Texto de Divulgación (PDS) del Certificado de la Autoridad Cualificada de Sellado de Tiempo Electrónico

Índice

Certificado de sello electrónico de Autoridad Cualificada de Sellado de Tiempo Electrónico

TEXTO DIVULGATIVO - PDS

Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación de la Entidad de Certificación ESFIRMA.

Este documento sigue la estructura definida en el Anexo A de la norma ETSI EN 319 411-1, de acuerdo con las indicaciones del apartado 4.3.4 de la norma ETSI EN 319 412-5.

Información general

Control documental

Clasificación de seguridad:	Público
Entidad de destino:	ESFIRMA
Versión:	1.5

Control de versiones

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
1.0	Original	Creación del documento	esFIRMA	7/05/2017
1.4		Subsanaciones	esFIRMA	7/06/2017
1.5	1.1 -1.3 8.6	Cambio de denominación	esFIRMA	6/11/2017

1. Información de contacto

1.1. Organización responsable

La Entidad de Certificación ESFIRMA, en lo sucesivo "ESFIRMA", es una iniciativa de:

ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (esFIRMA)
CALLE BARI 39 (Edif. Binary Building)
50197 - ZARAGOZA
(+34) 976300110

1.2. Contacto

Para cualquier consulta, diríjanse a:

ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (esFIRMA)
CALLE BARI 39 (Edif. Binary Building)
50197 - ZARAGOZA
(+34) 976300110

1.3. Contacto para procesos de revocación

Para cualquier consulta, diríjanse a:

ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (esFIRMA)
CALLE BARI 39 (Edif. Binary Building)
50197 - ZARAGOZA
(+34) 976300110

2. Tipo y finalidad del certificado

Este certificado dispone del siguiente OID:

1.3.6.1.4.1.47281.1.5.2	De acuerdo con la jerarquía de esFIRMA
0.4.0.194112.1.1	De acuerdo con la política UE (QCP-l)

Los certificados de Autoridad de Sellado Cualificado de Tiempo Electrónico son certificados cualificados de acuerdo con el artículo 38 y el Anexo III del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por las normativas técnicas identificadas con las referencias ETSI EN 319 412-3, ETSI EN 319 421 y ETSI EN 319 422.

Estos certificados permiten la firma de evidencias digitales de tiempo electrónico.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo “key usage” tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
    a. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
b) En el campo “extKeyUsage” se dispone de forma activada de la indicación:
    a. “timeStamping” para realizar la función de sellado de tiempo electrónico.
c) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
    a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
d) El campo “User Notice” describe el uso de este certificado.

2.1. Entidad de Certificación emisora

Estos certificados son emitidos por ESFIRMA, identificada mediante los datos indicados anteriormente.

3. Límites de uso del certificado

3.1. Límites de uso dirigidos a los firmantes

Se debe utilizar el servicio de sellado cualificado de tiempo electrónico, prestado por ESFIRMA exclusivamente para los usos autorizados en el contrato firmado entre ESFIRMA y el SUSCRIPTOR, y que se reproducen posteriormente (sección "obligaciones de los firmantes").

Se debe utilizar el servicio de sellado de tiempo electrónico de acuerdo con las instrucciones, manuales o procedimientos suministrados por ESFIRMA.

Se debe cumplir cualquier ley y regulación que pueda afectar al uso de las herramientas criptográficas que emplee.

No se pueden adoptar medidas de inspección, alteración o ingeniería inversa de los servicios de sellado de tiempo electrónico de ESFIRMA, sin previo permiso expreso.

3.2. Límites de uso dirigidos a los verificadores

Los certificados se emplean para su función propia y finalidad establecida, sin que puedan emplearse en otras funciones y con otras finalidades.

Del mismo modo, los certificados deben emplearse únicamente de acuerdo con la ley aplicable, especialmente teniendo en cuenta las restricciones de importación y exportación existentes en cada momento.

Los certificados no pueden emplearse para firmar peticiones de emisión, renovación, suspensión o revocación de certificados, ni para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados (LRC).

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de fallos, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un fallo pudiera directamente conllevar la muerte, lesiones personales o daños medioambientales severos.

Se deben tener en cuenta los límites indicados en los diversos campos de los perfiles de certificados, visibles en el web de ESFIRMA https://www.esfirma.com

El empleo de los certificados digitales en operaciones que contravienen este texto de divulgación (PDS), o los contratos con los suscriptores, tiene la consideración de uso indebido a los efectos legales oportunos, eximiéndose por tanto a ESFIRMA, en función de la legislación vigente, de cualquier responsabilidad por este uso indebido de los certificados que realice el firmante o cualquier tercero.

Asimismo, le será imputable al suscriptor cualquier responsabilidad que pudiese derivarse de la utilización del mismo fuera de los límites y condiciones de uso recogidas en este texto de divulgación, o en los contratos con los suscriptores, así como de cualquier otro uso indebido del mismo derivado de este apartado o que pueda ser interpretado como tal en función de la legislación vigente.

4. Obligaciones de los suscriptores

4.1. Generación de claves

El suscriptor autoriza a ESFIRMA a generar las claves, privada y pública, para la emisión de este certificado.

4.2. Solicitud de certificados

El suscriptor se obliga a realizar las solicitudes, cuando sea necesario, de estos certificados de acuerdo con el procedimiento y, si es necesario, los componentes técnicos suministrados por ESFIRMA, de conformidad con lo que se establece en la declaración de prácticas de certificación (DPC) y en la documentación de operaciones de ESFIRMA.

4.3. Obligaciones de información

El suscriptor se responsabiliza de que toda la información incluida en su solicitud del certificado sea exacta, completa para la finalidad del certificado y esté actualizada en todo momento.

El suscriptor tiene que informar inmediatamente a ESFIRMA:

- De cualquier inexactitud detectada en el certificado una vez se haya emitido.
- De los cambios que se produzcan en la información aportada y/o registrada para la emisión del certificado.
- De la pérdida, robo, sustracción, o cualquier otro tipo de pérdida de control de la clave privada por el custodio.

4.4. Obligaciones de custodia

El suscriptor se obliga a custodiar toda la información que genere en su actividad como entidad de registro.

A custodiar el código de identificación personal o cualquier soporte técnico entregado por ESFIRMA, las claves privadas y, si fuese necesario, las especificaciones propiedad de ESFIRMA que le sean suministradas.

En caso de pérdida o robo de la clave privada del certificado, o en caso de que se sospeche que la clave privada ha perdido fiabilidad por cualquier motivo, dichas

circunstancias han de ser notificadas inmediatamente a ESFIRMA por medio del suscriptor.

4.5. Obligaciones de uso correcto

Se debe utilizar el certificado exclusivamente para los usos autorizados en la DPC y en cualquier otra instrucción, manual o procedimiento suministrado al suscriptor.

Se debe cumplir cualquier ley y regulación que pueda afectar a su derecho de uso de las herramientas criptográficas empleadas.

No se podrán adoptar medidas de inspección, alteración o descompilación de los servicios de certificación digital prestados.

Además:

a) Que cuando se utilice cualquier certificado, y mientras el certificado no haya expirado ni haya sido suspendido o haya sido revocado, se habrá aceptado dicho certificado y estará operativo.

b) Que no se actúa como entidad de certificación y, por lo tanto, se obliga a no utilizar las claves privadas correspondientes a las claves públicas contenidas en los certificados con el propósito de firmar certificado alguno.

c) Que en caso de quedar comprometida la clave privada, su uso queda inmediata y permanentemente suspendido.

4.6. Transacciones prohibidas

Se indica la obligación a no utilizar las claves privadas, los certificados o cualquier otro soporte técnico entregado por ESFIRMA en la realización de transacción alguna prohibida por la ley aplicable.

Los servicios de certificación digital (y los de sellado de tiempo electrónico) prestados por ESFIRMA no han sido diseñados ni permiten su utilización o reventa como equipos de control de situaciones peligrosas, o para usos que requieran actuaciones a prueba de errores, como la operación de instalaciones nucleares, sistemas de navegación o comunicación aérea, sistemas de control de tráfico aéreo o sistemas de control de armamento, en las que un error pudiera directamente causar la muerte, daños físicos o daños medioambientales graves.

5. Obligaciones de los verificadores

5.1. Decisión informada

ESFIRMA informa al verificador que tiene acceso a información suficiente para tomar una decisión informada en el momento de verificar un certificado y confiar en la información contenida en dicho certificado.

Adicionalmente, el verificador reconocerá que el uso del Registro y de las Listas de Revocación de Certificados (en lo sucesivo, "las LRCs" o "las CRLs) de ESFIRMA, se rigen por la DPC de ESFIRMA y se comprometerá a cumplir los requisitos técnicos, operativos y de seguridad descritos en la mencionada DPC.

5.2. Requisitos de verificación del sello de tiempo

La comprobación será ejecutada normalmente de forma automática por el software del verificador y, en todo caso, de acuerdo con la DPC, con los siguientes requisitos:

- Es necesario utilizar el software apropiado para la verificación de un sello de tiempo con los algoritmos y longitudes de claves autorizados en el certificado y/o ejecutar cualquier otra operación criptográfica, y establecer la cadena de certificados en que

se basa el sello de tiempo a verificar, ya que éste se verifica utilizando esta cadena de certificados.

- Es necesario asegurar que la cadena de certificados identificada es la más adecuada para el sello de tiempo que se verifica, ya que un sello de tiempo puede basarse en más de una cadena de certificados, y es decisión del verificador asegurarse el uso de la cadena más adecuada para verificarla.

- Es necesario comprobar el estado de revocación de los certificados de la cadena con la información suministrada al Registro de ESFIRMA (con LRCs, por ejemplo) para determinar la validez de todos los certificados de la cadena de certificados, ya que únicamente puede considerarse correctamente verificado un sello de tiempo si todos y cada uno de los certificados de la cadena son correctos y se encuentran vigentes.

- Es necesario asegurar que todos los certificados de la cadena autorizan el uso de la clave privada por el suscriptor del certificado, ya que existe la posibilidad de que alguno de los certificados incluya límites de uso que impidan confiar en el sello de tiempo que se verifica. Cada certificado de la cadena dispone de un indicador que hace referencia a las condiciones de uso aplicables, para su revisión por los verificadores.

- Es necesario verificar técnicamente la firma de todos los certificados de la cadena antes de confiar en el certificado utilizado para el sellado de tiempo electrónico.

5.3. Confianza en un certificado no verificado

Si el verificador confía en un certificado no verificado, asumirá todos los riesgos derivados de esta actuación.

5.4. Uso correcto y actividades prohibidas

El verificador se obliga a no utilizar ningún tipo de información de estado de los certificados o de ningún otro tipo que haya sido suministrada por ESFIRMA, en la realización de transacción alguna prohibida para la ley aplicable a la citada transacción.

El verificador se obliga a no inspeccionar, interferir o realizar ingeniería inversa de la implantación técnica de los servicios públicos de sellado de tiempo electrónico o de certificación de ESFIRMA, sin previo consentimiento escrito.

Adicionalmente, el verificador se obliga a no comprometer intencionadamente la seguridad de los servicios públicos de sellado de tiempo electrónico ni de certificación de ESFIRMA.

Los servicios de sellado de tiempo electrónico y de certificación digital prestados por ESFIRMA no han sido diseñados ni permiten la utilización o reventa, como equipos de control de situaciones peligrosas o para usos que requieran actuaciones a prueba de errores, como la operación de instalaciones nucleares, sistemas de navegación o comunicación aérea, sistemas de control de tráfico aéreo, o sistemas de control de armamento, donde un error podría causar la muerte, daños físicos o daños medioambientales graves.

5.5. Cláusula de indemnidad

El tercero que confía en el certificado se compromete a mantener indemne a ESFIRMA 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.
- Falta de comprobación de la totalidad de medidas de aseguramiento prescritas en la DCP o resto de normas de aplicación.

ESFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

6. Obligaciones de ESFIRMA

6.1. En relación con la prestación de certificación digital

ESFIRMA se obliga a:

a) Emitir, entregar, administrar, suspender, revocar y renovar certificados, de acuerdo con las instrucciones suministradas por el suscriptor, en los casos y por los motivos descritos en la DPC de ESFIRMA.

b) Ejecutar los servicios con los medios técnicos y materiales adecuados, y con personal que cumpla las condiciones de cualificación y experiencia establecidas en la DPC.

c) Cumplir los niveles de calidad del servicio, en conformidad con lo que se establece en la DPC, en los aspectos técnicos, operativos y de seguridad.

d) Notificar al suscriptor, con anterioridad, la fecha de expiración de los certificados.

e) Comunicar a las terceras personas que lo soliciten, el estado de los certificados, de acuerdo con lo que se establece en la DPC para los diferentes servicios de verificación de certificados.

6.2. En relación con las comprobaciones del registro

ESFIRMA se obliga a la emisión de certificados en base a los datos suministrados por el suscriptor, por lo cual podrá realizar las comprobaciones que considere oportunas.

En el caso que ESFIRMA detecte errores en los datos que se deben incluir en los certificados o que justifican estos datos, podrá realizar los cambios que considere necesarios antes de emitir el certificado o suspender el proceso de emisión y gestionar con el suscriptor la incidencia correspondiente. En caso de que ESFIRMA corrija los datos sin gestión previa de la incidencia correspondiente con el suscriptor, deberá notificar los datos finalmente certificados al suscriptor.

ESFIRMA se reserva el derecho a no emitir el certificado, cuando considere que la justificación documental resulte insuficiente para la correcta identificación y autenticación del suscriptor y/o del dominio.

Las anteriores obligaciones quedarán en suspenso en los casos en que el suscriptor actúe como autoridad de registro y disponga de los elementos técnicos correspondientes a la generación de claves, emisión de certificados y grabación de dispositivos de firma corporativos.

6.3. Periodos de conservación

ESFIRMA archiva los registros correspondientes a las solicitudes de emisión y revocación de certificados durante al menos 15 años.

ESFIRMA almacena la información de los logs durante un periodo de entre 1 y 15 años, en función del tipo de información registrada.

7. Garantías limitadas y rechazo de garantías

7.1. Garantía de ESFIRMA por los servicios de certificación digital

ESFIRMA garantiza al suscriptor:

- Que no hay errores de hecho en las informaciones contenidas en los certificados, conocidos o realizados por la Entidad de Certificación.

- Que no hay errores de hecho en las informaciones contenidas en los certificados, debidos a falta de la diligencia debida en la gestión de la solicitud de certificado o en la creación del mismo.

- Que los certificados cumplen con todos los requisitos materiales establecidos en la DPC.

- Que los servicios de revocación y el empleo del depósito cumplen con todos los requisitos materiales establecidos en la DPC.

ESFIRMA garantiza al tercero que confía en el certificado:

- Que la información contenida o incorporada por referencia en el certificado es correcta, excepto cuando se indique lo contrario.

- En caso de certificados publicados en el depósito, que el certificado ha sido emitido al suscriptor y dominio identificado en el mismo y que el certificado ha sido aceptado.

- Que en la aprobación de la solicitud de certificado y en la emisión del certificado se han cumplido todos los requisitos materiales establecidos en la DPC.

- La rapidez y seguridad en la prestación de los servicios, en especial de los servicios de revocación y depósito.

Adicionalmente, ESFIRMA garantiza al suscriptor y al tercero que confía en el certificado:

- Que el certificado contiene las informaciones que debe contener un certificado cualificado de sello electrónico, de acuerdo con el Anexo III del Reglamento UE 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014, y con las indicaciones adicionales para la creación de sellos cualificados de tiempo de acuerdo con el artículo 42 de este mismo Reglamento.

- Que, en el caso de que genere las claves privadas del suscriptor se mantiene su confidencialidad durante el proceso.

- La responsabilidad de la Entidad de Certificación, con los límites que se establezcan. En ningún caso ESFIRMA responderá por caso fortuito y en caso de fuerza mayor.

7.2. Exclusión de la garantía

ESFIRMA rechaza toda otra garantía diferente a la anterior que no sea legalmente exigible.

Específicamente, ESFIRMA no garantiza software alguno utilizado por cualquier persona para firmar, verificar firmas, cifrar, descifrar, o utilizar de otra forma certificado digital alguno emitido por ESFIRMA, excepto en los casos en que exista una declaración escrita en sentido contrario.

8. Acuerdos y políticas

8.1. Acuerdos aplicables

Los acuerdos aplicables a este certificado son los siguientes:

- Contrato de servicios de certificación, que regula la relación entre ESFIRMA y la empresa suscriptora de los certificados.

- Condiciones generales del servicio incorporadas en el texto de divulgación del certificado o PDS.

- DPC, que regula la emisión y utilización de los certificados.

8.2. DPC

Los servicios de certificación y de sellado de tiempo de ESFIRMA se regulan técnicamente y operativamente por la DPC de ESFIRMA, por sus actualizaciones posteriores, así como por documentación complementaria.

La DPC y la documentación de operaciones se modifica periódicamente en el Registro y se puede consultar en la página de Internet: https://www.esfirma.com

8.3. Política de intimidad

ESFIRMA no puede divulgar ni puede ser obligada a divulgar información confidencial alguna en lo referente a certificados sin una solicitud específica previa que provenga de:

a) La persona con respecto a la cual ESFIRMA tiene el deber de mantener la información confidencial, o

b) Una orden judicial, administrativa o cualquier otra prevista en la legislación vigente.

Sin embargo, el suscriptor acepta que determinada información, personal y de otro tipo, proporcionada en la solicitud de certificados, sea incluida en sus certificados y en el mecanismo de comprobación del estado de los certificados, y que la información mencionada no tenga carácter confidencial, por imperativo legal.

ESFIRMA no cede a ninguna persona los datos entregados específicamente para la prestación del servicio de certificación.

8.4. Política de privacidad

ESFIRMA dispone de una política de privacidad en el apartado 9.4 de la DPC, y regulación específica de la privacidad en relación con el proceso de registro, la confidencialidad del registro, la protección del acceso a la información personal, y el consentimiento del usuario.

Asimismo, se contempla que la documentación justificativa de la aprobación de la solicitud debe ser conservada y debidamente registrada y con garantías de seguridad e integridad durante el plazo de 15 años desde la expiración del certificado, incluso todo en caso de pérdida anticipada de vigencia por revocación.

8.5. Política de reintegro

ESFIRMA no reintegrará el coste del servicio de certificación en ningún caso.

8.6. Ley aplicable y jurisdicción competente

Las relaciones con ESFIRMA se regirán por la ley española en materia de servicios de confianza vigente en cada momento, así como por la legislación civil y mercantil en lo que sea de aplicación.

La jurisdicción competente es la que se indica en la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

En caso de discrepancia entre las partes, las partes intentarán la previa resolución amistosa. A tal fin, las partes deberán dirigir una comunicación a esFIRMA por cualquier medio que deje constancia a la dirección de contacto indicada en el punto de información de contacto de esta PDS.

Si las partes no alcanzasen un acuerdo al respecto, cualquiera de ellas podrá someter el conflicto a la jurisdicción civil, con sujeción a los Tribunales del domicilio social de ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA.

8.7. Acreditaciones y sellos de calidad

Sin estipulación.

8.8. Vinculación con la lista de prestadores

http://www.minetur.gob.es/telecomunicaciones/es-es/servicios/firmaelectronica/paginas/prestadores.aspx

8.9. Divisibilidad de las cláusulas, supervivencia, acuerdo íntegro y notificación

Las cláusulas del presente texto de divulgación son independientes entre sí, motivo por el cual, si cualquier cláusula es considerada inválida o inaplicable, el resto de cláusulas de las PDS seguirán siendo aplicables, excepto acuerdo expreso en contrario de las partes.

Los requisitos contenidos en las secciones 9.6.1 (Obligaciones y responsabilidad), 8 (Auditoría de conformidad) y 9.3 (Confidencialidad) de la DPC de ESFIRMA continuarán vigentes tras la terminación del servicio.

Este texto contiene la voluntad completa y todos los acuerdos entre las partes.

Las partes se notifican hechos mutuamente mediante un procedimiento de envío de email a la dirección info@esfirma.com