MINISTERIO DE TRABAJO,
MIGRACIONES
Y SEGURIDAD SOCIAL

SUBSECRETARÍA

S.G. DE TECNOLOGÍAS DE LA
INFORMACIÓN Y COMUNICACIONES

Términos y condiciones de uso del Certificado de Empleado Público Centralizado y Gestionado por un HSM del Prestador de Servicios de Confianza del Ministerio

sgtic@meyss.es
EA0021880

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

Control de versiones

Identificador	D431
Título	Términos y condiciones de uso del Certificado de Empleado Público Centralizado y Gestionado por un HSM del Prestador de Servicios de Confianza del Ministerio
Versión	06
Estado del documento	Aprobado
Fecha de aprobación	20190613

Registro de Cambios

Versión	Fecha	Comentario
02	20170222	Versión inicial
03	20170508	Se añade portada Se amplían las condiciones de acuerdo al reglamento eIDAS
04	20170510	Añadida la revocación implícita
05	20180713	Cambio de nombre del ministerio Formato de fechas adaptado a ISO 8601: YYYYMMDD Cambios en la política de privacidad y protección de datos Cambio en el nombre del Organismo Supervisor
06	20190613	Actualización del DIR3 Eliminada la fecha de caducidad Añadida la aceptación implícita Actualización de la URL para presentación de quejas y sugerencias Actualización del Organismo Supervisor Actualización de las referencias con la LOPDGDD

Tabla de contenidos

1 Introducción 1
2 Tipo de certificado y límites de uso 1
3 Obligaciones del solicitante (suscriptor) 2
4 Obligaciones de verificación del estado de los certificados por las terceras partes 3
5 Limitaciones de responsabilidad 3
6 Ley aplicable, quejas y resolución de disputas 4
7 Licencias y repositorio, marcas confiables y auditoría 4
8 Datos de contacto del Prestador de Servicios de Confianza 5
9 Política de privacidad y protección de datos 5

1 Introducción

El presente documento recoge los términos y condiciones de uso del Certificado de Empleado Público Centralizado y Gestionado por un HSM (CEPCHSM), del Prestador de Servicios de Confianza del Ministerio de Trabajo, Migraciones y Seguridad Social (PSCM).

El Solicitante manifiesta que, una vez descargue e instale el Certificado de Empleado Público Centralizado y Gestionado por un HSM (CEPCHSM), utilizará el Certificado de conformidad con las condiciones adjuntas y atendiendo al contenido de la Declaración de Prácticas de Certificación del PSCM (DPCM) y Políticas de Certificación del PSCM disponibles en el sitio web https://ca.empleo.gob.es/ declarando expresamente que las acepta en toda su extensión.

Estas condiciones son un extracto de las Políticas de Certificación del PSCM, con las normas básicas para la expedición de estos certificados. Se pone a disposición del Solicitante la siguiente información básica y que, por razones de espacio, el deber de información quedará satisfecho con la DPCM y Políticas de Certificación del PSCM, puestas a disposición en formato digital en el anterior enlace.

2 Tipo de certificado y límites de uso

La Autoridad de Certificación del PSCM expide certificados de firma electrónica para empleados públicos, al servicio de la Administración Pública, órgano, organismo público o entidad de derecho público, en el ejercicio de sus funciones para el suscriptor del certificado.

El CEPCHSM confirma de forma conjunta, la identidad del personal al servicio de las Administraciones Públicas, el órgano, organismo o entidad de la Administración Pública, donde dicho personal ejerce sus competencias, presta sus servicios, o desarrolla su actividad y qué cargo desempeña en el mismo. También permite la autenticación del empleado público en sistemas y aplicaciones informáticas.

El CEPCHSM tiene como propósito que el empleado público pueda firmar trámites o documentos proporcionando las siguientes garantías:

- No repudio de origen.
- Integridad.

El CEPCHSM es el certificado previsto por la [Ley 39/2015] y en el artículo 43 de la [Ley 40/2015], para el personal al servicio de la Administración.

Estos certificados electrónicos son cualificados en cumplimiento con los requisitos del 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, y por la que se deroga la directiva 1999/93/CE.

La expedición y firma del Certificado se realizará por la "SubCA1 MEYSS" subordinada de la "CA Raíz MEYSS" del PSCM. La longitud de la clave utilizada en la "SubCA1 MEYSS" es de 4096 bits y en la "CA Raíz MEYSS" es de 4096 bits.

Los CEPCHSM expedidos por el PSCM tendrán validez durante un periodo máximo de cinco (5) años contados a partir del momento de la expedición del Certificado, siempre y cuando no se extinga su vigencia. Transcurrido este periodo y si el Certificado sigue activo, caducará, siendo necesaria la expedición de uno nuevo en caso de que se desee seguir utilizando los servicios del PSCM.

El CEPCHSM no podrá ser utilizado cuando expire su periodo de validez, cuando sea solicitada su revocación o se cumpla alguna de las otras causas de extinción de su vigencia, establecidas en la DPCM y en las Políticas de Certificación del PSCM. La solicitud de un nuevo CEPCHSM implica la revocación del CEPCHSM vigente en el momento de la solicitud.

La validación del estado de vigencia de este tipo de 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 el propio certificado. Estas condiciones de utilización no alteran o modifican la naturaleza, régimen jurídico y competencias de la Administración, Organismo o Entidad pública y del personal donde desarrolla su función pública o actividad, por lo que PSCM no será responsable de las actuaciones que este personal realice con los certificados emitidos por cuestiones que no tengan su origen, únicamente, en la organización y funcionamiento del PSCM en las condiciones expuestas en las Políticas y Prácticas de Certificación antes citadas.

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, pudiendo ser causa de revocación inmediata su uso indebido.

El PSCM no se responsabiliza del contenido de los documentos firmados con un CEPCHSM ni recomienda el uso del CEPCHSM y sus claves asociadas para cifrar ningún tipo de información. Queda fuera del ámbito de este documento y de la DPCM garantizar la viabilidad tecnológica de las aplicaciones que harán uso del CEPCHSM.

Ningún CEPCHSM debe utilizarse para actuar como Autoridad de Registro ni como Autoridad de Certificación (firmando certificados de clave pública de cualquier tipo o Listas de Certificados Revocados (CRL)).

Se garantiza que las claves privadas permanecen, con un alto nivel de confianza, bajo el control del empleado público titular del CEPCHSM. El titular deberá poner el cuidado y medios necesarios para garantizar la custodia de las claves de acceso a los certificados, evitando su pérdida, divulgación, modificación o uso no autorizado.

3 Obligaciones del solicitante (suscriptor)

El empleado público solicitante del CEPCHSM tiene la obligación de:

- Suministrar información exacta, completa y veraz con relación a los datos solicitados para la emisión del certificado, informar al PSCM de cualquier modificación de esta información y no usar el certificado cuando alguno de estos datos sea incorrecto.
- Conocer y aceptar las condiciones de utilización de los certificados. La aceptación del certificado electrónico y sus términos y condiciones de uso se produce al entrar en el portal para su generación, autenticarse y generar el mismo.
- Realizar un uso adecuado del Certificado en base a las competencias y facultades atribuidas por el cargo, puesto de trabajo o empleo como empleado público.
- Poner el cuidado y medios necesarios para garantizar la custodia de la contraseña que protege la clave privada del certificado, que se establece justo en el proceso de emisión del mismo. Evitar la pérdida, copia o uso no autorizado de dicha contraseña así como de cualquier otro factor de autenticación, que deberán estar bajo el control exclusivo del suscriptor del certificado.
- Solicitar inmediatamente la revocación del certificado en caso de detección de inexactitudes en la información contenida en el mismo o de tener conocimiento o sospecha de pérdida de fiabilidad de la contraseña que protege la clave privada asociada al certificado, entre otras causas por pérdida, compromiso, sospecha de copia o uso no autorizado. Las instrucciones para la revocación del certificado se encuentran disponibles en la Intranet del Departamento.
- No manipular o realizar actos de ingeniería inversa sobre el certificado.

- No transferir ni delegar a un tercero las responsabilidades sobre el certificado que le haya sido asignado.

4 Obligaciones de verificación del estado de los certificados por 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.
- 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.
- Asegurar que la confianza en los certificados emitidos bajo la política de certificación está restringida a los usos apropiados especificados en la DPCM y Políticas de Certificación del PSCM.

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.

El servicio de revocación y validación de certificados está disponible 24 horas al día, 7 días a la semana, salvo el tiempo mínimo obligatorio para operaciones de mantenimiento y resolución de incidentes graves.

5 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 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.

El PSCM registra y mantiene archivados aquellos eventos significativos necesarios para verificar la actividad de su Autoridad de Certificación durante un periodo nunca inferior a 15 años, conforme a la legislación aplicable.

6 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

7 Licencias y repositorio, marcas confiables y auditoría

El PSCM, como Prestador de Servicios de Confianza, mantiene varias acreditaciones y certificaciones de su infraestructura de clave pública, de las cuales aplican especialmente a estos tipos de certificados las siguientes:

- Expedición y administración de certificados electrónicos cualificados de conformidad con los estándares europeos ETSI EN 319 401 sobre Prestadores de Servicios de Confianza, ETSI

EN 319 411-1 sobre la emisión de certificados y ETSI EN 319 411-2 sobre la emisión de certificados cualificados. Esta auditoría se lleva a cabo con la periodicidad requerida y por un Organismo de Evaluación de la Conformidad acreditado para tal fin.

Los certificados de firma electrónica del personal al servicio de la Administración Pública, son cualificados conforme al Reglamento eIDAS. 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 del Organismo Supervisor en el enlace:

https://sede.minetur.gob.es/es-ES/datosabiertos/catalogo/lista-prestadores-tsl

8 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, Spain

admin_ca@mtin.es / admin_ca@meyss.es

Teléfono: + 34 91 363 11 88/9 - Fax: + 34 91 363 07 73

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, Migraciones y Seguridad Social (MITRAMISS) 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, Migraciones y Seguridad Social Paseo de la Castellana 63 Madrid 28071 España Correo electrónico: sgtic@meyss.es
DPD	Delegado de Protección de Datos Ministerio de Trabajo, Migraciones y Seguridad 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, Migraciones y Seguridad 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).