Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

POLÍTICA Y DECLARACIÓN DE PRÁCTICAS DEL SERVICIO DE SELLADO DE TIEMPO

	NOMBRE	FECHA
Elaborado por:	FNMT-RCM / 2.2	04/03/2015
Revisado por:	FNMT-RCM / 2.2	18/03/2015
Aprobado por:	FNMT-RCM / 2.2	23/03/2015

HISTÓRICO DEL DOCUMENTO			
Versión	**Fecha**	**Descripción**	**Autor**
1.1	01/05/2003	Creación del documento	FNMT-RCM
2.0	07/12/2009	Actualización de la declaración debida a la adecuación del servicio a ETSI 102 023	FNMT-RCM
2.1	19/12/2011	Ampliación de las algoritmias aceptadas para el resumen de la información que recibe el servicio. Cambio de certificados empleados para la emisión de sellos de tiempo bajo la política de sellado de tiempo de AC AP FNMT-RCM Inclusión de información sobre una nueva TSU.	FNMT-RCM
2.2	23/03/2015	Reducción a una unidad de sellado (TSU). Actualización de la algoritmia a RSA 3072 y de las URL de acceso.	FNMT-RCM

Referencia: DPST/DPST0202/SGPSC/2015

Documento clasificado como: *Público*

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

1. REFERENCIAS

[DGPC] – Declaración General de Prácticas de Certificación (http://www.cert.fnmt.es/dpcs/)

[ETSI TS 102 042] - ETSI TS 102 042 Policy requirements for certification authorities issuing public key certificates,

[ETSI TS 101 456] - ETSI TS 101 456 Policy requirements for certification authorities issuing qualified certificates,

[ETSI TS 102 023] - ETSI TS 102 023 Policy requirements for time-stamping authorities, y

[ETSI TS 101 861] - ETSI TS 101 861 Time stamping profile

[ETSI TS 102 176] - ETSI TS 102 176 Algorithms and Parameters for Secure Electronic Signatures

[RFC 3628] - RFC 3628 Policy Requirements for Time-Stamping Authorities (TSAs)

[RFC 3161] - RFC 3161 Internet X.509 Public Key Infrastructure – Time Stamp Protocol (TSP)

2. ACRÓNIMOS Y DEFINICIONES

1. A las definiciones dispuestas en la DGPC, para la interpretación del presente documento se añaden las siguientes:

   - *Prestador de Servicios de Confianza*: La persona física o jurídica que presta uno o más *Servicios de Confianza* de conformidad con lo establecido en el REGLAMENTO (UE) Nº 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

   (Los términos señalados en cursiva se definen en el presente documento o en la Declaración General de Prácticas de Certificación)

3. INTRODUCCIÓN Y OBJETO

2. La Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, de aquí en adelante FNMT-RCM, presta servicios de *Sellado de Tiempo* cuyo objeto es dar fe de la existencia de un conjunto de datos en un instante determinado en la línea de tiempo. Para ello utiliza la referencia temporal proporcionada por la Sección de Hora del Real Instituto y Observatorio de la Armada en San Fernando, que tiene como misión el mantenimiento de la unidad básica de tiempo, declarado a efectos legales como Patrón Nacional de dicha unidad, así como el mantenimiento y difusión oficial de la escala "Tiempo Universal Coordinado" (UTC -ROA-), considerada a todos los efectos como la base de la hora legal en todo el territorio español (Real Decreto 1308/1992, de 23 octubre 1992).

3. Las garantías que la FNMT-RCM proporciona a través de este tipo de servicios están basadas en la certificación, mediante técnicas de firma electrónica, de una representación del

conjunto de datos sobre los que proporcionar la evidencia. Así pues, para la prestación del servicio, la FNMT-RCM requiere una petición previa por parte del solicitante del *Sellado de Tiempo* (se envía la representación del conjunto de datos), a lo que contestará con el documento electrónico correspondiente (*Sello de tiempo*).

4. El presente documento se considera un anexo a la DGPC y constituye la *Política de Sellado de Tiempo* y la *Declaración de Prácticas del Servicio de Sellado de Tiempo*, de aquí en adelante PST y DPST respectivamente, de la FNMT-RCM)en su actividad como Prestador de Servicios de Confianza (PSC), y recoge el conjunto de políticas y prácticas operativas que emplea en la emisión de "*Fechados electrónicos*" o "*Sellos de tiempo*" para garantizar que el servicio que los origina cumple los requisitos de seguridad, disponibilidad y funcionalidad exigibles.

5. Este es un documento declarativo en el que se describen los aspectos más relevantes del *Servicio de Sellado de Tiempo* y los procedimientos empleados y/o definidos para su gestión y utilización. Asimismo se proporciona una autodeclaración de las medidas de salvaguarda de la infraestructura y de los controles de seguridad técnicos y no técnicos aplicados a los sistemas participantes en la prestación del servicio.

6. Por otra parte, la PST y la DPST representan el conjunto de condiciones de uso, responsabilidades y obligaciones de las partes, y limitaciones del *Servicio de Sellado de Tiempo* aplicables en el marco de la *Comunidad Electrónica* y previa suscripción de los pertinentes acuerdos de utilización.

7. En conclusión, el presente documento tiene por objeto la información pública de las condiciones y características del *Servicio de Sellado de Tiempo* por parte de la FNMT-RCM como PSC recogiendo, en concreto, las obligaciones que se compromete a cumplir en relación con la gestión de los *Datos de Creación y Verificación de Firma* y de los *Certificados* empleados para ofrecer el servicio y las condiciones aplicables a la solicitud, expedición, uso, y extinción de la vigencia de los *Sellos de Tiempo*.

8. Asimismo, el presente documento también recoge los derechos y obligaciones de todas las partes que confían y aceptan el servicio.

9. Como quiera que la prestación del *Servicio de Sellado de Tiempo* se enmarca dentro de los Servicios de Confianza de la FNMT-RCM, es de aplicación lo referido en la [DGPC] sobre el régimen de responsabilidad aplicable a los miembros de la *Comunidad Electrónica* y terceros que confían en dichos servicios, los controles de seguridad aplicados a sus procedimientos e instalaciones, la protección de datos de carácter personal y demás cuestiones de tipo informativo relacionadas con el *Sellado de Tiempo*.

10. Así pues, consideraremos la *Declaración de Prácticas de Sellado de Tiempo* de la *Política de Sellado de Tiempo* identificada en el presente documento como el conjunto de la [DGPC] más los apartados correspondientes de este documento.

4. ORDEN DE PRELACIÓN

11. La FNMT-RCM ofrece servicios de *Sellado de Tiempo* en el marco de su actividad como *Prestador de Servicios de Confianza* y a través de las correspondientes unidades de *Sellado de Tiempo* (TSU).

12. Por tanto, la FNMT-RCM está constituida como *Autoridad de Sellado de Tiempo* (TSA) y, con objeto de garantizar las prestaciones del servicio, se reserva el derecho de establecer cuantas unidades de sellado de tiempo (TSU) considere oportunas y la gestión de estas conforme a políticas y prácticas particulares y diferenciadas.

13. Con este marco de actuación se establece el siguiente orden de prelación (de mayor a menor) para la documentación de declaraciones del *Servicio de Sellado de Tiempo*:

    1) Si existieran condiciones particulares o *Leyes de Emisión* aplicables a determinadas unidades de sellado de tiempo, estas se identificarían de forma inequívoca y sus políticas y prácticas particulares se harían constar en el presente documento, teniendo prevalencia sobre las generalidades del *Servicio de Sellado de Tiempo*.

    2) Las presentes *Política y Declaración de Prácticas de Sellado de Tiempo* aplicables a la prestación del *Servicio de Sellado de Tiempo*, expuestas en la totalidad de este documento, tendrán prevalencia sobre las condiciones generales de la prestación de servicios de certificación por parte de la FNMT-RCM y expuestas en el documento [DGPC]

    3) La [DGPC], que afecta de manera general a cualquier servicio de confianza prestado por la FNMT-RCM y se aplicará supletoria y subsidiariamente sobre los documentos referidos en los apartados 1 y 2 anteriores.

5. DISPONIBILIDAD DE INFORMACIÓN Y COMUNICACIONES

14. Véase [DGPC]

6. CONTROLES DE SEGURIDAD, REGISTRO DE EVENTOS Y AUDITORÍAS

15. Véase [DGPC]

7. FUENTE DE TIEMPO EMPLEADA PARA LA PRESTACIÓN DEL SERVICIO Y PERIODO DE VALIDEZ DE LOS SELLOS DE TIEMPO

16. El Sistema de Sincronismo con el Real Observatorio de la Armada (SS-ROA) instalado en el Centro de Proceso de Datos (CPD) de la FNMT-RCM tiene como objetivo proporcionar una fuente de referencia temporal trazable a la escala de tiempo UTC (ROA), al *Servicio de Sellado de Tiempo* de la FNMT-RCM.

17. El SS-ROA, está compuesto principalmente por un patrón de frecuencia de Rubidio (Symmetricom Rubidium Frequency Standard 8040), un sistema de comparación de tiempo y frecuencia mediante sistema de navegación por satélites GPS (GPS Symmetricom SyncServer S200 y Dicom Time&Frequency Transfer REceiver GTR50) y dos Centrales de Sincronismo Externo mod. STF701.

18. El conjunto de estos equipos produce una serie de ficheros que contienen los datos de los seguimientos efectuados en un día y son utilizados por el ROA para elaborar los informes de diferencia de fase del patrón con la escala UTC(ROA).

19. La referencia de fecha y tiempo a la red se suministra mediante las Centrales de Sincronismo Externo STF701 a través de un servicio NTP. La referencia temporal es

suministrada a través de una señal proveniente del patrón de frecuencia de rubidio Symmetricom Rubidium Frequency Standard 8040.

20. El periodo durante el cual la FNMT-RCM estima que son válidos los *Sellos de Tiempo* emitidos por esta vendrá determinado por las algoritmias empleadas o por la normativa técnica y/o legal que sea de aplicación. Para determinar el periodo exacto de un determinado *Sello de tiempo* emitido bajo la política identificada en el presente documento, consultar [ETSI TS 102 176].

8. CESE DE LA ACTIVIDAD DE LA FNMT-RCM COMO AUTORIDAD DE SELLADO DE TIEMPO

21. Véase [DGPC]

9. PROPIEDAD INTELECTUAL E INDUSTRIAL

22. Véase [DGPC]

10. PROHIBICIÓN DE RESERVICIO CON O SIN REVENTA

23. El *Servicio de Sellado de Tiempo* de la FNMT-RCM no podrá ser objeto de reservicio, con o sin reventa, sin que exista valor añadido al mismo. En caso de que se proporcione ese valor añadido para terceras partes, basándose en el servicio prestado por la FNMT-RCM, se debe solicitar a esta entidad la suscripción de un contrato para el tramo mayorista.

24. La FNMT-RCM quedará exonerada de responsabilidad por actuaciones de personas, entidades u organizaciones que, sin suscribir un contrato para el tramo mayorista, procedan a realizar estos servicios para terceros. Todo ello sin perjuicio de las acciones legales que pudieran corresponder.

11. LEY APLICABLE, INTERPRETACIÓN Y JURISDICCIÓN COMPETENTE

25. Véase [DGPC]

12. MODIFICACIÓN DE LA PST Y DPST

26. Véase [DGPC]

13. POLÍTICA DE SELLADO DE TIEMPO DE FNMT

13.1. IDENTIFICACIÓN

27. La presente *Política de Sellado de Tiempo* de la FNMT-RCM para la expedición de *Sellos de Tiempo* tiene la siguiente identificación:

Tabla 1 Identificación Política de Sellado de Tiempo FNMT

Nombre	*Política de Sellado de Tiempo* de FNMT
Referencia/OID	1.3.6.1.4.1.5734.3.1.3
Versión	2.2
Localización	http://www.cert.fnmt.es/dpcs/
DPC relacionada	Declaración General de Prácticas de Certificación de la FNMT-RCM
Localización	http://www.cert.fnmt.es/dpcs/

28. Esta política es de aplicación a las distintas unidades de sellado de tiempo (TSU) que la FNMT-RCM pudiera establecer para la prestación del servicio.

29. Se encuentra identificada y referenciada por el *OID* 1.3.6.1.4.1.5734.3.1.3 pudiendo ser localizada en la dirección

http://www.cert.fnmt.es/dpcs

en su última versión en vigor.

30. Los procedimientos y contenidos aquí referenciados se basan principalmente en las normas del *European Telecommunications Standards Institute* (ETSI):

- ETSI TS 102 042 - Policy requirements for certification authorities issuing public key certificates,
- ETSI TS 101 456 - Policy requirements for certification authorities issuing qualified certificates,
- ETSI TS 102 023 - Policy requirements for time-stamping authorities, y
- ETSI TS 101 861 - Time stamping profile.

31. La presente política es conforme a la norma ETSI TS 102 023 y a la especificación equivalente del IETF, la RFC 3628 Policy Requirements for Time-Stamping Authorities (TSAs)

13.2. COMUNIDAD Y ÁMBITO DE APLICACIÓN

32. La presente política es de aplicación en la expedición de *Sellos de Tiempo* que tienen las siguientes características:

- Son emitidos por la FNMT-RCM como PSC cumpliendo con los criterios establecidos en la normativa técnica EESSI, concretamente [ETSI TS 102 023]

- Son emitidos con base en los criterios establecidos para tales en la normativa técnica EESSI [ETSI TS 101 861] y [RFC 3161]
- Están firmados electrónicamente con los *Certificados* y *Datos de Creación de Firma* de la FNMT-RCM, concretamente bajo la *Cadena de Certificación* de la *Autoridad de Certificación* raíz con CN=AC RAIZ FNMT-RCM.
- Incluyen expresamente datos para la adhesión a la presente política a través del campo "policy" del propio *Sello de Tiempo.*
- Son emitidos a petición de las *Entidades Usuarias* que forman parte de la *Comunidad Electrónica* tal y como se define en el apartado ***Definiciones*** de la [DGPC]

13.3. LÍMITES DE USO DEL SERVICIO DE SELLADO DE TIEMPO Y DE LOS SELLOS DE TIEMPO

33. Para poder usar el servicio de forma adecuada se deberá previamente formar parte de la *Comunidad Electrónica*, adquirir la condición de *Entidad Usuaria* y haber suscrito el correspondiente acuerdo para el uso del servicio. Sólo con este marco de trabajo la *Entidad Usuaria* obtendrá las instrucciones y privilegios suficientes para el envío de datos en forma electrónica a la FNMT-RCM con objeto de la creación de un *Sello de Tiempo* con los mismos.

34. Por otra parte, con la finalidad de que un tercero pueda depositar la confianza en los *Sellos de Tiempo* emitidos por la FNMT-RCM, esta Entidad cuenta con un *Servicio de información y consulta sobre el estado de los certificados* en el que se puede consultar el estado del *Certificado* empleado para la construcción del sello en cuestión.

35. Por tanto, sin haber hecho las comprobaciones pertinentes, no se debe confiar en un *Sello de Tiempo* emitido bajo esta *Política de Sellado de Tiempo* de la FNMT-RCM. En este caso, no se obtendrá cobertura de la presente política, y se carecerá de legitimidad alguna para reclamar o emprender acciones legales contra la FNMT-RCM por daños, perjuicios o conflictos provenientes del uso o confianza en un *Certificado*.

36. La FNMT-RCM no garantiza la veracidad de los contenidos representados por los datos electrónicos objeto del sellado de tiempo, ni su autoría. Asimismo, tampoco los avala, ni participa en su creación en modo alguno, ni es responsable del uso que se pudiera hacer de ellos ni de los efectos que pudiera tener en los interesados y/o terceras partes. FNMT-RCM no mantiene vínculo alguno con la procedencia o causalidad de dichos datos electrónicos.

37. La FNMT-RCM, a través de su *Servicio de Sellado de Tiempo*, exclusivamente garantiza la existencia de unos datos, que bien pudieran ser una representación particular de otros, en el instante de tiempo en el que recibe la solicitud y determinado por la referencia temporal empleada. Esta garantía se expresa a través de la firma electrónica conjunta de dichos datos y dicha referencia temporal con un *Certificado* cuyo titular es la FNMT-RCM, prestador del *Servicio de Sellado de Tiempo* y cuyo rol en este es el de *Autoridad de Sellado de Tiempo* y tercera parte de confianza. FNMT-RCM rechaza cualquier interpretación de las garantías que proporcionan los *Sellos de Tiempo* que emite más allá de lo expresado anteriormente. La *Autoridad de Sellado de Tiempo* de la FNMT-RCM es, por tanto, una tercera parte de confianza sin un interés particular en los documentos que se han fechado, aunque su firma probará la existencia de estos en un instante de tiempo.

13.4. RESPONSABILIDADES Y OBLIGACIONES DE LAS PARTES

38. Esta política de *Sellado de Tiempo* recoge las responsabilidades y obligaciones de las partes implicadas en la prestación del *Servicio de Sellado de Tiempo* y en la emisión y uso de los *Sellos de Tiempo*.

13.4.1. Responsabilidades de las partes

39. Para poder solicitar la emisión de *Sellos de Tiempo* se deberá previamente formar parte de la *Comunidad Electrónica*, y adquirir la condición de *Entidad Usuaria*.

13.4.1.1. Responsabilidades del Prestador de Servicios de Confianza (FNMT-RCM)

40. La FNMT-RCM únicamente responde de la variación de la referencia temporal, en relación a la proporcionada por la Sección de Hora del Real Instituto y Observatorio de la Armada en San Fernando, Cádiz, que introduce en los sellados de tiempo en el momento de la solicitud, más no de los datos anejos a dicha referencia temporal que figuran en el propio sello emitido ni de la implicaciones que pudiera tener su uso por parte de un tercero.

41. La FNMT-RCM no se hace responsable de la veracidad ni de los contenidos representados por los datos electrónicos objeto del *Sello de Tiempo* que emite.

42. La FNMT-RCM no será responsable de los daños y perjuicios y/o funcionamiento defectuoso que los *Sellos de Tiempo* emitidos por ella puedan producir en los usos que puedan realizarse, ya sean estos por culpa de los interesados o por defectos de origen de los elementos.

43. La FNMT-RCM no responderá ante personas cuyo comportamiento en la utilización del *Servicio de Sellado de Tiempo* y/o los propios *Sellos de Tiempo* haya sido negligente, debiendo considerarse a estos efectos y en todo caso como negligencia la falta de observancia de lo dispuesto en la presente Política y Declaración de Prácticas de Sellado de Tiempo, en la [DGPC], y, en especial, en lo dispuesto en los apartados referidos a las obligaciones y a la responsabilidad de las partes.

44. FNMT-RCM no responderá en los supuestos de caso fortuito, fuerza mayor, atentado terrorista, huelga salvaje, así como en los supuestos que se trate de acciones constitutivas de delito o falta que afecten a sus infraestructuras prestadoras, salvo que hubiera mediado culpa grave de la entidad. En todo caso, en los correspondientes contratos y/o convenios FNMT podrá establecer cláusulas de limitación de responsabilidad adicionales a las recogidas en este documento.

45. La FNMT-RCM no responderá por ningún software que no haya proporcionado directamente.

46. La FNMT-RCM no garantiza los algoritmos criptográficos ni responderá de los daños causados por ataques exitosos externos a los algoritmos criptográficos usados, si guardó la diligencia debida de acuerdo al estado actual de la técnica, y procedió conforme a lo dispuesto en las *Políticas y Declaraciones de Prácticas de Certificación* de aplicación y en la Ley.

47. En todo caso y con la condición de cláusula penal, las cuantías que en concepto de daños y perjuicios debiera satisfacer por imperativo judicial la FNMT-RCM a cada tercero perjudicado o miembro de la *Comunidad Electrónica* en defecto de regulación específica en los contratos o convenios, se limitan a un máximo de SEIS MIL EUROS (6.000€).

13.4.1.2. Responsabilidades de las Entidades Usuarias del servicio

48. Salvo contratación de esta obligación con la FNMT-RCM, es responsabilidad de la *Entidad Usuaria* la verificación de las *Firmas Electrónicas* empleadas para la emisión de los *Sellos de Tiempo*, así como de la comprobación del estado de los *Certificados* existentes en la cadena de confianza, no cabiendo, en ningún caso, presumir la autenticidad de los *Sellos* o *Certificados* sin dichas comprobaciones.

49. Será responsabilidad del *Solicitante* y poseedor de los *Sellos de Tiempo* el refirmado o resellado de los datos anejos en el *Sello de Tiempo* en caso de que la algoritmia empleada para la emisión de este haya quedado obsoleta, anulando así su carácter probatorio y veraz.

50. Será el *Solicitante* del *Sellado de Tiempo* y receptor del *Sello de Tiempo* (*Entidades Usuarias*) quien deba responder ante las partes confiantes sobre los datos anejos a la referencia temporal incluida en el *Sello de Tiempo* y de la implicaciones que pudiera tener su uso por parte de un tercero.

51. Asimismo, será responsabilidad de la *Entidad Usuaria* observar lo dispuesto en las *Políticas y Prácticas de Sellado de Tiempo* de aplicación, en la DGPC y sus posibles modificaciones futuras, con especial atención a los límites de uso establecidos para los *Sellos de Tiempo* en sus correspondientes políticas.

13.4.1.3. Responsabilidades de las partes confiantes

52. Será responsabilidad de las partes confiantes, salvo contratación de esta obligación con la FNMT-RCM, la verificación de las *Firmas Electrónicas* empleadas para la emisión de los *Sellos de Tiempo*, así como de los *Certificados* existentes en la cadena de confianza, no cabiendo en ningún caso presumir la autenticidad de los *Sellos* o *Certificados* sin dicha verificación.

53. No podrá considerarse que la parte confiante ha actuado con la mínima diligencia debida si confía en una *Firma Electrónica* basada en un *Certificado* emitido por la FNMT-RCM sin haber observado lo dispuesto en las *Políticas y Declaraciones de Prácticas de Certificación* de aplicación y comprobado que dicha *Firma Electrónica* puede ser verificada por referencia a una Cadena de certificación válida.

54. Si las circunstancias indican necesidad de garantías adicionales, la parte confiante deberá obtener garantías adicionales para que dicha confianza resulte razonable.

13.4.2. Obligaciones de la partes

13.4.2.1. Obligaciones del Prestador de Servicios de Certificación (FNMT-RCM)

55. La FNMT-RCM como prestador del *Servicio de Sellado de Tiempo* y *Autoridad de Sellado de Tiempo* en la que se constituye a través de dicho servicio, tiene la obligación de:

- Con carácter general, seguir los procedimientos y directrices expresadas en la presente política y declaración de prácticas para la emisión de *Sellos de Tiempo* así como en la DGPC.
- Mantener y calibrar la referencia temporal empleada para la emisión de *Sellos de Tiempo* con una desviación máxima de 50 ns de la referencia temporal proporcionada por la Sección de Hora del Real Instituto y Observatorio de la Armada en San Fernando, Cádiz.
- Incluir en los *Sellos de Tiempo* que emite los elementos necesarios para determinar la fecha y hora en la que el sello en cuestión se ha emitido así como los datos a fechar, recibidos de la *Entidad Usuaria*, sin realizar alteración o modificación alguna sobre los mismos.
- Gestionar las *Claves Privadas* empleadas para la emisión de *Sellos de Tiempo* y *Certificados* participantes en el servicio según lo descrito en el apartado "Gestión del ciclo de vida de las *Claves* del *Prestador de Servicios de Certificación*" de la [DGPC] y de forma que se garantice su confidencialidad e integridad.
- Emplear una fuente fiable de tiempo como referencia temporal en el proceso de emisión de *Sellos de Tiempo.*
- Conservar toda la información y documentación relativa a las peticiones de *Sellado de Tiempo,* y las respuestas correspondientes, con motivo de la prestación del servicio durante al menos quince (15) años.
- Hacer pública y de libre acceso la presente política y conservar las Políticas y Prácticas de Sellado de Tiempo durante 15 años desde el fin de su vigencia, por publicación de una nueva versión de éstas, en las debidas condiciones de seguridad.
- Mantener un *Directorio* seguro y actualizado de *Certificados* en el que se identifican los *Certificados* empleados para la prestación del servicio, así como su vigencia, incluyendo en forma de *Listas de Revocación* la identificación de los *Certificados* que hayan sido revocados o suspendidos. La integridad de este *Directorio* se protegerá mediante la utilización de sistemas conformes con las disposiciones reglamentarias específicas que al respecto se dicten en España y, en su caso, en la UE., y su acceso podrá efectuarse según se dispone en las *Políticas y Prácticas de Certificación Particulares correspondientes a los Certificados* en cuestión.
- Mantener un servicio de consulta sobre la vigencia de los *Certificados*. Este servicio se presta según lo descrito en la [DGPC] y las Políticas y Prácticas de Certificación Particulares correspondientes a los *Certificados* a validar.
- En caso de verse comprometida la calibración de la referencia temporal, o tener sospecha de ello, informar correspondientemente a todas las partes proporcionando una descripción de la situación
- No emitir *Sellos de Tiempo* en caso de que exista, o se tenga sospecha de ello, un compromiso de las operaciones del *Servicio de Sellado de Tiempo* (compromiso de las claves, pérdida de la calibración del reloj, etc.). En este caso, la FNMT-RCM pondrá a disposición de las partes y de la autoridad competente la información necesaria para

identificar los *Sellos de Tiempo* afectados. La FNMT-RCM restaurará el servicio cuando se reestablezcan las condiciones necesarias para ello.

13.4.2.2. Obligaciones de las Entidades Usuarias del servicio

56. Las partes que realizan uso del S*ervicio de Sellado de Tiempo* (peticiones) tienen la obligación de:

- Con carácter general, seguir los procedimientos y directrices expresadas en la presente política y declaración de prácticas para la emisión de *Sellos de Tiempo* así como en la DGPC.
- Ser miembro de la *Comunidad Electrónica* y haberse constituido como *Entidad Usuaria.*
- Haber suscrito el correspondiente acuerdo para el uso del servicio.
- Autenticarse mediante *Certificado* electrónico con las características pertinentes y en vigor previa petición de cualquier *Sellado de Tiempo*.
- Como paso previo al depósito de la confianza en los *Sellos de Tiempo*,
    1) Verificar que la *Firma electrónica* que acompaña a los *Sellos de Tiempo* es la de la FNMT-RCM y no otra y que además es correcta.
    2) Comprobar la validez de los *Certificados* empleados para la emisión del *Sello de Tiempo* en cuestión a través de los procedimientos indicados en las Políticas y Prácticas de Certificación Particulares correspondientes a los Certificados a validar.
- Usar los *Sellos de Tiempo* dentro de los límites y ámbito descrito en la presente política.
- No hacer valer los *Sellos de Tiempo* como referencia temporal en caso de que el *Prestador de Servicios de Certificación* haya cesado su actividad como *Autoridad de Sellado de Tiempo* que emite sellos bajo esta política y no se hubiera producido la subrogación prevista en la ley. En todo caso, tampoco utilizará los *Sellos de Tiempo* en los casos en los que los *Datos de Creación de Firma* del *Prestador* puedan estar amenazados y/o comprometidos, y así se haya comunicado por el *Prestador* o, en su caso, hubiera tenido noticia de estas circunstancias el propio *Solicitante* o tenedor del *Sello*.
- No hacer valer los *Sellos de Tiempo* como referencia temporal fuera de los límites de uso establecidos para estos en su correspondiente política.

13.4.2.3. Obligaciones de las partes confiantes

57. Las partes que confían en un *Sello de Tiempo* emitido por la FNMT-RCM tienen la obligación de:

- Con carácter general, seguir los procedimientos y directrices expresadas en la presente política y declaración de prácticas para la emisión de *Sellos de Tiempo.*

- Como paso previo al depósito de la confianza en los *Sellos de Tiempo*,
    1) Verificar que la *Firma electrónica* que acompaña a los *Sellos de Tiempo* es la de la FNMT-RCM y no otra y que además es correcta.
    2) Comprobar la validez de los *Certificados* empleados para la emisión del *Sello de Tiempo* en cuestión a través de los procedimientos indicados en las Políticas y Prácticas de Certificación Particulares correspondientes a los Certificados a validar.
- Aceptar los *Sellos de Tiempo* dentro de los límites y ámbito descrito en la presente política y prácticas de sellado de tiempo.

13.5. GESTIÓN DEL CICLO DE VIDA DE LAS CLAVES DEL PRESTADOR DE SERVICIOS DE CONFIANZA

58. Con objeto de la prestación del *Servicio de Sellado de Tiempo*, la FNMT-RCM realiza la gestión de las claves correspondientes de conformidad con lo descrito en el apartado "Gestión del ciclo de vida de las claves del Prestador de Servicios de Certificación" de la [DGPC].

59. Los *Sellos de Tiempo* emitidos bajo esta política son firmados por *Certificados* específicos, que a su vez han sido emitidos bajo la *Cadena de Certificación* de la *Autoridad de Certificación* raíz con CN=AC RAIZ FNMT-RCM.

60. Para obtener más información sobre la citada *Cadena de Certificación* de la *Autoridad de Certificación* raíz consultar el apartado "Cadenas de Certificación" de la [DGPC].

61. Los *Datos de Creación de Firma* de la unidad de *Sellado de Tiempo* están vinculados al siguiente *Certificado*.

Tabla 2 Perfil de *Certificado* de la unidad de *Sellado de Tiempo* empleada para la emisión de *Sellos de Tiempo* bajo la presente política

CAMPO	CONTENIDO
1. Versión	V3
2. Serial Number	26 3F 9B 10 3D FF 0A BB 54 F5 F5 1A A1 20 43 D4
3. Signature Algorithm	sha256withRSAEncryption

CAMPO	CONTENIDO
4. Issuer Distinguished Name	CN = AC Administración Pública SERIALNUMBER = Q2826004J OU = CERES O = FNMT-RCM C = ES
5. Validity	Desde: martes, 3 de marzo de 2015 Hasta: jueves, 3 de marzo de 2022
6. Subject	CN = AUTORIDAD DE SELLADO DE TIEMPO FNMT-RCM OU = CERES O = FNMT-RCM C = ES
7. Subject Public Key Info	(RSA 3072 bits)
8. subjectAltName	Dirección del directorio: OID.1.3.6.1.4.1.5734.1.8 (fnmtDescripcion) = AUTORIDAD DE SELLADO DE TIEMPO FNMT-RCM OID.1.3.6.1.4.1.5734.1.14 (fnmtPropEnt) = FNMT-RCM OID.1.3.6.1.4.1.5734.1.15 (fnmtPropCIF) = Q2826004J
basicConstrains	Tipo de asunto=Entidad final Restricción de longitud de ruta=Ninguno
keyUsage	Firma digital, sin repudio
extKeyUsage	Fechado digital
subjectKeyIdentifier	b6 d1 71 c8 6a 21 61 9a 79 74 89 e5 6b 18 bd 59 e9 82 16 81
authorityKeyIdentifier	14 11 e2 b5 2b b9 8c 98 ad 68 d3 31 54 40 e4 58 5f 03 1b 7d

CAMPO	CONTENIDO
crlDistributionPoints	ldap://ldapape.cert.fnmt.es/CN=CRL180,CN=AC%20Administraci%F3n%20P%FAblica,OU=CERES,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint http://www.cert.fnmt.es/crlsacap/CRL180.crl

13.6. PROVISIÓN Y DISPONIBILIDAD DEL SERVICIO DE SELLADO DE TIEMPO

62. La emisión de *Sellos de Tiempo* se realizará ante la petición de la *Entidad Usuaria*. Cuando esta desea obtener un *Sello de Tiempo* para un documento electrónico, calculará un valor o conjunto de valores hash a partir de este. Esto producirá una pequeña pero compacta cantidad de información que será enviada a la FNMT–RCM para que proceda a la emisión del *Sello de Tiempo* correspondiente.

63. Este *Sello de Tiempo* vinculará, a través de la firma electrónica de la FNMT-RCM, los datos recibidos y la fecha y hora de la recepción.

64. Hay que señalar que la FNMT-RCM decidirá si el algoritmo hash utilizado para representar al documento es suficientemente seguro de acuerdo con sus políticas de servicio y si lo es aceptará a trámite la solicitud. En concreto se aceptarán los siguientes algoritmos de hash:

- SHA-1,
- SHA-256,
- SHA-384,
- SHA-512

65. La FNMT-RCM no realizará comprobación o tratamiento alguno sobre la representación de los datos a sellar recibidos más allá de su inclusión en el propio *Sello de Tiempo* y en los sistemas de registro de eventos. La FNMT-RCM no verificará en modo alguno el contenido, ni la veracidad de la representación de los datos a sellar ni del origen de los mismos.

66. El *Servicio de Sellado de Tiempo* estará disponible las veinticuatro (24) horas del día, todos los días del año, salvo por circunstancias ajenas a la FNMT-RCM u operaciones de mantenimiento. La FNMT-RCM notificará esta última circunstancia en la dirección *http://www.ceres.fnmt.es* con al menos cuarenta y ocho (48) horas de antelación y tratará de solventarla en un periodo no superior a veinticuatro (24) horas.

67. Tanto las peticiones de *Sellado de Tiempo* como las respuestas se gestionan conforme a lo descrito en la recomendación [RFC 3161].

13.7. PETICIÓN DE UN SELLADO DE TIEMPO

68. Para solicitar un *Sello de Tiempo*, se deberá formar parte de la *Comunidad Electrónica* y tener la condición de *Entidad Usuaria* y haber suscrito el correspondiente acuerdo con la FNMT-RCM para la utilización del servicio.

69. Como paso previo a la realización de solicitudes, la *Entidad Usuaria* deberá obtener un *Certificado de Componente* que empleará como mecanismo de identificación y autenticación en cada solicitud de *Sellado de Tiempo.*

70. La *Entidad Usuaria*, utilizando el protocolo HTTPS y autenticándose con el *Certificado de Componente* mencionado anteriormente, compondrá una petición de *Sellado de Tiempo* según la recomendación [RFC 3161].

71. Las peticiones de *Sellado de Tiempo* se envían a la dirección https://tsa.cert.fnmt.es/ encapsuladas como Content-Type: application/timestamp-query, codificadas en DER y descritas en ASN.1 (Ver [RFC 3161]).

72. La estructura ASN.1 correspondiente a la petición es:

```
TimeStampRequest ::= SEQUENCE {
version Integer { v1(1) },
messageImprint MessageImprint,
reqPolicy PolicyInformation OPTIONAL,
nonce Integer OPTIONAL,
certReq BOOLEAN DEFAULT FALSE,
extensions [0] IMPLICIT Extensions OPTIONAL
}
```

`version` Entero. Describe la versión de la petición. Actualmente es versión 1.

`messageImprint` Secuencia. Estructura que contiene el hash del documento a fechar y el algoritmo de hash utilizado.

`reqPolicy` Identificador de la política que se solicita que sea aplicada en la prestación del servicio. Es opcional y puede omitirse, pero en caso de utilizarse deberá contener el OID de la presente política (1.3.6.1.4.1.5734.3.1.3).

`nonce` Entero. Número aleatorio opcional utilizado para enlazar petición con respuesta.

`certReq` Boolean. Si su valor es "Verdadero" se requiere a la TSA que incluya su certificado en la respuesta.

`extensions` Secuencia. Extensiones de la petición.

13.8. RESPUESTA A UNA PETICIÓN DE SELLADO DE TIEMPO

73. Las respuestas a una petición de *Fechado Digital* se reciben de la dirección https://tsa.cert.fnmt.es/ encapsuladas como Content-Type: application/timestamp-reply, codificadas en DER y descritas en ASN.1.

74. El contenido de la respuesta es una estructura ASN.1 en la que se incluye el resultado de la operación (status), es decir, si la operación se ha realizado de manera satisfactoria o no, y

una estructura CMSSignedData (timeStampToken) en la que se incluye el fechado digital (TSTInfo) firmado por la Autoridad de Fechado Digital.

75. El certificado de la Autoridad de Fechado Digital es un certificado emitido por la CA con la extensión id-kp-timestamping que indica que este certificado se utilizará con el fin exclusivo de fechar documentos digitales.

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

`status` Secuencia. Secuencia en la que haciendo uso de tres campos se indica el resultado de la operación como entero, una cadena descriptiva del resultado y otra cadena descriptiva utilizada en caso de error. Si el resultado no es satisfactorio el campo timeStampToken no estará presente.

`timeStampToken` Secuencia. Estructura firmada del tipo CMSSignedData en la que se incluye el fechado digital y la firma del mismo. Incluye los certificados de la Autoridad de Fechado Digital y de la CA en el caso de que haya sido solicitado en la petición.

```
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` Describe la versión de la respuesta. Actualmente es versión 1.

`policy` Identificador de la política utilizada para prestar el servicio, es decir, la presente política (OID 1.3.6.1.4.1.5734.3.1.3).

`messageImprint` Estructura que contiene el hash del documento fechado y el algoritmo de hash utilizado enviado por el cliente. Su valor es exactamente igual al recibido en la petición

`serialNumber` Número entero único asignado por la AFD al Fechado Digital generado.

`genTime` Marca temporal asignada por la Autoridad de Sellado de Tiempo. Se incluirá término fraccional hasta el milisegundo. Según RFC 3161 los términos fraccionales acabados en cero no se incluyen.

`accuracy` Indica la precisión del tiempo proporcionado.

`ordering` Valor falso. Sólo será posible ordenar dos Fechados Digitales cuando la diferencia entre los dos genTime sea superior a la suma de las precisiones de los dos.

`nonce` Entero. Número aleatorio utilizado para enlazar petición con respuesta. Debe estar presente si lo estaba en la petición.

`tsa` Secuencia. Identificador de la tsa que coincide con el subject del certificado de la AFD.

`extensions` Extensiones de la respuesta.

76. Los *Sellos de Tiempo* emitidos bajo esta política están firmados electrónicamente por los *Datos de Creación de Firma* de la FNMT-RCM haciendo uso de los siguientes algoritmos:

- SHA-256
- RSA 3072