MINISTERIO
DE EMPLEO
Y SEGURIDAD SOCIAL

SUBSECRETARÍA

S.G. TEGNOLOGÍAS DE LA
INFORMACION Y COMUNICACIONES

Perfil del Certificado de Sede Electrónica del Prestador de Servicios de Certificación del Ministerio de Empleo y Seguridad Social

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

sgtic@meyss.es

Control de versiones

Identificador	D302
Título	Perfil del Certificado de Sede Electrónica del Prestador de Servicios de Certificación del Ministerio de Empleo y Seguridad Social
Responsable	SG de Tecnologías de la Información y las Comunicaciones Ministerio de Empleo y Seguridad Social
Versión	1.5
Fecha	18.06.2015

Registro de Cambios

Versión	Fecha	Comentario
1.0	03.12.2009	Documento final
1.1	30.03.2010	Cambios en el número ISO/IANA del MPR e Identificador de Objeto (OID) del Certificado de Sede Electrónica emitido por el PSCM
1.2	10.09.2010	Eliminado del encabezado la DG de Servicios Eliminada la posibilidad futura de solicitud de certificados con certificados vigentes
1.3	02.08.2011	Cambio SGPD por SGTIC
1.4	30.06.2012	Actualización de la estructura organizativa y nuevo formato
1.5	18.06.2015	Se añade SHA-256

Tabla de contenidos

1 Introducción

1.1 Presentación

El presente documento recoge el **Perfil del Certificado de Sede Electrónica del Prestador de Servicios de Certificación del Ministerio (**PSCM**)**.

Este documento matiza y complementa la Declaración de Prácticas de Certificación del Prestador de Servicios de Certificación del Ministerio (DPCM) en lo referente a los Certificados de Sede Electrónica.

1.2 Descripción

El Certificado de Sede Electrónica es un sistema de autenticación recogido en varios artículos de la LAECSP y está previsto en el artículo 17 de la misma. Se trata de un instrumento técnico y legalmente válido que permite autenticar las sedes electrónicas de las AAPP frente a terceros.

Los Certificados de Sede Electrónica emitidos por el PSCM son certificados reconocidos según la LFE y se ajustan al nivel medio según el [EIFEBIII]. Según este esquema el nivel medio de aseguramiento se corresponde con sistemas de firma electrónica avanzada basados en certificados electrónicos reconocidos, de acuerdo con la LFE. Se utilizan certificados X.509 con soporte en contenedor software (en un servidor seguro de aplicación).

1.3 Nombre del documento e identificación

1.3.1 Identificación de este documento

Este documento se denomina **Perfil de Certificado de Sede Electrónica del Prestador de Servicios de Certificación del Ministerio de Empleo y Seguridad Social**, con la información reflejada en el control de versiones del documento (pág. ii).

La ubicación de la publicación de este documento se encuentra en el Anexo B.

1.3.2 Identificación de los tipos de certificado

Cada tipo de certificado recibe su propio *OID*, indicado a continuación e incluido dentro del certificado, en el campo *PolicyIdentifier*. Cada *OID* es unívoco y no se emplea para identificar diferentes tipos, políticas y versiones de los certificados emitidos. El Certificado de Sede Electrónica emitido por el PSCM tiene asignado el siguiente identificador de objeto (OID):

- Certificado de Sede Electrónica: *[1.3.6.1.4.1.27781.2.5.2.2.1]*

1.4 Usuarios finales

Los usuarios finales son las entidades o personas que disponen y utilizan los certificados electrónicos emitidos por las Entidades de Certificación del PSCM. En concreto, podemos distinguir los siguientes usuarios finales:

a. Los solicitantes de certificados.
b. Los suscriptores de certificados.

c. Los responsables de certificados.
d. Los verificadores de certificados.

Los solicitantes de Certificados de Sede Electrónica son empleados públicos del organismo.

Los suscriptores de los certificados de Sede Electrónica son las AAPP y así están identificados en el campo *Subject*. En el atributo *Common Name* se indica la sede (nombre lógico y DNS o IP) a la que están asociados.

Los responsables de la custodia del certificado son empleados públicos del organismo autorizados.

Los verificadores de certificados son las entidades (personas físicas, AAPP, personas jurídicas y otras organizaciones y entidades) que utilizan un certificado de Sede Electrónica emitido por el PSCM y se basan en la confianza de la validez de la relación entre la sede pública suscriptora del certificado y la clave pública para garantizar la identidad del sitio.

1.5 Uso del certificado

Los certificados de Sede Electrónica que se circunscriben a la DPCM deberán ser utilizados sólo para las transacciones definidas en los sistemas y aplicaciones permitidos. La expedición efectiva de los certificados de Sede Electrónica soportados en la DPCM obliga al suscriptor a la aceptación y uso de los mismos en los términos expresados en la DPCM.

Se recalca que está fuera del ámbito de la DPCM garantizar la viabilidad tecnológica de las aplicaciones que harán uso de cualquiera de los perfiles de certificados definidos en la DPCM.

No se permite en modo alguno el uso de los certificados de Sede Electrónica fuera del ámbito descrito en la DPCM, pudiendo ser causa de revocación inmediata de los certificados por el uso indebido de los mismos.

El certificado de Sede Electrónica emitido por el PSCM con correspondencia con el definido por la LAECSP tendrá su uso delimitado por lo dispuesto en la ley. El uso de los certificados de sede electrónica está limitado a la identificación de la sede, quedando excluida su aplicación para la firma electrónica de documentos y trámites.

1.6 Definiciones y acrónimos

1.6.1 Definiciones

En el ámbito de este documento se utilizan las siguientes definiciones:

C	Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.
CN	Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.
DN	Identificación unívoca de una entrada dentro de la estructura de directorio X.500.
O	Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura

	de directorio X.500.
OCSP	Este protocolo permite comprobar en línea la vigencia de un certificado electrónico.
OU	Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.
PIN	Contraseña que protege el acceso a una tarjeta criptográfica.
PKCS	Estándares de PKI desarrollados por RSA Laboratories y aceptados internacionalmente.
RFC	Estándar emitido por la IETF.

1.6.2 Acrónimos

AAPP	Administraciones Públicas.
AC	Entidad de Certificación, también denominada Autoridad de Certificación.
AR	Entidad de Registro, también denominada Autoridad de Registro.
AV	Entidad de Validación, también denominada Autoridad de Validación.
C	Country (País).
CA	Certification Authority, Entidad de Certificación.
CDP	CRL Distribution Point (Punto de Distribución de las CRL).
CN	Common Name (Nombre Común).
CP	Certificate Policy.
CRL	Certificate Revocation List, Lista de Revocación de Certificados.
CSP	Cryptographic Service Provider, Proveedor de Servicios Criptográficos.
CSR	Certificate Signing Request (petición de certificado).
CWA	CEN Workshop Agreement.
DN	Distinguished Name (Nombre Distintivo).
DPC	Declaración de Prácticas de Certificación.
DPCM	Declaración de Prácticas de Certificación del Prestador de Servicios de Certificación del Ministerio.
LAECSP	Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos
LFE	Ley 59/2003 de 19 de diciembre de Firma Electrónica.
MEYSS	Ministerio de Empleo y Seguridad Social.
MTIN	Ministerio de Trabajo e Inmigración
O	Organization.
OU	Organizational Unit (Unidad Organizativa).
OID	Object IDentifier (Identificador de objeto único).
OCSP	On-line Certificate Status Protocol.
PSCM	Prestador de Servicios de Certificación del Ministerio.
RA	Registration Authority.
RFC	Request For Comments.

SGPD	Subdirección General de Proceso de Datos.
SGTIC	Subdirección General de Tecnologías de la Información y las Comunicaciones.
VA	Validation Authority. Entidad o Autoridad de Validación.

2 Identificación

2.1 Gestión de nombres

2.1.1 Tipos de nombres

Todos los certificados contienen un nombre distintivo (*DN*) de la persona y/o organización, identificados en el certificado, definido de acuerdo con lo previsto en la recomendación [ITU-T X.501] y contenido en el campo *Subject*, incluyendo un componente *Common Name*. Todos los certificados emitidos cumplen, además, con la norma [IETF RFC 3280].

El PSCM asegura la unicidad de los *DN* (*Distinguished Names*) de los certificados de sede electrónica.

2.1.2 Normalización e Identidad Administrativa

El PSCM utiliza el esquema de nombres normalizado propuesto por la AGE *Identidad Administrativa* para cada tipo y perfil de certificado emitido.

El objeto Identidad Administrativa utiliza el número ISO/IANA del MPR *2.16.724.1.3.5.X.X* proporcionado por la AGE como base para identificarlo, de este modo se establece un identificador unívoco a nivel internacional.

El número de Identidad Administrativa del certificado es:

- Certificado de Sede Electrónica (Nivel Medio)

  2.16.724.1.3.5.1.2

Certificado	Campos "Identidad Administrativa" fijos
SEDE ELECTRÓNICA	• Tipo de certificado • Nombre de la entidad suscriptora • NIF entidad suscriptora • Nombre descriptivo de la sede electrónica • Denominación de nombre de dominio IP

Certificado	Campos "Identidad Administrativa" opcionales
SEDE ELECTRÓNICA	• Ninguno

3 Requisitos operativos

3.1 Solicitud y emisión de certificados

Para poder iniciar el procedimiento de solicitud de un certificado de Sede Electrónica se debe tener la condición de empleado público del organismo solicitante. La Entidad de Certificación comprobará que se trata en efecto de un empleado público dicho organismo.

Para la solicitud se permite la identificación sin presencia física, basada en bases de datos administrativas o en certificados vigente. El único método que se permite utilizar actualmente para solicitar certificados de sede electrónica es mediante correo electrónico de un empleado público autorizado, enviado desde una cuenta interna del organismo con la solicitud cumplimentada. Se prestará especial atención a que la solicitud contenga los datos correspondientes al responsable del certificado.

De esta forma se emplean métodos basados en la presencia física indirecta, ya que la validación de la identidad se ha producido en forma personal anteriormente y los registros del ministerio se mantienen permanentemente actualizados**.**

Los responsables del certificado son empleados públicos del organismo autorizados.

El responsable de la Entidad de Certificación aprobará o denegará las solicitudes de certificados de sede electrónica. En caso de que se deniegue la solicitud, la Entidad de Certificación notificará al solicitante la denegación de la misma.

Los procedimientos establecidos en esta sección también se aplican en caso de renovación de certificados, ya que ésta implica la emisión de nuevos certificados.

3.2 Emisión de certificados

Una vez aprobada la solicitud del certificado de sede electrónica se procederá a la emisión del mismo de forma segura. Se garantiza la entrega y la aceptación del certificado por el organismo suscriptor del mismo mediante su remisión de forma segura al responsable.

El PSCM utiliza un procedimiento de generación de certificados que vincula de forma segura los certificados con la información sobre el organismo, incluyendo la clave pública certificada. También se indican la fecha y la hora en las que se expidieron los certificados. Además se utilizan medidas contra la falsificación de certificados y para garantizar el secreto de las claves durante el proceso de generación de las mismas.

Los procedimientos establecidos en esta sección también se aplican en caso de renovación de certificados, ya que ésta implica la emisión de nuevos certificados.

3.3 Renovación de certificados

La renovación de certificados de sede electrónica supone la emisión de nuevos certificados, debiéndose proceder a una nueva solicitud y su posterior emisión como se indica en los apartados anteriores.

Al igual que sucede con la solicitud por primera vez, se podrá habilitar en un futuro mecanismos que permitan la renovación de los certificados de sede electrónica mediante el uso de certificados vigentes y, en tal caso, el solicitante habrá de autenticarse de forma remota mediante el certificado de autenticación en soporte hardware (tarjeta criptográfica), no permitiéndose método alternativo a esta práctica.

3.4 Revocación de certificados

El PSCM autentica las peticiones e informes relativos a la revocación de los certificados de sede electrónica comprobando que provienen de una persona autorizada. Las solicitudes de revocación deben enviarse al responsable de la Entidad de Certificación.

Sólo están autorizados a solicitar las revocaciones de este tipo de certificados, los responsables de los mismos y los empleados públicos del organismo con nivel 30 o rango superior.

Los mecanismos de revocación permitidos son a través de cuentas internas de correo electrónico o mediante un escrito firmado por el solicitante de la revocación.

4 Perfil del Certificado de Sede Electrónica

Los campos son los siguientes:

Campo	Descripción	Contenido
1. X.509v1 Field		
1.1. Version	Describe la versión del certificado	2 (= v3)
1.2. Serial Number	Número identificativo único del certificado	7c 88 54 93 b6 c9 (ejemplo)
1.3. Issuer Distinguished Name		
1.3.1. Country (C)	País	C = ES
1.3.2. Organization (O)	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado)	O = MINISTERIO DE TRABAJO E INMIGRACION
1.3.3. Locality (L)	Localidad del prestador de servicios de certificación	L = MADRID
1.3.4. Organizational Unit (OU)	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado	OU = SUBDIRECCION GENERAL DE PROCESO DE DATOS
1.3.5. Organizational Unit (OU)	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado	OU = PRESTADOR DE SERVICIOS DE CERTIFICACION MTIN
1.3.6. Common Name (CN)	Nombre común de la organización prestadora de servicios de certificación (emisor del certificado)	CN = AC1 RAIZ MTIN
1.3.7. Serial Number	NIF del Ministerio de Trabajo e Inmigración	S2819001E
1.4. Validity	3 años	
1.4.1. Not Before	Fecha de inicio de validez	Fecha de inicio de validez, formato: UTCTime YYMMDDHHMMSSZ
1.4.2. Not After	Fecha de fin de validez	Fecha fin de validez, formato: UTCTime YYMMDDHHMMSSZ
1.5. Subject		
1.5.1. Country (C)	País	C = ES
1.5.2. Organization (O)	Denominación (nombre "oficial" de la organización) del suscriptor de servicios de certificación (custodio del certificado)	O = MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL
1.5.3. Organizational Unit	Descripción del tipo de certificado	OU = SEDE ELECTRONICA

Campo	Descripción	Contenido
(OU)		
1.5.4. Organizational Unit (OU)	El nombre descriptivo de la sede	OU = SEDE DEL MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL (ejemplo)
1.5.5. Serial Number	NIF de la entidad responsable	SerialNumber = S2819001E
1.5.6. Common Name (CN)	Denominación de nombre de dominio (DNS o IP) donde residirá el certificado	CN = sede.mtin.es (ejemplo)
1.6. Subject Public Key Info	Clave pública de la sede, codificada de acuerdo con el algoritmo criptográfico	
1.7. Signature Algorithm	Algoritmo de firma	SHA-1/SHA-256 con RSA Signature y longitud de clave de 2048 bits

Y las extensiones son las siguientes:

Campo	Descripción	Contenido
2. X.509v3 Extensions		
2.1. Authority Key Identifier	Medio para identificar la clave pública correspondiente a la clave privada utilizada para firmar un certificado, por ejemplo en los casos en que el emisor tiene múltiples claves de firma	
2.1.1. Key Identifier	Identificador de la clave pública del emisor	
2.1.2. AuthorityCertIssuer	Path de identificación de certificación	C=ES, L=MADRID, O=MINISTERIO DE TRABAJO E INMIGRACION, OU=SUBDIRECCION GENERAL DE PROCESO DE DATOS, OU=PRESTADOR DE SERVICIOS DE CERTIFICACION, SERIALNUMBER=S2819001E, CN=AC1 RAIZ MTIN
2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA	
2.2. Subject Key Identifier	Identificador de la clave pública del suscriptor o poseedor de claves (derivada de utilizar la función de Hash sobre la clave pública del sujeto)	
2.3. cRLDistributionPoint	Indica cómo se obtiene la información de la CRL	
2.3.1. distributionPoint	Web donde resida la CRL (punto de distribución 1)	URL punto de distribución 1 CRL (ver anexo B)
2.3.2. distributionPoint	Web donde resida la CRL (punto de distribución 2)	URL punto de distribución 2 CRL (ver anexo B)

Campo	Descripción	Contenido
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	(dirección web)	URL servicio de validación OCSP (ver anexo B)
2.5. Issuer Alternative Name	Nombre alternativo de la persona de contacto de la Entidad de Certificación emisora	
2.5.1.rfc822Name	Correo electrónico de contacto de la Entidad de Certificación emisora	admin_ca@mtin.es
2.6. Key Usage	Campo crítico para determinar el uso	
2.6.1.Digital Signature	Se utiliza cuando se realiza la función de firma electrónica	Seleccionado “1”
2.6.2.Content Commitment	Se refiere a la cualidad de un tipo de certificado que indica al software en el que se usa que debe permitir que el usuario conozca lo que firma	No seleccionado “0”
2.6.3.Key Encipherment	Se utiliza para gestión y transporte de claves	Seleccionado “1”
2.6.4.Data Encipherment	Se utiliza para cifrar datos que no sean claves criptográficas	No seleccionado “0”
2.6.5.Key Agreement	Se usa en el proceso de acuerdo de claves	No seleccionado “0”
2.6.6.Key Certificate Signature	Se usa para firmar certificados. Se utiliza en los certificados de autoridades de certificación	No seleccionado “0”
2.6.7.CRL Signature	Se usa para firmar listas de revocación de certificados	No seleccionado “0”
2.7. Extended Key Usage		
2.7.1.Server Authentication	Autenticación TSL web Server	OID 1.3.6.1.5.5.7.3.1
2.8. Qualified Certificate Statements		
2.8.1.OcCompliance	Indicación de certificado reconocido	OID 0.4.0.1862.1.1
2.8.2.OcEuRetentionPeriod	Periodo de conservación de informaciones (15 años)	OID 0.4.0.1862.1.3
2.9. Certificate Policies	Políticas de certificación/DPC	
2.9.1.Policy Identifier	OID asociado a la DPC o PC	OID 1.3.6.1.4.1.27781.2.4.2.2.2
2.9.2.Policy Qualifier ID	Especificación de la DPC	
2.9.2.1. DPC	URL de la DPC	URL ubicación DPCM (ver anexo B)

Campo	Descripción	Contenido
Pointer		
2.9.2.2. User Notice	Campo explicitText	"Certificado reconocido de Sede Electrónica, nivel medio. Consulte las condiciones de uso en <URL ubicación DPCM (ver anexo B)>“
2.10. Subject Alternate Names		
2.10.1. rfc822Name	Correo electrónico de contacto de la sede electrónica	sedemtin@meyss.es (ejemplo)
2.10.2. dnsName	Nombre de Dominio DNS de la Sede	sede.mtin.es (ejemplo)
2.10.3. Directory Name	Identidad administrativa	
2.10.4. Tipo de certificado	Indica la naturaleza del certificado	2.16.724.1.3.5.1.2.1= SEDE ELECTRONICA
2.10.5. Nombre de la entidad suscriptora	La entidad propietaria de dicho certificado	2.16.724.1.3.5.1.2.2 = MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL
2.10.6. NIF entidad suscriptora	NIF del Ministerio de Trabajo e Inmigración.	2.16.724.1.3.5.1.2.3= S2833002
2.10.7. Nombre descriptivo de la sede electrónica	Breve descripción de la Sede indicando un nombre	2.16.724.1.3.5.1.2.4 = SEDE DEL MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL (ejemplo)
2.10.8. Denominación de nombre de dominio IP	Dominio al que pertenece la Sede	2.16.724.1.3.5.1.2.5 = sede.mtin.es (ejemplo)

Anexo A: Referencias

EIFEBIII	Esquema de identificación y firma electrónica de las Administraciones Públicas. Bloque III: Propuestas de condiciones generales adicionales en la AGE
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.

Anexo B: Enlaces (URL)

Ubicación de la DPCM y perfiles de certificados:

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

Servicio de validación OCSP:

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

Publicación de las CRL:

- Punto de distribución 1:

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

- Punto de distribución 2:

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