MINISTERIO
DE EMPLEO
Y SEGURIDAD SOCIAL

SUBSECRETARÍA

S.G. DE TECNOLOGÍAS DE LA
INFORMACIÓN Y COMUNICACIONES

Certification Policy for Public Employee Certificate Trusted Service Provider of the Ministry of Employment and Social Security

sgtic@meyss.es
E03721106

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

Version control

Identifier	D321
Title	Certification Policy for Public Employee Certificate Trusted Service Provider of the Ministry of Employment and Social Security
Version	05
Document status	Approved
Approval date	06.07.2017
Expiration date	06.07.2018

Change control

Version	Date	Comments
1.0	03.12.2009	Final document
1.1	30.03.2010	ISO/IANA number changes for Public Employee OID. Key length enlarged from 1024 to 2048 bit.
1.2	10.09.2010	Heading Change, suppression of DG de Servicios
1.3	10.09.2011	Name change from SGPD to SGTIC
1.4	17.11.2011	OID changes. Subject GivenName and Surname being suppressed. Key usage "key Encipherment" being suppressed.
1.5	30.06.2012	Organization Structure actualization and new format
1.6	10.02.2014	Correction of errors in Subject Alternate Names extension
1.7	18.06.2015	Added SHA-256
2.0	20.07.2016	Update to eIDAS profiles (OID 1.3.6.1.4.1.27781.2.5.4.1.1 and 1.3.6.1.4.1.27781.2.5.4.2.1)
03	07.04.2017	Documentation format, English version
04	08.05.2017	Section 1.4 updated Added section 1.6, CP administration Added section 1.8, general conditions of public employee 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
05	06.07.2017	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

Table of contents

1 Overview

1.1 Introduction

This document contains the **Certification Policy for the Public Employee Certificates issued by the Trusted Service Provider of the Ministry of Employment and Social Security (TSPM[1]).**

This document clarifies and supplements the Certification Practice Statement (CPSM) regarding Public Employee certificates.

1.2 Description

The Public Employee Certificate is a certification for public employees according to [Ley 39/2015] and to article 43 for [Ley 40/2015]. This certificate is used as 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.

These certificates are issued on a smart card, a qualified electronic signature creation device according to annex II of eIDAS[2] regulation. The TSPM shall monitor the smart card certification status until the end of the validity and will replace these smart cards once the certification is expired according to the procedure established.

The TSPM issues two types of Public Employee certificates for different usages:

- Certificate for electronic signature (non repudiation).
- Certificate for authentication.

Both certificate are considered independently as following the high assurance level.

The Public Employee certificate for electronic signature, 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-qscd according to [ETSI EN 319 411-2].

1.3 Document name and identification

1.3.1 Identification of this document

The name of this document is **Certification Policy for Public Employee Certificated Trusted Service Provider of the Ministry of Employment and Social Security**, 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. OIDs for Public Employee certificates are:

- Public Employee certificate for electronic signature (high level of assurance): *[1.3.6.1.4.1.27781.2.5.4.1.1]*
- Public Employee certificate for authentication (high level of assurance): *[1.3.6.1.4.1.27781.2.5.4.2.1]*

[1] PSCM, in Spanish

[2] 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.

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.
b. Certificate subscribers.
c. The responsible for the certificate.
d. The relying parties.

The requester of a Public Employee certificate is the employee himself who, after receiving the certificates, become subscriber and responsible for the certificates.

The subscriber of a Public Employee certificate is the person identified as that in the certificate field *Subject* and that must comply with an appropriate usage of the certificate and its linked private key according to the CPSM.

The Responsible for a Public Employee certificate is the natural person identified as such in the object *Identidad Administrativa* inside the *SubjectAltName* extension. The responsible for a Public Employee certificate is the subject of the certificate.

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

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

1.5 Certificate usage

The Public Employee Certificate for electronic signature as a means to electronically sign documents and proceedings offers:

- Origin non repudiation.
- Integrity.

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

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

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

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

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

1.6 CP administration

1.6.1 Organization administering the document

The responsible for the TSPM is the responsible for the definition, review and disclosure of this CP. There are two assistants to the responsible for the TSPM, 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 (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 responsible for the TSPM 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 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:

http://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 approved the document (or not) as stated in the TSPM Documentation Quality Plan.

Any new version will have an expiration date of 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 emitted by IETF (Internet Engineering Task Force).

1.7.2 Acronyms

C	Country (País).
CA	Certification Authority.
CDP	CRL Distribution Point.
CEC	Certificate Emision Code.
CN	Common Name.
CP	Certificate Policy.
CPS	Certification Practice Statement
CPSM	Certification Practice Stament of the TSPM.
CRL	Certificate Revocation List.
CSP	Cryptographic Service Provider.
CSR	Certificate Signing Request.
CWA	CEN Workshop Agreement.
DN	Distinguished Name.
MEYSS	Ministery of Employment and Social Security. Ministerio de Empleo y Seguridad Social.
O	Organization.
OU	Organizational Unit.
OID	Object IDentifier.
OCSP	On-line Certificate Status Protocol.
PA	Public Administration.
PSCM	Trusted Service Provider of the Ministry. Prestador de Servicios de Confianza del Ministerio.
RA	Registration Authority.
RFC	Request For Comments.
SGTIC	Subdirección General de Tecnologías de la Información y las Comunicaciones.
TSP	Trusted Service Provider.
TSPM	Trusted Service Provider of the Ministry.
VA	Validation Authority.

1.8 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 [RD 3/2011].

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 http://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 responsible for the TSPM management. 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 responsible for the TSPM approves the risk assessment and accepts the residual risk identified.

This risk assessment is reviewed and revised on a biennial basis 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 http://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
- also 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 and/or organization 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].

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:

- Electronic Signature certificate (High level of assurance): *2.16.724.1.3.5.7.1*
- Authentication certificate (High level of assurance): *2.16.724.1.3.5.7.1*

The Public Employee Certificates issued by TSPM include the following fields:

Certificate	Mandatory "Identidad Administrativa" fields
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 • email • Organizational Unit • Job title

Certificate	Optional "Identidad Administrativa" fields
PUBLIC EMPLOYEE	• Personal identification number

All other aspects related with the names management (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

In order to download the Public Employee certificates, the applicant must possess a cryptographic smart card that will house safely the certificates and some activation codes, which enable the download and acceptance of electronic certificates in the cryptographic device.

The management process used by the TSPM ensures that the cryptographic card is safely delivered to the public employee responsible for the certificates, verifying her identity.

The applicant must apply in person and identify herself at the Registration Authority to obtain the smart card. At this event she fills and signs an application form for the issuance of the Public Employee certificates 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 is complete and accurate. The units that will operate as Registration Authorities are *Subdirección General de Recursos Humanos* and *Subdirección General de Apoyo a la Gestión de la Inspección*

The authentication of the applicant's identity is done according to the requirements specified in the CPSM. After verifying the identity of the applicant, a copy of the completed form is returned to the applicant. In the event that the application is rejected, the applicant is notified of the denial thereof.

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 certificates

The issuance of certificates (electronic signature and authentication) is made electronically by using some activation codes sent to the email address given by the applicant. Certificates can be installed from the URL that appears on the copy of the form. The subscriber also receives the user manual for the application that allows the certificate issuance.

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 by the use of the computer mechanism that installs them on the smart card delivered to the subscriber.

The PSCM uses a procedure to generate the certificates that securely links the certificates with the public employee information, including the certified 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 secrecy of the keys during its generation process.

Issued certificates are stored in a repository without previous approval of its responsible. The private keys associated to the certificates are not stored under any circumstance.

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 and subsequent issuance as described in previous sections.

Like with the application for the first time, procedures could be established in the future for the certificate renewal in a telematic way (without physical presence), prior to its expiration, and when the time elapsed since the previous identification with physical presence is less than five years.

When using certificates in force for a renewal application, by default, every employee has to authenticate remotely, using the certificate of authentication stored in electronic hardware, allowing no alternative to this practice.

4.4 Certificate revocation

The PSCM authenticates requests and reports relating to revocation of Public Employee Certificates, checking that they come from an authorized person.

Persons authorized to request revocation of certificates of public employee are public employees themselves responsible for them, the Human Resources Division or a superior public employee (level 30 or higher rank).

Revocation mechanisms are allowed through internal e-mail accounts properly validated or by a writing form signed by the applicant for revocation.

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 the Organic Law 15/1999 about Protection of Personal Data and related laws, the TSPM informs the subscriber about the existence of an automated file whose responsible is the Subsecretary of the Ministry. The contact information is Paseo de la Castellana 63, Madrid 28071, email sgtic@meyss.es and web site http://ca.empleo.gob.es. The data are recorded in order to provide certification services by the authorities in the TSPM. The subscriber may exercise her right to access, correction, cancellation, and opposition at the contact information given.

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

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

The TSPM will not disclose or lease personal information, except as the one upon termination of the Certification Authority.

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

6 Profile of the Public Employee Certificate

6.1 Public Employee Certificate for authentication

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 of Employment and Social Security	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 = SUBCA2 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 EMPLEO Y SEGURIDAD 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	OU = SUBDIRECCION GENERAL DE ADMINISTRACION FINANCIERA (sample)
1.5.5. Title	Job title	T = JEFE SECCION APOYO GESTION (sample)
1.5.6. Serial Number	DNI/NIE/Passport of the Public Employee accordint to ETSI EN 319 412-1 semantics	SERIALNUMBER = IDCES-00000000G (sample)
1.5.7. Surname	First and second surnames, according to DNI/Passport	SN = DE LA CAMARA ESPAÑOL (sample)
1.5.8. Given name	Given name, according to DNI/Passport	G = JUAN ANTONIO (sample)
1.5.6.Common Name (CN)	Given name plus two surnames plus DNI/NIE/Passport number separated by a hyphen (-)	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 that is critical is the field 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 SHA1/SHA-256 hash)	
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
2.4.2. Access Location	OCSP URL	OCSP URL (see annex B)

Field	Description	Content
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	Non selected "0"
2.6.3. Key Encipherment	Used for keys management and transport	Non selected "0"
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
2.7.3. SmartCard Logon	Smart card logon	OID 1.3.6.1.4.1.311.20.2.2
2.8. Certificate Policies		
2.8.1. Policy Identifier	OID associated to the CPS	OID 1.3.6.1.4.1.27781.2.5.4.2.1
2.8.1.1. Policy Qualifier ID	CPS specification	
2.8.1.1.1. CPS Pointer	URL for the CPS	URL for the CPS (see annex B)
2.8.1.2. User Notice	explicitText field	"Certificado de personal, nivel alto, autenticación. Consulte las condiciones de uso en <CPS URL (see annex B) >"
2.8.2. Policy Identifier	OID associated to public employee certificate (high level)	2.16.724.1.3.5.7.1
2.8.3. Policy Identifier	NCP+	0.4.0.2042.1.2

Field	Description	Content
2.9. Subject Alternate Names		
2.9.1. rfc822Name	E-mail address of the certificate responsible	juanantonio.delacamara@meyss.es (sample)
2.9.2. User Principal Name (UPN)	UPN for smart card logon	00000000G@meyss.es (sample)
2.9.3. Directory Name	Administrative Identity	
2.9.3.1. Tipo de certificado		2.16.724.1.3.5.7.1.1 = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO DE NIVEL ALTO DE AUTENTICACION
2.9.3.2. Nombre de la entidad suscriptora	Entity where the subject is employed	2.16.724.1.3.5.7.1.2= MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL (sample)
2.9.3.3. NIF entidad suscriptora	NIF of subscribing entity	2.16.724.1.3.5.7.1.3= S2819001E (sample)
2.9.3.4. DNI/NIE del responsable	DNI or NIE of the certificate responsible	2.16.724.1.3.5.7.1.4 = 00000000G (sample)
2.9.3.5. Nombre de pila	Subscriber given name	2.16.724.1.3.5.7.1.6 = "JUAN ANTONIO" (sample)
2.9.3.6. Primer apellido	Subscriber first surname	2.16.724.1.3.5.7.1.7= "DE LA CAMARA" (sample)
2.9.3.7. Segundo apellido	Subscriber second surname	2.16.724.1.3.5.7.1.8 = "ESPAÑOL" (sample)
2.9.3.8. Correo electrónico	Subscriber email	2.16.724.1.3.5.7.1.9= juanantonio.delacamara@meyss.es (sample)
2.9.3.9. Unidad organizativa	Unit, inside the Administration, where the subscriber works	2.16.724.1.3.5.7.1.10= SUBDIRECCION GENERAL DE ADMINISTRACION FINANCIERA (sample)
2.9.3.10. Puesto o cargo	Job title	2.16.724.1.3.5.7.1.11= JEFE SECCION APOYO GESTION (sample)

6.2 Public Employee Certificate for electronic signature

Certificate fields are as follows:

Field	Description	Content
1. X.509v1 Field		

Field	Description	Content
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 of Employment and Social Security	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 = SUBCA2 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 EMPLEO Y SEGURIDAD SOCIAL (sample)
1.5.3. Organizational Unit (OU)	Certificate Type	OU = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO
1.5.4. Organizational Unit (OU)	Unit, within the Organization, where the public employee (subscriber) is working	OU = SUBDIRECCION GENERAL DE ADMINISTRACION FINANCIERA (sample)
1.5.5. Title	Job title	T = JEFE SECCION APOYO GESTION (sample)

Field	Description	Content
1.5.6. Serial Number	DNI/NIE/Passport of the Public Employee accordint to ETSI EN 319 412-1 semantics	SERIALNUMBER = IDCES-00000000G (sample)
1.5.7. Surname	First and second surnames, according to DNI/Passport	SN = DE LA CAMARA ESPAÑOL (sample)
1.5.8. Given name	Given name, according to DNI/Passport	G = JUAN ANTONIO (sample)
1.5.9. Common Name (CN)	Given name plus two surnames plus DNI/NIE/Passport number separated by a hyphen (-)	CN = JUAN ANTONIO DE LA CAMARA ESPAÑOL - 00000000G (FIRMA) (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 SHA1/SHA-256 hash)	
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
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 (see annex B)
2.5. Issuer Alternative Name	Issuer alternative name in the Certification Authority	

Field	Description	Content
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	Non selected "0"
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	Non selected "0"
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. Qualified Certificate Statements		
2.7.1. OcCompliance	Qualified certificate statement	OID 0.4.0.1862.1.1
2.7.2. OcEuRetentionPeriod	Information retention period (15 years)	OID 0.4.0.1862.1.3
2.7.3. OcSSCD	Secure Signature Creation Device	OID 0.4.0.1862.1.4
2.7.4. QcType	Qualified certificate type	OID 0.4.0.1862.1.6
2.7.4.1. QcType- esign	Electronic signature certificate	OID 0.4.0.1862.1.6.1
2.7.5. QcPDS	PDS URL	OID 0.4.0.1862.1.5 PDS URL in English and Spanish (see annex B)
2.7.6. Id-qcs-pkixQCSyntax-v2		OID 1.3.6.1.5.5.7.11.2
2.7.6.1. SemanticsId-Natural	Natural person semantics according to EN 319 412-1	OID 0.4.0.194121.1.1
2.8. Certificate Policies		
2.8.1. Policy Identifier	OID associated to the CPS	OID 1.3.6.1.4.1.27781.2.5.4.1.1
2.8.1.1. Policy Qualifier ID	CPS specification	
2.8.1.1.1. CPS Pointer	URL for the CPS	CPSM URL (see annex B)
2.8.1.2. User Notice	explicitText field	"Certificado cualificado de firma electrónica de empleado público,

Field	Description	Content
		nivel alto. Consulte las condiciones de uso en <URL ubicación DPCM (see annex B)>“
2.8.2. Policy Identifier	OID associated to public employee certificate (high level)	2.16.724.1.3.5.7.1
2.8.3. Policy Identifier	QCP-n-qscd	“Certificado cualificado de firma, almacenado en dispositivo cualificado acorde al Reglamento UE 910/2014” 0.4.0.194112.1.2
2.9. Subject Alternate Names		
2.9.1. Directory Name	Administrative Identity	
2.9.1.1. Tipo de certificado	Certificate type	2.16.724.1.3.5.7.1.1 = CERTIFICADO CUALIFICADO DE FIRMA DE EMPLEADO PUBLICO DE NIVEL ALTO
2.9.1.2. Nombre de la entidad suscriptora	Entity where the subject is employed	2.16.724.1.3.5.7.1.2 = MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL (sample)
2.9.1.3. NIF entidad suscriptora	NIF of subscribing entity	2.16.724.1.3.5.7.1.3 = S2819001E (sample)
2.9.1.4. DNI/NIE del responsable	DNI or NIE of the certificate responsible	2.16.724.1.3.5.7.1.4 = 00000000G (sample)
2.9.1.5. Nombre de pila	Subscriber given name	2.16.724.1.3.5.7.1.6 = “JUAN ANTONIO” (sample)
2.9.1.6. Primer apellido	Subscriber first surname	2.16.724.1.3.5.7.1.7 = “DE LA CAMARA” (sample)
2.9.1.7. Segundo apellido	Subscriber second surname	2.16.724.1.3.5.7.1.8 = “ESPAÑOL” (sample)
2.9.1.8. Correo electrónico	Subscriber email	2.16.724.1.3.5.7.1.9 = juanantonio.delacamara@meyss.es (sample)
2.9.1.9. Unidad organizativa	Unit, inside the Administration, where the subscriber works	2.16.724.1.3.5.7.1.10 = SUBDIRECCION GENERAL DE ADMINISTRACION FINANCIERA (sample)
2.9.1.10. Puesto o cargo	Job title	2.16.724.1.3.5.7.1.11 = 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.
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 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.
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:

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

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