El Prestador de Servicios de Certificación del Ministerio de Trabajo e Inmigración

Antonio Sanz Pulido
E-mail: antonio.sanz@mtin.es

Resumen. La Subdirección General de Proceso de Datos del Ministerio de Trabajo e Inmigración ha transformado su plataforma de certificación y firma electrónica en un Prestador de Servicios de Certificación, el PSCMTIN, que cumple con los requisitos de la LAECSP y el esquema de identificación y firma electrónica de las Administraciones Públicas.

En el ámbito del PSCMTIN ofrecen servicios la entidad de acreditación admitiendo, supervisando y acreditando entidades de certificación, las entidades de certificación, emitiendo certificados, las entidades de registro, registrando usuarios, la entidad de validación verificando firmas y certificados y la entidad de sellado de tiempo para certificar fechas y horas.

De acuerdo con la política de firma de la AGE [EIFE], el PSCMTIN emite certificados de Empleado Público, para el personal al servicio de la Administración, certificados de Sede Electrónica Administrativa, certificados de Sello Electrónico para la Actuación automatizada, certificados de Sellado de Respuestas OCSP, certificados de Sellado de Tiempo TSA y certificados de Firma de Software.

Adicionalmente, el PSCMTIN ofrece otros servicios de forma centralizada a todas las aplicaciones del ministerio que necesiten funciones tales como información del estado de revocación de certificados, firma de documentos, tanto de servidor como de cliente, servicios de sellado de tiempo (time stamping) etc.

El PSCMTIN se halla inmerso en el proceso de ser reconocido por el Ministerio de Industria, Turismo y Comercio y está desarrollando un ambicioso proyecto, denominado Firmas XL, para la conservación de firmas longevas en formatos CAdES y XAdES XLong.

1 Introducción

El creciente uso de las técnicas de firma electrónica en las aplicaciones informáticas del Ministerio de Trabajo e Inmigración (anteriormente Ministerio de Trabajo y Asuntos Sociales) así como la necesidad de dotar a los empleados del mismo de los instrumentos de autenticación y firma necesarios para utilizarlas, llevó a la decisión de implantar una plataforma de certificación y firma propia que permitiera ofrecer una serie de servicios relacionados.

A principios del año 2006 la Subdirección General de Proceso de Datos[1] desplegó una Plataforma de Certificación y Firma Electrónica de ámbito interno que permitía, por una parte, la emisión de certificados a todos los empleados del Ministerio y a servidores, aplicaciones, etc. sin las rigideces que impondría usar los certificados emitidos por Autoridades de Certificación externas; y por otra, la validación de los

[1] La Subdirección General de Proceso de Datos (SGPD), perteneciente al Ministerio de Trabajo e Inmigración (MTIN), se ocupa de la gestión de la infraestructura técnica y de comunicaciones y el desarrollo y mantenimiento de los sistemas de información y comunicación que precisen los distintos centros directivos y unidades del ministerio, así como la supervisión en materia de tecnologías de la información y de las comunicaciones de los organismos autónomos adscritos, a excepción del Servicio Público de Empleo Estatal (SPEE) y de los dependientes de la Secretaría de Estado de la Seguridad Social.

certificados y de las firmas electrónicas efectuadas con las claves privadas asociadas a los mismos, con total independencia de otras plataformas de validación.

Desde su puesta en marcha se fueron identificando una serie de problemas y surgieron nuevas necesidades que aconsejaron una revisión a fondo de la misma. Entre estas necesidades debemos destacar la publicación de la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, así como su normativa de desarrollo y la publicación del esquema de identificación y firma electrónica de las Administraciones Públicas, es decir, la política de certificación de la Administración General del Estado, las cuales suponen una auténtica revolución en el modo de entender los certificados y la firma electrónica en el ámbito de la Administración en España.

Considerando todo lo expuesto y tras un estudio de diversas alternativas se tomó la decisión de evolucionar y completar la plataforma hacia un Prestador de Servicios de Certificación, el Prestador de Servicios de Certificación del Ministerio de Trabajo e Inmigración (PSCMTIN), que emitiera certificados electrónicos reconocidos de acuerdo con la LFE y la LAECSP.

2 El PSCMTIN

Un Prestador de Servicios de Certificación (PSC) es una persona física o jurídica que expide certificados o presta otros servicios en relación con la firma electrónica, de acuerdo con la LFE. Un PSC genera los certificados electrónicos mediante la operación de entidades de certificación de su titularidad que firman electrónicamente los certificados. Todo PSC debe recoger sus prácticas de certificación en una Declaración de Prácticas de Certificación (DPC) y hacerla fácilmente accesible por vía electrónica y de forma gratuita.

El PSCMTIN detalla sus prácticas de certificación en el documento Declaración de las Prácticas de Certificación del Prestador de Servicios de Certificación del Ministerio de Trabajo e Inmigración, referido de ahora en adelante como DPCMTIN, disponible en el sitio web del PSCMTIN[2]. La DPCMTIN ha sido redactada conforme a las especificaciones de la RFC 3647 [IETF RFC 3647].

La DPCMTIN contiene, entre otros, las obligaciones que el PSCMTIN se compromete a cumplir en relación con las medidas de seguridad técnicas y organizativas; las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados electrónicos; la gestión de los datos de creación y verificación de firma electrónica y de los certificados electrónicos; los perfiles de los certificados y los mecanismos de información sobre su vigencia.

El PSCMTIN determina la idoneidad de la DPCMTIN con respecto a la Política de Certificación de la AGE y los perfiles de certificados publicados y admitidos según el esquema de identificación y firma electrónica de las AAPP. De acuerdo con este esquema, en el ámbito del PSCMTIN ofrecen servicios los prestadores siguientes:

- Entidad de Acreditación, prestador que admite, supervisa y acredita entidades de certificación.
- Entidad de Certificación, prestador que emite certificados.
- Entidades de Registro, prestadores que registran usuarios.
- Entidad de Validación, prestador que verifica firmas y certificados.
- Entidad de Sellado de Tiempo, prestador que emite sellos de tiempo.

2.1 Entidad de Acreditación

Las funciones de acreditación del PSCMTIN están atribuidas a la Subsecretaría del MTIN, la cual admite, acredita y supervisa las entidades de certificación.

[2] http://ca.mtin.es

2.2 Entidad de Certificación

La SGPD opera los componentes del PSCMTIN, de manera que da fe de la correcta correspondencia de los pares de claves de los suscriptores finales con la identidad que representan. Dicha vinculación de los pares de claves con la identidad tiene lugar a través de certificados X.509 v3 según lo descrito en su Declaración de Prácticas de Certificación (DPCMTIN) y en los perfiles de los certificados.

La Entidad de Certificación se compone, de manera única y exclusiva, de la Entidad de Certificación Raíz, estando cada tipo de certificado descrito en un documento con el perfil de dicho certificado.

2.3 Entidades de Registro

Las Entidades de Registro asisten al PSCMTIN en las funciones de identificación y autenticación de los suscriptores, así como en otras tareas relativas a la gestión de los certificados. Tienen como misión principal la de garantizar que la información contenida en la solicitud del certificado sea completa y veraz. Las tareas que desempeñan son:

- Identificación y autenticación de la identidad de las personas solicitantes y receptoras de los certificados.
- Entrega de los dispositivos seguros de creación de firma a los suscriptores o responsables de los certificados.
- Aprobación de la generación de los certificados.
- Almacenamiento de los documentos en relación con los servicios de certificación o envío de los mismos a la SGPD para su almacenamiento.

Las Entidades de Registro están compuestas, de manera conjunta, por los servicios telemáticos que permiten la gestión del ciclo de vida de los certificados y por los puestos de expedición presencial que operan dedicados a tal fin.

Las Entidades de Registro llevan a cabo la identificación de los solicitantes de certificados conforme a las normas de la DPCMTIN y el acuerdo suscrito con la Entidad de Certificación. En el caso de que las Entidades de Registro pertenezcan al MTIN, no será precisa la firma de ningún acuerdo y las relaciones entre ambas se regirán por la DPCMTIN y las Políticas de Certificación que sean de aplicación. Las Entidades de Registro competentes para la gestión de solicitudes de certificación se encuentran definidas para cada tipo de certificado.

La Entidad de Certificación podrá valerse de una o varias Entidades de Registro elegidas libremente para la prestación del servicio de certificación. Los servicios remotos ofrecidos por las Entidades de Registro están accesibles solamente a través de la Intranet del MTIN.

2.4 Entidades de Validación

Las Entidades de Validación son las encargadas de suministrar información sobre la vigencia de los certificados electrónicos emitidos por una Entidad de Certificación. Para proporcionar esta información, las Entidades de Validación usan los servicios de la lista de entidades de confianza (TSL), estructura que mantiene la relación de los servicios de certificación admitidos por todas las AAPP.

La Entidad de Validación del PSCMTIN presta servicio a los usuarios de forma que se puede comprobar el estado del certificado de forma instantánea, segura y fiable.

El acceso a los servicios de validación del estado de los certificados se ofrece de forma pública. El servicio de validación OCSP se presta en la siguiente dirección:

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

2.5 Entidades de Sellado de Tiempo

La Entidad de Sellado de Tiempo aporta evidencias criptográficas de existencia en un momento determinado, el indicado en el sello de tiempo. El acceso a los servicios de sellado de tiempo de firma electrónica se ofrece de forma generalizada a las aplicaciones del MTIN.

La Entidad de Sellado de Tiempo del MTIN proporciona servicio según determina la [ETSI TS 102 023] y las condiciones adicionales establecidas por la AGE para adaptar dicha norma a la normativa española y mejorar los niveles de calidad exigidos.

3 Certificados emitidos por el PSCMTIN

Basándose en los dos niveles de aseguramiento establecidos para los perfiles de los diferentes certificados emitidos conforme a la LAECSP y en las diferentes modalidades de firma electrónica recogidas en la LFE, el PSCMTIN emite sus certificados conforme al siguiente esquema:

- Nivel medio de aseguramiento: Sistemas de firma electrónica avanzada basada en certificado electrónico reconocido.
- Nivel alto de aseguramiento: Sistemas de firma electrónica reconocida.

Todos los certificados incluyen implícitamente, en cada perfil definido, el nivel de aseguramiento que le corresponde mediante un identificador único: el identificador del objeto Identidad Administrativa.

A continuación se muestra la descripción de los tipos de certificados definidos y que son pertinentes para el PSCMTIN con el fin de indicar correctamente el uso que se dará a los mismos.

- El Certificado de Empleado Público es el certificado previsto en el artículo 19 de la LAECSP, para el personal al servicio de la Administración.
- El Certificado de Sede Electrónica Administrativa es el certificado previsto en el artículo 17 de la LAECSP.
- El Certificado de Sello Electrónico para la Actuación automatizada es el certificado previsto en el artículo 18 de la LAECSP, también denominado certificado de sello electrónico de Administración Pública, órgano o entidad de derecho público

En el ámbito de la DPCMTIN y de la documentación específica para cada certificado, el PSCMTIN emite los siguientes tipos de certificados:

- Certificados de Empleado Público de nivel alto, con soporte en un dispositivo seguro de creación de firma de acuerdo con el artículo 24 de la LFE (tarjeta criptográfica o token USB).
- Certificados de Sede Electrónica de nivel medio, con soporte en contenedor software (en un servidor seguro de aplicación).
- Certificados de Sello Electrónico de nivel medio, con soporte en contenedor software (en un servidor seguro de aplicación).

Fuera del ámbito de la LAECSP, el PSCMTIN emite adicionalmente los siguientes tipos de certificados:

- El Certificado de Sellado de Respuestas OCSP es el certificado que permite firmar las respuestas emitidas por el servidor OCSP.
- El Certificado de Sellado de Tiempo TSA es el certificado que permite firmar las referencias temporales.
- El Certificado de Firma de Software es el certificado que permite firmar el código y los ejecutables del software.

Las especificidades relativas a cada tipo de certificado emitido por el PSCMTIN están reguladas en la documentación específica para cada certificado disponible en el sitio web del PSCMTIN. Un resumen de los principales perfiles es el siguiente.

3.1 Perfil del certificado de empleado público

El certificado de empleado público es el previsto en el artículo 19 de la LAECSP, para el personal al servicio de la Administración. Se emplea para la identificación de un empleado público en cualquiera de sus categorías: funcionario, laboral fijo etc. e incluye tanto al titular como a la entidad pública en la que presta servicios el empleado.

Los Certificados de Empleado Público emitidos por el PSCMTIN son certificados reconocidos según la LFE y se ajustan al nivel alto según el Esquema de identificación y firma electrónica de las Administraciones Públicas, Bloque III: Propuestas de condiciones generales adicionales en la AGE (EIFEBIII).

El nivel alto de aseguramiento según el EIFEBI implica certificados X.509 en soporte hardware. Los certificados están soportados en dispositivos seguros de creación de firma según la LFE. Como los certificados de empleado público son emitidos a personas, esto se corresponde con firma electrónica reconocida según la LFE.

El PSCMTIN emite dos tipos de certificados de empleado público según sus usos: autenticación y firma. Ambos certificados son generados y almacenados en un dispositivo seguro de creación de firma (tarjeta inteligente).

La tarjeta inteligente elegida por el MTIN integra un chip criptográfico de alta seguridad con certificado como Dispositivo Seguro de Creación de Firma de acuerdo con la directiva [DIR 1999/93/CE] y Dispositivo Seguro de Creación de Cifrados. El chip criptográfico de la misma dispone de la certificación Common Criteria EAL 4+. La tarjeta proporciona además las siguientes funciones:

- Realiza procesos de cifrado/descifrado con claves asimétricas siguiendo los algoritmos RSA 1024 bit y RSA 2048 bit.
- Realiza procesos de cifrado/descifrado con claves simétricas según los algoritmos DES y Triple-DES.
- Realiza otros procesos de firma con clave asimétrica siguiendo los algoritmos de RSA 1024 bit y RSA 2048 bit.
- Es capaz de generar y almacenar claves tanto simétricas como asimétricas.
- Es capaz de almacenar diferentes objetos (certificados, claves privadas, etc.) de forma segura.
- Capacidad de generación de solicitud y renovación de certificados.

3.2 Perfil del certificado de sede electrónica

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 PSCMTIN son certificados reconocidos según la LFE y se ajustan al nivel medio según el EIFEBI. Según este esquema el nivel medio de aseguramiento se corresponde con sistemas de firma electrónica avanzada basados en certificados electrónicos reconocidos.

Se utilizan certificados X.509 con soporte en contenedor software (en un servidor seguro de aplicación).

3.3 Perfil del certificado de sello electrónico

El certificado de sello electrónico es un sistema de identificación y autenticación en la actuación administrativa automatizada y está previsto en el artículo 18 de la

LAECSP. Se trata de un instrumento técnico que permite la identificación electrónica de las AAPP y autenticar los documentos electrónicos que éstas produzcan.

Los Certificados de Sello Electrónico emitidos por el PSCMTIN son certificados reconocidos según la LFE y se ajustan al nivel medio según el EIFEBI. Según este esquema el nivel medio de aseguramiento se corresponde con sistemas de firma electrónica avanzada basados en certificados electrónicos reconocidos.

Se utilizan certificados X.509 con soporte en contenedor software (en un servidor seguro de aplicación).

3.4 Política de sellado de tiempo de la TSA

La política de sellado de tiempo tiene por objeto describir las reglas generales y las condiciones del servicio de sellado de tiempo (TSS) prestado por la Autoridad de Sellado de Tiempo del Ministerio (TSA) de Trabajo e Inmigración. Se trata de un servicio prestado exclusivamente de forma interna cuyo fin último es ofrecer sellos de tiempo a las aplicaciones del MTIN y en ningún caso se presta este servicio a entidades externas a este Ministerio.

El MTIN presta dicho servicio a través de su propia TSA. El TSS se ha diseñado siguiendo las recomendaciones y estándares internacionales. La política de sellado de tiempo se ha elaborado con base a la norma [ETSI TS 102 023] V1.2.1 y a su especificación equivalente [IETF RFC 3628].

Esta política se basa en criptografía de clave pública, en fuentes de tiempo fiables y en certificados X.509 v3.

El servicio de sellado de tiempo que proporciona el MTIN es el sistema que genera y emite los tokens de sellos de tiempo. El TSS permite dejar constancia del momento en que se ha realizado una firma electrónica en el contexto de un trámite o procedimiento realizado por una aplicación del MTIN. El TSS se ha implementado acorde al protocolo definido en la [IETF RFC 3161].

4 Siguientes pasos

Por su propia naturaleza, el PSCMTIN no es ajeno a las dificultades inherentes a un sistema horizontal que presta servicio a usuarios, aplicaciones y otros sistemas hardware. Como todo sistema, debe ir siendo perfeccionado y complementado con otras funcionalidades que permitan avanzar en el desarrollo de la Administración Electrónica en la AGE.

En este momento los pasos van encaminados por un lado a la revisión, mejora y simplificación de los procedimientos relacionados con la emisión y registro de usuarios así como en el despliegue de las nuevas tarjetas y por otro lado, el PSCMTIN se halla inmerso en el proceso de ser un prestador de servicios de certificación reconocido por el Ministerio de Industria, Turismo y Comercio.

Finalmente, cabe destacar que la SGPD del MTIN ha desarrollado una aplicación para el soporte, conservación y archivo seguro de firmas longevas (firmas XL, firmas basadas en CAdES y XAdES XLong) que implanta distintas funcionalidades y componentes comunes de firma electrónica y está integrado con el PSCMTIN.

5 Acrónimos y referencias

AAPP	Administraciones Públicas.
AGE	Administración General del Estado.
CAdES	CMS Advanced Electronic Signatures, norma ETSI TS 101 733.
DIR 1999/93/CE	Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de Diciembre de 1999, por la que se establece un marco Comunitario para la firma electrónica.
DPC	Declaración de Prácticas de Certificación.

DPCMTIN	Declaración de las Prácticas de Certificación de las Entidades de Certificación del Servicio de Certificación del Ministerio de Trabajo e Inmigración.
EIFE	Esquema de identificación y firma electrónica de las Administraciones Públicas.
EIFEBI	Esquema de identificación y firma electrónica de las Administraciones Públicas. Bloque I: Perfiles de certificados electrónicos.
EIFEBIII	Esquema de identificación y firma electrónica de las Administraciones Públicas. Bloque III: Propuestas de condiciones generales adicionales en la AGE.
ETSI	European Telecommunications Standard Institute.
ETSI TS 102 023	ETSI Technical Specification TS 102 023. Policy requirements for time-stamping authorities.
IETF	Internet Engineering Task Force (Organismo de estandarización de Internet).
IETF RFC 3161	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).
IETF RFC 3628	Policy Requirements for Time-Stamping Authorities (TSAs).
IETF RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Framework.
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.
MITyC	Ministerio de Industria, Turismo y Comercio.
MTIN	Ministerio de Trabajo e Inmigración.
OCSP	On-line Certificate Status Protocol.
PSC	Prestador de Servicios de Certificación.
PSCMTIN	Prestador de Servicios de Certificación del Ministerio de Trabajo e Inmigración.
RFC	Request For Comments.
SGPD	Subdirección General de Proceso de Datos.
SPEE	Servicio Público de Empleo Estatal.
TSA	Time-Stamping Authority, Entidad de Sellado de Tiempo.
TSS	Time-Stamping Service, Servicio de Sellado de Tiempo.
TSL	Trust-service Status List, Lista de Entidades de Confianza.
VA	Validation Authority, Autoridad de Validación.
XAdES	XML Advanced Electronic Signatures, norma TS 101 903 v.1.3.2.