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

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.
Autoridad de Registro (RA)	Entidad responsable de la gestión de las solicitudes e identificación y registro de los solicitantes de un certificado.
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 emisión de certificados. Contiene información detallada sobre su sistema de seguridad, soporte, administración y emisión de los Certificados, 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 Certificación	Conjunto de reglas que definen la aplicabilidad de un certificado en una comunidad o aplicación, con requisitos de seguridad y utilización comunes. Debe definir la aplicabilidad de tipos de certificado para determinadas aplicaciones que exigen los mismos requisitos de seguridad y formas de usos.
Suscriptor	Persona cuya clave pública es certificada por la AC y dispone de una privada válida para generar firmas digitales.
Tercero que confía	Persona que voluntariamente confía en el certificado digital y lo utiliza como medio de acreditación de la autenticidad e integridad del documento firmado.

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 de un certificado en un entorno determinado, con requisitos de seguridad y utilización comunes. Debe definir la aplicabilidad de los tipos de certificado para determinadas aplicaciones que exigen los mismos requisitos de seguridad y formas de usos.

-Declaración de Prácticas de Sellado de Tiempo (DPC): Conjunto de prácticas adoptadas por una autoridad de certificación para la emisión de certificados. Contiene información detallada sobre su sistema de seguridad, soporte, administración y emisión de los certificados, 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 del Sello de Tiempo. En concreto, este documento trata la Política de Sellado de Tiempo (PC) sobre el servicio de emisión de certificados de una TSU, y sobre el de emisión del sello de tiempo, ambos prestados 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 Firma Electrónica de la Unión Europea y de España, cumpliendo con todos los requisitos técnicos y de seguridad exigidos para la emisión de certificados y de sellos de tiempo. A su vez, define las reglas y responsabilidades de las Autoridades de Certificación (AC) que deseen emitir los tipos de certificados.

Este documento cita obligaciones que han de ser tenidas en cuenta por los Firmantes y Partes Usuarias que confían en este tipo de certificados.

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 Certificación (AC) 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 certificados, como parte que confía, deberán consultar estas políticas y prácticas de certificación asociadas para obtener detalles de cómo se complementa esta política de certificación.

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 las encargadas de emitir los sellos de tiempo en representación de la TSA.

El servicio de sellado de tiempo se compone de una o varias AC emisoras de certificados para las TSU.

1.3.2 Autoridad de certificación (AC) emisora de certificados de TSU

Entidad responsable de la emisión y gestión de los certificados digitales de TSU. La AC vincula una determinada clave publica con una entidad, a través de la emisión de un certificado de TSU.

Cada TSU tiene asociada una clave privada que utiliza para la firma de los sellos de tiempo.

1.3.3 Autoridad de Registro (AR)

Ente que actúa conforme a esta PC mediante acuerdo suscrito con la TSA.

Sus funciones son la gestión de las solicitudes, identificación y registro de los solicitantes del certificado.

1.3.4 Solicitante

Persona física autorizada por una organización para solicitar el Certificado TSU, mediante un acuerdo con la TSA.

1.3.5 Suscriptor

Entidad a la que se encuentra asociado el Certificado de TSU. También es considerado suscriptor el poseedor de un acceso al servicio de sellado de tiempo ofrecido por una TSU bajo el control de DIGITEL TS.

1.3.6 Parte Usuaria que Confía (Tercero de Confianza)

Persona que voluntariamente confía en el certificado emitido a favor del suscriptor, lo utiliza como medio de acreditación de la autenticidad e integridad del documento sellado, no requiere acuerdo posterior.

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/ Juan García Hortelano 43, 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) y Autoridad de Certificación (AC)

Las Autoridades de Sellado de Tiempo (TSA) que actúan bajo esta PC deberán:

- Respetar lo dispuesto en la PC.
- Proteger sus claves privadas de forma segura.
- Emitir certificados según la PC y la información que tenga en su poder.
- Publicar los certificados emitidos en un directorio, respetando la política de protección de datos.
- Revocar los certificados que lo necesiten.
- 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 Autoridad de registro (RA)

Las Autoridades de Registro (RA) que actúen bajo esta PC están obligadas a:

- Respetar lo dispuesto en PC.
- Proteger sus claves privadas de forma segura.
- Comprobar la identidad de los solicitantes de Certificados de TSU.
- Verificar la exactitud y autenticidad de la información suministrada por el Solicitante acerca del Suscriptor del Sello de Tiempo.
- Archivar, por periodo dispuesto en la legislación vigente, los documentos suministrados por el Solicitante acerca del Suscriptor del Sello de Tiempo.
- Respetar lo dispuesto en los contratos firmados con la TSA y con el Solicitante en representación del Suscriptor del Sello de Tiempo.
- Informar a la TSA de las causas de revocación, siempre y cuando tomen conocimiento.

2.1.3 Solicitante del certificado TSU

El solicitante de un certificado solicitado a DIGITEL TS deberá:

- Suministrar a la TSA la información necesaria para realizar una correcta identificación.
- Custodiar su clave privada de manera diligente.
- Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.
- En el caso de tratarse de un certificado cualificado deberá identificarse ante la AR.

2.1.4 Suscriptor

El Suscriptor de un certificado de DIGITEL TS deberán verificar la firma electrónica de sello de tiempo y comprobar el estado de los certificados TSA-TSU.

Además, estará obligado a:

- Suministrar a la TSA la información necesaria para realizar una correcta identificación.
- Realizar el pago del certificado conforme a la forma y medios establecidos por la TSA.
- Realizar los esfuerzos que razonablemente estén a su alcance para confirmar la exactitud y veracidad de la información suministrada.
- Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.
- Proteger sus claves privadas de forma segura.
- Asegurarse de que su certificado de TSU no ha caducado ni este revocado antes de ofrecer el servicio de sellado.
- Emitir sello de tiempo conforme a esta Política de Certificación (PC).
- Ofrecer el servicio con los requisitos de disponibilidad y precisión.
- Informar inmediatamente a la TSA acerca de cualquier situación que pueda afectar a la validez del Certificado, o a la seguridad de las claves.
- Sincronizarse con las fuentes de tiempo marcadas por el prestador del servicio.
- Someterse a la auditoria de sus sistemas por parte de la TSA o un tercero autorizado.
- Facilitar el acceso de la TSA a su servicio de sellado a los aplicativos con el objeto de establecer los controles correspondientes respecto a la corrección de la marca de hora, así como para recopilar información de los sellos emitidos.
- Presentar un acta de creación de las claves en un entorno seguro, firmado por una organización competente.

2.1.5 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.

2.1.6 Repositorio

La AC deberá mantener un sistema seguro de almacén y recuperación de certificados y un repositorio de certificados revocados, pudiendo delegar estas funciones en una tercera entidad.

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

2.4.3 Tarifas de acceso a la información relativa al estado de los certificados

La TSA proveerá de un acceso a la información relativa al estado de los certificados o de los certificados revocados gratuito.

2.4.4 Tarifas por el acceso al contenido de estas Políticas de Certificación

El acceso al contenido de la presente Política de Certificación será gratuito.

2.4.5 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.

DIGITEL TS se asegura que en la distribución de las claves públicas se garantice su integridad y autenticidad. Esta distribución se realiza mediante un certificado digital emitido para las AC emisoras de Certificados de TSU y para los propios certificados.

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 certificado 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 certificados.
- La información sobre cómo validar los certificados, 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 AC 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.

Se publicarán los certificados revocados/suspendidos en el momento en que se reciba la petición autenticada.

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

2.5.4 Controles de acceso

La AC 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 generación de las claves privadas de firma digital que se proporciona.

Una vez generadas y entregadas las claves privadas, la AC se abstendrá de almacenar, copiar y conservar cualquier tipo de información que sea suficiente para reconstruir duchas claves.

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.
- La información contenida en los certificados siempre que el Suscriptor del sello tiempo haya otorgado su consentimiento.

- 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 certificación 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 de solicitud para la emisión de un certificado de TSU se realiza mediante oferta comercial, indicando en dicha oferta las condiciones de uso del certificado.

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.

3.1.1 Tipos de nombres

Todos los Suscriptores requieren un nombre distintivo (DN o *Distinguished Name*) conforme al *estándar X.500* incorporado en el certificado de TSU.

3.1.2 Reglas utilizadas para interpretar varios formatos de nombres

Se atenderá en todo caso a lo marcado por el *estándar X.500* de referencia en la *ISO/IEC 9594*.

3.1.3 Unicidad de los nombres

La AC se asegurará de que no existan dos certificados activos emitidos con igual titular teniendo estos titulares diferentes identidades.

3.1.4 Reconocimiento, autenticación y función de las marcas registradas

Se admitirá la identificación de marcas o acrónimos de entidades siempre que en el propio certificado aparezca, además, la razón social y el número de identificación fiscal de la Entidad u otro elemento de identificación inequívoco, como el número de identificación fiscal, titular del signo distintivo registrado o no.

La AC no asumirá ninguna responsabilidad respecto del uso de marcas u otros signos distintivos, registrados o no, en la emisión de los Certificados expedidos bajo la presente Política de Sellado.

3.1.5 Métodos de prueba de la posesión de la clave privada.

El Suscriptor dispone de un mecanismo de generación de claves en dispositivo homologado. La prueba de posesión de la clave privada en estos casos es la petición recibida por DIGITEL TS en formato *PKCS#10** conjuntamente con el acta de la creación de las claves.

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

3.2 Autenticación

3.2.1 Autenticación de la identidad de una Entidad

En el caso de los certificados emitidos bajo la presente Política donde se incorporan los datos de una Entidad, se exigirá, en todo caso, la acreditación de la existencia de la Entidad por un medio conforme a Derecho.

3.2.2 Autorización de la Entidad al Solicitante

Para solicitar los certificados emitidos bajo esta Política, el Solicitante deberá acreditar su identidad conforme dispone la legislación vigente y que esté debidamente autorizado por el Suscriptor para solicitar el certificado de sello electrónico.

Para la comprobación de la identidad del Solicitante se exigirá su presencia física y la entrega de la copia y del original (para su cotejo) de su documento de identidad en los casos en que sea legalmente necesario.

Para comprobar que el Solicitante está autorizado por el Suscriptor para solicitar el certificado de TSU, se exigirá la entrega de una autorización específica firmada por alguien con poder de representación suficiente de la Entidad creadora del sello de tiempo, acompañada con una copia del documento de identidad del autorizante.

3.3 Emisión de certificados de TSU

La AC utiliza todos los medios a su alcance para asegurar que la emisión y renovación de certificados se realiza de una forma segura. En particular:

- Cuando la AC genere las claves del Suscriptor del Sello, que el procedimiento de emisión del certificado está ligado de manera segura a la generación del par de claves por la AC.
- Que la clave privada ha sido generada de manera segura por el Suscriptor.
- La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar la unicidad de los DN asignados a los Firmantes.
- La confidencialidad y la integridad de los datos registrados serán especialmente protegidos cuando estos datos sean intercambiados con el Suscriptor.
- La AC deberá verificar que el registro de los datos es intercambiado con proveedores de servicios reconocidos, cuya identidad es autenticada.
- La AC deberá notificar al solicitante la emisión de su certificado.
- El par de claves generado usado para la emisión del certificado de TSU no se empleará para ningún otro uso en cualquier otro certificado.

3.4 Renovación de la clave y del certificado

La TSA informará al Suscriptor antes de renovar de los términos y condiciones que hayan cambiado respecto de la anterior emisión.

La TSA en ningún caso emitirá un nuevo certificado conteniendo la anterior clave pública.

3.5 Modificación de certificados

Ante cualquier necesidad de modificación de certificados, la TSA realizará una revocación del certificado y una nueva emisión con los datos corregidos.

3.6 Reemisión después de una revocación

La AC no realizará reemisiones.

3.7 Aceptación de certificados de TSU

Aceptando el certificado, el Suscriptor del Sello de tiempo confirma y asume la exactitud del contenido de este, con las consiguientes obligaciones que de ello se deriven frente a la TSA o cualquier tercero que de buena fe confíe en el contenido del Certificado de TSU.

3.8 Revocación de certificados

Se entenderá por revocación aquel cambio en el estado de un certificado motivado por la pérdida de validez de un certificado en función de alguna circunstancia distinta a la caducidad de este. Al hablar de revocación nos referiremos siempre a la pérdida de validez definitiva.

3.8.1 Causas de la revocación

La revocación puede ser solicitada por el representante de la Entidad, el suscriptor de Sello de Tiempo y la TSA. Los Certificados deberán ser revocados cuando concurra alguna de las circunstancias siguientes:

- Solicitud voluntaria del Suscriptor del sello de tiempo.
- Pérdida o inutilización por daños del soporte del certificado.
- Fallecimiento del Suscriptor del sello de tiempo (si es persona física) o de su representado, incapacidad sobrevenida, total o parcial, de cualquiera de ellos.
- Terminación o extinción de la entidad.
- Cese en su actividad del prestador de servicios de certificación salvo que los certificados expedidos por aquel sean transferidos a otro prestador de servicios.

- Inexactitudes graves en los datos aportados por el Solicitante para la obtención del certificado, así como la concurrencia de circunstancias que provoquen que dichos datos, originalmente incluidos en el Certificado, no se adecuen a la realidad.
- Resolución de la TSA indicando que el certificado no se ha emitido siguiendo los términos y condiciones marcadas por las políticas de certificación correspondientes.
- Pérdida de los derechos de la TSA para emitir certificados bajo esta política.
- La TSA es consciente de que el Suscriptor del sello ha sido añadido a una lista de personas no autorizadas o insolventes, o está operando desde un lugar donde la política de la AC impida la emisión de certificados.
- Por incumplimiento por parte de la TSA, del Solicitante o el Suscriptor del Sello de tiempo de las obligaciones establecidas en esta política.
- Por la resolución del contrato con el Suscriptor del Sello de tiempo.
- Por cualquier causa que razonablemente induzca a creer que el servicio de certificación haya sido comprometido hasta el punto de que se ponga en duda la fiabilidad del Certificado.
- Por resolución judicial o administrativa que lo ordene.
- Por la concurrencia de cualquier otra causa especificada en la presente política.

3.8.2 Procedimiento de la solicitud de revocación

La revocación de un certificado podrá solicitarse únicamente por el representante de la Entidad, por el Suscriptor del Sello de tiempo mediante solicitud a DIGITEL TS.

Todas las solicitudes deberán ser en todo caso autenticadas.

DIGITEL TS deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que los certificados son revocados basándose en peticiones de revocación autorizadas y validadas.

La información relativa al retraso máximo entre la recepción de una petición de revocación y su publicación estará disponible como máximo en un periodo de 3 horas.

El Suscriptor del Sello de tiempo cuyo certificado haya sido revocado deberá ser informado del cambio de estado de su certificado. Así mismo, el Suscriptor del Sello de tiempo deberá ser informado del levantamiento de la suspensión. DIGITEL TS utilizará todos los medios a su alcance para conseguir este objetivo, pudiendo intentar la mencionada comunicación por e-mail, teléfono, correo ordinario o cualquier otra forma adecuada al supuesto concreto.

Una vez que un certificado es revocado, este no podrá volver a su estado activo. La revocación de un certificado es una acción, por tanto, definitiva.

El servicio de gestión de las revocaciones estará disponible las 24 horas del día, los 7 días de la semana. En caso de fallo del sistema, servicio o cualquier otro factor que no esté bajo el control de la TSA, la TSA deberá realizar los esfuerzos que razonablemente estén

a su alcance para confirmar que este servicio no se encuentre indisponible durante más tiempo que el periodo máximo dispuesto en esta política.

La información relativa al estado de la revocación estará disponible las 24 horas del día, los 7 días de la semana. En caso de fallo del sistema, servicio o cualquier otro factor que no esté bajo el control de DIGITEL TS, éste deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que este servicio de información se encuentre disponible. Se deberán realizar los esfuerzos que razonablemente estén a su alcance para confirmar la autenticidad y la confidencialidad de la información relativa al estado de los certificados.

La información relativa al estado de los certificados deberá estar disponible públicamente.

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. Perfiles de Certificado

Todos los certificados emitidos bajo esta política serán conformes a ETSI EN 319 412-3 v1.1.1 "*Certificate Profiles-Part 3 Certificate profile for certificates issued to legal persons*".

5.1 Extensiones de los certificados

Los perfiles de certificados están redactados en documentos independientes. Dichos documentos deben estar a disposición de cualquier tercero que lo solicite.

5.2 Extensiones específicas

El certificado, emitido bajo la presente Política, podrá incluir por petición del Suscriptor del sello de tiempo extensiones adicionales con información específica de su propiedad. Esta información estará bajo la exclusiva responsabilidad del suscriptor. Dichas extensiones no se marcarán como críticas y sean reconocibles como tales.

6. Sello De Tiempo

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

6.1 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.

6.2 Algoritmo empleado

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

6.3 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*.

7. Control de revisiones

Salvo modificaciones en el proceso o actividad, mínimo la Dirección se reunirá con carácter bianual 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.

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.

8. Especificación de la Administración

8.1 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.

8.2 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.

8.3 Publicación y copia de la política

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

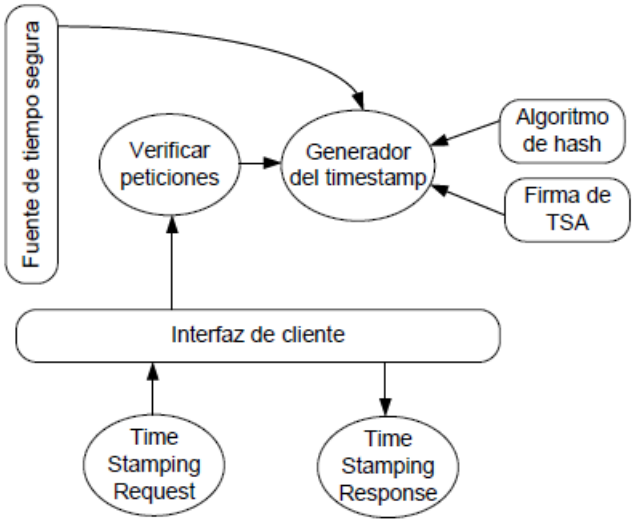
Gestión de publicación siguiendo la estructura RFC3647.

9. 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.

9.1 Recepción del sello



9.2 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.

9.3 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.