POLITICA DE SELLADO DE TIEMPO

DIGITEL TS OID: 1.3.6.1.4.1.54225.1.1

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

Contenido

1. Introducción

1.1 Definiciones

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

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 Cualificación 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"*.

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 Politicy 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 emitor los sellos de tiempo.

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

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. Su actividad estará sometida a la inspección de la Autoridad de Políticas (PA).

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 Usuaria que Confía

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

1.4 Ámbito de aplicación

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

1.4.1 Usos prohibidos/No autorizados

Bajo la presente política no está permitido el uso que se 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 TS ON TRUSTED SERVICES SLU
- *Denominación Comercial:* DIGITEL TS
- *CIF:* B47447560
- *Domicilio Social:* C/ Enrique Cubero, 9, 47014 Valladolid, VALLADOLID
- *Servicio de Atención al Cliente (SAC):* 902 602 555 – 91 015 05 10
- *Correo electrónico:* info@digitelts.com
- *Web:* www.digitelts.com

Datos incorporados adaptándose a la estructura RFC3647.

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.
- 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 perdida, destrucción o falsificación.
- Disponibilidad del servicio de sellado de tiempo según lo descrito en SLA de DIGITEL TS.
- La precisión de la fecha y hora incorporada en los sellos de tiempo basadas en el sistema UTC con una desviación máxima de 100 ms.
- Suministrar una fuente fiable de tiempo a las TSU delegadas.
- Que los sellos de tiempo emitidos estarán libres de datos falsos y errores.

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 ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.

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 Digital de Tiempo emitido.
- 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 cuanta cualquier limitación en el uso del sello de tiempo indicado en la política y prácticas de certificación correspondiente.

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.

2.2.1 Exoneración de responsabilidad

La TSA y las AR no serán responsable en ningún caso cuando se encuentran 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, 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 Usuaria 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 disponibles para las partes usuarias en la página web de DIGITEL TS.

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.

2.4.4 Política de reintegros

La TSA dispondrá de una política de reintegros puesta a disposición de las Partes Usuarias.

2.5 Publicación y repositorios

2.5.1 Publicación de información de la TSA

DIGITEL TS estará obligado a publicar la información relativa a sus Políticas y Prácticas de Sellado de Tiempo. *(https://digitelts.es/declaracion-de-practicas-de-digitel-ts/)*.

Estos dos documentos deben de ser públicos y estarán disponibles en su página web, así como los certificados de AC emisoras de certificados de TSU y los propios certificados de TSU.

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 proceder a la emisión del sello de tiempo o de entregar los datos de acceso a los servicios de sellado de tiempo. En concreto:

- DIGITEL TS pondrá a disposición de los suscriptores/creadores del Sello de Tiempo y Partes Usuarias los términos y condiciones relativos al uso de los sellos de tiempo.
- La información sobre cómo validar el certificado de la TSA, incluyendo los requisitos para comprobar si un certificado ha sido revocado.
- 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 o en el momento en el que se apruebe una modificación de éstas.

(https://digitelts.es/declaracion-de-practicas-de-digitel-ts/).

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 en el alcance de las en la evaluación de conformidad del *reglamento europeo e-IDAS* sobre servicios de sellado de tiempo realizado anualmente.

El auditor 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 ajustan a 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.

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.

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 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.

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

El servicio de sincronización de tiempos estará compuesto por tres fuentes distintas:

- Notas técnicas de prevención (NTP) del Real Observatorio de la Armada (ROA) que establece el tiempo de referencia en España vía Red Iris.
- GPS sincronizado con 3 satélites. Precisión 30 ms.
- Sincronización de tiempos vía Radio DCF77 con la estación transmisora en Mainflingen (Frankfurt). La precisión 10 ms.

El sistema calculará el tiempo en base a estas tres fuentes. El reloj del ordenador se controlará de acuerdo con los algoritmos de selección y sincronización de la *RFC1305*.

Los sistemas de mantendrán en todo momento sincronizados con una desviación máxima de 100 ms.

5.2 Algoritmo empleado

En el proceso de sellado de tiempo, se emplea una función hash del tipo *SHA256*.

No obstante, para líneas futuras, está habilitada la opción de poder emplear algoritmos *SHA384* y *SHA512*.

5.3 Perfil de CRL

El perfil del certificado de CRL está redactado en un documento independiente. Dicho documento debe estar a disposición de cualquier tercero que lo solicite.

El formato de las CRL utilizadas es *X509*.

5.4 Identificadores de objeto (OID) de los algoritmos criptográficos

SHA-256 With RSA Encryption (1.3.6.1.4.1.54225.1.1.1).

6. Control de revisiones

Salvo modificaciones en el proceso o actividad, mínimo la Dirección se reunirá con carácter bianual, con un intervalo de medio año en cada revisión, 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 (https://www.digitelts.es/), 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.

7. Especificación de la Administración

7.1 Autoridad de las políticas

El departamento jurídico constituye la autoridad de las políticas (PA) y es responsable de la administración de las políticas.

La PA pondrá a disposición estas políticas a los empleados afectados en el repositorio documental de la empresa.

7.2 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.

Cualquier acción tomada como resultado de unos comentarios queda a la discreción de la PA.

Si un cambio en la política afecta de manera relevante a un número significativo de terceros que confían de la política, la PA puede discrecionalmente asignar un nuevo OID a la política modificada.

7.3 Publicación y copia de la política

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

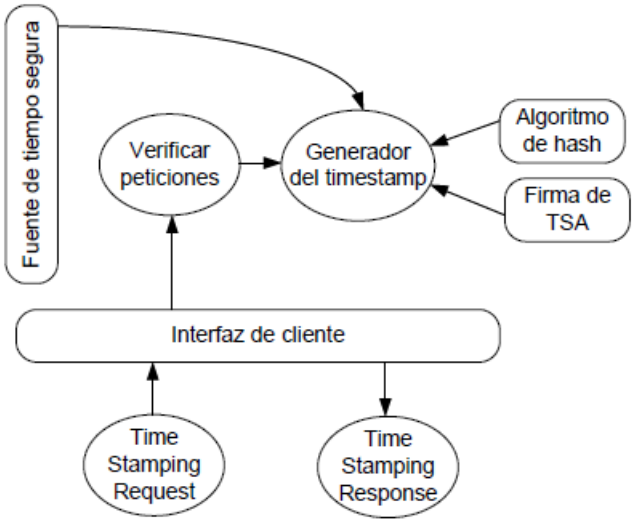
Gestión de publicación siguiendo la estructura RFC3647.

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



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 autentificación 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 dejaría de ser válidos y se deberían resellar todos los documentos afectados.

- 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.
- Tomar en consideración cualquier limite prescrito en la Declaración de Practicas de Certificación de DIGITEL TS o en cualquier otro aspecto descrito en las condiciones de uso del servicio.