POLÍTICA DE CERTIFICACIÓN

CAMERFIRMA SELLO DE TIEMPO

Versión 1.2.1

Idioma: **Castellano**

Fecha: **Junio 2015**

Estado del documento: **Activo**

Información sobre el documento

Nombre:	Política de Certificación Camerfirma para Sello de Tiempo
Código	PC-SELLO-TSA
Versión:	1.2.1
Elaborado por:	TSA Camerfirma SA
Idioma:	Castellano
Descripción:	Define los criterios básicos a seguir por el prestador de servicios de certificación que ofrezca servicios de sellado de tiempo.
Fecha de edición:	Junio 2015
Estado del documento:	Activo
Referencia (OID):	1.3.6.1.4.1.17326.10.13.1 TSA 1.3.6.1.4.1.17326.10.10.2 TSU-1 descontinuado 1.3.6.1.4.1.17326.10.13.1.2 TSU-2 1.3.6.1.4.1.17326.10.13.1.3 TSU-3 --- 1.3.6.1.4.1.17326.10.10.2.0 Sello TSU-1 descontinuado 1.3.6.1.4.1.17326.10.13.1.2.1 Sello TSU-2 1.3.6.1.4.1.17326.10.13.1.3.1 Sello TSU-3
Localización:	http://www.camerfirma.com/area-de-usuario/jerarquia-politicas-y-practicas-de-certificacion/

Control de versiones

VERSIÓN	MOTIVACIÓN DEL CAMBIO	FECHA
V1.1	Revisión para la emisión de certificados de TSU gestionadas por terceras partes.	Sep 2009
V1.2	Revisión OIDs	Noviembre 2010
V1.2.1	Revisión general y corrección de referencias erróneas entre apartados. Actualización del contenido de todos los apartados.	Junio 2015

Identificación de políticas

La forma de identificar distintos tipos de certificados digitales es a través de identificadores de objeto (OID's). Un OID concreto permite a las aplicaciones distinguir claramente el certificado que se presenta e identificar la política de certificación correspondiente.

En concreto el identificador correspondiente a este tipo de certificados es:

1.3.6.1.4.1.17326.10.13.1 TSA

1.3.6.1.4.1.17326.10.13.1.2 TSU-2 Camerfirma
Claves en SW almacenadas en HW con acceso autenticado al servicio. Clientes.

1.3.6.1.4.1.17326.10.13.1.3 TSU-3 Camerfirma
Claves en HW con acceso autenticado al servicio.

1.3.6.1.4.1.17326.10.13.1.2.1 Sello de tiempo TSU-2.

1.3.6.1.4.1.17326.10.13.1.3.1 Sello de tiempo TSU-3.

Índice de Contenido.

1. Introducción

1.1. Consideración Inicial

Por no haber una definición taxativa de los conceptos de Declaración de Practicas de Certificación y Políticas de Certificación y debido a algunas confusiones formadas, Camerfirma entiende que es necesario informar de su posición frente a estos conceptos.

Política de Certificación es el conjunto de reglas que definen la aplicabilidad de un certificado en una comunidad y/o en alguna aplicación, con requisitos de seguridad y utilización comunes, es decir, en general una Política de Certificación debe definir la aplicabilidad de tipos de certificado para determinadas aplicaciones que exigen los mismos requisitos de seguridad y formas de usos.

La Declaración de Practicas de Certificación es definida como un conjunto de prácticas adoptadas por una Autoridad de Certificación para la emisión de certificados. En general contiene información detallada sobre su sistema de seguridad, soporte, administración y emisión de los Certificados, además sobre la relación de confianza entre el Suscriptor o usuario y la Autoridad de Certificación. Pueden ser documentos absolutamente comprensibles y robustos, que proporcionan una descripción exacta de los servicios ofertados, procedimientos detallados de la gestión del ciclo vital de los certificados, etc.

Estos conceptos de Políticas de Certificación y Declaración de Practicas de Certificación son distintos, pero aún así es muy importante su interrelación.

Una CPS detallada no forma una base aceptable para la interoperabilidad de Autoridades de Certificación. Las Políticas de Certificación sirven mejor como medio en el cual basar estándares y criterios de seguridad comunes.

En definitiva una política define "**que"** requerimientos de seguridad son necesarios para la emisión de los certificados. La CPS nos dice "**como**" se cumplen los requerimientos de seguridad impuestos por la política.

1.2. Vista General

El presente documento especifica la Política de Certificación del Certificado Camerfirma para Sello de tiempos, y está basada en la especificación del estándar RFC 3628 – *Policy Requirements for Time-Stamping Authorities (TSAs)*, de IETF y del ETSI TS 102 023 V1.2.1 (2003-01) Electronic Signatures and Infrastructures (ESI) Policy requirements for time-stamping authorities.

Esta política al depender de una política superior de entidad raíz, se encuentra en conformidad con lo dispuesto por la PC de Chambers of Commerce Root, que podrá localizar en la siguiente dirección *http://www.camerfirma.com/area-de-*

usuario/jerarquia-politicas-y-practicas-de-certificacion/ y que establece las normas, políticas y procedimientos para la emisión de certificados de segundo nivel.

Esta política define las reglas y responsabilidades generales que debe seguir la Autoridad de Sellado de tiempo TSA para la emisión de sellos de tiempo. Este documento define los participantes del proceso sus responsabilidades y derechos así como el margen de aplicabilidad. Información más detallada de estos procedimientos puede ser encontrada en las Prácticas de certificación de AC Camerfirma SA.

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

El servicio de sellado de tiempo se compone de dos componentes diferenciados:

- Suministro de Sellos de Tiempo.
- Gestión del servicio de sellado de tiempo.

La división de estos componentes solamente se toma por motivos de clarificación de los requerimientos especificados en estas políticas.

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

- La firma digital de la autoridad de sellado de tiempo.
- Identificador electrónico único del documento (HASH o resumen)
- Fecha y hora recogida de una fuente fiable de tiempo.

Tanto los usuarios del servicio como la parte confiante deberá consultar estas políticas y las practicas de certificación de la TSA para obtener detalles de cómo se implementa esta política de certificación.

En lo que se refiere al contenido de esta Política de Certificación, se considera que el lector conoce los conceptos básicos de PKI, certificación y firma digital, recomendando que, en caso de desconocimiento de dichos conceptos, el lector se informe a este respecto. En la página Web de Camerfirma (www.camerfirma.com) hay algunas informaciones útiles. Se ha utilizado el estándar RFC 3647 "*Internet X.509 Public Key Infraestructure Certificate Policy and Certification Practices Framewortk*" del Internet Engineering Task Force (IETF) como guía de asistencia en la redacción de este documento

1.3. Identificación

Nombre de la Política:	Camerfirma Certificado de Sello de Tiempo
Descripción:	Emisión de certificados de Sellado de tiempo.
Versión:	1.2.1
Fecha de Emisión:	Junio 2015
Referencia (OID):	1.3.6.1.4.1.17326.10.13.1 1.3.6.1.4.1.17326.10.13.1.2 1.3.6.1.4.1.17326.10.13.1.2.1 1.3.6.1.4.1.17326.10.13.1.3 1.3.6.1.4.1.17326.10.13.1.3.1
Localización:	http://www.camerfirma.com/area-de-usuario/jerarquia-politicas-y-practicas-de-certificacion/

1.4. Comunidad y Ámbito de Aplicación

Este documento puede ser utilizado por terceros receptores de los sellos de tiempo de camerfirma y suscriptores del servicio de emisión de sellos de tiempo como base para confirmar la fiabilidad de los servicios descritos en el. La política de la autoridad de sellos de tiempo esta basada en criptografía de clave publica, fuentes seguras de tiempo y certificados digitales.

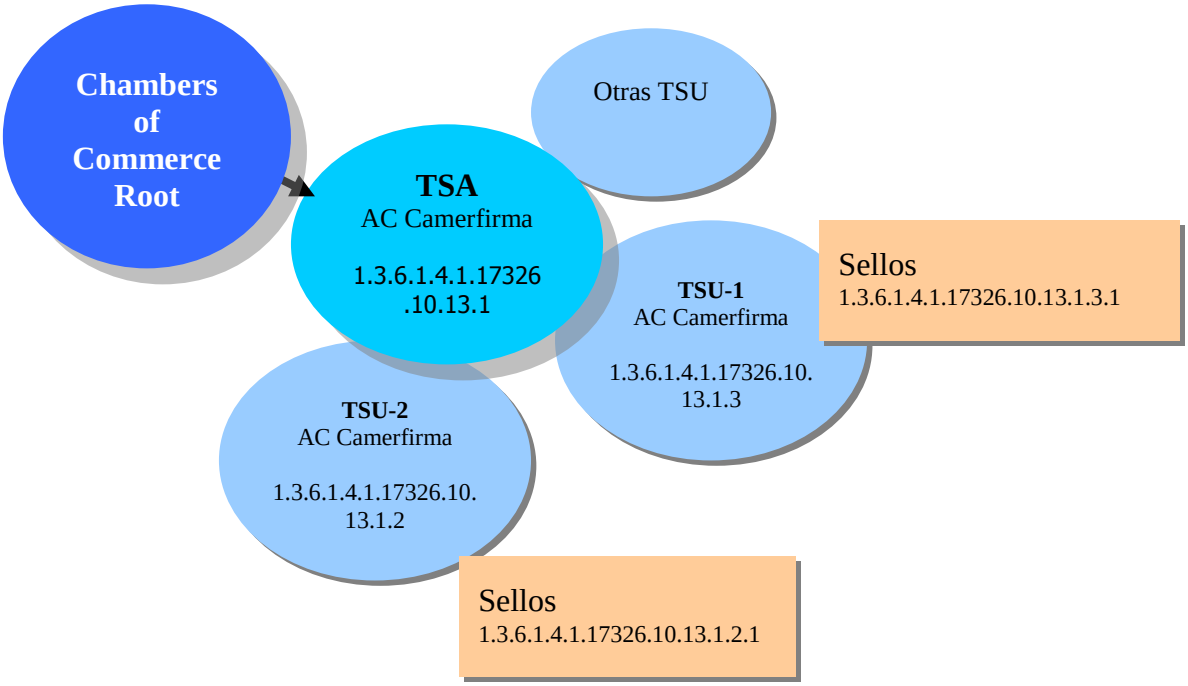
1.4.1 TSA-TSU

Una TSA (Autoridad de Sellado de tiempo) es un elemento de confianza en el que el usuario (suscriptores y terceras partes receptoras de sellos) confían para la emisión de sellos de tiempo. La TSA tiene la responsabilidad última sobre todos los servicios relacionados con la emisión de los sellos de tiempo. La TSA tiene la responsabilidad sobre las TSU (Unidades de sellado de tiempo) las cuales emiten los sellos de tiempo en representación de la TSA.

La TSA puede subcontratar todos o algunos componentes de la TSA incluidos los servicios de emisión de sellos usando las claves de TSU aunque en todo momento será la última responsable del servicio.

El servicio de sellado de tiempo se compone de una autoridad TSA y una o mas Unidades de Sellado de Tiempo (TSU). Esta última tiene asociada una clave privada que utiliza para la firmar de los sellos de tiempo. Esta estructura permite una mayor flexibilidad a la hora de implantar distintos servicios de sellado con requerimientos diferenciados.

El servicio de sellado de tiempo de AC Camerfirma tiene la siguiente estructura:



Existe una autoridad de Sellado de tiempo TSA que emite certificados a TSU. Las TSU (Unidades de Sellado de Tiempo) pueden emitir sellos de tiempo en nombre de la TSA bajo condiciones distintas en lugares distintos y con recursos independientes. Estas a su vez podrán emitir sellos de tiempo.

En el esquema gestionado por Camerfirma representado en la ilustración previa, la TSU-1 emite sellos de tiempo desde unas claves gestionadas en software y sin garantías de disponibilidad y rendimiento. La TSU-2 emite sellos de tiempo desde claves gestionadas en dispositivo hardware y con las garantías de servicio descritas en este documento.

Los sellos de tiempo se distinguirán por las TSU emisora y por el OID de política descrito en él.

1.4.2 Suscriptor

Bajo esta Política, el Suscriptor es una entidad que posee un certificado Camerfirma de TSU para la creación de un servicio de sellado de tiempo o la propia AC Camerfirma SA.

1.4.3 Tercero que confía o usuario

En esta Política se entiende por Tercero que confía o usuario, a la persona que voluntariamente confía en los sellos de tiempo emitidos bajo esta política y se sujeta a lo dispuesto en ella por lo que no se requerirá acuerdo posterior alguno.

1.4.4 Solicitante

A los efectos de esta Política, se entenderá por Solicitante la persona física que solicita un certificado para la implantación de una unidad de sellado de tiempo de TSU Camerfirma o un servicio de emisión de sellos de tiempo bajo alguna de las TSU existentes.

1.4.5 Ámbito de Aplicación y Usos

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

1.4.6 Usos Prohibidos y no Autorizados

Bajo la presente Política no se permite 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 se permite la utilización distinta de lo establecido en esta Política y en la Declaración de Practicas de Certificación.

No están autorizadas las alteraciones en los Certificados, que deberán utilizarse tal y como son suministrados por la TSA.

1.5. Contacto

Esta política de certificación está administrada y gestionada por el Departamento de Operaciones de Camerfirma SA, pudiendo ser contactado por los siguientes medios:

E-mail:	juridico@camerfirma.com
Teléfono:	+34 902 361 207
Fax:	+34 902 930 422
Dirección:	Camerfirma – Departamento Jurídico C/ Ribera del Loira, 12 - 28042 Madrid
Localización:	https://www.camerfirma.com/address

2. Cláusulas Generales

2.1. Obligaciones

Este apartado incluye todas las obligaciones, garantías y responsabilidades de la TSA frente a los usuarios y terceras partes que voluntariamente confían en los servicios de sellado de tiempo, así como las obligaciones asumidas por las partes.

2.1.1 TSA

La TSA Garantizará:

- Cumplir lo dispuesto en esta política.
- Proteger su información contra pérdidas, destrucciones y falsificaciones.
- Proteger sus claves privadas de forma segura.
- Emitir certificados a las TSU de forma segura
- Revocar los certificados según lo dispuesto en esta política y publicar la correspondiente ARL.
- Informar a las AC's delegadas de los cambios que se produzcan en las presentes políticas
- El acceso permanente a los servicios de sellado de tiempo excluyéndose las tareas de mantenimiento programadas y aquellas descritas en el apartado 2.2.1 de estas políticas.
- La exactitud de la fecha y hora incorporada en los sellos de tiempo basadas en el sistema UTC. Como mínimo la exactitud del sistema estará por debajo de las centésimas de segundo.
- Suministrar una fuente fiable de tiempo a las TSU delegadas y establecer los mecanismos técnicos necesarios para detectar cualquier variación de los datos de tiempo utilizados por las TSU.
- Que los sellos de tiempo emitidos estarán libres de datos falsos y errores

2.1.2 Solicitante

El solicitante de un Certificado de TSU estará obligado a cumplir con lo dispuesto por la normativa aplicable y además a:

1. Respetar lo dispuesto en esta política de certificación.

2. Suministrar a la TSA la información necesaria para realizar una correcta identificación.

3. Confirmar la exactitud y veracidad de la información suministrada.

4. Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.

2.1.3 Suscriptor

El suscriptor para hacer uso del Sistema de Certificación TSA, asume la obligación de conocer y comprender plenamente las características y limitaciones determinadas en esta Declaración de Practicas de Certificación y de las Políticas y contratos comerciales vinculados.

El suscriptor de un Certificado de TSU estará obligado a:

5. Respetar lo dispuesto en esta política de certificación.

6. Proteger sus claves privadas de forma segura.

7. Emitir sello de tiempo conforme a esta Política y a los estándares de aplicación.

8. En caso de utilizar recursos técnicos propios para la emisión de los certificados La utilización de la fuente de tiempo suministrada por la TSA y utilizar mecanismos técnicos que permitan detectar cualquier variación sobre esta.

2.1.4 Tercero que confía o usuario.

Las terceras partes que voluntariamente confíen en los Sistemas de Certificación de esta TSA, asumen la obligación de:

- Verificar el estado de activación en que se encuentra el Certificado de la TSA 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.

- 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 empleo 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 practicas de certificación correspondientes.

- Tomar en consideración cualquier limite prescrito en otros acuerdos de servido.

2.2. Responsabilidad

La TSA será responsable del daño causado ante el Suscriptor o cualquier persona que de buena fe confíe en el certificado, siempre que exista dolo o culpa grave, respecto de:

1. La exactitud de toda la información contenida en sello de tiempo o en los certificados de TSU emitidos.

2. La garantía de que la clave pública y privada funcionan conjunta y complementariamente.

3. Cualquier responsabilidad que se establezca por la legislación vigente.

2.2.1 Exoneración de responsabilidad

La TSA no será responsable en ningún caso cuando se encuentran ante cualquiera de estas circunstancias:

1. Estado de Guerra, desastres naturales o cualquier otro caso de Fuerza Mayor

2. Por el uso de los certificados de TSU siempre y cuando exceda de lo dispuesto en la normativa vigente y la presente Política de Certificación

3. Por el uso indebido o fraudulento de los sellos de tiempo o CRL's emitidos por la TSA.

4. Por el uso de la información contenida en el Certificado de TSU o en la CRL.

5. Por el incumplimiento de las obligaciones establecidas para el Suscriptor o usuario en la normativa vigente, en la presente Política de Certificación, en las Prácticas Correspondientes o en los contratos establecidos por las partes.

6. Por el perjuicio causado en el periodo de verificación de las causas de revocación.

7. Fraude en la información presentada por el solicitante

2.2.2 Límite de responsabilidad en caso de pérdidas por transacciones

La TSA no se responsabilizará por las pérdidas por transacciones.

2.3. Responsabilidad financiera

La TSA no asume ningún tipo de responsabilidad financiera.

Podrán establecerse garantías particulares a través de seguros específicos que se negociarán individualmente.

2.4. Interpretación y ejecución

2.4.1 Legislación

La ejecución, interpretación, modificación o validez de las presentes Políticas se regirá por lo dispuesto en la legislación española vigente.

2.4.2 Independencia

La invalidez de una de las cláusulas contenidas en esta Política de Certificación no afectará al resto del documento. En tal caso se tendrá la mencionada cláusula por no puesta.

2.4.3 Notificación

Cualquier notificación referente a la presente Política de Certificación se realizará por correo electrónico o mediante correo certificado dirigido a cualquiera de las direcciones referidas en el apartado datos de contacto.

2.4.4 Procedimiento de resolución de disputas

Toda controversia o conflicto que se derive del presente documento, se resolverá definitivamente, mediante el arbitraje de derecho de un árbitro, en el marco de la Corte Española de Arbitraje, de conformidad con su Reglamento y Estatuto, a la que se encomienda la administración del arbitraje y la designación del árbitro o tribunal arbitral. Las partes hacen constar su compromiso de cumplir el laudo que se dicte

2.5. Tarifas

2.5.1 Tarifas de emisión de certificados y renovación

Los precios de los servicios de certificación o cualquier otro servicio relacionado estarán disponibles para los usuarios en la página Web de Camerfirma http://www.camerfirma.com/certificados.

2.5.2 Tarifas de acceso a los certificados

Sin estipular.

2.5.3 Tarifas de acceso a la información relativa al estado de los certificados o los certificados revocados

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

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

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

2.5.5 Política de reintegros

Sin estipular.

2.6. Políticas y Prácticas de Certificación

2.6.1 Declaración de Practicas de la TSA

La TSA demostrara que cuanta con la fiabilidad necesaria para la provisión del servicio de sellado de tiempos

En particular:

- Dispondrá de un análisis de riesgos para evaluar los activos de empresa y las amenazas de tal forma que determine si son necesarios controles de seguridad u operativos para protegerlos.
- Dispondrá de una Declaración de Prácticas y procedimientos usados para dar respuesta a todos los requerimientos expuestos en estas políticas.

- Las Declaración de Practicas identificara las obligaciones de todos los agentes (internos y externos) implicados en el soporte al servicio de sellado de tiempos.

- La TSA pondrá a disposición de suscriptores y usuarios la Declaración de Prácticas y cualquier documentación relevante que garantice la conformidad con esta política. La TSA no tiene que publicar la documentación que considere de uso confidencial.

- La TSA distribuirá a todos los suscriptores y usuarios los términos y condiciones de uso.

- La TSA dispondrá de un responsable de alto nivel con autoridad para aprobar la Declaración de Practicas.

- La autoridad responsable de la declaración de prácticas se asegurara que estas están implantadas de forma correcta.

- La TSA comunicara los cambios que valla a realizar en la Declaración de Practicas, estas deberán ser aprobadas y puestas a disposición de suscriptores y usuarios.

2.6.2 Declaración Informativa de la TSA-TSU.

La TSA o la TSU de forma delegada informará a todos los suscriptores y potenciales usuarios, los términos y condiciones sobre el uso del servicio de sellado de tiempo.

Esta Declaración al menos especificará por cada política distinta utilizada por la TSA:

- Contacto de la TSA
- Política de sello de tiempo aplicada
- Al menos un algoritmo resumen que se utilizara para representar a los datos a sellar en tiempo.
- Tiempo estimado de validez de la firma usada para firmar el token de tiempo. (Depende del algoritmo resumen usado el algoritmo de firma usado y la longitud de la clave).
- La exactitud de la fuente de tiempo empleada respecto a UTC.
- Cualquier limitación en el uso del servicio.
- Las obligaciones del suscriptor.
- Las obligaciones de los usuarios.
- Información de cómo verificar los sellos de tiempo de forma que un usuario puede considerar razonable confiar en un sello de tiempo y cualquier posible limitación en la validez de este.
- El periodo de tiempo de retención de los ficheros de auditoria.
- El marco jurídico aplicable, incluido cualquier declaración de cumplimiento de las regulaciones jurídicas nacionales.
- Limitaciones de responsabilidad.
- Proceso de resolución de disputas.
- Si la TSA ha sido auditada por un organismo independiente respecto a la conformidad con estas políticas de sellado de tiempo.

- Disponibilidad del servicio y expectativas de resolución ante incidentes que afecten a la provisión del servicio de sellado de tiempo.

2.7. Publicación y repositorios

2.7.1 Publicación de información de la TSA

La TSA estará obligada a publicar la información relativa a sus Políticas y Prácticas de Certificación.

La presente Política de Certificación es pública y se encontrará disponible en Internet.

Las Prácticas de Certificación de referencia serán así mismo públicas y se pondrán a disposición del público en una dirección de Internet.

2.7.1.1 Difusión de los certificados

La TSA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que los certificados son accesibles para los Suscriptores y usuarios.

En concreto:

a) El certificado de la TSA y TSUs son públicos y se encontrarán disponibles en la página Web de Camerfirma http://www.camerfirma.com/certificados.

b) La información a la que se refiere el punto a) estará disponible 24 horas al día, 7 días por semana. En caso de fallo del sistema u otros factores que no se encuentran bajo el control de la TSA , la TSA hará todos los esfuerzos para conseguir que este servicio informativo no esté inaccesible durante un período máximo de 24 horas.

2.7.2 Frecuencia de publicación

Las Políticas y Prácticas de Certificación se publicarán una vez hayan sido creadas o en el momento en que se apruebe una modificación de las mismas.

2.7.3 Controles de acceso

El acceso a la información catalogada como pública será gratuito y estará a disposición de los suscriptores y usuarios.

2.8. Auditorias

2.8.1 Frecuencia de las auditorias

Se realizará una auditoria con una periodicidad mínima bianual, salvo que se establezca un plazo menor por la normativa vigente.

2.8.2 Identificación y cualificación del auditor

El auditor debe poseer conocimientos y experiencia en sistemas de PKI y en seguridad de sistemas informáticos.

2.8.3 Relación entre el auditor y la TSA

La auditoria deberá ser realizada por un auditor independiente y neutral.

No obstante, lo anterior no impedirá la realización de auditorias internas periódicas.

2.8.4 Tópicos cubiertos por la auditoria

La auditoria deberá verificar en todo caso:

a) Que la TSA tiene un sistema que garantice la calidad del servicio prestado

b) Que la TSA cumple con los requerimientos de esta Política de Certificación

c) Que las Prácticas de Certificación de la TSA 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.

2.9. Confidencialidad

2.9.1 Tipo de información a mantener confidencial

Se determinará por la TSA la información que deba ser considerada confidencial, debiendo cumplir en todo caso con la normativa vigente en materia de protección de datos.

2.9.2 Tipo de información considerada no confidencial

Se considerará como información no confidencial:

a) La contenida en la presente Política y en las Prácticas de Certificación

b) La información contenida en los certificados de TSA y TSU.

c) Cualquier información cuya publicidad sea impuesta normativamente

d) Las que así se determinen por las Prácticas de Certificación siempre que no contravengan ni la normativa vigente ni lo dispuesto en esta Política de Certificación.

2.9.3 Divulgación de información de revocación de certificados

La forma de difundir la información relativa a la revocación de un certificado se realizará mediante la publicación de las correspondientes CRLs.

2.9.4 Envío a la Autoridad Competente

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

2.10. Derechos de propiedad intelectual

La TSA es titular en exclusiva de todos los derechos de propiedad intelectual que puedan derivarse del sistema de certificación que regula esta Política de Certificación. 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 la TSA 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 Certificación.

3. Gestión de claves de la TSA

3.1.1 Generación de claves de la TSA

La TSA se asegurará que sus claves criptográficas son generadas bajo un estricto control.

En particular:

- Las claves de TSA se generan en un ambiente de seguridad, directamente controlado por personal confiable de AC Camerfirma.
- La generación de las claves de TSA se generan dentro de un módulo criptográfico que reúna los requisitos FIPS 140-1 nivel 3.
- La generación de las claves de TSU pueden ser realizadas entornos diferentes, tanto en dispositivos hardware como software, estando este hecho descrito dentro del certificado asociado a las claves. Cuando las claves se generen en un dispositivo hardware este deberá cumplir los requerimientos identificados en FIPS 140-1 [FIPS 140-1] level 3 o superior, o Cumpla los requerimientos identificados en CEN Workshop Agreement CWA14167-2, o Es un sistema confiable certificado EAL 4 o superior
- Los Algoritmos criptográficos usados para la creación de la clave la firma y la longitud de la clave estarán reconocidos por un organismo de supervisión nacional o de acuerdo con las prácticas comunes en la gestión de sellos de tiempo.

3.1.2 Protección de la clave privada de la TSA-TSU.

La TSA se asegurara que la clave privada de la TSU y de la TSA permanecen confidenciales y mantienen su integridad.

En particular:

- La clave privada de la TSA se mantendrá en un dispositivo criptográfico que cumpla los requerimientos identificados en FIPS 140-1 [FIPS 140-1] level 3 o superior, o Cumpla los requerimientos identificados en CEN Workshop Agreement CWA14167-2, o en un sistema confiable certificado EAL 4 o superior.
- La clave privada de la TSU se mantendrá en un dispositivo criptográfico que cumpla los requerimientos identificados en FIPS 140-1 [FIPS 140-1] level 3 o superior, o Cumpla los requerimientos identificados en CEN Workshop Agreement CWA14167-2, o en un sistema confiable certificado EAL 4 o superior.

- Bajo esta política se permitirá la opción de almacenar las claves de la TSU en un almacén software aunque esta situación será reflejada en el contenido del certificado asignando uno de los OIDs que identifican esta política.

- No se recomienda la copia de las claves privadas para minimizar el riesgo de compromiso de clave. Si se realiza la copia, se utilizara tanto para la copia como la restauración de la clave un entorno seguro así como al menos el concurso de dos personas cualificadas y confiables, encargadas expresamente en la declaración de prácticas para realizar estas operaciones.

- Cualquier copia de la clave privada, será debidamente protegida para garantizar su confidencialidad.

3.1.3 Distribución de la clave pública de la TSU-TSA

LA TSA se asegurará que en la distribución de las claves públicas se garantice su integridad y autenticidad.

La clave pública de verificación se pondrá a disposición de las parte confiantes a través de un certificado de identidad.

3.1.4 Cambio de claves de TSU

El periodo de validez de las claves de TSU y TSA no será superior al periodo de tiempo que los algoritmos criptográficos elegidos sean adecuados para este uso.

Se requiere en esta política que los registros de actividad del servicio sean mantenidos al menos una año más de la duración del certificado asociado a la clave de la TSA-TSU.

Si la clave de la TSA-TSU está comprometida, habrá un número mayor de sellos de tiempo afectados cuanto más duración tenga el certificado asociado.

El compromiso de la clave de la TSA-TSU no solo depende de las características del módulo criptográfico sino de los procedimientos usados en la inicialización y exportación (cuando esta esté implementada).

3.1.5 Fin del ciclo de vida de la clave de TSA-TSU.

La TSA garantizara que la clave privada de la TSA-TSU no será usada después del final de su ciclo de vida.

En particular:

Que se utilizaran procedimientos técnicos y operacionales para generar nuevas claves cuando la actual caduca.

La clave privada de la TSA-TSU o cualquier parte de ella, es destruida completamente de tal forma que no pueda ser recuperada.

El sistema no permitirá la emisión de un sello de tiempo firmado con una clave privada de TSU caducada, ni que se firme un certificado de TSU con una clave privada de TSA caducada.

3.1.6 Gestión del ciclo de vida del dispositivo criptográfico usado para firmar sello de tiempo

La TSA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar la seguridad del hardware criptográfico a lo largo de su ciclo de vida. En particular, que:

a) el hardware criptográfico usado para la firma de sellos de tiempo no se manipula durante su transporte

b) el hardware criptográfico usado para la firma de sellos de tiempo no se manipula mientras está almacenado

c) el uso del hardware criptográfico usado para la firma de sellos de tiempo requiere el uso de al menos dos empleados de confianza.

d) el hardware criptográfico usado para la firma de sellos de tiempo está funcionando correctamente; y;

e) La clave privada de firma de la TSU almacenada en el hardware criptográfico se eliminará una vez se ha retirado el dispositivo

Antes de que el uso de la clave privada de la TSA caduque se deberá realizar un cambio de claves. La vieja TSA y su clave privada se desactivarán y se generará una nueva TSAcon una clave privada nueva y un nuevo DN.

Los siguientes certificados serán puestos a disposición pública en el directorio:

- Clave pública de la nueva TSA firmada por la clave privada de la vieja TSA
- Clave pública de la vieja TSA firmada con la clave privada de la nueva TSA.

3.2. Recuperación en caso de compromiso de la clave o desastre

La TSA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar en caso de desastre o compromiso de la clave privada de la TSA que éstas serán restablecidas tan pronto como sea posible. En particular:

3.2.1 La clave de la TSA se compromete

El plan de la continuidad de negocio de la TSA (o el plan de contingencia) tratará el compromiso o el compromiso sospechado de la clave privada de la TSA como un desastre.

En caso de compromiso, la TSA tomará como mínimo las siguientes medidas:

Informar a todos los suscriptores, usuarios y otras TSA s con los cuales tenga acuerdos u otro tipo de relación del compromiso.

Indicar que los certificados e información relativa al estado de la revocación firmados usando esta clave pueden no ser válidos.

3.2.2 Instalación de seguridad después de un desastre natural u otro tipo de desastre

La TSA debe tener un plan apropiado de contingencias para la recuperación en caso de desastres.

La TSA debe reestablecer los servicios de acuerdo con esta política dentro de las 48 horas posteriores a un desastre o emergencia imprevista. Tal plan incluirá una prueba completa y periódica de la preparación para tal reestablecimiento.

3.3. Cese de la TSA

La TSA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que se minimizan los posibles perjuicios que se puedan crear a los suscriptores o usuarios como consecuencia del cese de su actividad y en particular del mantenimiento de los registros necesarios a efectos probatorios en los procedimientos legales. En particular:

a) Antes del cese de su actividad deberá realizar, como mínimo, las siguientes actuaciones:

Informar a todos los suscriptores, usuarios y otras TSA s con los cuales tenga acuerdos u otro tipo de relación del cese.

La TSA revocará toda autorización a entidades subcontratadas para actuar en nombre de la TSA en el procedimiento de emisión de certificados.

La TSA realizará las acciones necesarias para transferir sus obligaciones relativas al mantenimiento de la información del registro y de los logs durante el periodo de tiempo indicado a los suscriptores y usuarios que confían.

Las claves privadas de la TSA serán destruidas o deshabilitadas para su uso.

b) La TSA tendrá contratado un seguro que cubra hasta el límite contratado los costes necesarios para satisfacer estos requisitos mínimos en caso de quiebra o por cualquier otro motivo por el que no pueda hacer frente a estos costes por sí mismo.

c) Se establecerán en la CPS las previsiones hechas para el caso de cese de actividad. Estas incluirán:

informar a las entidades afectadas

transferencia de las obligaciones de la TSA a otras partes

cómo debe ser tratada la revocación de certificados emitidos cuyo periodo de validez aún no ha expirado.

En particular, la TSA deberá:

Informar puntualmente a todos los suscriptores, empleados y usuarios con una anticipación mínima de 6 meses antes del cese

Transferir todas las bases de datos importantes, archivos, registros y documentos a la entidad designada durante las 24 horas siguientes a su terminación

4. Controles de Seguridad Física, Procedimental y de Personal

4.1. Controles de Seguridad física

La TSA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el acceso físico a los servicios críticos y que los riesgos físicos de estos elementos sean minimizados. En particular:

TSA General

El acceso físico a las instalaciones vinculadas a la generación de certificados y servicios de gestión de revocaciones deberá ser limitado a las personas autorizadas y las instalaciones en las que se firman los certificados deberán ser protegidas de las amenazas físicas.

Se establecerán controles para impedir la perdida, daño o compromiso de los activos de la empresa y la interrupción de la actividad

Se establecerán controles para evitar el compromiso o robo de información

Emisión de certificados sellos de tiempo y gestión de revocaciones.

Las actividades relativas a la emisión de certificados, sellos de tiempo y gestión de revocaciones serán realizadas en un espacio protegido físicamente de accesos no autorizados al sistema o a los datos.

La protección física se conseguirá por medio de la creación de unos anillos de seguridad claramente definidos (p.ej. barreras físicas) alrededor de la emisión de certificados y gestión de revocaciones. Aquellas partes de esta tarea compartidas con otras organizaciones quedarán fuera de este perímetro.

Los controles de seguridad física y medioambiental serán implementados para proteger las instalaciones que albergan los recursos del sistema, los recursos del sistema en si mismos y las instalaciones usadas para soportar sus operaciones. Los programas de seguridad física y medioambiental de la TSA relativos a la generación de certificados y servicios de gestión de revocaciones estarán provistos de controles de acceso físico, protección ante desastres naturales, sistemas anti-incendios, fallos eléctricos y de telecomunicaciones, humedad y protección antirrobo.

Se implementarán controles para evitar que los equipos, la información, soportes y software relativos a los servicios de la TSA sean sacados de las instalaciones sin autorización.

4.1.1 Ubicación y construcción

Las instalaciones de la TSA deben estar ubicadas en una zona de bajo riesgo de desastres y que permita un rápido acceso a las mismas conforme al plan de contingencias.

Así mismo, las instalaciones estarán equipadas con los elementos y materiales adecuados para poder albergar información de alto valor.

4.1.2 Acceso físico

El acceso físico a las zonas de seguridad estará limitado al personal autorizado previa autenticación.

4.1.3 Alimentación eléctrica y aire acondicionado

La TSA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que la alimentación eléctrica y el aire acondicionado son suficientes para soportar las actividades del sistema de la TSA

4.1.4 Exposición al agua

La TSA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el sistema de TSA está protegido de la exposición al agua.

4.1.5 Protección y prevención de incendios

La TSA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el sistema de TSA está protegido con un sistema anti-incendios.

4.1.6 Sistema de almacenamiento.

La TSA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el sistema de almacenamiento usado por el sistema de TSA está protegido de riesgos medioambientales como la temperatura, el fuego, la humedad y la magnetización.

4.1.7 Eliminación de residuos

La TSA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que los medios usados para almacenar o transmitir la información de carácter sensible como las claves, datos de activación o archivos de la TSA serán destruidos, así como que la información que contengan será irrecuperable

4.1.8 Backup remoto

La TSA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que las instalaciones usadas para realizar back-up externo, que tendrán el mismo nivel de seguridad que las instalaciones principales

4.2. Controles procedimentales

4.2.1 Roles de confianza

Los roles de confianza, en los cuales se sustenta la seguridad de la TSA, serán claramente identificados.

Los roles de confianza incluyen las siguientes responsabilidades:

Responsable de seguridad: asume la responsabilidad por la implementación de las políticas de seguridad así como gestión y revisión de logs.

Administradores de sistema: Están autorizados para instalar, configurar y mantener de los sistemas y aplicaciones de confianza de la TSA que soportan las operaciones de Certificación

Operador de sistema: Está autorizado para realizar funciones relacionadas con el sistema de backup y de recuperación

Administrador de CA: Responsable de la Administración y control de gestión de los sistemas de confianza de la TSA.

Operador de CA: Realizan funciones de apoyo en el control dual de las operaciones de la CA.

Auditor de CA: Realiza las labores de supervisión y control de la implementación de las políticas de seguridad

La TSA debe asegurarse que existe una separación de tareas para las funciones críticas de la CA, para prevenir que una persona use el sistema el sistema de TSA y la clave de la TSA sin detección.

La separación de los roles de confianza serán detallados en la CPS

4.2.2 Número de personas requeridas por tarea

Las siguientes tareas requerirán al menos un control dual:

- La generación de la clave de la TSA /TSU
- La recuperación y back-up de la clave privada de la TSA/TSU.

- Activación de la clave privada de la TSA.
- Cualquier actividad realizada sobre los recursos HW y SW que dan soporte a la autoridad de certificación.

4.2.3 Identificación y autentificación para cada rol

La TSA establecerá los procedimientos de identificación y autenticación de las personas implicadas en roles de confianza.

4.3. Controles de seguridad de personal

4.3.1 Requerimientos de antecedentes, calificación, experiencia, y acreditación

La TSA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el personal cumple con los requisitos mínimos razonables para el desempeño de sus funciones. En concreto:

TSA General

La TSA empleará personal que posea el conocimiento, experiencia y calificaciones necesarias y apropiadas para el puesto.

Los roles de seguridad y responsabilidades especificadas en la política de seguridad de la TSA, serán documentadas en la descripción del trabajo.

Se deberá describir el trabajo del personal de la TSA (temporal y fijo) desde el punto de vista de realizar un separación de tareas, definiendo los privilegios con los que cuentan, los niveles de acceso y una diferenciación entre las funciones generales y las funciones específicas de la TSA.

El personal llevará a cabo los procedimientos administrativos y de gestión de acuerdo con los procedimientos especificados para la gestión de la seguridad de la información.

Registro, generación de certificados y gestión de revocaciones

e) Deberá ser empleado el personal de gestión con responsabilidades en la seguridad que posea experiencia en tecnologías de firma electrónica y esté familiarizado con procedimientos de seguridad.

f) Todo el personal implicado en roles de confianza deberá estar libre de intereses que pudieran perjudicar su imparcialidad en las operaciones de la TSA

g) El personal de la TSA será formalmente designado para desempeñar roles de confianza por el responsable de seguridad

h) La TSA no asignará funciones de gestión a una persona cuando se tenga conocimiento de la existencia de la comisión de algún hecho delictivo que pudiera afectar al desempeño de estas funciones.

4.3.2 Procedimientos de comprobación de antecedentes

La TSA no podrá asignar funciones que impliquen el manejo de elementos críticos del sistema a aquellas personas que no posean la experiencia necesaria en la propia TSA que propicie la confianza suficiente en el empleado. Se entenderá como experiencia necesaria el haber pertenecido al Departamento en cuestión durante al menos 6 meses.

4.3.3 Requerimientos de formación

La TSA debe realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el personal que realiza tareas de operaciones de TSA o AR, recibirá una formación relativa a:

Los principales mecanismos de seguridad de TSA y/o AR

Todo el software de PKI y sus versiones empleados en el sistema de la TSA

Todas las tareas de PKI que se espera que realicen

Los procedimientos de resolución de contingencias y continuidad de negocio

4.3.4 Requerimientos y frecuencia de la actualización de la formación

La formación debe darse con una frecuencia anual para asegurar que el personal está desarrollando sus funciones correctamente.

4.3.5 Frecuencia y secuencia de rotación de tareas

No estipulado

4.3.6 Sanciones por acciones no autorizadas

La TSA deberá fijar las posibles sanciones por la realización de acciones no autorizadas.

4.3.7 Requerimientos de contratación de personal

Ver apartado 4.3.1.

4.3.8 Documentación proporcionada al personal

Todo el personal de la TSA deberá recibir los manuales de usuario en los que se detallen al menos los procedimientos para el registro de certificados, creación, actualización, renovación, revocación y la funcionalidad del software empleado.

5. Controles de Seguridad Técnica

5.1. Estándares para los módulos criptográficos

Todas las operaciones criptográficas deben ser desarrolladas en un módulo validado por al menos FIPS-140-1 nivel 3 o por un nivel de funcionalidad y seguridad equivalente.

5.1.1 Control multipersona (n de entre m) de la clave privada

Se requerirá un control multipersona para la activación de la clave privada de la TSA. Este control deberá ser definido adecuadamente por la CPS en la medida en que no se trate de información confidencial o pueda comprometer de algún modo la seguridad del sistema.

5.1.2 Depósito de la clave privada (key escrow)

La clave privada de la TSA debe ser almacenada en un medio seguro protegido criptográficamente y al menos bajo un control dual.

La clave del suscriptor (TSA) deberá estar almacenada en un formato seguro y particionada de tal forma que ni pueda ser manipulada de forma individual.

5.1.3 Copia de seguridad de la clave privada

La TSA deberá realizar una copia de back up de su propia clave privada que haga posible su recuperación en caso de desastre o de pérdida o deterioro de la misma de acuerdo con el apartado anterior.

Las copias de las claves privadas del suscriptor (TSA) se regirán por lo dispuesto en el punto anterior.

5.1.4 Archivo de la clave privada

La clave privada de la TSA no podrá ser archivada de acuerdo una vez finalizado su ciclo de vida.

Las claves privadas de la TSU no podrán ser archivadas una vez finalizado su ciclo de vida

5.1.5 Introducción de la clave privada en el módulo criptográfico

Las claves que se generaran dentro del módulo criptográfico. Solo saldrán cifradas del dispositivo. Tanto para extraerlas como introducirlas en el dispositivo se utilizara al menos la colaboración de dos personas.

5.1.6 Método de activación de la clave privada

La clave privada de la TSA deberá ser activada conforme al apartado 6.3.1.

5.1.7 Método de desactivación de la clave privada

No estipulado.

5.1.8 Método de destrucción de la clave privada

La TSA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que la clave privada de la TSA no será usada una vez finalizado su ciclo de vida.

Todas las copias de la clave privada de firma de la TSA deberán ser destruidas o deshabilitadas de forma que la clave privada no pueda ser recuperada.

5.2. Otros aspectos de la gestión del par de claves

5.2.1 Archivo de la clave pública

La TSA deberá conservar todas las claves públicas de verificación

5.2.2 Periodo de uso para las claves públicas y privadas

El periodo de uso de la clave privada de la TSA será de 30 años.

El periodo de uso de la clave privada de la TSU será de 5 años.

5.3. Controles de seguridad informática

La TSA empleará sistemas fiables y productos que estén protegidos contra modificaciones.

En particular se aplicaran como referencia los controles de seguridad descritos en ISO17799 para la gestión de sistemas de información, así como los requerimientos para sistemas confiables para la gestión de certificados de firma electrónica descritos en CWA14167-1.

6. Perfiles de Certificado y CRL

6.1. Perfil de Certificado

Todos los certificados emitidos bajo esta política serán conformes al estándar X.509 versión 3 y al RFC 2459 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

6.1.1 Número de versión

Deberá indicarse en el campo versión que se trata de la v.3

6.1.2 Extensiones del certificado TSA

EXTENSIÓN DEL CERTIFICADO		VALOR
Versión **Serial Number (certificate)** **Algoritmo de firma**		V3 12 Sha1RSA
Emisor (issuer)	CN O OU C	Chambers of Commerce Root Camerfirma SA CIF A82743287 http://www.chambersign.org EU
Válido desde **Válido hasta**		jueves, 19 de mayo de 2005 9:20:50 domingo, 20 de mayo de 2035 9:20:50
Asunto.	C CN O L E SN	ES TSA Camerfirma TSA CA AC Camerfirma SA Madrid (see current address at www.camerfirma.com/address) ac_camerfirma_tsa_ca@camerfirma.com A82743287
Clave pública		RSA 2.048 Bits
Identificador de clave de asunto		bf fa 7e ae b9 9d aa 65 69 72 c6 32 16 8d e0 10 2e a5 9b 22
Identificador de clave del emisor		Id. de clave=e3 94 f5 b1 4d e9 db a1 29 5b 57 8b 4d 76 06 76 e1 d1 a2 8a Emisor de certificado: Dirección del directorio: CN=Chambers of Commerce Root OU=http://www.chambersign.org O=AC Camerfirma SA CIF A82743287 C=EU Número de serie del certificado=00
Punto de distribución CRL		http://crl.chambersign.org/chambersroot.crl

Nombre alternativo del sujeto	ac_camerfirma_tsa_ca@camerfirma.com
Nombre alternativo del Emisor	chambersroot@chambersign.org
Bases del certificado	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.17326.10.13.1 [1,1]Información de calificador de directiva: Id. de calificador de directiva=CPS Calificador: http://cps.camerfirma.com/cps/ac_camerfirma_tsa_ca.html
Restricción básicas<critica> **Uso de la clave <critica>**	Tipo de asunto= Entidad emisora de certificados (CA) Restricción de longitud de ruta=11 Firma digital, Firma de certificados, Firma CRL sin conexión, Firma CRL (86)
Algoritmo de identificación	Sha1
Huella digital	e3 f1 5b b2 da ea 3b 0e 8d 61 75 17 af 9d fe a1 fd ca 6a f0

6.1.3 Extensiones del certificado TSU

EXTENSIÓN DEL CERTIFICADO		VALOR
Versión		V3
Serial Number (certificate)		05
Algoritmo de firma		Sha1RSA
Emisor (issuer)	C CN O L E SN	ES TSA Camerfirma TSA CA AC Camerfirma SA Madrid (see current address at www.camerfirma.com/address) ac_camerfirma_tsa_ca@camerfirma.com A82743287
Válido desde		<fecha de inicio de la validez>
Válido hasta		<fecha de fin de la validez>
Asunto.	C CN O L E SN	ES TSU 1 AC Camerfirma AC Camerfirma SA Madrid (see current address at www.camerfirma.com/address) tsa_camerfirma@camerfirma.com A82743287
Clave pública		RSA 1024
Identificador de clave de asunto		SHA-1 Clave
Identificador de clave del emisor		Id. de clave Emisor de certificado Número de serie del certificado
Punto de distribución CRL		http://crl.camerfirma.com/tsa_camerfirma.crl http://crl1.camerfirma.com/tsa_camerfirma.crl
Nombre alternativo del sujeto		Nombre RFC822=tsa_camerfirma@camerfirma.com

Bases del certificado	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.17326.10.13.1.1 [1,1]Información de calificador de directiva: Id. de calificador de directiva=CPS Calificador: http://cps.camerfirma.com/cps/ac_camerfirma_tsa_ca.html [1,2]Información de calificador de directiva: Id. de calificador de directiva=Aviso de usuario Calificador: Texto de aviso=**TSU Software AC Camerfirma**
Restricción básicas<critica> **Uso de la clave <critica>** **Uso Mejorado de Clave**	Tipo de asunto=Entidad final Restricción de longitud de ruta=Ninguno Firma digital, Sin repudio (c0) Impresión de fecha (1.3.6.1.5.5.7.3.8)
Algoritmo de identificación	Sha1
Huella digital	<fingerprint>

6.1.4 Sellos de tiempo

El sello de tiempo tendrá seguirá 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),
grantedWithMods (1),
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

unacceptedExtension (16),

The requested extension is not supported

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 **timestampToken** 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,
serialNumber	INTEGER,
genTime	GeneralizedTime,
accuracy	Accuracy OPTIONAL,
ordering	BOOLEAN DEFAULT FALSE,
nonce	INTEGER OPTIONAL,
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

6.1.5 Acceso al servicio:

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

6.1.6 Sincronización del reloj con UTC

El servicio de sincronización de tiempos estará 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 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 (NTP v3).

6.1.7 Identificadores de objeto (OID) de los algoritmos

El identificador de objeto del algoritmo de firma será 1. 2. 840. 113549. 1. 1. 5

El identificador de objeto del algoritmo de la clave pública será rsaEncryption 1. 2. 840. 113549. 1. 1. 1

6.1.8 Restricciones de los nombres

No estipulado

6.2. Perfil de CRL

Para el certificado de TSA.

C	V2
Emisor	CN = Chambers of Commerce Root OU = http://www.chambersign.org O = TSA Camerfirma SA CIF A82743287 C = EU
Periodo máximo de validez	6 Meses
Algoritmo de firma	Sha1withRSA
2.5.29.20 Nº de serie	Presente
Identificador de clave de autoridad	Id. de clave=e3 94 f5 b1 4d e9 db a1 29 5b 57 8b 4d 76 06 76 e1 d1 a2 8a Emisor de certificado: Dirección del directorio: CN=Chambers of Commerce Root OU=http://www.chambersign.org O=AC Camerfirma SA CIF A82743287 C=EU Número de serie del certificado=00
Versión	V2

Para el certificado de TSU.

Version	V2
Emisor	CN = AC Camerfirma TSA CA O = AC Camerfirma SA Número de serie = A82743287 L = Madrid (see current address at www.camerfirma.com/address) E = ac_camerfirma_tsa_ca@camerfirma.com C = ES
Periodo máximo de validez	1 Mes
Algoritmo de firma	Sha1withRSA
2.5.29.20 Nº de serie	Presente
Identificador de clave de autoridad	Id. de clave=bf fa 7e ae b9 9d aa 65 69 72 c6 32 16 8d e0 10 2e a5 9b 22 Emisor de certificado:

Dirección del directorio: CN=Chambers of Commerce Root OU=http://www.chambersign.org O=AC Camerfirma SA CIF A82743287 C=EU Número de serie del certificado=12

6.2.1 Número de versión

Deberá indicarse en el campo versión que se trata de la v.2

6.2.2 CRL y extensiones

No estipulado

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

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 Camerfirma.

En la Web de Camerfirma se mantendrá un histórico con las versiones anteriores de las políticas.

Los usuarios 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 usuarios 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 una dirección de Internet definida en la CPS.

7.4. Procedimientos de aprobación de la CPS

Para la aprobación y autorización de una TSA se deberán respetar los procedimientos especificados por la PA. Las partes de la CPS de una TSA que contenga información relevante en relación a su seguridad, toda o parte de esa CPS no estará disponible públicamente.

Anexo I. Acrónimos

AC	Autoridad de Certificación
AR	Autoridad de Registro
CPS	*Certification Practice Statement*. Declaración de Prácticas de Certificación
CRL	*Certificate Revocation List.* Lista de certificados revocados
CSR	*Certificate Signing Request.* Petición de firma de certificado
DES	*Data Encryption Standard*. Estándar de cifrado de datos
DN	*Distinguished Name.* Nombre distintivo dentro del certificado digital
DSA	*Digital Signature Algorithm.* Estándar de algoritmo de firma
DSCF	Dispositivo seguro de creación de firma
DSADCF	Dispositivo seguro de almacén de datos de creación de firma
FIPS	*Federal Information Processing Standard Publication*
IETF	*Internet Engineering Task Force*
ISO	*International Organization for Standardization.* Organismo Internacional de Estandarización
ITU	*International Telecommunications Union.* Unión Internacional de Telecomunicaciones
LDAP	*Lightweight Directory Access Protocol*. Protocolo de acceso a directorios
OCSP	*On-line Certificate Status Protocol.* Protocolo de acceso al estado de los certificados
OID	*Object Identifier*. Identificador de objeto
PA	*Policy Authority.* Autoridad de Políticas
PC	Política de Certificación
PIN	*Personal Identification Number*. Número de identificación personal
PKI	*Public Key Infrastructure*. Infraestructura de clave pública

RSA Rivest-Shimar-Adleman. Tipo de algoritmo de cifrado

SHA-1 *Secure Hash Algorithm.* Algoritmo seguro de Hash

SSL *Secure Sockets Layer.* Protocolo diseñado por Netscape y convertido en estándar de la red, permite la transmisión de información cifrada entre un navegador de Internet y un servidor.

TCP/IP *Transmission Control. Protocol/Internet Protocol*. Sistema de protocolos, definidos en el marco de la IEFT. El protocolo TCP se usa para dividir en origen la información en paquetes, para luego recomponerla en destino. El protocolo IP se encarga de direccionar adecuadamente la información hacia su destinatario.

Anexo II. Definiciones

Autoridad de Certificación	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 políticas	Persona o conjunto de personas responsable de todas las decisiones relativas a la creación, administración, mantenimiento y supresión de las políticas de certificación y CPS.
Autoridad de Registro	Entidad responsable de la gestión de las solicitudes e identificación y registro de los solicitantes de un certificado.
Certificación cruzada	El establecimiento de una relación de confianza entre dos AC's, mediante el intercambio de certificados entre las dos en virtud de niveles de seguridad semejantes.
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.** La clave privada de la AC será usada para firma de certificados y firma de CRL's
CPS	Conjunto de prácticas adoptadas por una Autoridad de Certificación para la emisión de certificados en conformidad con una política de certificación concreta.

CRL	Archivo que contiene una lista de los certificados que han sido revocados en un periodo de tiempo determinado y que es firmada por la AC.
Datos de Activación	Datos privados, como PIN's o contraseñas empleados para la activación de la clave privada
DSADCF	*Dispositivo seguro de almacén de los datos de creación de firma.* Elemento software o hardware empleado para custodiar la clave privada del suscriptor de forma que solo él tenga el control sobre la misma.
DSCF	*Dispositivo Seguro de creación de firma*. Elemento software o hardware empleado por el suscriptor para la generación de firmas electrónicas, de manera que se realicen las operaciones criptográficas dentro del dispositivo y se garantice su control únicamente por el suscriptor.
Entidad	Dentro del contexto de las políticas de certificación de Camerfirma, 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)
OID	Identificador numérico único registrado bajo la estandarización ISO y referido a un objeto o clase de objeto determinado.
Par de claves	Conjunto formado por la clave pública y privada, ambas relacionadas entre si matemáticamente.
PKI	Conjunto de elementos hardware, software, recursos humanos, procedimientos, etc., que

	componen un sistema basado en la creación y gestión de certificados de clave pública.
Política de certificación	Conjunto de reglas que definen la aplicabilidad de un certificado en una comunidad y/o en alguna aplicación, con requisitos de seguridad y de utilización comunes
Suscriptor	Dentro del contexto de las políticas de certificación de Camerfirma, persona cuya clave pública es certificada por la AC y dispone de una privada válida para generar firmas digitales.
Tercero que confía	Dentro del contexto de las políticas de certificación de Camerfirma, persona que voluntariamente confía en el certificado digital y lo utiliza como medio de acreditación de la autenticidad e integridad del documento firmado