

# **TIMESTAMPING**



***Camerfirma***

**Certificado Digital**

## **SERVICIO DE SELLADO DE TIEMPO**

**Versión 1.1**

## Información sobre el documento

---

**Nombre:** Servicio de Sellado de Tiempo

---

**Código** PC-CAM-SST

---

**Versión:** 1.1

---

**Elaborado por:** AC Camerfirma SA

---

**Idioma:** Castellano

---

**Descripción:** Define las características del servicio de sellado de tiempo.

---

**Fecha de edición:** Enero 2006

---

**Estado del documento:** Activo

---

**Referencia (OID):**

---

**Localización:**

---

## Control de versiones

<b>VERSIÓN</b>	<b>MOTIVACIÓN DEL CAMBIO</b>	<b>PUBLICACIÓN</b>
1.0	Creación	9/01/06
1.1	Revisión	15/12/06

# Índice de Contenido

<b>1. Introducción</b>	<b>5</b>
<b>1.1. Generalidades</b>	<b>5</b>
<b>1.2. Referencias</b>	<b>5</b>
<b>1.3. Contacto</b>	<b>6</b>
<b>2. Aspectos Generales</b>	<b>7</b>
<b>2.1. Servicio de Sellado de Tiempo (Timestamping)</b>	<b>7</b>
<b>2.2. Rendimientos</b>	<b>7</b>
<b>2.3. Entidades que intervienen</b>	<b>8</b>
1.1.1 Requester	8
1.1.2 Verifier	8
1.1.3 TSA	8
<b>3. Proceso de Sellado</b>	<b>10</b>
<b>3.1. Proceso de petición (TimeStamp Request)</b>	<b>11</b>
<b>3.2. Proceso de sellado</b>	<b>12</b>
<b>3.3. Proceso de verificación</b>	<b>16</b>
<b>4. Objetivos de Seguridad</b>	<b>17</b>
<b>4.1. Objetivos de Seguridad de los servicios</b>	<b>17</b>
▪ Integridad	17
▪ Autenticación y Registro de la actividad de los usuarios	17
▪ Garantías de los procesos de desarrollo y operacionales	17
<b>4.2. Objetivos de Seguridad para el Entorno</b>	<b>___ ;Error! Marcador no definido.</b>
▪ Disponibilidad de los activos críticos	<b>___ ;Error! Marcador no definido.</b>
▪ Entorno operativo confiable	<b>___ ;Error! Marcador no definido.</b>
▪ Integridad de los sistemas de bases de datos y de operación	<b>___ ;Error! Marcador no definido.</b>
▪ Responsabilidad y Autenticación de los recursos informáticos del entorno	<b>___ ;Error! Marcador no definido.</b>
▪ Confidencialidad de los Dispositivos de Seguridad	<b>___ ;Error! Marcador no definido.</b>

# 1. Introducción

## 1.1. Generalidades

El presente documento especifica las características del Servicio de Sellado de Tiempo de AC Camerfirma S.A., y está basada en la especificación del estándar RCF 3161 – *Internet X. 509 Public Key Infrastructure, ETSI TS 102 023, Time-Stamp Protocol, Electronic Signatures and Infrastructures (ESI) Policy requirements for time-stamping authorities* y ETSI TS 101 861, Time stamping profile.

## 1.2. Referencias

[1] IETF RFC 3161: "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".

[2] FIPS Publication 180-1 (1995): "Secure Hash Standard".

[3] IETF RFC 2313 (1998): "PKCS #1: RSA Encryption Version 1.5".

[4] IETF RFC 1321 (1992): "The MD5 Message-Digest Algorithm".

[5] IETF RFC 2437: "PKCS #1: RSA Cryptography Specifications Version 2.0".

[6] ISO/IEC 10118-3: "Information technology - Security techniques - Hash-functions - Part 3: Dedicated hash-functions".

[7] ISO 9594-6: "Information technology - Open Systems Interconnection - The Directory: Selected attribute types".

[8] ITU-T Recommendation X.520: "Information technology - Open Systems Interconnection – The Directory: Selected attribute types".

[9] EESSI Conformity Assessment Guidance - Part 7: Cryptographic modules used by Certification Service Providers for signing operations and key generation services

[10] CWA 14172-8. EESSI Conformity Assessment Guidance - Part 8: Time-stamping Authority services and processes

Este servicio de Sellado de Tiempo está en conformidad con las disposiciones legales que rigen el asunto de Firma Electrónica en la Comunidad Europea y en España, cumpliendo todos los requisitos técnicos y de seguridad exigidos para la prestación de estos servicios.

### 1.3. Contacto

El presente documento, está administrada y gestionada por el Departamento Técnico de AC Camerfirma SA, pudiendo ser contactado por los siguientes medios:

---

**E-mail:** [soporte@camerfirma.com](mailto:soporte@camerfirma.com)

---

**Teléfono:** +34 902 100 096

---

**Fax:** +34 920 25 27 32

---

**Dirección:** <http://www.camerfirma.com/address>

---

## 2. Aspectos Generales

### 2.1. Servicio de Sellado de Tiempo (Timestamping)

El time stamping o sellado de tiempo es el complemento ideal a la seguridad que ofrecen los certificados digitales de identidad. Mediante la aplicación del sellado de tiempo garantizamos el momento exacto en el tiempo en que la firma de un documento se produjo.

Los certificados de sellado de tiempo de esta manera se convierten en un elemento imprescindible en determinados procedimientos, fundamentalmente en las relaciones entre administración y administrado, las cuales exigen en la mayoría de las ocasiones la constatación de la fecha y hora exactas en la que el acto jurídico tuvo lugar.

Actualmente el servicio de sincronización de tiempos de Camerfirma esta compuesto por tres fuentes distintas:

- NTP del ROA (Real Observatorio de la Armada, que establece el tiempo de referencia en España) vía RedIris.
- GPS sincronizado con 3 satélites. Precisión milisegundos.
- Sincronización de tiempos vía Radio DCF77 con la estación transmisora en Mainflingen (Frankfurt). La precisión 10 mseg.

El sistema calcula el tiempo en base a estas tres fuentes. El reloj del ordenador se controla de acuerdo con los algoritmos de selección y sincronización de la RFC1305 (NTP v3).

### 2.2. Rendimientos

Actualmente la plataforma está dimensionada para gestionar aproximadamente 10 peticiones por segundo con una única instancia de ejecución del sistema de sellado de tiempo.

Este sistema puede ampliarse a petición del cliente a 50 firmas/segundo, 250 firmas/segundo, 450 firmas/segundo.

## 2.3. Entidades que intervienen

### 1.1.1 Requester

Es la entidad que posee documentos, información o, en general, cualquier tipo de datos electrónicos a los que quiere incluir un sello de tiempo para probar que existían en un determinado instante.

### 1.1.2 Verifier

Es la entidad que quiere comprobar que los datos sellados que ha recibido contienen un sello de tiempo válido. Puede ser la misma entidad que utilizó el servicio de sellado de tiempo, para comprobar que el sello generado es válido y correcto.

### 1.1.3 TSA

La autoridad de sellado de tiempo (Time Stamping Authority) es el proveedor del servicio. Su finalidad es la de comprobar la validez de los datos a sellar y generar el sello de tiempo que irá unido a esos datos. De esta forma, la TSA asegura que esos datos existían en un determinado instante de tiempo y garantiza que el parámetro de tiempo de ese sello es correcto.

El IETF da una definición más extensa de por qué es necesaria una TSA en el proceso de sellado de tiempo:

- para utilizar una fuente fiable de tiempos
- para incluir un valor de tiempo fiable en cada sello
- para incluir un entero único para cada nuevo sello
- para producir un nuevo sello cuando se reciba una petición válida de un *requester*
- para incluir en cada sello un identificador que indique la política de seguridad bajo la cuál ha sido creado
- para sellar únicamente el hash de los datos
- para verificar que la longitud del hash es conforme al algoritmo de hashing utilizado
- para que no sean examinados los datos que se están siendo sellados nada más que para comprobar su longitud, tal y como se especificaba en el punto anterior
- para firmar cada sello usando una clave generada exclusivamente para este propósito. Para ello, debe poseer distintas claves privadas para emplear diferentes políticas de seguridad, diferentes algoritmos, diferentes tamaños de clave privada.
- para que no se incluya ninguna identificación del *requester* en el sello

- para incluir información adicional en el sello a petición del *requester* usando los campos de extensión, únicamente para las extensiones que esa TSA soporte. Si no fuera posible, la TSA respondería con un mensaje de error.

### 3. Proceso de Sellado

El Servicio de sellado de tiempo proporciona pruebas de la existencia de unos datos en un instante de tiempo determinado (prueba de existencia). Si los datos fueron firmados por el peticionario, antes de ser enviados a la Autoridad de Sellado de Tiempo (TSA), entonces este servicio proporciona una prueba, de la existencia de los datos y de que fueron firmados en ese instante de tiempo.

El proceso de sellado está distribuido en las siguientes fases:

- **Usuario peticionario:**

El proceso de petición, en el cual el solicitante debe realizar la preparación del objeto a sellar (Timestamp Request RFC3161).

- **Autoridad de sellado de tiempo:**

- Revisión de la corrección de la petición

Este componente 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

Este componente 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.

- Time Stamp Token (TST)

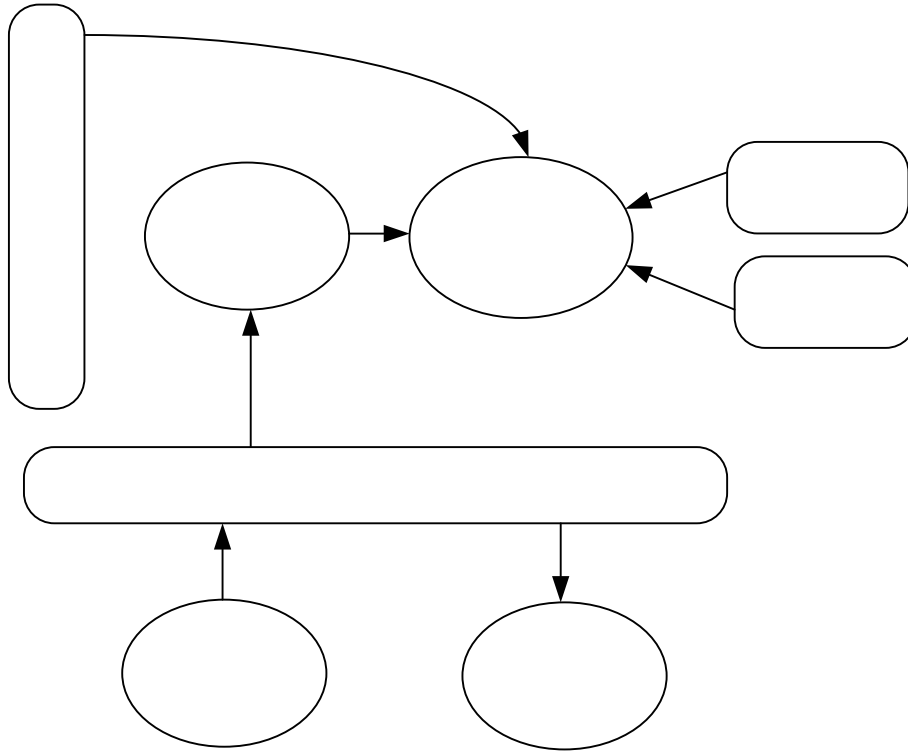
Este componente calcula el indicador del sello de tiempo que se devolverá al cliente. Es el que realmente hace la firma criptográfica de los datos que proporciona la función de generación del indicador de sello de tiempo.

- **Recepción del sello:**

El proceso de verificación del sello, en el que se evalúa la autenticidad del sello de tiempo recibido.

El proceso de sellado de tiempo es el servicio que proporciona Camerfirma, basado en un servidor de Timestamp alojado en el CPD de la Autoridad de Certificación.

El proceso de preparación del documento a sellar y la verificación y almacenamiento de la respuesta obtenida es un proceso a desarrollar por terceros que deseen acceder al servicio. Camerfirma puede proporcionar a modo de consultoría, apoyo en el desarrollo de estas fases.



### 3.1. Proceso de petición (TimeStamp Request)

El proceso comienza con la petición por parte de un tercero de un sello de tiempo a aplicar a un determinado documento.

Para ello el peticionario debe generar una petición TimeStamp Request según la RFC3161.

Los parámetros que el peticionario deberá enviar son:

- Hash del documento a sellar.
- Nombre del algoritmo de hash a utilizar.
- OID de política bajo la cual se proporcionará el sello.

```

TimeStampReq ::= SEQUENCE {
    version                INTEGER { v1(1) },
    messageImprint         MessageImprint,
    --a hash algorithm OID and the hash value of the data to be
    --time-stamped

    reqPolicy              TSAPolicyId          OPTIONAL,
    nonce                  INTEGER              OPTIONAL,
    certReq                BOOLEAN              DEFAULT FALSE,
    extensions              [0] IMPLICIT Extensions OPTIONAL }

```

El significado de los campos principales es el siguiente:

- **Versión:** Número de versión de la sintaxis utilizada. La versión actual es 1.
- **MessageImprint:** Contiene el hash de los datos que se quiere sellar. La longitud del hash tiene que coincidir con la longitud de hash del algoritmo utilizado. El algoritmo utilizado podrá ser SHA1, MD5 o RIPEMD160.

```

MessageImprint ::= SEQUENCE {
    hashAlgorithm          AlgorithmIdentifier,
    hashedMessage          OCTET STRING }

```

- **reqPolicy:** indica a la TSA la política bajo la cual quiere que se proporcione el sello. Este parámetro será indicado por Camerfirma.

```

TSAPolicyId ::= OBJECT IDENTIFIER

```

### 3.2. Proceso de sellado

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 la misma. 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. Anteriormente se ha mencionado los posibles valores del algoritmo de hash soportados por el servicio, SHA-1, MD5 y RIPDEM60.

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 Camerfirma.

Finalmente se genera la respuesta TimeStamp Response, siguiendo las especificaciones de la RFC3161, disponiendo de la siguiente representación.

```
TimeStampResp ::= SEQUENCE {
    status                PKIStatusInfo,
    timeStampToken        TimeStampToken OPTIONAL }

```

- El campo status está basado en la definición de la estructura PKIStatusInfo de la [RFC2510](#):

```
PKIStatusInfo ::= SEQUENCE {
    status                PKIStatus,
    statusString          PKIFreeText OPTIONAL,
    failInfo              PKIFailureInfo OPTIONAL }

```

- Status: Si este campo está a cero o a uno indica que el sello viene en el mensaje de respuesta. Para cualquier otro valor indica que no viene en el mensaje de respuesta.

```
PKIStatus ::= INTEGER {
    granted                (0),
    -- when the PKIStatus contains the value zero a TimeStampToken,
    as requested, is present.
    grantedWithMods        (1),
    -- when the PKIStatus contains the value one a TimeStampToken,
    with modifications, is present.
    rejection              (2),
    waiting                (3),
    revocationWarning      (4),
    -- this message contains a warning that a revocation is
    -- imminent
    revocationNotification (5)
}

```

```
-- notification that a revocation has occurred}
```

- **StatusString**: Se usa para indicar eventos de error.
- **FailInfo**: indica las causas por las que no se ha generado el sello de tiempo. Siendo los posibles errores:

```
PKIFailureInfo ::= BIT STRING {  
    badAlg          (0),  
        -- Unrecognized or unsupported Algorithm Identifier  
    badRequest     (2),  
        -- Transaction not permitted or supported  
    badDataFormat  (5),  
        -- The data submitted has the wrong format  
    timeNotAvailable (14),  
        -- The TSA's time source is not available  
    unacceptedPolicy (15),  
        -- The requested TSA policy is not supported by the TSA  
    unacceptedExtension (16),  
        -- The requested extension is not supported by the TSA  
    addInfoNotAvailable (17)  
        -- The additional information requested could not be understood  
        -- or is not available  
    systemFailure  (25)  
        -- the request cannot be handled due to system failure}
```

- El campo **timestampTokenInfo** contiene el sello de tiempo generado. Se define como:

```
TimeStampToken ::= ContentInfo  
    -- contentType is id-signedData ([CMS])  
    -- Content is SignedData ([CMS])
```

ContentInfo es una estructura que encapsula la información firmada en una estructura TSTInfo. Está definida en la RFC2630 y tiene los siguientes campos:

```
TSTInfo ::= SEQUENCE {  
    version                INTEGER { v1(1) },  
    policy                 TSAPolicyId,  
    messageImprint         MessageImprint,  
        -- MUST have the same value as the similar field in  
        -- TimeStampReq  
    serialNumber           INTEGER,  
        -- Time-Stamping users MUST be ready to accommodate integers  
        -- up to 160 bits.  
    genTime                GeneralizedTime,  
    accuracy               Accuracy OPTIONAL,  
    ordering               BOOLEAN DEFAULT FALSE,  
    nonce                  INTEGER OPTIONAL,  
        -- MUST be present if the similar field was present  
        -- in TimeStampReq. In that case it MUST have the same value.  
    tsa                    [0] GeneralName OPTIONAL,
```

extensions [1] IMPLICIT Extensions OPTIONAL }

- *version*: indica la versión del sello
- *policy*: si se ha generado el sello, será igual al del mensaje de petición
- *messageImprint*: será igual al del mensaje de petición
- *serialNumber*: es un entero asignado por la TSA y debe ser único para cada sello que genere. Por tanto, un sello será identificado por el nombre de la TSA que lo generó y el número de serie asignado
- *genTime*: es el instante de tiempo en el que se creó el sello. Tanto ISO como el IETF expresan el instante de tiempo referido a la escala *UTC*, para evitar confusiones con las horas locales. El formato debe ser el siguiente:

CC YY MM DD hh mm ss Z

CC representa el siglo (19-99)

YY representa el año (00-99)

MM representa el mes (01-12)

DD representa el día (01-31)

hh representa la hora (00-23)

mm representa los minutos (00-59)

ss representa los segundos (00-59)

Z viene de *zulu*, que es como se conoce a la escala *UTC*

- *accuracy*: en los casos que sea necesario, proporciona una precisión incluso de microsegundos:

Accuracy ::= SEQUENCE {

seconds [1] Integer OPTIONAL,

millis [2] Integer (1..999) OPTIONAL,

micros [3] Integer (1..999) OPTIONAL,

}

- *nonce*: aparece si lo hace en el mensaje de petición, y tendrá el mismo valor
- *tsa*: sirve para identificar a la TSA
- *extensions*: están definidas en la RFC 2459

El método de comunicación entre las entidades y el servicio de sellado de tiempo de Camerfirma se realizará mediante protocolo HTTPS con autenticación en cliente, con el fin de poder validar las peticiones realizadas.

Adicionalmente existirá un modelo basado en servicios Web, que permitirá la comunicación con el servicio. Este modelo está en fase de análisis y desarrollo. Básicamente el servicio Web deberá recoger los parámetros del hash a sellar y la autenticación inequívoca del usuario, pudiendo ser este sistema de autenticación la firma electrónica del hash a sellar con el certificado cliente.

### 3.3. *Proceso de verificación*

La entidad que recibe la petición TimeStamp Response, debe validarla y extraer los datos necesarios para su almacenamiento.

## 4. Objetivos de Seguridad

Esta sección identifica y define los objetivos de seguridad de los servicios de Camerfirma. Los objetivos de seguridad reflejan la intención señalada y contrarrestan las amenazas identificadas, al mismo tiempo que cumplen con las políticas de seguridad organizativas.

### 4.1. Objetivos de Seguridad de los servicios

- **Integridad**

La integridad de los productos y sistemas de Camerfirma asegura la integridad del usuario y de los datos que se transfieren internamente dentro del sistema. Los datos remitidos por los clientes de Camerfirma, están protegidos contra posibles alteraciones no autorizadas.

- **Autenticación y Registro de la actividad de los usuarios**

Los usuarios serán identificados, autenticados con mecanismos fuertes y responsables de las acciones relativas a los diferentes servicios consumidos. Este registro de la actividad comienza una vez que el usuario ha sido correctamente identificado y autenticado por la plataforma, y por lo tanto, pasa a ser considerado un usuario con permisos que accede a los servicios que tiene contratados.

- **Garantías de los procesos de desarrollo y operacionales**

Garantizar la no existencia de vulnerabilidades en los productos de Camerfirma derivada de la introducción de medidas de seguridad en los procesos de ingeniería del software y durante la vida operativa del sistema, de acuerdo con los estándares y normativas técnicas. Este objetivo pretende principalmente salvaguardar las garantías de seguridad, mediante el establecimiento de procedimientos de seguridad operacional.