DIGITELTS

by MADISON®

PDS Servicio de sellado de tiempo

DIGITELTS Qualified Trust Service Provider

Control documental

Líder	Área de servicios de confianza		
Tipo	Texto de Divulgación (PDS)		
Distribución	**Público**		
Fecha	2024		
Descripción	PDS SERVICIO CUALIFICADO DE SELLADO DE TIEMPO		
Aprobado	Gerencia área de Servicios de Confianza	Fecha	5 junio 2023
Estado	Aprobado		

Control de Cambios

Versión	Fecha	Detalle
V1.0	Abril 2024	Versión Inicial
V1.1	Junio 2024	Corrección de erratas punto 1.1.3 Mejora redacción punto 1.2 Adecuación estilo del documento Adecuación de obligaciones de los subuscriptores, autoridad de certificación y verificadores punto 1.7 y 1.8 y 1.9 Modificación del punto 1.13. Acreditaciones y sellos de calidad

1 Introducción

Este documento contiene las informaciones esenciales a conocer en relación con el servicio cualificado de sellado de tiempo electrónico de la Autoridad de Certificación de DIGITELTS.

Este documento sigue la estructura definida en el Anexo B de la norma ETSI EN 319 421-1.

1.1 Acuerdo completo

El presente documento proporciona declaraciones de alto nivel con respecto al servicio de Sellado cualificado de tiempo electrónico de la Autoridad de Certificación de DIGITEL TS.

1.1.1 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 esta TSADS seguirán siendo aplicables, excepto acuerdo expreso en contrario de las partes.

Los requisitos contenidos en las secciones de Obligaciones y responsabilidad", de "Auditoría de conformidad" y de "Confidencialidad" de la DPC de la Autoridad de Certificación de DIGITELTS 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 envío email a las siguientes direcciones:

- pki@digitelts.es por parte de la Autoridad de Certificación de DIGITELTS.
- La dirección electrónica, indicada por el suscriptor en el contrato con la Autoridad de Certificación de DIGITELTS.

1.1.2 Información de contacto

La Autoridad de Sellado Cualificado de Tiempo Electrónico de DIGITELTS, en lo sucesivo “la Autoridad de Certificación de DIGITELTS”, es una iniciativa de:

DIGITEL ON TRUSTED SERVICES S.L.U

Contacto

C/ Enrique Cubero, 9, 47014 Valladolid (España)

Teléfono: +34 91 015 05 10

Contacto para procesos de revocación

Email: pki@digitelts.es

1.1.3 Tipos y usos de los sellos de tiempo electrónico

El servicio de sellado cualificado de tiempo electrónico sigue las indicaciones de la PDS del Certificado de TSA con el OID: 1.3.6.1.4.1.54225.10.1.1

Los sellos cualificados de tiempo electrónico disponen del OID: 0.4.0.2023.1.1

Los sellos de tiempo electrónico declarados como cualificados siguen las indicaciones del Reglamento UE 910/2014 y son de conformidad con los estándares europeos ETSI EN 319 421 y ETSI EN 319 422.

Los sellos de tiempo se encuentran dentro de la jerarquía de la Autoridad de Certificación de DIGITELTS, en la que la autoridad raíz dispone del CN = DIGITEL TS CA ROOT 01

Los algoritmos utilizados para la creación de los sellos de tiempo electrónico son SHA-256 , SHA-384 y SHA-512.

Los clientes que reciben este servicio de sellado electrónico están obligados a cumplir con lo dispuesto por la normativa vigente, a respetar lo indicado en los contratos firmados con esta Autoridad de Sellado, verificar la corrección de la firma del sello de tiempo, la validez del certificado de la TSA, así como verificar que el hash del sello de tiempo coincide con el que se envió.

1.2 Validación de certificados

La comprobación del estado de los certificados se realiza desde:

Acceso al servicio de OCSP en: http://ocsp.pki.digitelts.es, utilizando el certificado de ocsp de necesario para la validación en la web https://pki.digitelts.es/

Descarga de las CRL desde la dirección DIGITEL TS QUALIFIED CA TSA G1 crl1 o DIGITEL TS QUALIFIED CA TSA G1 crl2.

1.3 Subscriptores

El Suscriptor es la persona física o jurídica que ha contratado los servicios de sellado de tiempo electrónico de la Autoridad de Certificación de DIGITELTS.

1.4 Entidad de Sellado emisora

Los servicios de sellado cualificado de tiempo electrónico son emitidos por la TSA de la Autoridad de Certificación de DIGITELTS, identificada mediante los datos indicados anteriormente.

1.5 Comunidad de usuarios y aplicabilidad

Los usuarios del servicio serán principalmente las aplicaciones y/o sistemas de los clientes (personas físicas o jurídicas) que han contratado estos servicios de la Autoridad de Certificación de DIGITELTS.

Los servicios de sellado de tiempo electrónico proporcionados por la TSA de la Autoridad de Certificación de DIGITELTS se incluyen como servicios proporcionados por la Autoridad de

Certificación de DIGITELTS, ante el supervisor nacional, cumpliendo las normativas técnicas y legales vigentes.

1.6 Límites de uso del certificado

Los sellos de tiempo electrónico limitan su uso en las aplicaciones y/o sistemas de los clientes (personas físicas o jurídicas) que han contratado estos servicios.

No se utilizarán los sellos de tiempo electrónico para fines distintos de los especificados anteriormente.

1.6.1 Exactitud de la hora en el sello cualificado de tiempo electrónico

Los registros están fechados con una fuente fiable vía NTP con conexión a la plataforma EQUINIX.

Los servidores de la Autoridad de Certificación de DIGITELTS están conectados a las fuentes primarias Equinix Precision Time NTP, con un nivel Stratum 1, desde Frankfurt, balanceada mediante dos IP como fuentes de tiempo en los appliance de la Autoridad de Certificación.

Los sistemas que proporcionan el sellado de tiempo se mantendrán en todo momento sincronizados con las fuentes de tiempo asegurando una desviación máxima de 1 segundo (Accuracy).

1.6.2 Usuarios

Las partes usuarias son las personas y las organizaciones que precisan confiar en los sellos de tiempo electrónicos.

Como paso previo a confiar en los certificados, las partes usuarias deben verificarlos, como se establece en esta declaración de prácticas de confianza y, en su caso, en las correspondientes instrucciones disponibles en la página web de la Autoridad de Certificación de DIGITELTS. la Autoridad de Certificación de DIGITELTS https://pki.digitelts.es

1.7 Obligaciones y responsabilidades

DIGITELTS, como Entidad que emite sellos de tiempo de acuerdo con la presente Política de Sellado de Tiempo asume las siguientes obligaciones:

1.7.1 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:

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

1.7.2 Obligaciones de la Entidad Emisora de Sellos de Tiempo

La Autoridad de Sellado de Tiempo de DIGITELTS:

- Emite tokens de sello de tiempo (TST) seguros para usuarios de servicios de sellado de tiempo (se incluyen tanto suscriptores como terceras partes.
- Asume la responsabilidad de proporcionar los servicios de sellado de tiempo.

- Puede operar con diferentes unidades identificables de sellado de tiempo (TSUs), cada una de las cuales puede tener su propia clave de firma.
- Está identificada en el certificado digital utilizado para los servicios de sellado de tiempo.
- Ofrece sus servicios a todos los suscriptores y terceras partes verificadoras de sellos de tiempo que se comprometan a cumplir con sus obligaciones
- Garantizar que la hora y fecha incluidas en los sellos se mantienen dentro de los márgenes precisión establecida en el contrato entre el cliente y DIGITEL TS que en ningún caso pueden ser superiores a un segundo.
- Emitir sellos de tiempo según la información enviada por el cliente y libres de errores de entrada de datos.
- Establecer los mecanismos de generación de la información relevante en las actividades descritas, protegiéndolas ante pérdida, destrucción o falsificación

1.7.3 Obligaciones del suscriptor de sellos de tiempo

El suscriptor de sellos de tiempo puede utilizar el Servicio de Sellado de Tiempo únicamente según especificaciones de ETSI EN 319 422.

El suscriptor debe verificar que el token de sello de tiempo ha sido correctamente firmado por la autoridad de sellado de tiempo, y que la clave privada utilizada para firmar el token de sello de tiempo no ha sido revocado.

El suscriptor debe cumplir con la presente Política de Sellado de Tiempo de DIGITELTS, disponible en https://pki.digitelts.es/

1.7.4 Obligaciones de terceras partes verificadoras de sellos de tiempo

Cuando se recibe un token de sello de tiempo, la tercera parte debe verificar que el token está correctamente firmado y que la clave privada utilizada para firmar el sello de tiempo no ha sido revocada.

Mientras el certificado utilizado para generar sellos de tiempo no esté caducado, es posible comprobar su validez en la CRL o OCSP correspondiente.

En el caso de que la verificación se realice después del periodo de validez del certificado, la tercera parte deberá comprobar que la función hash empleada, los algoritmos y longitud de claves criptográficas se pueden seguir considerando seguras.

1.7.5 Efecto de la verificación

En virtud de la correcta verificación de los certificados de sello de tiempo electrónico, de conformidad con este texto divulgativo (TSADS), el verificador puede confiar en la información suministrada.

1.7.6 Uso correcto y actividades prohibidas

El verificador se obliga a no utilizar ningún tipo de información de estado de los sellos cualificados de tiempo electrónico o de ningún otro tipo que haya sido suministrada por la Autoridad de Certificación de DIGITELTS, 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 certificación de la Autoridad de Certificación de DIGITELTS, sin previo consentimiento escrito.

Adicionalmente, el verificador se obliga a no comprometer intencionadamente la seguridad de los servicios públicos de sellado de tiempo de la Autoridad de Certificación de DIGITELTS.

Los servicios de sellado cualificado de tiempo electrónico prestados por la Autoridad de Certificación de DIGITELTS 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.

1.8 Garantías limitadas y rechazo de garantías

1.8.1 Garantía de la Autoridad de Certificación de DIGITELTS por los servicios de sellado cualificado de tiempo electrónico

La Autoridad de Certificación de DIGITELTS garantiza al suscriptor que los sellos de tiempo cumplen con todos los requisitos materiales establecidos en la DPC.

La Autoridad de Certificación de DIGITELTS garantiza al tercero que confía en el sello cualificado de tiempo electrónico que la información contenida o incorporada por referencia en el sello es correcta, excepto cuando se indique lo contrario.

Adicionalmente, la Autoridad de Certificación de DIGITELTS garantiza al suscriptor y al tercero que confía en el sello de tiempo la responsabilidad de la Autoridad de Certificación, con los límites que se establezcan, sin que en ningún caso la Autoridad de Certificación de DIGITELTS responda por caso fortuito y en caso de fuerza mayor.

La Autoridad de Certificación de DIGITELTS no será responsable de los daños y perjuicios ocasionados en los términos indicados en el artículo 11 de Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

1.8.2 Exclusión de la garantía

La Autoridad de Certificación de DIGITELTS rechaza toda otra garantía diferente a la anterior que no sea legalmente exigible.

1.9 Acuerdos aplicables y DPC

1.9.1 Acuerdos aplicables

Los acuerdos aplicables al sello cualificado de tiempo electrónico son los siguientes:

- Contrato de servicios de sellado electrónico, que regula la relación entre la Autoridad de Certificación de DIGITELTS y la empresa que ha contratado los sellos cualificados de tiempo electrónico.
- Condiciones generales del servicio incorporadas en el texto de divulgación (PDS) del certificado de la TSA.
- Las condiciones incorporadas en este texto de divulgación-TSADS de los sellos de tiempo electrónico
- DPC, que regulan la emisión y utilización de los certificados de sello de tiempo electrónico.

1.9.2 DPC

Los servicios de sellado cualificado de tiempo electrónico de la Autoridad de Certificación de DIGITELTS se regulan técnicamente y operativamente por la DPC de la Autoridad de Certificación de DIGITELTS, 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://pki.digitelts.es

1.10 Política de privacidad

Ver apartado 9.4 de la DPC de la Autoridad de Certificación de DIGITELTS

1.11 Política de reintegro

La Autoridad de Certificación de DIGITELTS no reintegrará el coste del servicio de sellado en ningún caso.

1.12 Ley aplicable, jurisdicción competente y régimen de reclamaciones y disputas

Las relaciones con la Autoridad de Certificación de DIGITELTS 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 la Autoridad de Certificación de DIGITELTS por cualquier medio que deje constancia a la dirección de contacto indicada en el punto 1 de este documento.

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 la Autoridad de Certificación de DIGITELTS.

1.13 Acreditaciones y sellos de calidad

La Autoridad de Certificación de DIGITELTS se encuentra incluida en la lista de prestadores de confianza (TSL) española https://sedediatid.mineco.gob.es/Prestadores/Paginas/Inicio.aspx

1.14 Auditorías de conformidad

De acuerdo con lo indicado en el Reglamento UE 910/2014, la Autoridad de Certificación de DIGITELTS realizará auditorías de conformidad cada 2 años y de seguimiento en los años intermedios.