MINISTERIO
DE EMPLEO
Y SEGURIDAD SOCIAL

SUBSECRETARÍA

S.G. DE TECNOLOGÍAS DE LA
INFORMACIÓN Y COMUNICACIONES

Certification Policy for Electronic Seal 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	D323
Title	Certification Policy for Electronic Seal Certificate Trusted Service Provider of the Ministry of Employment and Social Security
Version	03
Document status	Approved
Approval date	10.04.2017
Expiration date	10.04.2018

Change control

Version	Date	Comments
1.0	03.12.2009	Final document
1.1	30.03.2010	ISO/IANA number changes of the MPR and in the OID of the Electronic seal certificate issued by CSPM
1.2	10.09.2010	Heading Change, suppression of DG de Servicios Suppression of the future possibility of certificate request using valid certificates
1.3	02.08.2011	Changed SGPD to SGTIC Certificate description change (ELECTRONIC SEAL FOR AUTOMATED PROCESSING to ELECTRONIC SEAL) and OID change (1.3.6.1.4.1.27781.2.4.3.2.3)
1.4	30.06.2012	Organization Structure actualization and new format
1.5	18.06.2015	Added SHA-256
2.0	20.07.2016	Update to eIDAS profiles (OID 1.3.6.1.4.1.27781.2.5.3.2.1)
03	10.04.2017	Updated to established template for documentation

Table of contents

1 Overview

1.1 Introduction

This document contains the **Certification Policy for the Electronic Seal Certificate 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 electronic seal certificates.

1.2 Description

The Electronic Seal Certificate is a certificate for public entities according to [Ley 39/2015] and to the articles 40 and 42 of [Ley 40/2015] as a means to automated electronic administrative proceedings of the Public Administrations.

The Electronic Seal Certificate issued by the TSPM, is a qualified electronic signature according to annex III requirements of eIDAS[2] regulation.

This certificate is issued for advanced electronic seals, as defined in the articles 36 and 37 of eIDAS regulation.

1.3 Document name and identification

1.3.1 Identification of this document

The name of this document is **Certification Policy for Electronic Seal Certificate 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. The OID for the Electronic Seal Certificate is as follows:

- Electronic Seal Certificate: *[1.3.6.1.4.1.27781.2.5.3.2.1]*

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.

The requester of an Electronic Seal Certificate is a public employee (a natural person) of the entity requesting the certificate.

The subscriber of an Electronic Seal Certificate is the public entity identified as such in the field *Subject* of the certificate. The *Common Name* attribute states the name of the device, application or server name linked to the certificate.

The responsible person for an Electronic Seal Certificate (responsible for its custody) is the public employee (natural person) who works in the public entity.

[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.

The relying parties are the entities (including natural and legal persons, Public Administrations and other organizations) that, using an Electronic Seal Certificate issued by the Certification Authority operating under the CPSM, that trust on the validity of the relationship between the subscriber computer component or system and the public key of the certificate provided by the certification authority. Any relying party shall use the information contained in the Electronic Seal Certificate to ensure the identity and authenticate.

1.5 Certificate usage

The Electronic Seal Certificate issued under the CPSM shall be only used in the defined transactions inside authorized systems and applications. The issue of the Electronic Seal Certificate under the CPSM obliges the subscriber to the acceptance and use thereof in the terms expressed in the CPSM. On the contrary, this could cause the immediate revocation of the certificates by its misusage. It is emphasized that falls outside the scope of the CPSM to ensure the technological feasibility of applications that make use of any of this certificate profiles defined by the CPSM.

The Electronic Seal Certificate shall be used to generate advanced electronic seals, as defined in the articles 36 and 37 of eIDAS. The Electronic Seal Certificate is a certificate for public entities according to [Ley 39/2015] and to the articles 40 and 42 of [Ley 40/2015] as a means to identification and automated electronic administrative proceedings of the Public Administrations.

1.6 Definitions and acronyms

1.6.1 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).

1.6.2 Acronyms

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.
CSR	Certificate Signing Request.
CWA	CEN Workshop Agreement.
DN	Distinguished Name.
HSM	Hardware Security Module
MEYSS	Ministry 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.
PDS	PKI Disclosure Statement.
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.

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 5280].

The TSPM ensures the unicity of the *DN (Distinguished Names)* for the Electronic Seal Certificates.

2.1.2 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 Seal Certificate (Medium level of assurance): *2.16.724.1.3.5.6.2*

The Electronic Seal Certificates issued by the TSPM include the following fields according to schema *Identidad Administrativa*:

Certificate	Mandatory “Identidad Administrativa” fields
Electronic Seal Certificate	Type of certificate Name of the subscriber entity NIF of the subscriber entity System or component name

Certificate	Optional “Identidad Administrativa” fields
Electronic Seal Certificate	Responsible DNI/NIE Responsible given name Responsible first surname Responsible second surname Responsible email

3 Operational requirements

3.1 Application for the certificates

Only the public employees working for a public administration entity are entitled to initiate the application request of an electronic seal certificate. The Certification Authority shall verify that the applicant really is a public employee belonging to the applicant entity.

It is allowed the application without physical presence, based on administrative databases or valid electronic certificates. The only method currently allowed to request electronic seal certificates is via email of an authorized public employee, sent from an internal account of the public entity with the application form filled, attached and electronically signed. The signed application form should include a PKCS#10 request with the public key.

Some special attention will be paid to make sure the application form contains all the data corresponding to the certificate responsible person.

The TSPM main responsible shall approve or deny applications for electronic seal certificates. If the application form is not approved, the TSPM shall notify the applicant this denial.

3.2 Issuance of the Electronic Seal Certificate

Once the application form of the electronic seal certificate has been approved, its issuance (by using the PKCS#10) will be made safely. Delivery and acceptance of the certificate by the subscriber will be guaranteed by safe delivery to the responsible person.

The TSPM uses a procedure to generate the certificates that securely links the certificates with the organization information, including the certified public. 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.

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 Electronic Seal 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 physical presence), prior to its expiration date, in which case the applicant should authenticate by using a qualified electronic signature.

3.4 Certificate revocation

The PSCM authenticates requests and reports relating to revocation of Electronic Seal Certificates, validating that they come from an authorized person. Any revocation request shall be sent by email to the PSCM.

The only people authorized to request revocation of Electronic Seal Certificates are the responsible for them and the responsible for the public entity subscriber of the certificate.

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

4 Policy for the electronic seal certificate

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 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 that created the electronic seal	O = MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL (sample)
1.5.3. Organizational Unit (OU)	Certificate Type	OU = SELLO ELECTRONICO
1.5.4. Organization Identifier	Organization Identifier according to ETSI EN 319 412-1	VATES- S2819001E

Field	Description	Content
1.5.5. Serial Number	Organization unique identifier, NIF	SERIALNUMBER = S2819001E (sample)
1.5.6.Common Name (CN)	System or component name for the automated procedure	CN = REGISTRO CENTRAL DEL MINISTERIO DE DE EMPLEO Y SEGURIDAD SOCIAL (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:

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
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	

Field	Description	Content
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
2.7.3. CodeSigning	Code signing	OID 1.3.6.1.5.5.7.3.3
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- esign	Electronic seal certificate	OID 0.4.0.1862.1.6.2
2.8.4. QcPDS	PDS URL	OID 0.4.0.1862.1.5 PDS URL (see annex B)
2.8.5. SemanticsId-Legal	Semantics Id of the legal person as defined in EN 319412-1	OID 0.4.0.194121.1.2
2.9. Certificate Policies		
2.9.1. Policy Identifier	OID associated to the CPS	OID 1.3.6.1.4.1.27781.2.5.3.2.1
2.9.2. Policy Qualifier ID	CPS specification	
2.9.2.1. CPS Pointer	CPS URL	CPS URL (see annex B)
2.9.2.2. User Notice	explicitText field	"Certificado cualificado de sello electrónico de Administración, órgano o entidad de derecho público, nivel medio/sustancial. Consulte las condiciones de uso en <URL ubicación DPCM (ver anexo B)>“

Field	Description	Content
2.9.3. Policy Identifier	OID associated to electronic seal certificate (medium level)	2.16.724.1.3.5.6.2
2.9.4. Policy Identifier	QCP-l (qualified certificate according to eIDAS)	OID 0.4.0.194112.1.1
2.10. Subject Alternate Names		
2.10.1. rfc822Name	E-mail address of the public entity certificate subscriber	juanantonio.delacamara@meyss.es (sample)
2.10.2. Directory Name	Administrative Identity	
2.10.2.1. Tipo de certificado	Certificate type	2.16.724.1.3.5.6.2.1 = SELLO ELECTRONICO DE NIVEL MEDIO
2.10.2.2. Nombre de la entidad suscriptora	Public entity that owns the certificate	2.16.724.1.3.5.6.2.2 = MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL (sample)
2.10.2.3. NIF entidad suscriptora	NIF of subscriber entity	2.16.724.1.3.5.6.2.3 = S2819001E (sample)
2.10.2.4. Denominación de sistema o componente	Summary description of the system or computer where the electronic seal certificate is installed	2.16.724.1.3.5.6.2.5= REGISTRO CENTRAL DEL MINISTERIO DE DE EMPLEO Y SEGURIDAD SOCIAL (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 319 411-2 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 and PDS:

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