


DIGITELTS

by MADISON™

POLITICA DE SELLADO DE TIEMPO

DIGITEL ON TRUSTED SERVICES -

OID: 1.3.6.1.4.1.54225


	Área: EXPLOTACIÓN	Asunto: Certificación e-IDAS
		Proyecto: Política de Sellado de Tiempo
Autor/es: DIGITEL TS	Fecha: 10/08/2021	Versión: 10.0

Control de ediciones

Fecha	Versión	Descripción	Autor
29/03/2019	1.0	Versión Inicial	DIGITEL TS
16/05/2019	2.0	Modificaciones	DIGITEL TS
11/07/2019	3.0	Modificaciones tras Fase I eIDAS	DIGITEL TS
20/08/2019	4.0	Revisión punto 7 tras Fase II eIDAS	DIGITEL TS
29/11/2019	5.0	Modificación diferentes apartados para alineamiento pleno con la cualificación del servicio	DIGITEL TS
18/05/2020	6.0	Modificación apartado 6	DIGITEL TS
19/08/2020	7.0	Modificación tras auditoria eIDAS año 2020. Algoritmo empleado y OID.	DIGITEL TS
20/10/2020	8.0	Modificación precisión Accuracy.	DIGITEL TS
29/01/2021	9.0	Revisión tras implantación de segunda TSU	DIGITEL TS
10/08/2021	10.0	Revisión anual. Actualización fuentes NTP. Actualización algoritmos permitidos.	DIGITEL TS


DERECHOS DE USO:

La presente documentación es propiedad de DIGITEL ON TRUSTED SERVICES (Digitel TS) y tiene carácter de confidencial y no podrá ser objeto de reproducción total o parcial, tratamiento informático ni transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, registro o cualquiera otro medio/formato. Asimismo, tampoco podrá ser objeto de préstamo, alquiler o cualquier forma de cesión de uso sin el permiso previo y escrito de Digitel TS, titular del copyright. El incumplimiento de las limitaciones señaladas por cualquier persona que tenga acceso a la documentación será perseguido conforme a ley.


	Área: EXPLOTACIÓN	Asunto: Certificación e-IDAS
		Proyecto: Política de Sellado de Tiempo
Autor/es: DIGITEL TS	Fecha: 10/08/2021	Versión: 10.0

Contenido

1.	Introducción	5
1.1	Definiciones	5
1.2	Vista general.....	7
1.3	Comunidad	8
1.3.1	Autoridad de sellado de tiempo (TSA).....	8
1.3.2	Solicitante.....	8
1.3.3	Suscriptor	8
1.3.4	Parte Usuaría que Confía.....	8
1.3.5	Autoridad de certificación (AC).....	9
1.4	Ámbito de aplicación	9
1.4.1	Usos prohibidos/No autorizados.....	9
1.5	Contacto.....	9
2.	General	10
2.1	Obligaciones	10
2.1.1	Autoridad de Sellado de Tiempo (TSA).....	10
2.1.2	Suscriptor de sellos de tiempo.....	10
2.1.3	Tercero de confianza	11
2.1.4	Autoridad de certificación	11
2.2	Responsabilidad.....	11
2.2.1	Exoneración de responsabilidad	12
2.2.2	Responsabilidad financiera	12
2.3	Interpretación y ejecución	12
2.4	Tarifas.....	12
2.4.1	Tarifas de emisión de certificados y renovación	12
2.4.2	Tarifas de acceso a los certificados	13
2.4.3	Tarifas por el acceso al contenido de estas Políticas de Sellado de Tiempo.....	13
2.5	Publicación y repositorios	13
2.5.1	Publicación de información de la TSA	13
2.5.2	Términos y condiciones	13
2.5.3	Distribución de certificados	13
2.5.4	Controles de acceso	14
2.6	Auditorías	14
2.6.1	Frecuencia de las auditorías	14
2.6.2	Tópicos cubiertos por la auditoría	14
2.7	Confidencialidad.....	14

	Área: EXPLOTACIÓN	Asunto: Certificación e-IDAS
		Proyecto: Política de Sellado de Tiempo
Autor/es: DIGITEL TS	Fecha: 10/08/2021	Versión: 10.0


2.7.1	Tipo de información considerada confidencial	14
2.7.2	Tipo de información considerada no confidencial.....	14
2.7.3	Divulgación de información de revocación/suspensión de certificados	15
2.7.4	Envío a la Autoridad Competente	15
2.8	Derechos de propiedad intelectual.....	15
3.	Requerimientos Operacionales	15
3.1	Registro inicial	15
4.	Procedimientos de Control de Seguridad.....	16
5.	Sello De Tiempo.....	17
5.1	Sincronización del reloj con UTC	17
5.2	Algoritmo empleado	17
5.3	Identificadores de objeto (OID) de los algoritmos criptográficos	17
6.	Control de revisiones	18
7.	Especificación de la Administración.....	19
7.1	Procedimientos de especificación de cambios.....	19
7.2	Publicación y copia de la política.....	19
8.	ANEXO: PROCESO DE SELLADO DE TIEMPO.....	20
8.1	Recepción del sello	20
8.2	Proceso de petición (TimeStamp Request)	21
8.3	Proceso de verificación	21

	Área: EXPLOTACIÓN	Asunto: Certificación e-IDAS
		Proyecto: Política de Sellado de Tiempo
Autor/es: DIGITEL TS	Fecha: 10/08/2021	Versión: 10.0


1. Introducción

1.1 Definiciones

<u>CONCEPTO</u>	<u>DEFINICIÓN</u>
Autoridad de Certificación (AC)	Es la entidad responsable de la emisión, y gestión de los certificados digitales. Actúa como tercera parte de confianza, entre el Suscriptor y el Tercero que confía, vinculando una determinada clave pública con una persona.
Certificado	Archivo que asocia la clave pública con algunos datos identificativos del suscriptor y es firmada por la AC.
Clave pública	Valor matemático conocido públicamente y usado para la verificación de una firma digital o el cifrado de datos. También llamada datos de verificación de firma.
Clave privada	Valor matemático conocido únicamente por el suscriptor y usado para la creación de una firma digital o el descifrado de datos. También llamada datos de creación de firma.
Declaración de Prácticas de Certificación	Conjunto de prácticas adoptadas por una Autoridad de Certificación para la gestión de sus servicios. Contiene información detallada sobre su sistema de seguridad, soporte, administración y emisión de los tokens de tiempo, además sobre la relación de confianza entre el suscriptor del sello, la parte usuaria y la autoridad de certificación.
Entidad	Aquella empresa u organización de cualquier tipo a la cual pertenece o se encuentra estrechamente vinculado el suscriptor.
Firma digital	El resultado de la transformación de un mensaje, o cualquier tipo de dato, por la aplicación de la clave privada en conjunción con unos algoritmos conocidos, garantizando de esta manera: a) que los datos no han sido modificados (integridad). b) que la persona que firma los datos es quien dice ser (identificación). c) que la persona que firma los datos no puede negar haberlo hecho (no repudio en origen).
Política de Sellado de Tiempo	Conjunto de reglas que definen la aplicabilidad al prestador de servicio de confianza de expedición de sellos de tiempo cuando genera tokens de sello de tiempo, con requisitos de seguridad y utilización comunes.
Suscriptor	Persona que utiliza los servicios prestados por el Prestador de servicio de confianza de expedición de Sellos de Tiempo.

	Área: EXPLOTACIÓN	Asunto: Certificación e-IDAS
		Proyecto: Política de Sellado de Tiempo
Autor/es: DIGITEL TS	Fecha: 10/08/2021	Versión: 10.0

Tercero que confía	Persona que voluntariamente confía en el sello de tiempo emitido por Digitel TS.
---------------------------	--

	Área: EXPLOTACIÓN	Asunto: Certificación e-IDAS
		Proyecto: Política de Sellado de Tiempo
Autor/es: DIGITEL TS	Fecha: 10/08/2021	Versión: 10.0

1.2 Vista general

Por no haber una definición precisa de los conceptos de Declaración de Prácticas de Sellado de Tiempo (DPC) y Políticas de Sellado de Tiempo (PC), se entiende que es necesario aclarar dichos conceptos.

-Política de Sellado de Tiempo (PC): Conjunto de reglas que definen la aplicabilidad al prestador de servicio de confianza de expedición de sellos de tiempo cuando genera tokens de sello de tiempo

-Declaración de Prácticas de Sellado de Tiempo (DPC): Conjunto de prácticas adoptadas por una Autoridad de Sellado de Tiempo (TSA) para la emisión tokens de sello de tiempo. Contiene información detallada sobre su sistema de seguridad, soporte, administración y emisión de los sellos de tiempo, además de la relación de confianza entre el suscriptor del sello, la parte usuaria y la Autoridad de Certificación (AC).

Estos dos documentos serán desarrollados por DIGITEL TS para la obtención de la Certi como Servicio de Confianza Cualificado. En concreto, este documento trata la Política de Sellado de Tiempo (PC) sobre el servicio de emisión de sellos de tiempo de una TSA, prestado por DIGITEL TS.

Para ello, se toma como referencia:

- **IETF RFC 3628** – *Policy Requirements for Time-Stamping Authorities (TSAs)*.
- **ETSI EN 319 421** - "*Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps*".


Así mismo, esta política está alineada con las especificaciones marcadas en "[Baseline Requirements for the Issuance and Management of Publicly-trusted Certificates](#)", elaborado por el CA / Browser Forum en su última versión.

En el caso de que exista alguna incongruencia entre la presente Política de Sellado de Tiempo y los Baseline Requirements, tendrán prioridad estos últimos sobre el presente documento.

Adicionalmente hay que destacar que la estructura de este documento está basada en la especificación del estándar "[RFC3647-Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework](#)" propuesto por Network Working Group para este tipo de documentos.

Por tanto, esta PC está en conformidad con las disposiciones legales expuestas en los documentos sobre Servicios de Confianza de la Unión Europea y de España, cumpliendo con todos los requisitos técnicos y de seguridad exigidos para la emisión de sellos de tiempo. A su vez, define las reglas y responsabilidades de las Autoridades de Sellado de Tiempo (TSA) que deseen emitir los sellos de tiempo, y definirá "**qué**" requerimientos de seguridad son necesarios para la emisión de sellos de tiempo cualificados.

Este documento cita obligaciones que han de ser tenidas en cuenta por los usuarios y Partes Usuaras que confían en estos sellos de tiempo.

	Área: EXPLOTACIÓN	Asunto: Certificación e-IDAS
		Proyecto: Política de Sellado de Tiempo
Autor/es: DIGITEL TS	Fecha: 10/08/2021	Versión: 10.0

Los sellos de tiempo emitidos bajo esta PC pueden ser usados para proteger firmas electrónicas de larga duración, código ejecutable y transacciones realizadas en servicios electrónicos ofrecidos telemáticamente.

El certificado de Sello de Tiempo es necesario para garantizar la existencia de un documento, en un tiempo concreto a través de:

- Firma digital de la autoridad de sellado de tiempo.
- Identificador electrónico único del documento (función HASH).
- Fecha y hora recogida de una fuente fiable de tiempo.

La información personal obtenida del Suscriptor se recogerá con el debido consentimiento del interesado y únicamente para los fines propios del servicio de certificación.

La Autoridad de Sellado de Tiempo (TSA) deberá respetar la normativa aplicable en materia de protección de datos.

Los usuarios de servicios asociados a estos sellos de tiempo, como parte que confía, deberán consultar estas políticas y prácticas de sellado de tiempo asociadas para obtener detalles de cómo se complementa esta política de Sellado de Tiempo.

1.3 Comunidad

El servicio puede ser utilizado por los suscriptores que poseen un acuerdo comercial con DIGITEL TS y por los receptores del servicio de emisión de sellos de tiempo de forma libre para confirmar la existencia de un documento electrónico en una fecha y hora determinada.

1.3.1 Autoridad de sellado de tiempo (TSA)

Una TSA es una entidad de confianza en el que el usuario (suscriptores y terceras partes) confían para la emisión de sellos de tiempo. Tiene la responsabilidad última sobre todos los servicios relacionados con la emisión de sellos de tiempo.

Además, tiene responsabilidad sobre las TSU (Unidades de sellado de tiempo), que son unidades identificables de sello de tiempo, que pueden tener asociada su propia clave privada para firmar los sellos de tiempo en representación de la TSA.

1.3.2 Solicitante


Persona física que en nombre propio o autorizada por una organización solicita la obtención de sellos de tiempo mediante un acuerdo con la TSA.

1.3.3 Suscriptor

El poseedor de un acceso al servicio de sellado de tiempo ofrecido por la TSA de DIGITEL TS.

1.3.4 Parte Usaria que Confía

Persona que voluntariamente confía en el sello de tiempo emitido por la TSA de DIGITEL TS.

	Área: EXPLOTACIÓN	Asunto: Certificación e-IDAS
		Proyecto: Política de Sellado de Tiempo
Autor/es: DIGITEL TS	Fecha: 10/08/2021	Versión: 10.0

1.3.5 Autoridad de certificación (AC)

Se trata de una entidad de confianza, responsable de emitir y revocar los certificados, en este caso de DIGITEL TS.

La AC de DIGITEL TS se encargará de expedir sus certificados digitales, con las identificaciones numéricas y contraseñas necesarias para este proceso. Así mismo pone a disposición de DIGITEL TS el procedimiento de verificación de este certificado emitido.

1.4 Ámbito de aplicación

El certificado de TSU emitido bajo esta política solo será utilizado para la emisión de sellos de tiempo **cualificados**.

1.4.1 Usos prohibidos/No autorizados

Bajo la presente política no está permitido el uso que sea contrario a la normativa española y comunitaria, a los convenios internacionales ratificados por el estado español, a las costumbres, a la moral y al orden público.


Tampoco está permitida la utilización distinta a lo establecido en esta Política de Sellado de Tiempo (PC) y en la Declaración de Prácticas de Sellado de Tiempo (DPC).

No están autorizadas las alteraciones en los certificados, que se deberán utilizar tal cual son suministrados por la TSA.

1.5 Contacto

- Razón Social: DIGITEL ON TRUSTED SERVICES S.L.U
- Denominación Comercial: DIGITEL TS
- CIF: B47447560
- Domicilio Social: C/ Enrique Cubero, 9, 47014 Valladolid, VALLADOLID
- Servicio de Atención al Cliente (SAC): 91 015 05 10
- Correo electrónico: comercial@digitelts.com
- Web: www.digitelts.es

Datos incorporados adaptándose a la estructura RFC3647.

	Área: EXPLOTACIÓN	Asunto: Certificación e-IDAS
		Proyecto: Política de Sellado de Tiempo
Autor/es: DIGITEL TS	Fecha: 10/08/2021	Versión: 10.0

2. General

2.1 Obligaciones

A continuación, se muestran las obligaciones, garantías y responsabilidades de la Autoridad de Sellado de Tiempo (TSA) frente a los usuarios y terceros de confianza.

2.1.1 Autoridad de Sellado de Tiempo (TSA)

La Autoridad de Sellado de Tiempo (TSA) que actúa bajo esta PC deberán:


- Respetar lo dispuesto en la PC.
- Conservará la responsabilidad general en el cumplimiento de los procedimientos prescritos en su política de seguridad de la información.
- Proteger sus claves privadas de forma segura.
- Emitir sellos de tiempo según la PC y la información que tenga en su poder.
- Publicar esta PC y las prácticas correspondientes en su página web.
- Informar de modificaciones de esta política y Declaración de Prácticas de Sellado de Tiempo (DPC).
- Establecer mecanismos de generación y custodia de la información, protegiéndolas de pérdida, destrucción o falsificación.
- Disponibilidad del servicio de sellado de tiempo según lo descrito en SLAs.
- La precisión de la fecha y hora incorporada en los sellos de tiempo basadas en el sistema UTC con una desviación máxima de 1 segundo (Accuracy).
- Suministrar una fuente fiable de tiempo a las TSU delegadas.
- Que los sellos de tiempo emitidos estarán libres de datos falsos y errores.
- Así mismo, los sistemas intervinientes en la plataforma de sello de tiempo cualificado de la TSA de DIGITEL TS, sólo serán empleados para los fines y requerimientos propios y relacionados con este servicio, de acuerdo con la normativa ETSI EN 309 401, en concreto el REQ. 7.8-09.

2.1.2 Suscriptor de sellos de tiempo

El Suscriptor de los sellos de tiempo de la TSA de DIGITEL TS deberán verificar que el token de sello de tiempo ha sido firmado debidamente por la TSA de Digitel TS y comprobar que la clave privada con la que se firmó dicho token no ha sido revocada.

El suscriptor de los sellos de tiempo de la TSA de DIGITEL TS puede utilizar este servicio solo según las especificaciones que marca la normativa:

- ETSI EN 319 401 *Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers*
- ETSI EN 319 421 *Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps*
- ETSI EN 319 422 *Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.*

	Área: EXPLOTACIÓN	Asunto: Certificación e-IDAS
		Proyecto: Política de Sellado de Tiempo
Autor/es: DIGITEL TS	Fecha: 10/08/2021	Versión: 10.0

2.1.3 Tercero de confianza

Asume la obligación de:

- Verificar el estado de activación en que se encuentra el Certificado de la TSA-TSU al que se vincula el Sello de Tiempo emitido, garantizando que no se emitan sellos si en alguno de estos certificados se ha excedido su fecha de validez.
- En el supuesto de que el certificado haya expirado o haya perdido su validez por revocación deberá comprobar que:
 - La fecha de revocación o de caducidad es posterior a la fecha en que se emitió el sello de tiempo.
 - La función criptográfica que se empleó para obtener el sello sigue siendo segura.
 - Que la longitud de la Clave criptográfica y el algoritmo de firma electrónica siguen siendo de práctica habitual.
- Tener en cuenta cualquier limitación en el uso del sello de tiempo indicado en la política y prácticas de certificación correspondiente.


2.1.4 Autoridad de certificación

La autoridad de certificación, responsable de emitir y revocar los certificados de DIGITEL TS. Cumplirá con las siguientes obligaciones:

- Respetar lo dispuesto en esta Política.
- Proteger las claves privadas de forma segura.
- Emitir certificados conforme a esta Política y a los estándares de aplicación. Según la información proporcionada por DIGITEL TS.
- Revocar los certificados en el caso de que así lo solicite DIGITEL TS, de acuerdo con la política y condiciones de éste.
- Conservar la información sobre el certificado emitido por el período mínimo exigido por la normativa vigente.

2.2 Responsabilidad

DIGITEL TS dispondrá en todo momento de un seguro de responsabilidad civil en los términos que marque la legislación vigente. Actuará en la cobertura de sus responsabilidades por sí mismo o a través de la entidad aseguradora, satisfaciendo los requerimientos recibidos.

	Área: EXPLOTACIÓN	Asunto: Certificación e-IDAS
		Proyecto: Política de Sellado de Tiempo
Autor/es: DIGITEL TS	Fecha: 10/08/2021	Versión: 10.0

2.2.1 Exoneración de responsabilidad

DIGITEL TS no será responsable en ningún caso cuando se encuentre ante cualquiera de estas circunstancias:

- Estado de Guerra, desastres naturales o cualquier otro caso de fuerza mayor.
- Por el uso de los certificados de TSU siempre y cuando exceda de lo dispuesto en la normativa vigente y la presente Política de Sellado de Tiempo.
- Por el uso indebido o fraudulento de los certificados de TSU y/o sellos de tiempo emitidos por la TSA.
- Por el uso de la información contenida en el Certificado de TSU.
- Por el incumplimiento de las obligaciones establecidas para el Suscriptor del Sello de Tiempo o Parte Usaria en la normativa vigente, en la presente Política de Sellado, en la Declaración de Prácticas Correspondientes o en los contratos establecidos por las partes.
- Por el perjuicio causado en el periodo de verificación de las causas de revocación/suspensión.
- Por el contenido de los mensajes o documentos sellados en tiempo o cifrados digitalmente.
- Por la no recuperación de documentos cifrados con la clave pública del Suscriptor del Sello de tiempo.
- Fraude en la información presentada por el solicitante.

2.2.2 Responsabilidad financiera

La TSA no asume ningún tipo de responsabilidad financiera.

2.3 Interpretación y ejecución

La ejecución, interpretación, modificación o validez de la PC se regirá por lo dispuesto en la legislación española y europea.


La invalidez de una de las cláusulas contenidas en la PC no afectará al resto del documento.

Cualquier notificación referente a la PC se realizará por correo electrónico o mediante correo certificado dirigido a cualquiera de las direcciones referidas en datos de contacto.

2.4 Tarifas

2.4.1 Tarifas de emisión de certificados y renovación

Los precios de los Servicios de Sello de Tiempo o cualesquiera de otros servicios relacionados estarán registrados en acuerdos / contrato con el cliente del servicio prestado por DIGITEL TS.

	Área: EXPLOTACIÓN	Asunto: Certificación e-IDAS
		Proyecto: Política de Sellado de Tiempo
Autor/es: DIGITEL TS	Fecha: 10/08/2021	Versión: 10.0

2.4.2 Tarifas de acceso a los certificados

El acceso a los sellos de tiempo emitidos es gratuito, no obstante, la TSA se reserva el derecho de imponer alguna tarifa para los casos de descarga masiva o cualquier otra circunstancia que a juicio de la TSA deba de ser grabada.

2.4.3 Tarifas por el acceso al contenido de estas Políticas de Sellado de Tiempo

El acceso al contenido de la presente Política de Sellado de Tiempo será gratuito.

2.5 Publicación y repositorios

2.5.1 Publicación de información de la TSA

DIGITEL TS publicará la información relativa a sus Políticas y Prácticas de Sellado de Tiempo en su [página web](#).

Estos dos documentos estarán en acceso públicos y estarán disponibles en su página web, así como el [certificado de TSA](#) y el [certificado de TSU de DIGITEL TS](#).

Gestión de publicación y repositorios de los certificados siguiendo la estructura RFC3647.

2.5.2 Términos y condiciones


DIGITEL TS pondrá a disposición de los suscriptores los términos y condiciones del servicio antes **de hacer efectiva la relación contractual con el cliente**. En concreto:

- DIGITEL TS pondrá a disposición de los suscriptores/creadores del Sello de Tiempo y Partes Usuarías los términos y condiciones relativos al uso de los sellos de tiempo.
- Los límites de responsabilidad y de uso.
- El periodo de tiempo en que la información registrada será almacenada.
- Los procedimientos para la resolución de disputas.
- El ordenamiento jurídico aplicable.
- Si la TSA ha sido acreditada conforme a la Política identificada en el certificado.

2.5.3 Distribución de certificados

El certificado de la TSA es público y está disponible en la página web DIGITEL TS. La información de referencia estará disponible 24 horas los 7 días de la semana. DIGITEL TS hará todos los esfuerzos para conseguir que este servicio informativo no esté inaccesible durante un periodo máximo de 24 horas.

Las [políticas y prácticas de sellado](#) de tiempo se publicarán una vez hayan sido creadas y aprobadas.

	Área: EXPLOTACIÓN	Asunto: Certificación e-IDAS
		Proyecto: Política de Sellado de Tiempo
Autor/es: DIGITEL TS	Fecha: 10/08/2021	Versión: 10.0

2.5.4 Controles de acceso

La TSA podrá establecer sistemas de seguridad para controlar el acceso a la información contenida en el web con el fin de evitar usos indebidos que afecten la protección de datos personales.

2.6 Auditorias

2.6.1 Frecuencia de las auditorias

El servicio de TSA es evaluado en el alcance de la *certificación ISO27001* que anualmente realiza DIGITEL TS.

Adicionalmente el servicio de TSA también es evaluado en el alcance de la evaluación de conformidad del *reglamento europeo e-IDAS* sobre servicios de sellado de tiempo realizado anualmente.

En esta última auditoria, la TSA DIGITEL TSA, garantizará que el auditor externo encargado de la misma debe poseer conocimientos y experiencia en sistemas de PKI y en seguridad de sistemas informáticos.

2.6.2 Tópicos cubiertos por la auditoria

La auditoría deberá verificar en todo caso:

- Que DIGITEL TS tiene un sistema que garantice la calidad del servicio prestado.
- Que cumple con los requerimientos de esta Política de Sellado de Tiempo.
- Que la Declaración de Prácticas de Sellado de Tiempo de DIGITEL TS se ajusta con lo establecido en esta Política, con lo acordado por la Autoridad aprobadora de la Política y con lo establecido en la normativa vigente.

2.7 Confidencialidad

2.7.1 Tipo de información considerada confidencial


Se determinará por DIGITEL TS la información considerada confidencial, debiendo cumplir en todo caso con la totalidad de la normativa vigente en materia de protección de datos.

DIGITEL TS pondrá todos los medios a su alcance para garantizar la confidencialidad frente a terceros, durante el proceso de sellos de tiempo que se proporciona.

2.7.2 Tipo de información considerada no confidencial

Se considerará información no confidencial:

- La contenida en la presente Política y en las Prácticas de Sellado de Tiempo.
- Cualquier información cuya publicidad sea impuesta normativamente.
- Las que así se determinen por la Declaración de Prácticas de Sellado de Tiempo siempre que no contravengan ni la normativa vigente ni lo dispuesto en esta Política de Sellado.

	Área: EXPLOTACIÓN	Asunto: Certificación e-IDAS
		Proyecto: Política de Sellado de Tiempo
Autor/es: DIGITEL TS	Fecha: 10/08/2021	Versión: 10.0

2.7.3 Divulgación de información de revocación/suspensión de certificados

La forma de difundir la información relativa a revocación/suspensión de un certificado de TSU se realizará mediante la publicación de las correspondientes listas de revocación de certificados (CRL) y mediante protocolo de acceso en línea.

2.7.4 Envío a la Autoridad Competente

Se proporcionará la información solicitada por la autoridad competente en los casos y forma establecidos legalmente.

2.8 Derechos de propiedad intelectual

DIGITEL TS es titular en exclusivo de todos los derechos de propiedad intelectual que puedan derivarse del sistema de sellado de tiempo que regula esta Política de Sellado. Se prohíbe, por tanto, cualquier acto de reproducción, distribución, comunicación pública y transformación de cualquiera de los elementos que son titularidad exclusiva de la TSA sin la autorización expresa por su parte.

No obstante, no necesitará autorización de DIGITEL TS para la reproducción del Certificado cuando la misma sea necesaria para su utilización por parte del Usuario legítimo y con arreglo a la finalidad del Certificado, de acuerdo con los términos de esta Política de Sellado.


3. Requerimientos Operacionales

3.1 Registro inicial

El registro para el acceso directo al servicio de sellado de tiempo se realiza mediante oferta comercial, indicando en dicha oferta las condiciones de uso del servicio.

**PKCS#10: Formato de los mensajes enviados a una Autoridad de certificación para solicitar la certificación de una clave pública.*

Requerimientos operacionales siguiendo la estructura RFC3647.

	Área: EXPLOTACIÓN	Asunto: Certificación e-IDAS
		Proyecto: Política de Sellado de Tiempo
Autor/es: DIGITEL TS	Fecha: 10/08/2021	Versión: 10.0


4. Procedimientos de Control de Seguridad

El prestador de los servicios deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que toda la información relevante concerniente a los servicios descritos en este documento es gestionada y protegida de forma segura durante el periodo de tiempo que pueda ser necesario a efectos probatorios en los procedimientos legales utilizando los medios ajustados al estado del arte en seguridad de la información.

Al ser procedimientos comunes a otros servicios de emisión, se desarrollará en la Declaración de Prácticas de Sellado de Tiempo (DPC) correspondiente, los aspectos relativos a los procedimientos de Control de seguridad, cubriendo los siguientes aspectos:

- Archivo de registros
- Análisis de vulnerabilidades
- Gestión de contingencias
- Controles de Seguridad física
- Controles procedimentales
- Controles de seguridad de personal
- Controles de Seguridad Técnica de las claves
- Controles de seguridad informática
- Controles de gestión de la seguridad
- Controles de seguridad de la red
- Controles de ingeniería de los módulos criptográficos

**Controles de seguridad siguiendo la estructura RFC3647.*

	Área: EXPLOTACIÓN	Asunto: Certificación e-IDAS
		Proyecto: Política de Sellado de Tiempo
Autor/es: DIGITEL TS	Fecha: 10/08/2021	Versión: 10.0

5. Sello De Tiempo

El sello de tiempo tendrá seguirá las especificaciones de la RFC3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).

5.1 Sincronización del reloj con UTC

La modalidad del servicio ofrecido por DIGITEL TS se basa en la disposición de una plataforma tecnológica para llevar a cabo Procesos de Sello de Tiempo cualificados.

El sello electrónico de tiempo es aquél que vincula la fecha y la hora con los datos de forma que no se puedan modificar los datos sin que se detecte. Se basa en una fuente de información temporal vinculada al Tiempo Universal Coordinado (UTC) y que ha sido firmado/sellado por un Prestador de Servicios de Confianza, en este caso DIGITEL TS.

El sistema de sincronización de tiempos empleará el [NTP tiempo.camerfirma.com](http://ntp.tiempo.camerfirma.com).

Los sistemas de mantendrán en todo momento sincronizados con una desviación máxima de 1 segundo (Accuracy).

El reloj del ordenador se controlará de acuerdo con los algoritmos de selección y sincronización de la RFC 1305.

Así mismo, el registro de eventos, para registro de auditoria se realizará sincronizando al menos una vez al día con UTC.


5.2 Algoritmo empleado

En el proceso de sellado de tiempo, se emplea [por defecto una](#) función hash del tipo SHA256.

No obstante, está permitido también en este proceso, bajo demanda de cliente, el empleo de los algoritmos SHA384 y SHA512.

5.3 Identificadores de objeto (OID) de los algoritmos criptográficos

SHA-256 With RSA Encryption (1.3.6.1.4.1.54225.1.1.1).

	Área: EXPLOTACIÓN	Asunto: Certificación e-IDAS
		Proyecto: Política de Sellado de Tiempo
Autor/es: DIGITEL TS	Fecha: 10/08/2021	Versión: 10.0

6. Control de revisiones

Salvo modificaciones en el proceso o actividad, mínimo la Dirección se reunirá con carácter bianual, junto con la Dirección del TSP y/o responsables del servicio prestado para revisar este documento, y evidenciar que todo sigue según lo estipulado. En el caso de ser necesario que Dirección se reúna con más departamentos, como puede ser el caso de jurídico, así se hará constar en la correspondiente acta.

En el control de versiones se actualizará a fecha de esta revisión.


Tras las modificaciones necesaria, según marca el *Artículo 6.1 de ETSI EN 319-401*, la Dirección firmará el acta de aprobación correspondiente a esta actualización de políticas de TSP.

En el caso de alguna modificación en el proceso o actividad, se reunirá la Dirección, junto con los responsables de los departamentos o procesos implicados en dichas modificaciones, en fechas en la que éstas tengan lugar, fuera de las marcadas con carácter de revisión bianual, de forma que se aprueben las correspondientes modificaciones, quedando este documento actualizado y aprobado por Dirección con el acta correspondiente, así como referenciado en el control de versiones de la forma habitual.

Tras la aprobación de las correspondientes actualizaciones, la última versión del documento se hará pública en la [web de DIGITEL TS](#), avisando de ello mediante la vía habitual de comunicación y según el *control 6.1 de la normativa ETSI EN 319 401*, a los clientes de este servicio, así como a las unidades de negocio involucradas.

Este mismo procedimiento es el que se sigue de forma habitual en el resto de los documentos pertenecientes a la certificación e-IDAS.

Control de revisiones siguiendo la estructura RFC3647.

	Área: EXPLOTACIÓN	Asunto: Certificación e-IDAS
		Proyecto: Política de Sellado de Tiempo
Autor/es: DIGITEL TS	Fecha: 10/08/2021	Versión: 10.0

7. Especificación de la Administración

7.1 Procedimientos de especificación de cambios

Cualquier elemento de esta política es susceptible de ser modificado.


Todos los cambios realizados sobre las políticas serán inmediatamente publicados en la [web de DIGITEL TS](#), que mantendrá un histórico con las versiones anteriores de las políticas.

Los terceros que confían afectados pueden presentar sus comentarios a la organización de la administración de las políticas dentro de los 15 días siguientes a la publicación.

7.2 Publicación y copia de la política

Una copia de esta política estará disponible en formato electrónico en la página web de DIGITEL TS.

Gestión de publicación siguiendo la estructura RFC3647.

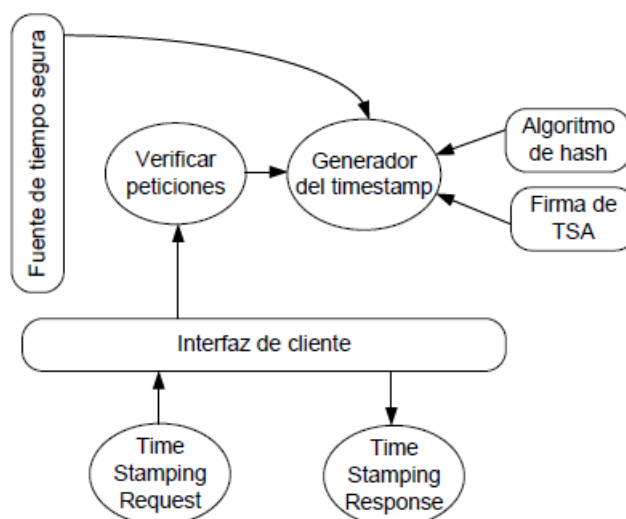
	Área: EXPLOTACIÓN	Asunto: Certificación e-IDAS
		Proyecto: Política de Sellado de Tiempo
Autor/es: DIGITEL TS	Fecha: 10/08/2021	Versión: 10.0


8. ANEXO: PROCESO DE SELLADO DE TIEMPO

El procedimiento de sellado implica:

- **Usuario peticionario:** El solicitante debe realizar la preparación del objeto a sellar. (*RFC3161* y *RFC5816 Timestamp Request*).
- **Unidad de sellado de tiempo:** Se encargará de:
 - Revisión de la corrección de la petición: Está diseñado para revisar que la petición es completa y correcta. Si el resultado es positivo, los datos se envían como entrada a la Generación de Sello de Tiempo.
 - Generación del parámetro tiempo: Usa una fuente de confianza para la distribución de parámetros de tiempo. Estos parámetros serán usados como entrada al proceso de Generación de Sellado de Tiempo.
 - Generación de Sello de Tiempo: Esta función es la responsable de crear un sello de tiempo que asocie el instante de tiempo actual, un número de serie único, los datos proporcionados para el sellado de tiempo y garantizar los requerimientos de política a la que se adhiere.
 - Sello de tiempo -Time Stamp Token (TST): Este componente calcula el indicador del sello de tiempo que se devolverá al cliente.

8.1 Recepción del sello



	Área: EXPLOTACIÓN	Asunto: Certificación e-IDAS
		Proyecto: Política de Sellado de Tiempo
Autor/es: DIGITEL TS	Fecha: 10/08/2021	Versión: 10.0

8.2 Proceso de petición (TimeStamp Request)

En el proceso de sellado, el sistema realiza diferentes acciones, primero realiza una revisión de la petición, verificando la correcta estructuración del objeto "TimeStamp Request" y el origen de esta. Durante esta verificación se comprueba que se han introducido los parámetros esperados como el algoritmo de hash y la política de sellado y que son correctos.

Posteriormente se obtiene de la fuente segura de tiempo y se genera el token de tiempo que es firmado electrónicamente con las claves privadas de sellado de DIGITEL TS.

En caso de que sea imposible la obtención de la exactitud requerida por parte de la fuente de tiempos por cualquiera de los caminos establecidos, el token de sello de tiempo no será emitido.

Finalmente se genera la respuesta TimeStamp Response, siguiendo las especificaciones de la RFC3161 y RFC5816.

El método de comunicación entre las entidades y el servicio de sellado de tiempo de DIGITEL TS se realizará:

- Mediante protocolo HTTP/HTTPS con autenticación en cliente, con el fin de poder validar las peticiones realizadas.
- Mediante usuario y contraseña.

8.3 Proceso de verificación


Los certificados de las AC emisoras de certificados de TSU y los certificados de TSU están disponibles en la página [web de DIGITEL TS](#).

Verificar el estado de activación en que se encuentra el certificado de las AC emisoras de certificados de TSU al que se vincula el Sello Digital de Tiempo emitido, mediante consulta a la CRL u otro medio que se disponga para la verificación de estado del certificado.

Validar que la firma del sello de tiempo está realizada con la clave privada del certificado de TSU utilizando el certificado de clave pública del certificado de TSU una vez validado su origen y su validez temporal y su no revocación.

En el supuesto de que el certificado haya expirado o haya perdido su validez por revocación deberá comprobar que:

- La fecha de caducidad del certificado que emitió el sello de tiempo es posterior a la fecha en que se emitió este.
- Comprobar que el certificado emisor del sello de tiempo no ha sido revocado por compromiso de la clave. En este caso todos los sellos de tiempo emitidos por este certificado dejarían de ser válidos y se deberían resellar todos los documentos afectados.
- La función criptográfica que se empleó para obtener el sello sigue siendo segura.

	Área: EXPLOTACIÓN	Asunto: Certificación e-IDAS
		Proyecto: Política de Sellado de Tiempo
Autor/es: DIGITEL TS	Fecha: 10/08/2021	Versión: 10.0

- Que la longitud de la clave criptográfica y el algoritmo de firma electrónica siguen siendo de práctica habitual.
- Tener en cuenta cualquier limitación en el uso del sello de tiempo indicado en la política y prácticas de certificación correspondiente.
- Tomar en consideración cualquier límite prescrito en la Declaración de Practicas de Certificación de DIGITEL TS o en cualquier otro aspecto descrito en las condiciones de uso del servicio.