MINISTERIO DE TRABAJO
Y ECONOMÍA SOCIAL

SUBSECRETARÍA

S.G. DE TECNOLOGÍAS DE LA
INFORMACIÓN Y COMUNICACIONES

Declaración Informativa del Prestador de Servicios de Confianza del Ministerio

sgtic@meyss.es
EA0041850

C/ PASEO DE LA CASTELLANA 63
28071 MADRID
TEL: 91 363.11.88
FAX: 91 363.07.73

Control de versiones

Identificador	D005
Título	Declaración Informativa del Prestador de Servicios de Confianza del Ministerio
Versión	06
Estado del documento	Aprobado
Fecha de aprobación	20200612

Registro de Cambios

Versión	Fecha	Comentario
01	20170331	Primera versión del documento
02	20180709	Cambio de nombre del ministerio Corregido error en código DIR3 Formato de fechas adaptado a ISO 8601: YYYYMMDD Añadido en los límites de uso el plazo de caducidad de los certificados Cambios en la política de privacidad Cambio en el nombre del Organismo Supervisor
03	20190520	Se elimina la fecha de caducidad Se deja genérico el Organismo Supervisor Se recalca la nota del Organismo Supervisor sobre firmantes y custodia de datos de firma en la introducción Actualizado el apartado referente a ley aplicable y quejas
04	20190613	Actualizado DIR3 Actualizado el apartado referencias con la LOPDGDD
05	20190930	Añadido un nuevo apartado con los términos y condiciones para la verificación del estado de los certificados
06	20200612	Actualizado el nombre del Ministerio Actualizado DIR3 Actualizado el apartado relativo a la verificación del estado de los certificados alineado con la DPC Añadido el anexo A para indicar las URL

Tabla de contenidos

1 Introducción

Este documento tiene una finalidad informativa y no sustituye en ningún caso a la Declaración de Prácticas de Certificación del Prestador de Servicios de Confianza del Ministerio (PSCM), en adelante DPCM, que es de obligatorio cumplimiento y conocimiento por los usuarios de los certificados.

La DPCM, publicada en la URL http://ca.empleo.gob.es/meyss/DPCyPoliticas, recoge la información pública de las condiciones y características de los servicios de confianza y servicios de expedición de certificados electrónicos por parte del PSCM como Prestador de Servicios de Confianza, recogiendo las obligaciones y procedimientos que se compromete a cumplir en relación con la expedición de estos tipos de certificados.

El artículo 3 del Reglamento (UE) 910/2014, define al firmante (titular de un certificado electrónico) como "una persona física que crea una firma electrónica", mientras que su anexo I indica que los certificados cualificados incluirán "al menos el nombre del firmante o un seudónimo".

Asimismo, el Reglamento (UE) 910/2014 define en su artículo 3.13) los «datos de creación de la firma electrónica» como "los datos únicos que utiliza el firmante para crear una firma electrónica". Por su parte, el artículo 24.1 de la Ley 59/2003 indica que "los datos de creación de firma son los datos únicos, como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica".

En este sentido, se limita la responsabilidad de los prestadores ante los daños y perjuicios causados, en caso de negligencia por parte del firmante en la conservación de sus datos de creación de firma, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación.

En consecuencia, **los certificados electrónicos son de uso personal e intransferible** y se deben tomar las precauciones necesarias para evitar el uso indebido de los mismos. **La posibilidad de que el titular/firmante de un certificado electrónico expedido a su nombre transfiera su posesión y revele sus claves de acceso a un tercero, no es conforme con la legislación vigente, nacional y comunitaria, en materia de servicios electrónicos de confianza**.

2 Datos de contacto del Prestador de Servicios de Confianza

Subdirección General de Tecnologías de la Información y las Comunicaciones

C/ Paseo de la Castellana 63

28071 Madrid

admin_ca@mtin.es / admin_ca@meyss.es

Teléfono: 91 363 11 88/9 - Fax: 91 363 07 73

3 Tipos de certificados

El PSCM emite, revoca y ofrece información de validación de los siguientes tipos de certificados:

1. El Certificado de Empleado Público[1] para firma electrónica se emplea para la firma electrónica de trámites o documentos electrónicos. Este certificado se expide en una tarjeta inteligente.
2. El Certificado de Empleado Público para autenticación se emplea para la identificación y autenticación de un empleado público (funcionario, laboral fijo, etc.) en sistemas y aplicaciones informáticas. Este certificado se expide en una tarjeta inteligente.
3. El Certificado de Empleado Público Centralizado y Gestionado por un HSM se emplea para la firma electrónica de trámites o documentos electrónicos y para la identificación y

[1] Todos los certificados de empleado público (en cualquiera de sus variedades) incluyen al titular y a la entidad pública en la que presta sus servicios el empleado público.

autenticación de un empleado público en sistemas y aplicaciones informáticas. Este certificado se expide y gestiona en un HSM.

4. El Certificado de Sello Electrónico de Administración Pública, órgano, organismo público o entidad de derecho público se emplea para la identificación y la actuación administrativa automatizada de las Administraciones Públicas.

Estos certificados electrónicos son cualificados[2] en cumplimiento con los requisitos del Reglamento eIDAS[3].

Puede comprobarse su inclusión en la lista de confianza de prestadores de servicios de confianza (TSL, por sus siglas en inglés) de España, a través de la sede electrónica del Organismo Supervisor, cuyo enlace es, https://sede.minetur.gob.es/

4 Límites de uso

Constituyen límites de uso de este tipo de certificados las diferentes competencias y funciones propias de las Administraciones Públicas suscriptoras actuando, en su caso, a través del personal a su servicio en calidad de firmante, de acuerdo con su cargo, empleo y condiciones de autorización.

Los certificados electrónicos emitidos por el PSCM caducan a los cinco años.

5 Obligaciones del suscriptor

Es obligación del suscriptor (titular) de cada tipo de certificado lo dispuesto en la DPCM y perfiles correspondientes incluyendo:

- Suministrar información exacta, completa y veraz con relación a los datos solicitados para la emisión del certificado e informar al PSCM de cualquier modificación de esta información.
- Conocer, aceptar y seguir las condiciones de utilización de los certificados. La aceptación se produce tras autenticarse correctamente y generar el certificado.
- Poner el cuidado y medios necesarios para garantizar la custodia de la clave privada asociada al certificado, evitando su pérdida, copia o uso no autorizados.
- Solicitar inmediatamente la revocación del certificado en caso de modificación de la información contenida en el mismo o sospecha de pérdida de fiabilidad de la clave privada asociada al certificado.
- No monitorizar, manipular o realizar actos de ingeniería inversa sobre el certificado y clave privada asociada.
- No transferir ni delegar a un tercero las responsabilidades sobre el certificado que le haya sido expedido.

6 Condiciones del servicio de verificación del estado de los certificados

El PSCM proporciona a cualquier parte interesada información sobre el estado de validez o revocación de los certificados cualificados que expide. Esta información está disponible para cada certificado en cualquier momento y con posterioridad al período de validez del certificado de forma pública, internacional, automatizada, fiable, gratuita y eficiente por medio del servicio OCSP y listas CRL.

[2] Excepto el Certificado de Empleado Público para autenticación

[3] Reglamento (UE) No 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

El PSCM asegura un nivel de servicio, garantizando la disponibilidad de todos los servicios de certificación ofrecidos y, en especial, los de información del estado de la vigencia de los certificados. El PSCM asegura la integridad y autenticidad de la información del estado de los certificados.

El servicio está disponible en línea 24 horas al día, 7 días a la semana. En caso de fallo del sistema, el PSCM lanzará el Plan de Continuidad de Negocio para solventar el incidente tan pronto como sea posible.

En el caso de compromiso de las claves de alguna Autoridad de Certificación (CA o SubCA) del PSCM se revocarán todos los certificados activos emitidos y se seguirá ofreciendo el servicio OCSP firmando las respuestas con un certificado emitido por una Entidad de Certificación distinta a la comprometida.

En el caso de caducidad de cualquier certificado de la CA o SubCA del PSCM: en un período anterior al momento de caducidad que será fijado en función del tiempo de validez de los certificados emitidos por dicha CA:

- se paralizará la emisión de nuevos certificados
- en un momento próximo a la fecha de caducidad se revisará si existe algún certificado emitido activo, revocándose en su caso y se emitirá una última CRL
- se seguirá ofreciendo el servicio OCSP firmando las respuestas con un certificado emitido por una Autoridad de Certificación distinta a la caducada.

En el caso de terminación del PSCM, este emitirá una última CRL que se publicará en el sitio web del PSCM indicado por el campo *cRLDistributionPoints* definido en la especificación técnica IETF RFC 5280[4]. Este sitio web será mantenido al menos durante 15 años por el departamento sustituto del Ministerio. El departamento sustituto del Ministerio decidirá la viabilidad del mantenimiento del servicio OSCP.

6.1 Servicio de verificación a través de CRL

En cada certificado emitido por el PSCM se especifica la dirección de la CRL que le corresponda, mediante la extensión *cRLDistributionPoints*. La lista de revocación de certificados de las entidades finales se emite al menos una vez cada 24 horas o bien cuando ocurre una revocación con un período de validez de 24 horas. La ubicación de la lista de certificados revocados se encuentra en el Anexo A: Enlaces (URL).

El cambio de estado de la vigencia de un certificado se indica en la CRL transcurridos menos de 5 minutos desde que se produjo dicho cambio. Esto implica que el retraso máximo entre la confirmación de la revocación del certificado, o su suspensión, para que sea efectivo y el cambio real en la información de su estado es de 5 minutos.

El PSCM no elimina de la CRL revocada certificados después de que estos hayan caducado e incluye la extensión X.509 *ExpiredCertsOnCRL* tal y como se define en la Recomendación ISO / IEC 9594-8 / UIT-T X.509[5].

En caso de emisión por parte del PSCM de una última CRL, esta se emitirá y publicará en el punto de distribución de CRL de acuerdo con lo especificado en la norma ETSI EN 319 411-1[6].

[4] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

[5] ISO/IEC 9594-8/Recommendation ITU-T X.509: "Information technology - Open Systems Interconnection - The Directory - Part 8: Public-key and attribute certificate frameworks".

[6] ETSI Europe 319 411-1. Policy and security requirements for Trust Service Providers issuing certificates. Part 1: General requirements

La última CRL existe al no haber ya más certificados válidos en el alcance de la CRL, cuando caduca el certificado que firma la CRL o cuando la clave privada del certificado que firma la CRL está fuera de servicio.

El PSCM preservará la integridad y la disponibilidad de la última CRL durante 15 años tal y como especifica la Ley 59/2003 de Firma Electrónica (LFE) usando preferiblemente firmas longevas de acuerdo con formatos estándar.

El PSCM no emitirá una última CRL hasta que todos los certificados en el ámbito de la CRL estén caducados o revocados.

6.2 Servicio de verificación a través de OCSP

El PSCM ofrece el servicio de verificación de estado de certificados mediante protocolo OCSP de acuerdo con la IETF RFC 6960[7] indicando esta circunstancia dentro de los certificados, mediante el empleo de la extensión Información de Acceso a Autoridad (*AuthorityInfoAccess*) definida en las especificaciones técnicas IETF RFC 6818[8] y IETF RFC 6960, de la siguiente forma:

- Se incluye una Descripción de Acceso, que contiene el OID reservado para el acceso a servicios OCSP y la URL en que se encuentra el servidor OCSP.

El servicio OCSP devuelve en su respuesta la extensión *ArchiveCutOff* tal y como se define en la norma IETF RFC 6960 con el valor *valid from* del certificado de la Entidad de Certificación en el campo fecha *archiveCutOff*.

La ubicación del servicio OCSP se encuentra en el Anexo A: Enlaces (URL).

El PSCM ofrecerá el servicio OCSP una vez caducado el certificado raíz o finalizado sus servicios de certificación de acuerdo con lo especificado por la LFE y la norma ETSI EN 319 411-1 desde la ubicación indicada en el campo de los certificados.

7 Obligaciones de verificación del estado de los certificados de las terceras partes

Cualquier tercera parte que confíe de manera razonable en un certificado deberá:

- Determinar que dicho certificado ofrece garantías suficientes para el uso apropiado definidos en la DPCM y perfiles asociados.
- Verificar la validez del certificado, asegurándose de que no ha caducado.
- Asegurarse de que el certificado no ha sido suspendido o revocado, accediendo a la información sobre el estado actual de revocación, disponible en la ubicación especificada en el propio certificado.

La validación del estado de vigencia de los certificados se puede comprobar a través del servicio de información y consulta del estado de los certificados que provee el PSCM mediante el protocolo OCSP, disponible en la ubicación especificada en los propios certificados.

8 Limitaciones de responsabilidad

El PSCM limita su responsabilidad a la emisión y gestión de certificados y, en su caso, de pares de claves de suscriptores y de dispositivos criptográficos suministrados por el PSCM (de autenticación, de firma y verificación de firma).

El PSCM incluye, en el documento que le vincula con el suscriptor, una cláusula por la cual el suscriptor se compromete a mantener indemne al PSCM de todo daño proveniente de cualquier

[7] IETF RFC 6960: "Internet X.509 Public Key Infrastructure Online Certificate Status Protocol - OCSP".
[8] IETF FRC 6818: “Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”.

acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Falsedad o manifestación errónea realizada por el usuario del certificado.
- Error del usuario del certificado al facilitar los datos de la solicitud, si en la acción u omisión medió dolo o negligencia con respecto al PSCM, la entidad de registro o cualquier persona que confía en el certificado.
- Negligencia en la protección de la clave privada, en el empleo de un sistema fiable o en el mantenimiento de las precauciones necesarias para evitar el compromiso, la pérdida, la divulgación, la modificación o el uso no autorizado de dicha clave.
- Empleo por el suscriptor de un nombre (incluyendo nombres comunes, dirección de correo electrónico y nombres de dominio), u otras informaciones en el certificado, que infrinja derechos de propiedad intelectual o industrial de terceros.

El tercero que confía en el certificado se compromete a mantener indemne al PSCM de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Incumplimiento de las obligaciones del tercero que confía en el certificado.
- Confianza temeraria en un certificado, a tenor de las circunstancias.
- Falta de comprobación del estado de un certificado, para determinar que no se encuentra suspendido o revocado.

El PSCM estará exento de toda responsabilidad ante los efectos que pudieran producirse por causas fortuitas o de fuerza mayor.

En caso de terminación de la actividad del Prestador de Servicios de Confianza, el PSCM informará debidamente y con antelación suficiente a los titulares de los certificados, así como a los usuarios de los servicios afectados y transferirá, con el consentimiento expreso de los titulares, aquellos certificados que sigan siendo válidos en la fecha efectiva de cese de actividad a otro Prestador de Servicios de Confianza que los asuma. De no ser posible esta transferencia la vigencia de los certificados quedará extinguida.

9 Política de privacidad y protección de datos

De acuerdo con el art. 14 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (Reglamento General de Protección de Datos Personales, RGPD) le comunicamos que la Subsecretaría del Ministerio de Trabajo y Economía Social (MTES) es responsable de todos los tratamientos de datos de carácter personal que se realicen para la prestación de servicios de confianza, esto es, para la gestión de certificados de empleado público y sello electrónico que emite el Ministerio.

La Subsecretaría, a través del Prestador de Servicios de Confianza constituido, realiza estos tratamientos de acuerdo con la normativa vigente en materia de protección de los datos personales, de seguridad de la información y la propia normativa específica que regula su actividad y que recoge todos los aspectos relativos a las condiciones en las que se pueden realizar tratamientos de datos de los interesados, principalmente el Estatuto Básico de Empleado Público, la ley 39/2015 y la ley 40/2015 que regulan el funcionamiento de la Administración General del Estado y sus Empleados Públicos.

En este sentido, se han adoptado las medidas técnicas y organizativas necesarias para evitar la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles

en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales. Las medidas adoptadas tienen en cuenta el estado de la tecnología, la naturaleza de los datos y los riesgos a los que están expuestos y se revisan periódicamente para garantizar su adaptación a nuevas situaciones o escenarios de riesgo.

La Subsecretaría, como responsable de todos los tratamientos de los datos de carácter personal de los interesados y de acuerdo con los requisitos de información al mismo recogidos en el artículo 14 del Reglamento (UE) 2016/679, indica a continuación la información básica relativa a estos tratamientos:

Responsable	Subsecretaría del Ministerio de Trabajo y Economía Social Paseo de la Castellana 63 Madrid 28071 España Correo electrónico: sgtic@meyss.es
DPD	Delegado de Protección de Datos Ministerio de Trabajo y Economía Social Paseo de la Castellana 63 Madrid 28071 España Correo electrónico: dpd@meyss.es
Finalidad	Gestión de la prestación de servicios de confianza incluyendo la gestión de los certificados electrónicos de empleado público y certificados electrónico de sello electrónico de acuerdo con el Estatuto Básico de Empleado Público y leyes 39 y 40/2015
Categoría de datos	Datos identificativos: NIF/DNI, nombre y apellidos, fecha de nacimiento, correo electrónico, puesto de trabajo, unidad a la que pertenece. Datos de características personales: claves pública y privada, número de serie del certificado, código de solicitud del certificado.
Origen de datos	Fichero de Empleados Públicos que desempeñan sus servicios en el Ministerio SG de Recursos Humanos Ministerio de Trabajo y Economía Social
Comunicaciones de datos	Comunicaciones a las fuerzas y cuerpos de seguridad del estado y órganos judiciales. Datos públicos del certificado.
Transferencias internacionales de datos	No se realizan transferencias fuera de la UE
Plazo de conservación	15 años de acuerdo con la normativa vigente
Tratamientos automatizados	No se realiza ninguna elaboración de perfiles con los datos de carácter personal

Derechos del interesado: los interesados podrán ejercer los derechos de acceso, rectificación, supresión (olvido), limitación de tratamiento, oposición y portabilidad de los datos, conforme a lo establecido en los artículos 15 a 22 del RGPD.

Cómo ejercer sus derechos: dirigiéndose al responsable del tratamiento por vía electrónica, o a través de cualquier Oficina de Atención en Materia de Registros tal y como dicta la ley 39/2015.

También podrá ponerse en contacto con el Delegado de Protección de Datos en lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos (art 38.4 RGPD).

Derecho a reclamar ante la Autoridad de Control: contacte con la Agencia Española de Protección de Datos: C/ Jorge Juan, 6. 28001. Madrid. España. (http://www.aepd.es).

10 Ley aplicable, quejas y resolución de disputas

La provisión de servicios de confianza del PSCM se regirá por lo dispuesto por las Leyes del Reino de España.

La ley aplicable a la prestación de los servicios, incluyendo la política y prácticas de certificación, es la ley española, en especial:

- La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- El Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, más conocido como reglamento eIDAS.
- El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos o RGPD).
- La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
- La Ley 59/2003, de 19 de diciembre, de Firma Electrónica (LFE).
- El Real Decreto 951/2005, de 29 de julio, por el que se establece el marco general para la mejora de la calidad en la Administración General del Estado.

El procedimiento para la presentación de quejas y sugerencias se puede consultar en la siguiente página:

http://www.mitramiss.gob.es/es/contacto_ministerio/quejasysugerencias/quejas.htm

Anexo A: Enlaces (URL)

Datos de contacto por correo electrónico de la organización:

admin_ca@meyss.es

DPCM, perfiles de certificados, Declaración Informativa (PDS) y Términos y Condiciones:

http://ca.empleo.gob.es/meyss/DPCyPoliticas

https://ca.empleo.gob.es/en/CA_MEYSS/declaracion.htm (versión en inglés)

Certificado raíz de la CA, de las SubCA y certificado OCSP:

http://ca.empleo.gob.es/meyss/certificados

Servicio de validación de OCSP:

http://ca.empleo.gob.es/meyss/ocsp

CRL Raíz - 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