MINISTERIO
DE EMPLEO
Y SEGURIDAD SOCIAL

SUBSECRETARÍA

S.G. DE TECNOLOGÍAS DE LA
INFORMACIÓN Y COMUNICACIONES

Certification Service Provider of the Ministry of Employment and Social Security

Profile for Public Employee certificates

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

sgtic@meyss.es

Version Control

Identifier	D301
Title	Certification Service Provider of the Ministry of Employment and Social Security Profile for Public Employee certificates
Responsible	SG de Tecnologías de la Información y las Comunicaciones Ministerio de Empleo y Seguridad Social
Version	1.7
Date	18.06.2015

Version History

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

Contents

1 Introduction

1.1 Presentation

This document contains the **profile of the Public Employee Certificates issued by the Certification Service Provider of the Ministry of Employment and Social Security (CSPM).**

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

1.2 Description

Public Employee certificates are defined in LAECSP article 19, for staff serving in the Administration. They are used to authenticate a public employee of any category, providing data of both the owner and the unit where he is serving.

Public Employee certificates issued by the CSPM are qualified certificates as defined in the LFE and they meet the requirements for high level assurance as defined in [EIFEBIII]. Following this scheme, high level assurance implies X.509 certificates stored in hardware devices.

These certificates are created using secure signature creation devices as defined in LFE. Due to the fact that they are issued to natural persons, they allow qualified electronic signature according to the LFE.

CSPM issues two types of Public Employee certificates, depending on its usage:

- Public employee certificate for non repudiation.
- Public employee certificate for authentication (digital signature).

As these certificates must follow the high level assurance classification, they are handled as two separate profiles.

1.3 Document name and identification

1.3.1 Identification of this document

This document name is **Certification Service Provider of the Ministry of Employment and Social Security. Profile for Public Employee certificates**, with the information in the control version (p. ii)

Internet address of this document is listed in Annex B.

1.3.2 Identification of certificate types

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. OID's for Public Employee certificates are:

- Public Employee certificate for non repudiation (high level of assurance): *[1.3.6.1.4.1.27781.2.4.4.1.3]*
- Public Employee certificate for authentication (high level of assurance): *[1.3.6.1.4.1.27781.2.4.4.2.3]*

1.4 End Users

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

a. Certificate requester.
b. Certificate subscriber.
c. Certificate responsible.
d. Certificate verifier.

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

Subscriber of a Public Employee certificate is the person identified as that in the certificate field *Subject* and that is obliged to use the certificate and the associated key according to the CPSM.

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

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

1.5 Certificate usage

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

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

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

Public Employee certificate issued by the CSPM, corresponding to the one defined in the LAECSP, has its usage limited by the law dispositions.

CSPM, as a certification service provider (CSP) is not responsible of the contents of documents signed using Public Employee certificates nor any other use of the certificates, as message or communications encipherment processes.

1.6 Definitions and acronyms

1.6.1 Definitions

Within 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).

1.6.2 Acronyms

PPAA	Public Administrations.
C	Country.

CA	Certification Authority.
CDP	CRL Distribution Point.
CEC	Certificate Emision Code.
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.
CSPM	Cryptographic Service Provider of the Ministry.
CSR	Certificate Signing Request.
CWA	CEN Workshop Agreement.
DN	Distinguished Name.
LAECSP	Law 11/2007 of June 22nd, on electronic access of citizens to Public Services (Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos).
LFE	Law 59/2003 of December 19th on Electronic Signature (Ley 59/2003 de 19 de diciembre de Firma Electrónica).
O	Organization.
OU	Organizational Unit.
OID	Object IDentifier.
OCSP	On-line Certificate Status Protocol.
RA	Registration Authority.
RFC	Request For Comments.
VA	Validation Authority.

2 Identification

2.1 Management of names

2.1.1 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 3280].

2.1.2 Normalization and Administrative Identity

The CSPM uses the normalized naming schema *Administrative Identity* proposed by the Spanish administration for every type of certificate and profile.

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:

- Non Repudiation certificate (High level of assurance): *2.16.724.1.3.5.3.1*
- Authentication certificate (High level of assurance): *2.16.724.1.3.5.3.1*

Certificate	Mandatory "Administrative Identity" 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

Certificate	Optional "Administrative Identity" fields
PUBLIC EMPLOYEE	• Personal identification number • E-mail address • Organizational unit • Position held

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 of the CSPM.

3 Operational requirements

3.1 Application for certificates

To download the Public Employee certificates, the applicant must possess a cryptographic card that will house safely the certificates and the CEC (Certificate Issuing Code), which enables the download and acceptance of electronic certificates in the cryptographic device. The CEC is non-transferable and associated with each user.

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

The applicant must apply in person and identify himself at the Registration Authority to obtain the CEC. At this event he fills and signs an application form for the issuance of the Public Employee certificates issued by the CSPM. This form summarizes the terms and conditions applicable to the certificate present in the CPSM and in the profile documents.

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, Subdirección General de Apoyo a la Gestión de la Inspección de Trabajo y Seguridad Social, Inspecciones Provinciales, Secretarías Generales de las Consejerías de Trabajo,* Subdirección General de Gestión de Recursos y Organización del SEPE and Direcciones Provinciales del SEPE.

The authentication of the applicant's identity is done according to the requirements specified in the DPCM. After verifying the identity of the applicant, the CEC is delivered with a copy of the completed form. In the event that the application is rejected, the applicant is notified of the denial thereof. The CEC is then used to electronically generate and download the certificates inside the cryptographic card.

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

3.2 Issuance of certificates

After the certificate application, these are safely issued and made available to the applicant in a telematic way. The issuance of the certificates implies the approval of the application. Two certificates are issued: Authentication and non repudiation.

The issuance of the Public Employee certificates (authentication and non repudiation) is electronically made, using the CEC delivered at the application time to the applicant.

The download place for the certificates is detailed in the application form. There is also available to the applicant a user manual to ease the certificates download process.

Certificates are considered accepted by the use of the telematic mechanism downloading them on the cryptographic card delivered to the user.

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.

3.3 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.

3.4 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.

4 Profile for Public Employee certificates

4.1 Public Employee certificate for authentication

The fields are the following:

Field	Description	Contents
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. Organization (O)	Official name of the cryptographic service provider (certificate issuer)	O = MINISTERIO DE TRABAJO E INMIGRACION
1.3.3. Locality (L)	Cryptographic service provider locality	L = MADRID
1.3.4. Organizational Unit (OU)	Organizational unit within the service provider, responsible for issuing the certificate	OU = SUBDIRECCION GENERAL DE PROCESO DE DATOS
1.3.5. Organizational Unit (OU)	Organizational unit within the service provider, responsible for issuing the certificate	OU = PRESTADOR DE SERVICIOS DE CERTIFICACION MTIN
1.3.6. Common Name (CN)	Common name of the cryptographic service provider (certificate issuer)	CN = AC1 RAIZ MTIN
1.3.7. Serial Number	NIF of the Ministry of Employment and Social Security	SERIALNUMBER =S2819001E
1.4. Validity	Validity period: 3 years	
1.4.1. Not Before	Start of validity period	UTCTime YYMMDDHHMMSSZ
1.4.2. Not After	End of validity period	UTCTime YYMMDDHHMMSSZ
1.5. Subject	Public employee responsible of the certificate	
1.5.1. Country (C)	Country	C = ES
1.5.2. Organization (O)	Name of the Administration, Agency or public entity where the employee is working	O = MINISTERIO DE EMPLEO y SEGURIDAD SOCIAL
1.5.3. Organizational Unit (OU)	Certificate type description	OU = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO

Field	Description	Contents
1.5.4. Organizational Unit (OU)	Unit, within the Organization, where the employee is working	OU = SUBDIRECCIÓN GENERAL DE ADMINISTRACIÓN FINANCIERA (sample)
1.5.5. Title (T)	Position or title of the public employee that links him to the Administration, Agency or public entity.	T = JEFE SECCION APOYO GESTION (sample)
1.5.6. Serial Number	Employee's DNI/NIE/passport	SERIALNUMBER = 00000000G (sample)
1.5.6.Common Name (CN)	Given name plus two surnames plus DNI/NIE/Passport number separated by a vertical bar(|)	CN = JUAN ANTONIO DE LA CAMARA ESPAÑOL |00000000G (AUTENTICACION) (sample)
1.5.7. E-mail (E)	Employee's e-mail address	E=juanantonio.delacamara@meyss.es (sample)
1.6. Subject Public Key Info	Public key, codified following the cryptographic algorithm	
1.7. Signature Algorithm	Signature algorithm	SHA-1/SHA-256 RSA Signature, 2048 bit key length

And the extensions are the following:

Field	Description	Contents
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	
2.1.2. AuthorityCertIssuer	Issuer certification path	C=ES, L=MADRID, O=MINISTERIO DE TRABAJO E INMIGRACION, OU=SUBDIRECCION GENERAL DE PROCESO DE DATOS, OU=PRESTADOR DE SERVICIOS DE CERTIFICACION MTIN, SERIALNUMBER=S2819001E, CN=AC1 RAIZ MTIN
2.1.3. AuthorityCertSerial Number	Serial number of the CA certificate	05 0b 41 5e 82 7b
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 CRL distribution point 1(see annex B)

Field	Description	Contents
2.3.2. distributionPoint	Website where CRL is found (distribution point 2)	URL CRL distribution point 2(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 Web address	OCSP URL (see annex B)
2.5. Issuer Alternative Name	Alternative name for the contact person at the Issuer CA	
2.5.1. rfc822Name	E-mail contact address at the issuer CA	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	Not selected “0”
2.6.3. Key Encipherment	Used for keys management and transport	Not selected “0”
2.6.4. Data Encipherment	Used to encipher data other tan cryptographic keys	Not selected “0”
2.6.5. Key Agreement	Used in key agreement protocol	Not selected “0”
2.6.6. Key Certificate Signature	Used to sign certificates. It is used in the CA certificates	Not selected “0”
2.6.7. CRL Signature	Used to sign certificate revocation lists	Not 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. Qualified Certificate Statements		
2.8.1. OcCompliance	Qualified certificate statement	OID 0.4.0.1862.1.1
2.8.2. OcEuRetentionPeriod	Retention period for information (15 years)	OID 0.4.0.1862.1.3
2.8.3. OcSSCD	Secure signature creation device usage	OID 0.4.0.1862.1.4
2.9. Certificate Policies		

Field	Description	Contents
2.9.1. Policy Identifier	OID associated to the CPS	OID 1.3.6.1.4.1.27781.2.4.4.2.3
2.9.2. Policy Qualifier ID	CPS specification	
2.9.2.1. DPC Pointer	URL for the CPS	CPSM URL location (see annex B)
2.9.2.2. User Notice	explicitText field	"Employee qualified certificate, high level of assurance, authentication. See the terms of use at < CPSM URL location (see annex B)>“
2.10. Subject Alternative Names		
2.10.1. rfc822Name	E-mail address of the certificate responsible	juanantonio.delacamara@meyss.es (sample)
2.10.2. User Principal Name (UPN)	UPN for smart card logon	00000000G@trabajo.dom (sample)
2.10.3. Directory Name	Administrative Identity	
2.10.3.1. Certificate type		2.16.724.1.3.5.3.1.1= CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO (PUBLIC EMPLOYEE ELECTRONIC CERTIFICATE)
2.10.3.2. Name of subscribing entity	Entity where the subject is employed	2.16.724.1.3.5.3.1.2 = MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL (MINISTRY OF EMPLOYMENT AND SOCIAL SECURITY) (sample)
2.10.3.3. NIF of subscribing entity	NIF of subscribing entity	2.16.724.1.3.5.3.1.3 = S2819001E (sample)
2.10.3.4. Subject’s DNI/NIE	DNI or NIE of the certificate responsible	2.16.724.1.3.5.3.1.4 = 00000000G (sample)
2.10.3.5. Personal identification number	Personal identification number of the certificate responsible (expected to be univocal). Could be the Personal Registration Number	2.16.724.1.3.5.3.1.5 = (Not used)
2.10.3.6. Given name	Given name of the certificate responsible	2.16.724.1.3.5.3.1.6 = “JUAN ANTONIO” (sample)
2.10.3.7. First surname	First surname of the certificate responsible	2.16.724.1.3.5.3.1.7 = “DE LA CAMARA” (sample)
2.10.3.8. Second	Second surname of the certificate responsible	2.16.724.1.3.5.3.1.8 = “ESPAÑOL” (sample)

Field	Description	Contents
surname		
2.10.3.9. E-mail	E-mail address of the certificate responsible	2.16.724.1.3.5.3.1.9 = juanantonio.delacamara@meyss.es (sample)
2.10.3.10. Organizational Unit	Unit, inside the Administration, where the certificate responsible is included	2.16.724.1.3.5.3.1.10 = SUBDIRECCION GENERAL DE ADMINISTRACION FINANCIERA (sample)
2.10.3.11. Position	Position held by the certificate responsible inside the administration	2.16.724.1.3.5.3.1.11= JEFE SECCION APOYO GESTION (sample)

4.2 Public Employee certificate for non repudiation

The fields are the following:

Field	Description	Contents
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. Organization (O)	Official name of the cryptographic service provider (certificate issuer)	O = MINISTERIO DE TRABAJO E INMIGRACION
1.3.3. Locality (L)	Cryptographic service provider locality	L = MADRID
1.3.4. Organizational Unit (OU)	Organizational unit within the service provider, responsible for issuing the certificate	OU = SUBDIRECCION GENERAL DE PROCESO DE DATOS
1.3.5. Organizational Unit (OU)	Organizational unit within the service provider, responsible for issuing the certificate	OU = PRESTADOR DE SERVICIOS DE CERTIFICACION MTIN
1.3.6. Common Name (CN)	Common name of the cryptographic service provider (certificate issuer)	CN = AC1 RAIZ MTIN
1.3.7. Serial Number	NIF of the Ministry of Employment and Social Security	SERIALNUMBER =S2819001E
1.4. Validity	Validity period: 3 years	
1.4.1. Not Before	Start of validity period	UTCTime YYMMDDHHMMSSZ

Field	Description	Contents
1.4.2. Not After	End of validity period	UTCTime YYMMDDHHMMSSZ
1.5. Subject	Public employee responsible of the certificate	
1.5.1. Country (C)	Country	C = ES
1.5.2. Organization (O)	Name of the Administration, Agency or public entity where the employee is working	O = MINISTERIO DE EMPLEO y SEGURIDAD SOCIAL
1.5.3. Organizational Unit (OU)	Certificate type description	OU = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO
1.5.4. Organizational Unit (OU)	Unit, within the Organization, where the employee is working	OU = SUBDIRECCIÓN GENERAL DE ADMINISTRACIÓN FINANCIERA (sample)
1.5.5. Title (T)	Position or title of the public employee that links him to the Administration, Agency or public entity.	T = JEFE SECCION APOYO GESTION (sample)
1.5.6. Serial Number	Employee's DNI/NIE/passport	SERIALNUMBER = 00000000G (sample)
1.5.7. Common Name (CN)	Given name plus two surnames plus DNI/NIE/Passport number separated by a vertical bar(|)	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-1/SHA-256 RSA Signature, 2048 bit key length

And the extensions are the following:

Field	Description	Contents
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	
2.1.2. AuthorityCertIssuer	Issuer certification path	C=ES, L=MADRID, O=MINISTERIO DE TRABAJO E INMIGRACION, OU=SUBDIRECCION GENERAL DE PROCESO DE DATOS, OU=PRESTADOR DE SERVICIOS DE CERTIFICACION MTIN, SERIALNUMBER=S2819001E, CN=AC1 RAIZ MTIN

Field	Description	Contents
2.1.3. AuthorityCertSerial Number	Serial number of the CA certificate	05 0b 41 5e 82 7b
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 CRL distribution point 1(see annex B)
2.3.2. distributionPoint	Website where CRL is found (distribution point 2)	URL CRL distribution point 2(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 Web address	OCSP URL (see annex B)
2.5. Issuer Alternative Name	Alternative name for the contact person at the Issuer CA	
2.5.1. rfc822Name	E-mail contact address at the issuer CA	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	Not 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	Not selected “0”
2.6.4. Data Encipherment	Used to encipher data other tan cryptographic keys	Not selected “0”
2.6.5. Key Agreement	Used in key agreement protocol	Not selected “0”
2.6.6. Key Certificate Signature	Used to sign certificates. It is used in the CA certificates	Not selected “0”
2.6.7. CRL Signature	Used to sign certificate revocation lists	Not 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	Retention period for information (15 years)	OID 0.4.0.1862.1.3
2.7.3. OcSSCD	Secure signature creation device usage	OID 0.4.0.1862.1.4

Field	Description	Contents
2.8. Certificate Policies		
2.8.1. Policy Identifier	OID associated to the CPS	OID 1.3.6.1.4.1.27781.2.4.4.1.3
2.8.2. Policy Qualifier ID	CPS specification	
2.8.2.1. DPC Pointer	URL for the CPS	CPSM URL location (see annex B)
2.8.2.2. User Notice	explicitText field	"Employee qualified certificate, high level of assurance, non repudiation. See the terms of use at < CPSM URL location (see annex B)>“
2.9. Subject Alternate Names		
2.9.1. Directory Name	Administrative Identity	
2.9.1.1. Certificate type		2.16.724.1.3.5.3.1.1= CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO (PUBLIC EMPLOYEE ELECTRONIC CERTIFICATE)
2.9.1.2. Name of subscribing entity	Entity where the subject is employed	2.16.724.1.3.5.3.1.2 = MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL (MINISTRY OF EMPLOYMENT AND SOCIAL SECURITY) (sample)
2.9.1.3. NIF of subscribing entity	NIF of subscribing entity	2.16.724.1.3.5.3.1.3 = S2819001E (sample)
2.9.1.4. Subject’s DNI/NIE	DNI or NIE of the certificate responsible	2.16.724.1.3.5.3.1.4 = 00000000G (sample)
2.9.1.5. Personal identification number	Personal identification number of the certificate responsible (expected to be univocal). Could be the Personal Registration Number	2.16.724.1.3.5.3.1.5 = (Not used)
2.9.1.6. Given name	Given name of the certificate responsible	2.16.724.1.3.5.3.1.6 = “JUAN ANTONIO” (sample)
2.9.1.7. First surname	First surname of the certificate responsible	2.16.724.1.3.5.3.1.7 = “DE LA CAMARA” (sample)
2.9.1.8. Second surname	Second surname of the certificate responsible	2.16.724.1.3.5.3.1.8 = “ESPAÑOL” (sample)
2.9.1.9. E-mail	E-mail address of the certificate responsible	2.16.724.1.3.5.3.1.9 = juanantonio.delacamara@meyss.es (sample)

Field	Description	Contents
2.9.1.10. Organizational Unit	Unit, inside the Administration, where the certificate responsible is included	2.16.724.1.3.5.3.1.10 = SUBDIRECCION GENERAL DE ADMINISTRACION FINANCIERA (sample)
2.9.1.11. Position	Position held by the certificate responsible inside the administration	2.16.724.1.3.5.3.1.11= JEFE SECCION APOYO GESTION (sample)

Annex A: References

EIFEBIII	Esquema de identificación y firma electrónica de las Administraciones Públicas. Bloque III (Public Administrations scheme for identification and electronic signature. Part III)
ITU-T X.501	ITU-T Recommendation X.501 TC2 (08/1997) | ISO/IEC 9594-2:1998.
IETF RFC 3280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

Annex B: Links (URL)

CPSM and certificate profile location:

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

OCSP Location:

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

CRL publication address:

- Distribution point 1:

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

- Distribution point 2:

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