the certificates by the use of *Distribution Points* extension of the CRL (*cRLDistributionPoints*) defined in IETF Technical Specification [IETF RFC 5280], as follows:

- It includes at least two CRL distribution points linking to separate servers.
- Each CRL Distribution Point contains the name of the CRL location in URL form.

The location of the CRL is in Annex B:

In the event of termination of the TSPM, the TSPM will issue a final CRL which will be published on the TSPM website indicated by the *cRLDistributionPoints* field. This website will be maintained for at least 15 years by the department that would replace the current Ministry. The new department will decide the feasibility of maintaining the OSCP service.

In case of issuance by the TSPM of a last CRL, this will be issued and published at the CRL distribution point according to what is specified in [ETSI EN 319 411-1].

The last CRL exists as there are no more valid certificates in the scope of the CRL, when the certificate that signs the CRL expires, or when the private key of the certificate that electronically signs the CRL is out of order.

The TSPM will preserve the integrity and availability of the last CRL for 15 years as specified by the LFE preferably using long-term valid signatures in accordance with standard formats.

The TSPM will not issue a last CRL until all certificates within the CRL are expired or revoked.

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 is included, indicating the OID reserved for OCSP service access and the URL where the OSCP server is located.

The OCSP service returns in its response the *ArchiveCutOff* extension [IETF RFC 6960] with the *valid from* value of the Certification Authority certificate in the *archiveCutOff* date field.

The location of the OCSP service is in Annex B:

The TSPM will offer the OCSP service once the root certificate has expired or its certification services have ended in accordance with what is specified by the LFE and the standard [ETSI EN 319 411-1] from the location indicated in the certificated field.

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.

In the case of compromise of the keys of any TSPM Certification Authority (CA or SubCA), all the active certificates issued will be revoked and the OCSP service will continue to be offered by signing the responses with a certificate issued by a Certification Entity other than the one compromised.

In the case of expiration of any certificate from the TSPM CA or SubCA: in a period prior to the expiration time that will be set based on the certificate validity time issued by said CA:

- the issuance of new certificates will be stopped
- at a time close to the expiration date, the existence of any active issued certificate will be reviewed, revoking where appropriate and a last CRL will be issued
- the OCSP service will continue to be offered by signing the responses with a certificate issued by a Certification Authority other than the expired one.

4.10 Certificate status services

4.10.1 Operational characteristics

The CRL can be downloaded from the repository of the Certification Authority and should 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.

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 means 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 is kept by the TSPM Certification Authority, taking into account that access to this key is made by some 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 is 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 does 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 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 counts with the Ministry security staff at its 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 staff 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. Media are protected against damage, theft, deterioration and obsolescence.

Access to these media, including its 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, they are formatted or permanently erased. In other cases, they are physically destroyed. For paper documents, it is subjected to a physical treatment of destruction.

5.1.8 Off-site backup

The TSPM keeps backup copies of essential information and software in a safe and secure environment protected against accidents and at a sufficient distance to prevent damage in the event of a disaster or media failure.

Back-up arrangements are regularly tested to ensure that they meet the requirements of the business continuity plan.

5.2 Procedural controls

The TSPM staff exercises administrative and management procedures in line with the TSPM information security management procedures and in line with the CPSM.

5.2.1 Trusted Roles

A "trusted role" is a role defined with responsibilities than can lead to security problems if not performed satisfactorily, whether accidentally or maliciously.

The trusted roles are defined and documented by the TSPM security officer and approved by the TSPM Director.

The TSPM staff is formally appointed to trusted roles by the TSPM Director requiring the principle of "least privilege" and taking into account their training, experience and staff security controls as described in this document. If needed, the TSPM provides adequate technical and security training for the appointed people.

The staff appointed to any TSPM Trusted Role who violate any TSPM policy or procedure will be investigated and sanctioned according to the current legislation.

5.2.2 Number of persons required per task

To reinforce system security, more than one person is assigned to each role, with the exception of the role of the Security Officer.

5.2.3 Identification and authentication for each role

Trusted roles require verification of identity by secure means; all trusted roles are performed by individuals. The TSPM has specific documentation giving further details of each role.

5.2.4 Roles requiring separation of duties

The TSPM follows the general security requirements of [CWA 14167] to define the separation of duties by roles. This separation is documented and approved by the TSPM Director.

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 staff appointed to trusted roles are free from any commercial, financial and other interests which might adversely influence trust in the services it provides.

The TSPM does not assign any person who is not suitable for the job to any trusted role, especially for having been convicted of crime or offense concerning their suitability for the job.

5.3.2 Background check procedures

Not applicable under Spanish law.

5.3.3 Training requirements

The TSPM trains 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 performs an update on its personnel training at least every twelve months focused on updates on new threats and current security practices.

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 [Law 9/2017] and [RD 5/2015] 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 trusted role, in which case they must submit to the same controls as the other employees. The hiring process comply with [Law 9/2017].

In the event that the professional does not need to undergo such checks, she is 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 staff.
- 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 staff.

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 staff 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 NTP server that holds the official time and date (UTC) in Spain.

The precise time of significant TSPM events is recorded, and the time used to record events as required in the audit log is synchronized with UTC at least once a day.

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 staff has access to archived data, whether in the same premises of TSPM or external location. In particular, any access or attempt to access audit data is stored.

5.6 Key changeover

Not applicable.

5.7 Compromise and disaster recovery

The TSPM has procedures to respond quickly to incidents and notify the appropriate parties any breach of security within 24 hours of being identified. If any loss of integrity affects to a public employee, the notification is performed at the moment according to the Contingency Plan. Any incident reporting and response procedures are employed in such a way that any damage from security incidents and malfunctions are minimised.

The TSPM addresses any critical vulnerability within 48 hours after its discovery.

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 are taken, in accordance with the Contingency 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 ensures 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, executes 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.

Following a disaster, the TSPM shall, if possible, take steps to avoid the repetition of the disaster.

5.8 CA or RA termination

The TSPM has got an up-to-date termination plan which specifies the procedure to be carried out should such an event occur. This plan minimizes potential disruptions to subscribers and relying parties as a result of the termination of its services as a provider

The TSPM shall notify subscribers at least two months prior to the termination of operations, by any means that ensure the proper transmission and reception of its intent to cease its activity as a TSP.

The TSPM Director is responsible for such notification and shall determine the most appropriate mechanism to do so.

The TSPM Director will decide how to publish the last CRL in order to make available the revocation status information beyond the validity period of the certificate.

If the TSPM decides to transfer its operations to another certification service provider, it shall notify the Spanish Supervisory Body and the subscribers of its certificates of the transfer agreements. For that purpose, the TSPM will send a document explaining the terms and conditions of transfer and the terms and conditions of use which will govern the relationship between the subscriber and the new TSP. Notification will be made by any means that will ensure the proper transmission and reception thereof at least two months prior to the cessation of its operations.

Subscribers shall express their express consent to the transfer of certificates, thus accepting the terms and conditions put forward by the new TSP. If the two-month period has elapsed with no transfer agreement or the subscriber has not given his or her express consent, the certificates shall be revoked.

If the two-month period has elapsed and no agreement has been reached with another TSP, all of the certificates will be automatically revoked.

Any authorisation with a thirty party with whom the TSPM holds a service provision contract (identification, issue, hosting, etc.) will be taken as finalised.

Any private key, including backup copies shall be destroyed or withdrawn from use in a manner such that the keys cannot be retrieved.

After the Registration Authority ceases to perform its operations, it shall transfer to the TSPM any records it is required to retain; any other information will be cancelled and destroyed.

Covering the costs needed to fulfil these minimum requirements fall under the liability of the Public Administration.

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 level 3 and [CCEAL4+]. The key pairs for VAs and RAs were generated on secure servers.

Before expiration of the TSPM CA certificate which is used for signing subject keys), the TSPM CA shall generate a new certificate for signing subject key pairs and shall apply all necessary actions to avoid disruption to the operations of any entity that may rely on the CA certificate. The new CA certificate shall also be generated and distributed in accordance with this policy.

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). • Key generation using software. It implies that the user uses these keys in secure software container. Key generation by the requester in PKCS#10 format (software support). Delivery of the certificate in PKCS#7 format. • Key generation by the user, using software.

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

The TSPM produced a report proving that the ceremony was carried out in accordance with the stated procedure and that the integrity and confidentiality of the key pair was ensured. This report was be signed according to [ETSI EN 319 411-1].

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 takes place the first time the public employee access to the procedure for the certificate generation.

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

In the case of electronic seal certificates and certificate private key is generated by the Certification Authority 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

CA signature verification (public) keys is available to relying parties by its publication in a format (self-signed certificate) according to the market standards on the TSPM repository.

In order to check the authenticity and integrity of any "self-signed certificate", the corresponding digital fingerprint can be checked with the hash published on the section 1.3.1 of this document.

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-4096

Medium	Root CA	RSA-4096
Medium	Subordinate CA	RSA-4096

- 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, i.e., the 4th Fermat number ([4]).

CEPCHSM public key is encrypted according to [IETF RFC 6818] 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

[4] 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

The TSPM logs the events relating to the preparation and management of its cryptographic modules.

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.

The TSPM ensures that the secure cryptographic device were not been tampered with during shipment and while stored. The TSPM ensures that the devices are functioning correctly.

All qualified signature creation devices used by the TPSM are periodically checked on the SSCD and QSCD list notified by Member States (*Compilation of Member States notification on SSCDs and QSCDs*) in order to review its expiration and replacement.

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 access to the HSM that stores securely the private key of the TSPM root CA is under multipersonal control. Its activation and use requires at least two people.

The custody of the private keys of other certificates is done by the subscribers themselves. The access to the private keys is protected at least by a PIN only known by the subscriber. In this case the access is 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 a two-factor authentication method.

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.

In case of certificates for Public Employees, the keys are generated directly and locally by the cryptographic device.

6.2.4 Method of activating private key

The activation of the Certification Authority private key needs:

- the HSM PED
- the System Admin with the black token (protected by PIN) plus the partition password
- the System Operator.

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

The private key of the TSPM Root CA is deactivated by deactivating the HSM partition and turning off-line the server machine until the next operation that requires an activation.

The private key of the TSPM Sub CA is deactivated by deactivating the HSM partition that requires:

- the HSM PED
- the System Admin with the black token (protected by PIN) plus the partition password
- the System Operator.

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

For Cryptographic Modules (HSM), the private keys are destroyed following the section Removing/Destroying Content for Safe Disposal of the HSM Administration Guide.

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. The whole set of private keys are destroyed following the section Removing/Destroying Content for Safe Disposal of the HSM Administration Guide.

6.2.7 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 staff subject to the trusted staff policy. The staff is 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: the subscribers are the only ones that store the only copy of this key in their cryptographic module or equivalent. Only in cases where the recovery service of private key exists, for purposes other than non-repudiation, these keys can be stored.

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

6.2.8 Private key archival

Private keys of the TSPM CA are destroyed at the end of its period of operation, permanently.

6.3 Other aspects on key pair management

6.3.1 Public key archival

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

6.3.2 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.

6.4 Activation data

6.4.1 Activation data generation and installation

For the establishment of any Certification Authority, some cryptographic keys must be created, used for recovery and functioning activities. The TSPM Certification Authority operates with two types of roles, each one with its corresponding security mechanisms:

- The administrator keys and passwords.
- The operator passwords.

The set of cryptographic keys is duplicated in case of damage or operation malfunctioning. If some keys are lost or stolen, this fact is communicated to the TSPM Security Officer who informs to the TSPM Director who manages the risks and decides what to do.

When the TSPM provides the subscriber a secure signature creation device, the 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.

6.4.2 Activation data protection

Only authorized staff, in this case the operators and administrators of the Certification Authority, possesses the cryptographic keys 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 her 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.

6.5 Computer security controls

The TSPM uses trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them.

At the time of its acquisition, the TSPM evaluated the certifications of these products and reviews that the certifications are still valid. If any product, especially the QSCD, loses the certification (it is no longer certified as QSCD), the TSPM will catalogue this as an operational incident and the incident management procedure will be activated to respond to such eventuality.

6.5.1 Specific computer security technical requirements

A series of controls are in place in the different components making up the TSPM services.

Operational controls:

- All of the operations procedures are duly documented in the corresponding operations manuals. The TSPM maintains a Contingency Plan (Business Continuity Plan).

- Tools have been implemented to protect the integrity of the TSPM systems against viruses, malicious and unauthorized software.
- The TSPM applies a procedure for updating security patches within a reasonable time after they are available. The TSPM Director may approve not to apply these patches so as the reasons for that (problems outweigh the benefits) are documented.
- The equipment is maintained on an ongoing basis to ensure uninterrupted availability and integrity.
- Procedures exist for saving, deleting and safely eliminating storage media, removable media and obsolete equipment.
- The revocation service is available on a 24x7 basis.
- When external registration service providers are used, registration data are exchanged securely and only with recognized registration service providers, whose identity is authenticated.

Access controls:

- Unique accounts or user ids are used in such a way that users are associated with, and can be held responsible for, their actions.
- Rights are assigned according to the principle of providing users with the least amount of system privileges they need to do their jobs.
- Access rights are immediately cancelled whenever users change jobs or leave the organization.
- System privileges are assigned on a case-by-case basis and terminated once the reason for their assignation is no longer valid.
- The TSPM maintains password quality guidelines.

6.5.2 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.

6.6 Life cycle technical controls

6.6.1 System development controls

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

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

6.6.2 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.

6.6.3 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 products used by the TSPM.

6.7 Network security controls

The TSPM protects its network and systems from attack.

The TSPM segments its systems into networks or zones based on risk assessment considering relationship between trustworthy systems and services. The TSPM applies the same security controls to all systems co-located in the same zone.

The TSPM restricts access and communications between zones to those necessary for the operation of the TSPM. Not needed connections and services are explicitly forbidden or deactivated. The established rule set are reviewed on a regular basis.

The TSPM keeps all systems that are critical to the TSPM operation in one or more secured zone(s).

The production systems for the TSPM services are separated from systems used in development and testing.

The TSPM undergoes or performs a regular vulnerability scan and penetration test on public and private IP addresses identified by the TSPM on an annual basis.

The TSPM configures all CA systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the CA's operations.

The TSPM maintains its Root CA System in an offline state.

The TSPM maintains its Root SubCA System in a High Security Zone.

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.
- Remote accesses are exceptionally allowed in cases of force majeure to TSPM operational personnel for exclusive monitoring, control, updating and emergencies when they cannot be carried out at TSPM facilities.

6.8 Time-stamping

Not applicable.

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 is 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	• *Version* • *Serial Number* • *Issuer Distinguished Name (Country (C), Organization (O), Organizational Unit (OU), Common Name (CN))* • *Validity (Not Before, Not After)* • *Subject (Country (C), Organization (O), Organizational Unit (OU), OI, Common Name (CN))* • *Subject Public Key Info* • *Signature Algorithm*

PUBLIC EMPLOYEE[5]	• *Version* • *Serial Number* • *Issuer Distinguished Name (Country (C), Organization (O), Organizational Unit (OU), Common Name (CN))* • *Validity (Not Before, Not After)* • *Subject (Country (C), Organization (O), Organizational Unit (OU), Serial Number, Surname, Given Name, Common Name (CN))* • *Subject Public Key Info* • *Signature Algorithm*

CERTIFICATE	RECOMMENDED FIELDS
ELECTRONIC SEAL	• *Issuer Distinguished Name (Locality, Serial Number, Organization Identifier)* • *Subject (Surname, Given Name, Organization Identifier)*
PUBLIC EMPLOYEE[6]	• *Issuer Distinguished Name (Locality, Serial Number)* • *Subject (Organizational Unit (OU), Organizational Unit (OU), Organization Identifier, Title)*

CERTIFICATE	MANDATORY EXTENSIONS
ELECTRONIC SEAL	• *Authority Key Identifier* • *Subject Key Identifier* • *Key Usage* • *CRLDistributionPoint (distributionPoint)* • *Authority Info Access (Access Method, OCSP Access Location and calssuer)* • *Qualified Certificate Statements* • *Certificate Policies (Policy Identifier, Policy Qualifier ID [CPS Pointer, User Notice], EU qualified certificate policy Identifier (only if ALTO FIRMA o MEDIO / SUSTANCIAL)* • *Subject Alternative Names (Directory Name)*
PUBLIC EMPLOYEE[7]	• *Authority Key Identifier* • *Subject Key Identifier* • *CRLDistributionPoint (distributionPoint)* • *Authority Info Access (Access Method, OCSP Access Location and calssuer)* • *Key Usage* • *Subject Alternative Names (Directory Name= Identidad Administrativa)*

[5] CEPCHSM included
[6] CEPCHSM included
[7] CEPCHSM included

CERTIFICATE	RECOMMENDED EXTENSIONS
ELECTRONIC SEAL	• *Issuer Alternative Name* • *Subject Alternative Names*
PUBLIC EMPLOYEE[8]	• *Issuer Alternative Name* • *Subject Alternative Names*

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 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 only certifies the public key associated with the cryptographic algorithms identified above and only uses the cryptographic signature algorithms described above for signing certificates, certificate revocation lists and any other element of the Certification Authority.

[8] CEPCHSM included

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, the fields *Subject* and *SubjectAlternativeName* are used according to the normalized scheme proposed by the AGE and described in CPs.

7.1.6 Certificate Policy Object identifier

Issued certificates 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 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 CRLs 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.

7.3 OCSP profile

The profile for the Online Certificate Status Protocol (OCSP) messages issued by the TSPM conform to the specifications contained in the [IETF RFC 6960].

7.3.1 Version number

Certificates used by the Certificate validity status information and consultation service, via OCSP, comply with the X.509 version 3 standard.

7.3.2 OCSP extensions

The OCSP responses of the Certificate status information service on the validity status of the certificates include, for requests that request it, the global extension *nonce*, used to link a request with a response, in order to prevent repetition attacks.

Additionally, the extension *Extended Revoked Definition* is included in those cases in which the status of a certificate that the CA acknowledges as not issued is consulted. Then, the service responds to the query of certificates not issued by the CA as revoked certificate.

8 Compliance audits and other assessments

8.1 Compliance audits

The TSPM conducts regular internal and external audits to test compliance of legal, security and operational requirements.

8.2 Frequency or circumstances of assessment

According to eIDAS, the CSPM conducts 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 is carried out by a conformity assessment body complying with eIDAS and applicable regulation (ETSI norms, etc.).

8.4 Assessor's relationship to assessed entity

The auditor does not belong in any case to the staff in charge of the operation of the Certification Authority. Besides, 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 are be carried out by an independent body of TSPM, which should have no conflict of interest that impairs its ability to perform audit services.

The auditor requires 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 are always be operated by SGTIC staff, providing the required information.

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

8.5 Topics covered by assessment

The elements to audit are at least the following:

- The trust service(s) provided and its scope and boundaries in terms of the characteristics of the business, the organization, facilities, assets and technology.
- The information security risk assessment and risk treatment.
- 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 they are 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 are carried out:

- The auditor prepares a report with the results of the audit.
- The auditor notifies the non-compliance to the parties involved.
- After receiving the report of the compliance audit conducted, the TSPM discusses the deficiencies found with the entity that performed the audit, and develop and implement a corrective plan to solve such deficiencies.
- Once the deficiencies are corrected, the auditor verifies 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 by the TSPM Director:

- 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 delivers the reports of the audit results to the Spanish Supervisory Body or to the appropriate entity within the AGE, within 15 days after receiving the final reports from the Conformity Assessment Body.

9 Other business and legal matters

9.1 Fees

There are no charges established for the service offered by the TSPM.

9.2 Financial Responsibity

The TSPM has a sufficient level of coverage for public liability, under the terms covered in article 20.2 of LFE.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

The TSPM considers at least the following information as confidential 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 plans and security operational measures.
- Documentation of operations and other operational plans, as archives, monitoring and similar.

Cryptographic information that allows access to the TSPM Certification Authority is severely protected by physical means already established on the SGTIC.

Access to the operational and management cards that allow access to the cryptographic modules that support the Certification Authority, as well as the serial numbers and activation of the cryptographic hardware devices, are severely protected.

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

9.3.2 Information not within the scope of confidential information

The following information is considered non-confidential, to be known by the third parties:

- CPS and certificate policies.
- Terms, conditions and disclosure statement.
- Any information published on the TSPM public web repository.
- 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 and that is not confidential.

9.3.3 Disclosure of suspension and revocation information

See section above.

9.3.4 Responsibility to protect confidential information

The TSPM only discloses the information identified as confidential in cases provided by law to do so. Specifically, records that support the reliability of the data contained in the certificate are 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 9.4 of this document.

9.3.5 Information disclosure by request of the subscriber

The TSPM includes in the privacy policy under Section 9.4 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.

9.4 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 informs the subscribers about their privacy rights in the registration process.

According to article 14 in the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, GDPR), we inform you that the Subsecretary of the Ministry of Labour and Social Economy (Ministerio de Trabajo y Economía Social, in Spanish) is the controller for

all personal data used for providing trusting services, that is, for the management of public employee and electronic seal public key certificates issued by the Ministry.

The Subsecretary, through its Trust Service Provider, carries out the data processing following the existing regulation on personal data protection, information security and its own activity regulation that allows the data processing, mainly the Public Employee Statute, the law 39/2015, and the law 40/2015, which regulate how the Public Administration and its public employees must operate.

In this sense, technical and organizational security measures have been adopted in order to guarantee the security of the personal data and avoid its unauthorized alteration, processing or access, responsible for causing material and immaterial damages. All the security measures have been adopted taking into account the current technology, the data categories and the degree of risks and are periodically reviewed in order to ensure that the measures are updated according to new risk scenarios.

As the main controller for all data subject and according to information requirements of article 14 in GDPR, the Subsecretary states the following basic information for data processing:

Data Controller	Subsecretaría del Ministerio de Trabajo y Economía Social Paseo de la Castellana 63 Madrid 28071 España (Spain) email: sgtic@meyss.es
DPO	Data Protection Officer (Delegado de Protección de Datos) Ministerio de Trabajo y Economía Social Paseo de la Castellana 63 Madrid 28071 España (Spain) email: dpd@meyss.es
Purpose and legal basis	Providing trusting services including the management of public employee and electronic seal public key certificates according to the Public Employee Basic Statute and 39/2015 and 40/2015 laws.
Data categories	Identification data: NIF/DNI, name and surnames, birth date, email, job description, entity. Other data: public and private key, certificate serial number, certificate request code.
Data origin	Database with the Ministry Public Employees SG de Recursos Humanos e Inspección de Servicios (Human Resources Area and Service Control) Ministerio de Trabajo y Economía Social
Data transfer	Data transfer to police and justice bodies according to law. Certificate public data.
International data transfers	No international transfers outside EU are allowed.
Cancellation period	15 years according to regulation.
Automated decision making	There is not any automated decision-making including profiling with the data subject.

Subject rights: Subjects can exercise the right of access, the right to rectification, to erasure (to be forgotten), to restriction of processing, to data portability as well as the right to object to processing and not to be subject to a decision based solely on automated processing, in accordance with the provisions of articles 15 to 22 of the GDPR.

How to exercise these rights: by contacting the controller electronically, or through any Registry Office according to 39/2015 law.

Should you have any questions about your personal data or exercising your rights, please contact with the DPO (article 38.4 GDPR).

Right to lodge a complaint with a supervisory authority: please contact with Agencia Española de Protección de Datos (Spanish Data Protection Agency) at Jorge Juan 6 street. 28001. Madrid. España (Spain). (http://www.aepd.es).

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

The TSPM does not disclose or lease personal information, except as provided in Sections 9.3 of this document, and in section 5.8, upon termination of the Certification Authority.

Confidential information in accordance with the LOPDGDD is protected from loss, destruction, damage, forgery and unauthorized or unlawful processing.

9.5 Intellectual Property Rights

9.5.1 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.

9.5.2 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 and reciprocally of the AGE.

9.5.3 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.

9.5.4 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.

9.6 Representations and warranties

9.6.1 TSPM 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 issuance and delivery of a certificate to a subscriber, the TSPM informs the potential subscriber of the terms and conditions regarding certificate use and fees – when established – as well as usage limitations and the binding legal instruments.

The requirement is met by a "Terms and conditions of use of certificates" document through a durable (i.e. with integrity over time) means of communication, which may be transmitted electronically, and in readily understandable language.

Any change to these terms is published in the TSPM repository and by internal means (startup message etc.).

The TSPM informs the subscriber or private key holder about the expiry of their certificate prior to or at the same time as the electronic certificate expires, specifying the reasons and date and time that the certificate is no longer to be effective.

The TSPM gives signer two months notification of the termination of service and, where applicable, informs them of the characteristics of the service provider to which it proposes to transfer the management of certificates. Notification to signers are conducted in accordance with the stipulations of this document.

The TSPM has a termination of service plan which specifies the conditions under which such an event would take place.

All of this public information connected to certificates is included in the TSPM repository.

The TSPM links the subscribers and relying parties through proper legal instruments.

9.6.2 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 eIDAS and subsequent law.

- That, in the case of generating the private keys of the subscriber their confidentiality is maintained throughout the process.

9.7 Limitations of warranties

The TSPM rejects any other warranties not legally required, other than those referred to in section 9.6.2.

9.8 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) according to article 23 of LFE.

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.

9.8.1 Disclaimer of warranties

9.8.1.1 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-authorised 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.

9.8.1.2 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.

9.8.2 Fortuitous event or force majeure

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

9.9 Indemnities

Not stipulated.

9.10 Term and Termination

9.10.1 Term

The CPSM and Certification Policies shall become valid from the moment of the TSPM and their publication on the TSPM web page public repository and shall remain valid until new versions are approved according to section 1.5.3 of this document.

9.10.2 Termination

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

9.10.3 Effects of termination and survival

The obligations and restrictions established in this CPSM and the corresponding Certification Policies shall be still valid for any certificates previously issued even if a new version has been approved.

9.11 Individual notices and communications with participants

The TSPM establishes notification mechanisms between parties for the corresponding policies and relevant internal procedures.

In addition, it shall publish any significant notifications that may affect the services provided on its web page and shall try as much as possible (low volume, email availability, communication urgency, communication importance, etc.) to contact by email.

9.12 Amendments to this document

9.12.1 Amendment procedure

The TSPM may unilaterally update and amend this document, assuming it complies with the following procedures:

- The update should be justified from a technical, legal, or commercial standpoint.
- The update proposed by the TSPM may not contravene any of the certification policies established by it.
- The update will be reviewed to guarantee that in each situation the resulting specifications comply with the requirements that the modification intend to fulfil and that prompted the change.
- Any implications that the change of specifications may have on the user are established, and the necessity of notifying them regarding said changes is set forth.
- The CPSM shall be approved by the TSPM according to the procedure established.

9.12.2 Notification period and mechanism

In the event that the modifications made may affect the validity of certificates, the TSPM shall notify the users via its website and shall make the new version of the CPSM public.

9.12.3 Circumstances under which an OID must be changed

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

9.13 Dispute resolution procedures

The TSPM will resolve any disputes that may arise concerning the interpretation or applicability of the CPSM following Spanish Public Administration certificate policy.

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.

9.14 Governing law

The provision of trusted services of the TSPM are governed by the provisions of the Laws of the Kingdom of Spain, in special:

- The 59/2003 Law, of December 19, 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).
- The 39/2015 Law, of October 1, about Common Administrative Procedure of the Public Administrations.
- The 40/2015 Law, of October 1, about Legal Framework of the Public Sector.
- The Organic Law 3/2018, of December 5, on Data Protection and Guarantee of Digital Rights (LOPDGDD)
- The 56/2007 Law, of December 28, Measures to Promote the Information Society.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation / GDPR in short).
- The Royal Decree 3/2010, of January 8, National Security Framework for the Electronic Administration.
- The Royal Decree 4/2010, of January 8, National Interoperability Framework for the Electronic Administration.
- The Royal Decree 1/1996, of April 12, consolidated text for Intellectual Property Law.

- The Technical Standard for Interoperability of Electronic Signature and Certificate Policy for the Spanish Public Administration (AGE).
- The Royal Decree 1112/2018, of 7 September, on the accessibility of websites and mobile applications in the public sector.
- UNE-EN 301549:2019, Spanish version of ETSI EN 301 549 V2.1.2 (2018-08). Accessibility Requirements for ICT products and services.
- Commission Decision of February 25th, 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.

Additionally, the practices of the trust services provided by the TSPM follow the following standards:

- ETSI EN 319 401: General Policy Requirements for Trust Service Providers.
- ETSI EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates. General requirements.
- ETSI EN 319 411-2: Requirements for trust service providers issuing EU qualified certificates.
- ETSI EN 319 412: Electronic Signatures and Infrastructures (ESI); Certificate Profiles.

9.15 Compliance with Applicable Law

The TSPM declares its compliance with applicable law.

9.16 Miscellaneous Provisions

9.16.1 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, 9.3, and 9.6, 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.

9.16.2 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.

9.17 Other Provisions

In case of loss of the QSCD certification of any of the qualified signature devices used by TSPM as a Trusted Service Provider, appropriate measures will be taken to reduce as much as possible its impact. The supervisory body will be informed about this and TSPM will stop issuing certificates on those devices.

The TSPM allows third parties to check and test all types of certificates issued. For this reason, the TSPM has got a set of test certificates that can be requested through the contact data in section 1.5.2.

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.
CompQSCD	Compilation of Member States notification on SSCDs and QSCDs. Member States' notifications on Designated Bodies under Article 30(2) and 39(2) of Regulation 910/2014 and Certified Qualified Signature Creation Devices under Article 31(1)-(2), and Certified Qualified Seal Creation Devices under Article 39(3) of Regulation 910/2014, and information from Member States on: Secure Signature Creation Devices benefiting from the transitional measure set in article 51(1) of Regulation 910/2014.
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 on electronic signatures and the European directive.
ETSI EN 301 549	ETSI European Standard 301 549 Accessibility requirements for ICT products and services.
ETSI EN 319 401	ETSI European Standard 319 401. General Policy Requirements for Trust Service Providers.
ETSI EN 319 403	ETSI European Standard 319 403. Trust Service Provider Conformity Assessment – Requirements for conformity assessment bodies assessing Trust Service Providers.
ETSI EN 319 411-1	ETSI European Standard 319 411-1. Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
ETSI EN 319 411-2	ETSI European Standard 319 411-2. Policy requirements for certification authorities issuing qualified certificates.
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 con 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 119 403-3	ETSI Technical Specification 119 403-3. Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers.
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 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (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 9/2017	9/2017 Law, November 8th, on public procurement and transposition to the Spanish legislation of EU directives on public procurement 2014/23/EU and 2014/24/EU of 2014 February 26th.
Ley 39/2015	39/2015 Law, of October 1, of the Common Administrative Procedure of the Public Administrations.
Ley 40/2015	40/2015 Law, of October 1, about Legal Regime of the Public Sector.
RD 5/2015	Royal Decree 5/2015, of October 30 that approves the updated Public Employee Basic Statute Law.
UTF-8	8-bit Unicode Transformation Format.

Annex B: Electronic Links (URLs)

Email Organization Data:

admin_ca@meyss.es

CPSM, Certificate Policies, PDS and Terms and Conditions:

http://ca.empleo.gob.es/meyss/DPCyPoliticas

https://ca.empleo.gob.es/en/CA_MEYSS/declaracion.htm (English version)

CA Root certificate, SubCA certificates and OCSP certificate:

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

OCSP Service Validation Status:

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

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

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

CPSM and Certificate Policies:

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

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 an email to admin_ca@meyss.es, stating date of publication and/or serial number requested.