MINISTERIO DE TRABAJO
Y ECONOMÍA SOCIAL

SUBSECRETARÍA

S.G. DE TECNOLOGÍAS DE LA
INFORMACIÓN Y COMUNICACIONES

Ministry Trust Service Provider
Certification Policy for Public Employee Certificate
Centralized and Managed by HSM

sgtic@mites.gob.es
EA0041850

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

Version control

Identifier	D326
Title	Ministry Trust Service Provider Certification Policy for Public Employee Certificate Centralized and Managed by HSM
Version	12
Document status	Approved
Approval date	20211102

Change control

Version	Date	Comments
0.9	20140210	Initial version.
1.0	20140321	Final document.
1.1	20140514	Updated section 3.1.
1.2	20150618	Added SHA-256.
1.3	20160318	Usage of centralized term. References updated. Operating requirements updated.
2.0	20160720	Update to eIDAS profiles (*OID 1.3.6.1.4.1.27781.2.5.4.7.1*).
2.1	20170124	Issuing procedure clarified. References updated.
03	20170410	Updated to established template for documentation.
04	20170410	DIR3 updated. Minor mistakes in section 2.1 updated.
05	20170508	Section 1.4 updated. Added section 1.6, CP administration. Added section 1.8, general conditions of CEPCHSM certification services. Added section 2, publication and repository responsibilities. Section 4.4 updated. Added section 5, other business and legal matters. Conformance to eIDAS preassessment audit.
06	20170707	Annex B updated with URL Link to DPC and CPS. Annex B updated using HTTPS. Changes in extension Qualified Certificate Statements: *QcType* added Added *id-qcs-pkixQCSyntax-v2.*
07	20180727	Use of *trust service provider* term instead of *certification service provider* term. Ministry name updated. Date format adapted to *ISO 8601: YYYYMMDD.* GDPR reference added. Privacy and data protection clause updated. Change in the name of the National Supervisory Body. Reference to procurement contract law updated. *TSPM Director* term replaces *Responsible for the TSPM* term Information service URL updated to HTTPS.
08	20190617	Expiration date deleted. Updated DIR3.

		Updated the implicit acceptance of the certificate. Updated references with LOPDGDD.
09	20190819	Change in extensions: - Authority Information Access (field *caIssuers*). - Certificate Policy (field *user notice*). Update of annex B: URL of SubCA certificate.
10	20201026	DIR3 updated. Ministry name updated. Updated section 1.8.2 Risk Analysis to include the annual periodicity of the analysis. Minor mistakes corrected in sections 1.7.2, 2.1, 3.1.1, 4.2, and 4.3.
11	20211001	Updated SGTC email address
12	20211102	Added maximum field sizes of subject field

Table of contents

1 Overview

1.1 Introduction

This document contains the **Certification Policy for the Public Employee Certificates Centralized and Managed by HSM and issued by the Trust Service Provider of the Ministry of Labour and Social Economy (TSPM[1]).**

This document clarifies and supplements the Certification Practice Statement (CPSM) regarding Public Employee certificates centralized and managed by HSM (CEPCHSM from now on).

1.2 Description

The CEPCHSM issued by the TSPM, is a qualified electronic signature according to annex I requirements of eIDAS, as a means of signing documents with a qualified electronic signature as defined in article 3 (12) of eIDAS, QCP-n[2] according to [ETSI EN 319 411-2].

The CEPCHSM is issued on HSM and according to annex II of eIDAS[3] regulation, article 8, section 4, follows the substantial assurance level. The TSPM shall monitor the HSM certification status until the end of the validity and will replace this HSM once the certification is expired according to the procedure established.

The CEPCHSM is a certificate for public employees according to [Ley 39/2015] and to article 43 of [Ley 40/2015]. This certificate is used as a means to identify and authenticate a Public Employee in computer systems and applications. The certificate includes both the subscriber and the public entity in which the public employee works.

1.3 Document name and identification

1.3.1 Identification of this document

The name of this document is **Ministry Trust Service Provider Certification Policy for Public Employee Certificate Centralized and Managed by HSM**, whose information appears on the version control of this document (page ii).

This document can be found on the URL that appears on the Annex B:

1.3.2 Certificate types identification

Each certificate type has a dedicated *OID*, included in the *PolicyIdentifier* field of the certificate. Each *OID* is univocal and is not used to identify different types, policies or versions of issued certificates. The OID for the CEPCHSM is as follows:

- CEPCHSM: *[1.3.6.1.4.1.27781.2.5.4.7.1]*

1.4 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:

a. Certificate requesters (applicants).
b. Certificate subscribers.
c. The responsible for the certificate.
d. The relying parties.

[1] PSCM, in Spanish

[2] QCP-n-remote sometimes to emphasize that the private key is stored on a remote qscd

[3] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014, concerning electronic identification and trust services for electronic transactions in the internal market.

The requester of a CEPCHSM is a public employee (a natural person) who, after receiving the certificate, becomes subscriber and responsible for the certificate.

The subscriber of a CEPCHSM is the public employee (a natural person) identified as such in the field *Subject* of the certificate and who must comply with an appropriate usage of the certificate and its linked private key according to the CPSM.

The responsible for a CEPCHSM is the natural person identified as such in the object *Identidad Administrativa* on the *SubjectAltName* extension. The responsible for a CEPCHSM is the subject of the certificate.

The relying parties are the entities (including natural and legal persons, Public Administrations and other organizations) that, using a CEPCHSM issued by the Certification Authority operating under the CPSM, verify the integrity of any electronically signed message or 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 relying party shall use the information contained in the CEPCHSM to determine the certificate usage in each particular case.

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

1.5 Certificate usage

The CEPCHSM for electronic signature as a means to electronically sign documents and proceedings offers:

- Non repudiation in origin.
- Integrity.

The CEPCHSM is also used for authentication as a means to identify and authenticate a Public Employee in computer systems and applications.

The CEPCHSM issued under the CPSM shall be only used in the defined transactions inside authorized systems and applications. The issue of the CEPCHSM under the CPSM obliges the subscriber to the acceptance and use thereof in the terms expressed in the CPSM.

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

It is not allowed in any way the use of CEPCHSMs outside the scope described in the CPSM, which could cause immediate revocation of the certificates by its misuse.

The TSPM, as a trust service provider (TSP) shall not be liable of the contents of documents signed using CEPCHSMs nor any other use of the certificates, as message or communications encrypt processes.

TSPM ensures that private keys linked to the CEPCHSM are, with a high level of assurance, under the exclusive control of the CEPCHSM subscriber. The subscriber shall take care of the password and activation keys to the CEPCHSM, avoiding loss, copy or non-authorized use.

1.6 CP administration

1.6.1 Organization administering the document

The TSPM Director is the responsible for the definition, review and disclosure of this CP. There are two assistant directors 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 directors are the Assistants Directors of the SGTIC (Subdirección General de Tecnologías de la Información y las Comunicaciones).

1.6.2 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

1.6.3 CP administration procedures

1.6.3.1 Change Control

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

The security officer of the TSPM will review this CP annually or should a significant change have happened in that period. Errors, updates, suggestions or improvements on this document will be communicated to the organization whose contact data appear in section 1.5.2. All communications should include a description of the change, its justification and the information of the person requesting the modification.

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

1.6.3.2 Publication

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

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

1.6.3.3 CP Approval

The TSPM security officer will request the approval of this CP to the TSPM responsible who should approve the document (or not) as stated in the TSPM Documentation Quality Plan.

Any new version will expire one year after the date it has been approved.

1.7 Definitions and acronyms

1.7.1 Definitions

In this document the following definitions are used:

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.
DN	Univocal identification for an item within a X.500 directory.
O	Organization: Distinguished Name attribute for an object within X.500 directory structure.
OCSP	On line Certificate Status Protocol: This protocol allows checking the revocation status of an electronic certificate.
OU	Organizational Unit: Distinguished Name attribute for an object within a X.500 directory structure.
PIN	Personal Identification Number: Password that protects access to a cryptographic card.

PKCS	Public Key Cryptography Standards is a set of standards defined by RSA Laboratories and internationally accepted.
RFC	Request For Comments, standard documents issued by IETF (Internet Engineering Task Force).

1.7.2 Acronyms

C	Country.
CA	Certification Authority.
CDP	CRL Distribution Point.
CEC	Certificate Emission Code.
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 TSPM.
CRL	Certificate Revocation List.
CSP	Cryptographic Service Provider.
CSR	Certificate Signing Request.
CWA	CEN Workshop Agreement.
DN	Distinguished Name.
HSM	Hardware Security Module
LOPDGDD	Organic Law about Personal Data Protection and Digital Rights Guarantee (Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales).
O	Organization.
OU	Organizational Unit.
OID	Object IDentifier.
OCSP	On-line Certificate Status Protocol.
PA	Public Administration.
PDS	PKI Disclosure Statement.
PSCM	Trust Service Provider of the Ministry. Prestador de Servicios de Confianza del Ministerio.
QSCD	Qualified Signature Creation Device.
RA	Registration Authority.
RFC	Request For Comments.
SGTIC	Subdirección General de Tecnologías de la Información y las Comunicaciones.
TSP	Trust Service Provider.
TSPM	Trust Service Provider of the Ministry.
VA	Validation Authority.

1.8 General conditions of the CEPCHSM 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 [Ley 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.

The TSPM shall publish the general terms and conditions of its services via its website https://ca.empleo.gob.es. Any relevant change will be notified via this website by publishing an announcement in the home page plus the old version and the new version. After 30 days, the old version will be removed but will be retained by the TSPM for at least 15 years and may be consulted by interested parties with justifiable cause.

1.8.1 Information Security Policy

The TSPM defines an information security policy which is approved by the TSPM Director. This information security policy sets out the TSPM approach to managing its information security.

The TSPM publishes and communicates this information security policy to its employees on the Intranet.

This information 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 information security policy is communicated to subscribers and third parties (relying parties, assessment and supervisory bodies, etc.), where applicable.

1.8.2 Risk Analysis

As stated in the information security policy, the TSPM follows a specific risk analysis methodology 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 every year or if there has been any significant event affecting the TSPM.

2 Publication and Repository Responsibilities

2.1 Repositories

The TSPM has a public information repository on https://ca.empleo.gob.es available 24 hours a day, 7 days a week.

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.
- Issues Certificate Revocation Lists (CRLs) and real-time certificate verification services, using Online Certificate Status Protocol (OCSP) in URLs stated in Annex B.
- Publishes the general terms and conditions of the certificates.

The TSPM revocation and validation service is available 24 hours a day, 7 days a week except the minimum required time for maintenance operations and serious incident resolution.

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

This certification policy is published as soon as it has been approved.

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

The TSPM shall notify users of changes in specifications or in the terms and conditions of services via the TSPM website. There will be an announcement of changes in the home page and both versions of the document will be published. After 30 days, the previous version will be removed, but will be 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.

3 Identification

3.1 Management of names

3.1.1 Types of names

Every certificate contains the *DN*, defined following the rules of the recommendation [ITU-T X.501], of the person identified in the certificate, contained in the *Subject* field, including a *Common Name* attribute. All the issued certificates also meet the standard [IETF RFC 5280]. The maximum size of the fields of the certificates will be adjusted to what is stated in RFC5280, unless otherwise indicated in this document.

3.1.2 Normalization and Administrative Identity

The TSPM uses the normalized naming schema *Identidad Administrativa* proposed by the Spanish administration for every type of certificate and policy.

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.

The Administrative Identity number for the Public Employee certificates are:

- CEPCHSM (Medium level of assurance): *2.16.724.1.3.5.7.2*

The CEPCHSMs issued by the TSPM include the following fields according to schema *Identidad Administrativa*:

Certificate	Mandatory "Identidad Administrativa" fields
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 Email Organizational Unit Job title

Certificate	Optional "Identidad Administrativa" fields
CEPCHSM	Personal identification number

All other aspects related with the management of names (meaning, use of pseudonymous and anonymous, name format interpretation, name unicity and conflicts resolution) are specified in the CPSM.

4 Operational requirements

4.1 Application for the certificates

The public employee applicant must apply in person and identify herself at the Registration Authority to obtain an activation code. At this event the public employee fills and signs an application form for the issuance of the CEPCHSM issued by the TSPM. This form summarizes the terms and conditions applicable to the certificate present in the CPSM and in the CPs.

The completed and signed form is submitted to the corresponding Registration Authority, which authenticates the identity of the applicant and ensures that the application form is complete and accurate. The units that will operate as Registration Authorities are *Subdirección General de Recursos Humanos e Inspección de Servicios* and *Subdirección General de Apoyo a la Gestión de la Inspección*.

The TSPM shall check through the Registration Authority, the identity and any other data provided by the CEPCHSM applicant.

The authentication of the applicant's identity is done according to the requirements specified in the CPSM. Once the identity of the applicant has been verified, a copy of the completed form is returned to the applicant and an Activation Code is provided. The Activation Code allows, with some additional factors, the issuance of the CEPCHSM.

Another way of issuing the CEPCHSM is by using a qualified electronic certificate that allows signing the application form, confirming its data and accepting the terms and conditions.

The procedures established in this section also apply in case of renewal of certificates, as it involves the issuance of new certificates

4.2 Issuance of the CEPCHSM

The telematics issuance of the CEPCHSM may be done by the applicant by using the Certificate Activation Code, its DNI, its birth date and one OTP receive by email as a second authentication factor.

Another way of issuing the CEPCHSM is by using a qualified electronic certificate once the application form has been signed, its data confirmed, and the terms and conditions accepted.

The system shall inform the applicant (the public employee) about the issuance of the CEPCHSM. Then the system shall ask to establish and enter the password needed to protect the certificate and at that very moment the private key will be generated and stored on the system. The password is used to protect the CEPCHSM and to ensure that the private key remains under the subscriber's exclusive control.

The CEPCHSM key pair is generated on the HSM according to Common Criteria EAL 4+ ALC_FLR.1, AVA_VAN.5, as well as FIPS 140-2 Level 3 or equivalent.

The CEPCHSM issuance is performed according to the legal requirements that establish the validity timeframe of the issuance in person in the Registration Authority.

The PSCM uses a procedure to issue the certificates that securely links the certificates with the public employee information, including the public key. It also indicates the date and time in which they were issued and measures are taken against forgery of certificates and to ensure the privacy of the key pair during its generation process.

Any issued CEPCHSM is stored in a repository without previous subject approval.

The issuance of the activation codes implies the approval of the application form. If the application form is not approved, the Certification Authority will communicate this to the applicant by email, phone or any other means related to the contact data of the form.

Certificates are considered accepted through the authentication in the portal and through the use of the computer mechanism for generating them remotely on the server.

When the CEPCHSM issuing process finishes, the subscriber (public employee) is notified that the CEPCHSM is already available for its usage: for authentication and electronic signature purposes.

The CEPCHSM private key is activated when the subscriber enters the password that protects the CEPCHSM, under her exclusive control, as well as the second authentication factor.

The procedures established in this section also apply in case of renewal of certificates, as it involves the issuance of new certificates.

4.3 Certificate renewal

The renewal of Public Employee Certificates means the issuance of new certificates, being necessary to carry out a new application form and subsequent issuance as described in previous sections.

Any procedures could be established in the future for the certificate renewal in an electronic way (without face to face presence), prior to its expiration date, and when the time elapsed since the previous identification with physical presence is less than five years.

4.4 Certificate revocation

The revocation is automatically done when there has been an update in the subscriber data or the subscriber is not anymore a public employee of the organization.

In other case, the subscriber shall proceed to the revocation manually through the autoservice web site.

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.

The state change of the validity of a certificate will be 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, or its suspension, to become effective and the actual change of the status information of this certificate is 5 minutes.

5 Other business and legal matters

5.1 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 Services Control Area). 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 and does not disclose nor transfer any data except in those legally established cases.

6 Profile of the Centralized Public Employee Certificate

6.1 CEPCHSM for authentication and electronic signature

The certificate fields are as follows:

Field	Description	Content
1. X.509v1 Field		
1.1. Version	X.509 Standard version for the certificate	2 (= v3)
1.2. Serial Number	Certificate univocal identification number	7c 88 54 93 b6 c9 (sample)
1.3. Issuer Distinguished Name		
1.3.1. Country (C)	Country	C = ES
1.3.2. Locality (L)	Locality of the Trust Service Provider	L = MADRID
1.3.3. Organization (O)	Official name of the Trust Service Provider (certificate issuer)	O = MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL
1.3.4. Organizational Unit (OU)	Organizational unit within the service provider, responsible for issuing the certificate	OU = S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES
1.3.5. Organizational Unit (OU)	Organizational unit within the service provider, responsible for issuing the certificate	OU = PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS
1.3.6. Serial Number	NIF of the Ministry	SERIALNUMBER = S2819001E
1.3.7. OrganizationIdentifier	Organization identifier or legal person identifier normalized under ETSI EN 319 412-1	VATES- S2819001E
1.3.8. Common Name (CN)	Common name of the Trust Service Provider (certificate issuer)	CN = SUBCA1 MEYSS
1.4. Validity	Validity period (5 years)	
1.4.1. Not Before	Start of validity period	Format: UTCTime YYMMDDHHMMSSZ
1.4.2. Not After	End of validity period	Format: UTCTime YYMMDDHHMMSSZ
1.5. Subject		
1.5.1. Country (C)	Country	C = ES
1.5.2. Organization (O)	Name of the Administration, Agency or public entity where the public employee is working	O = MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL (sample)
1.5.3. Organizational Unit (OU)	Certificate Type	OU = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO

Field	Description	Content
1.5.4. Organizational Unit (OU)	Unit, within the Organization, where the public employee (subscriber) is working. Maximum size 100 characters.	OU = SUBDIRECCIÓN GENERAL DE ADMINISTRACIÓN FINANCIERA (sample)
1.5.5. Title	Job title. Maximum size 100 characters.	T = JEFE SECCION APOYO GESTION (sample)
1.5.6. Serial Number	DNI/NIE/Passport of the Public Employee according to ETSI EN 319 412-1 semantics	SERIALNUMBER = IDCES-00000000G (sample)
1.5.7. Surname	First and second surnames, according to DNI/NIE/Passport	SN = DE LA CAMARA ESPAÑOL (sample)
1.5.8. Given name	Given name, according to DNI/NIE/Passport. Maximum size 30 characters	G = JUAN ANTONIO (sample)
1.5.6.Common Name (CN)	Given name plus two surnames plus DNI/NIE/Passport number separated by a hyphen (-). Maximum size 125 characters.	CN = JUAN ANTONIO DE LA CAMARA ESPAÑOL - 00000000G (AUTENTICACION) (sample)
1.6. Subject Public Key Info	Public key, codified following the cryptographic algorithm	
1.7. Signature Algorithm	Signature algorithm	SHA-256 with RSA Signature and key length 2048 bits

The field extensions are as follows taking into account that **the only field extension that is critical is the field extension Key Usage**:

Field	Description	Content
2. X.509v3 Extensions		
2.1. Authority Key Identifier	Identification of the public key corresponding to the private key used to sign a certificate. This extension is used where an issuer has multiple signing keys	
2.1.1. Key Identifier	Issuer public key identifier	
2.2. Subject Key Identifier	Subject public key identifier (derived from the subject public key using hash function)	
2.3. cRLDistributionPoint	Indicates how to obtain the CRL information	
2.3.1. distributionPoint	Website where CRL is found (distribution point 1)	URL distribution point 1 CRL (see annex B)
2.3.2. distributionPoint	Website where CRL is found (distribution point 2)	URL distribution point 2 CRL (see annex B)
2.4. Authority Info Access		
2.4.1. Access Method	Id-ad-ocsp	OID 1.3.6.1.5.5.7.48.1

Field	Description	Content
2.4.2. Access Location	OCSP URL	OCSP URL (see annex B)
2.4.3. Access Method	Id-ad-caIssuers	OID 1.3.6.1.5.5.7.48.2
2.4.4. Access Location	URL location for CA certificate.	URL location for CA certificate (annex B)
2.5. Issuer Alternative Name	Issuer alternative name in the Certification Authority	
2.5.1. rfc822Name	Email address for the Certification Authority	admin_ca@meyss.es
2.6. Key Usage	**Critical extension** to determine certificate usage	
2.6.1. Digital Signature	Used when the subject public key is used for verifying digital signatures	Selected "1"
2.6.2. Content Commitment	Used when the software must allow user to know what is signing	Selected "1"
2.6.3. Key Encipherment	Used for keys management and transport	Selected "1"
2.6.4. Data Encipherment	Used to encipher data other than cryptographic keys	Non selected "0"
2.6.5. Key Agreement	Used in key agreement protocol	Non selected "0"
2.6.6. Key Certificate Signature	Used to sign certificates. It is used in the CA certificates	Non selected "0"
2.6.7. CRL Signature	Used to sign certificate revocation lists	Non selected "0"
2.7. Extended Key Usage		
2.7.1. Email Protection	Email protection	OID 1.3.6.1.5.5.7.3.4
2.7.2. Client Authentication	Client authenticatioon	OID 1.3.6.1.5.5.7.3.2
2.8. Qualified Certificate Statements		
2.8.1. OcCompliance	Qualified certificate statement	OID 0.4.0.1862.1.1
2.8.2. OcEuRetentionPeriod	Information retention period (15 years)	OID 0.4.0.1862.1.3
2.8.3. QcType	Qualified certificate type	OID 0.4.0.1862.1.6
2.8.3.1. QcType- esign	Electronic signature certificate	OID 0.4.0.1862.1.6.1
2.8.4. QcPDS	PDS URL	OID 0.4.0.1862.1.5 PDS URL in English and Spanish (see annex B)
2.8.5. Id-qcs-pkixQCSyntax-v2		OID 1.3.6.1.5.5.7.11.2

Field	Description	Content
2.8.5.1. SemanticsId-Natural	Semantics Id of the natural person as defined in EN 319412-1	OID 0.4.0.194121.1.1
2.9. Certificate Policies		
2.9.1. Policy Identifier	OID associated to the CPS	OID 1.3.6.1.4.1.27781.2.5.4.7.1
2.9.1.1. Policy Qualifier ID	CPS specification	
2.9.1.1.1. CPS Pointer	CPS URL	CPS URL (see annex B)
2.9.1.1.2. User Notice	explicitText field	"Certificado cualificado centralizado de firma electrónica de empleado público, nivel medio/sustancial. Consulte las condiciones de uso en <URL ubicación DPCM (ver anexo B)>"
2.9.2. Policy Identifier	OID associated to public employee certificate (high level)	2.16.724.1.3.5.7.2
2.9.3. Policy Identifier	QCP-n	Certificado cualificado de firma acorde al Reglamento UE 910/2014 OID 0.4.0.194112.1.0
2.10. Subject Alternate Names		
2.10.1. rfc822Name	E-mail address of the certificate responsible	juanantonio.delacamara@meyss.es (sample)
2.10.2. Directory Name	Administrative Identity	
2.10.2.1. Tipo de certificado	Certificate type	2.16.724.1.3.5.7.2.1 = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO DE NIVEL MEDIO
2.10.2.2. Nombre de la entidad suscriptora	Entity where the subject is employed	2.16.724.1.3.5.7.2.2= MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL (sample)
2.10.2.3. NIF entidad suscriptora	NIF of subscribing entity	2.16.724.1.3.5.7.2.3= S2819001E (sample)
2.10.2.4. DNI/NIE del responsable	DNI or NIE of the certificate responsible	2.16.724.1.3.5.7.2.4 = 00000000G (sample)
2.10.2.5. Nombre de pila	Subscriber given name	2.16.724.1.3.5.7.2.6 = "JUAN ANTONIO" (sample)
2.10.2.6. Primer apellido	Subscriber first surname	2.16.724.1.3.5.7.2.7= "DE LA CAMARA" (sample)
2.10.2.7. Segundo apellido	Subscriber second surname	2.16.724.1.3.5.7.2.8 = "ESPAÑOL" (sample)

Field	Description	Content
2.10.2.8. Correo electrónico	Subscriber email	2.16.724.1.3.5.7.2.9= juanantonio.delacamara@meyss.es (sample)
2.10.2.9. Unidad organizativa	Unit, inside the Administration, where the subscriber works	2.16.724.1.3.5.7.2.10= SUBDIRECCION GENERAL DE ADMINISTRACION FINANCIERA (sample)
2.10.2.10. Puesto o cargo	Job title	2.16.724.1.3.5.7.2.11= JEFE SECCION APOYO GESTION (sample)

Annex A: References

CCN-STIC-405	TI Security Guide. Parameters and algorithms for secure electronic signature.
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 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 certificate.
ETSI EN 319 411-3	ETSI European Standard 319 411-3. Policy requirements for Certification Authorities issuing public key certificates.
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 TS 102 158	ETSI Technical Specification 102 158. Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates.
ETSI TS 102 176-1	ETSI Technical Specification 102 176-1. Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms.
ETSI TS 102 176-2	ETSI Technical Specification 102 176-2. Algorithms and Parameters for Secure Electronic Signatures; Part 2: Secure channel protocols and algorithms for signature creation devices.
ETSI TS 119 412-2	ETSI Technical Specification 119 412-2. Profiles for Trust Service Providers issuing certificates; Part 2: Certificate Profile for certificates issued to natural persons.
GDPR	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).
ITU-T X.501	ITU-T Recommendation X.501 TC2 (08/1997) | ISO/IEC 9594-2:1998.
IETF RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
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, October 1st, about Common Administrative Procedure of the Public Administrations.
Ley 40/2015	40/2015 Law, October 1st, about Legal Framework of the Public Sector.
LOPDGDD	3/2018 Organic Law, December 5th, about Personal Data Protection and Digital Rights Guarantee.

Reg 2015/1502	Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

Annex B: Electronic Links (URLs)

Email Organization Data:

admin_ca@meyss.es

CPSM, Certificate Policies, PDS, and Terms and Conditions:

Spanish: https://ca.empleo.gob.es/meyss/DPCyPoliticas

English: https://ca.empleo.gob.es/meyss/DPCyPoliticas-en

CA Root certificate, SubCA certificates and OCSP certificate:

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

SUBCA1 certificate:

http://ca.empleo.gob.es/meyss/documentos/subca1.cer

SUBCA2 certificate:

http://ca.empleo.gob.es/meyss/documentos/subca2.cer

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