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 Securityp

Profile for Electronic seal certificate

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

sgtic@meyss.es

Version control

Identifier	D303
Title	Certification Service Provider of the Ministry of Employment and Social Security. Profile for Electronic seal certificate
Responsible	SG de Tecnologías de la Información y las Comunicaciones Ministerio de Empleo y Seguridad Social
Version	1.4
Date	30.06.2012

Version history

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 certficate issued by CSPM
1.2	10.09.2010	Heading Change, suppression of DG de Servicios Suppression of the posibility 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

Contents

1 Introduction

1.1 Presentation

This document contains the **profile of the Electronic Seal Certificate 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 Electronic Seal certificates.

1.2 Description

Electronic Seal certificate is an authentication system for the automated administrative procedures and is described in LAECSP article 18th. It is a technical instrument that allows the electronic authentication of the public administration as well as the Electronic documents produced by them.

The Electronic Seal certificates issued by the CSPM are qualified certificates as defined in the LFE and they meet the requirements for medium level assurance as defined in [EIFEBIII]. Following this scheme, medium level assurance implies X.509 certificates.

The Electronic Seal certificates are X.509 qualified certificates stored in software containers, located in secure application servers.

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 Electronic Seal certificate**, with the following information:

- Document version	1.4
- Document status	Published
- Emission date	June 30th 2012
- Expiration date	NA

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 od issued certificates. OID for Electronic Seal certificate is:

- Electronic Seal Certificate: *[1.3.6.1.4.1.27781.2.4.3.2.3]*

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.

Certificate requesters are the public employees of the Administration department.

Certificate subscribers of the Electronic Seal are the Public Administrations identified as such in the *Subject* Field. In the *Common Name* attribute is the name of the device, application or Server (name of the system) to which the certificate is associated.

Those responsible for the custody of the certificate are the authorized public employees.

Verifiers are the entities (including natural and legal persons, Public Administrations and other organizations) who, using an Electronic Seal certificate, issued by CPSM, verify the identity and authenticity of the automated administrative procedure, trusting on the validity of the relationship between an electronic system or device belonging to the administrative entity subscriber of the certificate and the public key of the certificate.

1.5 Certificate Usage

Electronic Seal certificates issued under the CPSM shall be used only in the defined transactions inside the permitted systems and applications. Issuance of the Electronic Seal 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 Electronic Seal certificates outside the scope described in the CPSM what could cause immediate revocation of the certificates by the misuse of the same.

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

1.6 Definitions and acronyims

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.
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

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 Electronic Seal certificate is:

- Electronic Seal for automated administrative procedures (Medium level of assurance)

  2.16.724.1.3.5.2.2

Certificate	Mandatory "Administrative Identity" fields
ELECTRONIC SEAL FOR AUTOMATED ADMINISTRATIVE PROCEDURES	• Type of certificate • Name of the subscriber entity • NIF of the subscriber entity • System or component denomination

Certificate	Optional "Administrative Identity" fields
ELECTRONIC SEAL FOR AUTOMATED ADMINISTRATIVE PROCEDURES	• DNI/NIE of the responsible • Given name • First surname • Second surname • E-mail address

3 Operational requirements

3.1 Application for certificates

Only the public employees working for an administration body are allowed to start the application procedure for an electronic seal certificate for that body. The Certification Authority shall verify that he is indeed a public employee of the applicant organization.

It is permitted the application without physical presence, based on administrative databases or applicable certificate. 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 organism with the completed application form. Special attention will be paid to make sure the application form contains all the data corresponding to the certificate responsible person.

Thus, methods based on indirect physical presence are used, since the physical identity validation has occurred previously and ministry records are constantly kept updated**.**

The responsible of the certificates are the authorized public employees of the organization.

The person responsible the Certification Entity shall approve or deny applications for certificates of electronic seal. If the request is refused, the Certification Entity shall notify the applicant thereof denial.

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

Upon approval of the application of the electronic seal certificate, the issuance of the same will be made safely. Delivery and acceptance of the certificate by the subscriber of the same is guaranteed by safe delivery to the responsible person.

The CSPM 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 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 using valid certificates, and, if so, the applicant must authenticate remotely by certificate authentication in hardware support(cryptographic card), allowing no alternative to this practice.

3.4 Certificate revocation

The CSPM authenticates requests and reports relating to revocation of Electronic Seal Certificates, checking that they come from an authorized person. Revocation requests must be sent to SGTIC (Subdirección General de Tecnologías de la Información y las Comunicaciones).

Persons authorized to request revocation of this kind are the responsible persons of the same and the public employees within the organization with a rank level equal o higher to 30.

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 Electronic Seal certificate

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	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		
1.5.1. Country (C)	País	C = ES
1.5.2. Organization (O)	Official name of the subscriber entity	O = MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL (sample)
1.5.3. Organizational Unit (OU)	Certificate type description	OU = SELLO ELECTRONICO
1.5.4. Serial Number	NIF of the subscriber entity	SerialNumber = S2819001E (sample)
1.5.5. Common Name	Name of the system or application where the	CN = REGISTRO CENTRAL DEL MEYSS (sample)

Field	Description	Contents
(CN)	automated procedure is	
1.6. Subject Public Key Info	Public key, codified following the cryptographic algorithm	
1.7. Signature Algorithm	Signature algorithm	SHA-1 RSA Signature, 1024 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 TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. OU=PRESTADOR DE SERVICIOS DE CERTIFICACION, SERIALNUMBER=S2819001E, CN=AC1 RAIZ MTIN
2.1.3. AuthorityCertSerial Number	Serial number of the CA certificate	
2.2. Subject Key Identifier	Subject public key identifier (derived from the subject public key using SHA1 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

Field	Description	Contents
2.6. Key Usage	Critical extension to determine certificate usage	
2.6.1. Digital Signature	Used when the subject public key is used for verifying digital signatures	Selected “1”
2.6.2. Content Commitment	Used when the software must allow user to know what is signing	Selected “1”
2.6.3. Key Encipherment	Used for keys management and transport	Selected “1”
2.6.4. Data Encipherment	Used to encipher data other tan cryptographic keys	Selected “1”
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
2.8. 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
2.9. Certificate Policies		
2.9.1. Policy Identifier	OID associated to the CPS	OID 1.3.6.1.4.1.27781.2.4.3.2.3
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	" Qualified Electronic Seal certificate for Administration, Agency or Public entity, medium level of assurance. See the terms of use at < CPSM URL location (see annex B)>“
2.10. Subject Alternate Names		
2.10.1. rfc822Name	Contact E-mail address at the subscriber entity	registro@meyss.es (sample)

Field	Description	Contents
2.10.2. Directory Name	Administrative Identity	
2.10.3. Certificate Type	Certificate Type	2.16.724.1.3.5.2.2.1 = SELLO ELECTRONICO
2.10.4. Name	Name of the subscriber entity	2.16.724.1.3.5.2.2.2 = MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL (sample)
2.10.5. NIF of the subscriber entity	NIF of the subscriber entity	2.16.724.1.3.5.2.2.3 = S2833002
2.10.6. DNI/NIE of the responsible	DNI/NIE of the person responsible for the certificate	2.16.724.1.3.5.2.2.4=”” (not used)
2.10.7. Denomination of the system or component	Short description of the component that uses the Electronic Seal certificate	1.3.6.1.4.1.14862. 1.4.3.2.5 = REGISTRO CENTRAL DEL MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL (sample)
2.10.8. Given name	Given name of the person responsible for the certificate	2.16.724.1.3.5.2.2.6 = ”” (not used)
2.10.9. First surname	First surname of the person responsible for the certificate	2.16.724.1.3.5.2.2.7 = ”” (not used)
2.10.10. Second surname	Second surname of the person responsible for the certificate	2.16.724.1.3.5.2.2.8 = ”” (not used)
2.10.11. E-mail	E-mail address of the person responsible for the certificate	2.16.724.1.3.5.2.2.9 = “” (not used)

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