Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

POLÍTICA Y PRÁCTICAS DEL SERVICIO CUALIFICADO DE SELLADO DE TIEMPO

	NOMBRE	FECHA
Elaborado por:	FNMT-RCM / 1.1	17/11/2017
Revisado por:	FNMT-RCM / 1.1	11/12/2017
Aprobado por:	FNMT-RCM / 1.1	22/12/2017

HISTÓRICO DEL DOCUMENTO			
Versión	**Fecha**	**Descripción**	**Autor**
1.0	03/01/2017	Creación del documento	FNMT-RCM
1.1	22/12/2017	Revisión anual del documento.	FNMT-RCM

Referencia: DPSCST/DPSCST0101/SGPSC/2017

Documento clasificado como: *Público*

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

1. REFERENCIAS

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

[ETSI EN 319 401] - General Policy Requirements for Trust Service Providers

[ETSI EN 319 421] - Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

[ETSI EN 319 422] - Time-stamping protocol and time-stamp token profiles

[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:

   - *Sello cualificado de tiempo electrónico: Sello de tiempo electrónico* que vincula la fecha y la hora con los datos de forma que no se puedan modificar los datos sin que se detecte, que se basa en una fuente de información temporal vinculada al Tiempo Universal Coordinado (UTC) y que ha sido firmado / sellado mediante firma / sello electrónico avanzado de un *Prestador cualificado de Servicios de Confianza*.

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

3. INTRODUCCIÓN Y OBJETO

2. La Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, de aquí en adelante FNMT-RCM, es un *Prestador cualificado de 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 como fuente de información temporal vinculada al Tiempo Universal Coordinado (UTC) la proporcionada por la Sección de Hora del Real Instituto y Observatorio de la Armada (ROA) en San Fernando, mediante el acuerdo alcanzado entre dicha Entidad y la FNMT-RCM para la sincronización continua de sus sistemas. El ROA 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. La prestación del presente servicio por parte de la FNMT-RCM requiere una petición previa por parte del solicitante del *Sellado de Tiempo* (remisión de la representación del conjunto de datos), a lo que contestará con la evidencia electrónica correspondiente (*Sello de tiempo electrónico*). La citada representación del conjunto de datos recibida por la FNMT-RCM consiste en una *Función hash* de dichos datos, de forma que estos no pueden ser deducidos.

Por tanto, la FNMT-RCM no tiene acceso a la información sobre la cual crea el *Sello de tiempo electrónico.*

4. Este *Servicio cualificado de Sellado de Tiempo* es ofrecido por la FNMT-RCM de conformidad con 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 el que se deroga la Directiva 1999/93/CE (Reglamento eIDAS).

4. ORGANIZACIÓN DEL DOCUMENTO

5. El presente documento, de Política y Prácticas del *Servicio Cualificado de Sellado de Tiempo*, forma parte integrante de la *Declaración General de Prácticas de Certificación* (DGPC) de la FNMT-RCM, como *Prestador de Servicios de Confianza* (PSC), recogiendo las obligaciones y procedimientos que se compromete a cumplir en relación con la prestación del *Servicio cualificado de Sellado de Tiempo.* Por tanto, dicho documento recoge 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.

6. 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.

7. 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 cualificado de Sellado de Tiempo* aplicables en el marco de la *Comunidad Electrónica* y previa suscripción de los pertinentes acuerdos de utilización.

8. En conclusión, el presente documento tiene por objeto la información pública de las condiciones y características del *Servicio cualificado de Sellado de Tiempo* proporcionado por la FNMT-RCM como PSC, recogiendo las obligaciones que se compromete a cumplir en relación con la gestión de los *Datos de Creación y Verificación de Firma / Sello* 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 cualificados de tiempo electrónicos*, así como los derechos y obligaciones de todas las partes que confían y aceptan el servicio.

9. Como quiera que la prestación del *Servicio cualificado 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 citado servicio.

5. ORDEN DE PRELACIÓN

10. La FNMT-RCM está constituida como *Autoridad de Sellado de Tiempo* (TSA) y, con objeto de garantizar las prestaciones de sus *Servicios de Sellado de Tiempo*, puede establecer cuantas unidades de sellado de tiempo (TSU) considere oportunas y la gestión de estas conforme a

políticas y prácticas particulares y diferenciadas. No obstante, el presente documento de Política y Prácticas particulares hace referencia al *Servicio Cualificado de Sellado de Tiempo,* cuya Política queda perfectamente identificada con su correspondiente OID y es ofrecido con una TSU concreta.

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

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

    2) La [DGPC], que afecta de manera general a cualquier servicio de confianza prestado por la FNMT-RCM y se aplicará supletoria y subsidiariamente sobre el documento referido en el apartado 1 anterior.

6. DISPONIBILIDAD DE LA INFORMACIÓN Y FORMA DE CONTACTO

12. Véase [DGPC]

7. CONTROLES DE SEGURIDAD, REGISTRO DE EVENTOS Y AUDITORÍAS

13. Véase [DGPC]

14. Adicionalmente, la FNMT-RCM implementa medidas específicas para evitar amenazas relativas a la calibración del reloj empleado en este servicio, que se describen en los apartados siguientes.

7.1. FUENTE DE TIEMPO EMPLEADA PARA LA PRESTACIÓN DEL SERVICIO CUALIFICADO

15. 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), para la prestación del *Servicio cualificado de Sellado de Tiempo* de la FNMT-RCM.

16. El SS-ROA, está compuesto principalmente por un patrón de frecuencia de Rubidio, un sistema de comparación de tiempo y frecuencia mediante sistema de navegación por satélites GPS y dos Centrales de Sincronismo Externo.

17. 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).

18. La referencia de fecha y tiempo a la red se suministra mediante las Centrales de Sincronismo Externo a través de un servicio NTP. La referencia temporal es suministrada a través de una señal proveniente del patrón de frecuencia de rubidio.

7.2. ACUERDO CON ROA PARA GARANTIZAR LA CALIBRACIÓN DEL RELOJ

19. El acuerdo de la FNMT-RCM con el ROA, citado anteriormente, garantiza que cualquier cambio en la calibración de la central de sincronismo es detectado por el sistema de monitorización del citado Observatorio de la Armada, dejando trazabilidad de dicho evento y corrigiendo dicho error de sincronismo.

7.3. PRECISIÓN DE LA SINCRONIZACIÓN PARA LA EMISIÓN DEL SELLO DE TIEMPO ELECTRÓNICO

20. La FNMT-RCM sincroniza su TSU con la central de sincronismo del ROA, monitorizando en todo momento dicha sincronización.

21. La precisión declarada para la sincronización de la TSU con UTC es de 100 milisegundos, cumpliendo así sobradamente con los requisitos del estándar europeo [ETSI EN 319 421]. El *Servicio cualificado de Sellado de Tiempo* de la FNMT-RCM no expedirá ningún *Sello cualificado de tiempo electrónico* durante el periodo de tiempo en el que existiera un desfase mayor de 100 milisegundos entre los relojes de la TSU y la fuente de tiempo UTC del ROA.

7.4. GENERACIÓN, ALMACENAMIENTO Y SALVAGUARDA DE LAS CLAVES PRIVADAS DE LA TSU

22. Las claves privadas de la TSU utilizada por el *Servicio cualificado de Sellado de Tiempo* de la FNMT-RCM son generadas y custodiadas por un dispositivo criptográfico que cumple los requisitos de seguridad FIPS PUB 140-2 Level 3, con algoritmos y parámetros adecuados para el uso de la clave (*Sellado de tiempo*) y la duración prevista, de acuerdo con las recomendaciones de la normativa ETSI TS 119 312 o normativa nacional equivalente. Los componentes técnicos necesarios para la creación de Claves están diseñados para que una Clave sólo se genere una vez, y para que una Clave Privada no pueda ser calculada desde su Clave Pública.

23. La actividad de creación de *Sellos cualificados de tiempo electrónico* es llevada a cabo dentro del dispositivo criptográfico, que dota de *Confidencialidad* a los *Datos de creación de Sellos* del *Prestador de Servicios de Confianza*. Cuando los *Datos de creación de Sellos* se encuentran fuera del dispositivo criptográfico, la FNMT-RCM aplica las medidas técnicas y organizativas apropiadas para garantizar su *Confidencialidad*.

24. Las operaciones de copia, salvaguarda o recuperación de los *Datos de creación de Sellos* se realizan bajo control exclusivo del personal autorizado, usando, al menos, control dual y en un entorno seguro.

25. Se mantiene una copia de los ficheros y componentes necesarios para la restauración del entorno de seguridad del dispositivo criptográfico, para el caso de que haya que hacer uso de ellos, en sobres de seguridad debidamente custodiados dentro de un armario ignífugo, que solo pueden ser obtenidos por personal autorizado.

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

26. Véase [DGPC]

9. PROPIEDAD INTELECTUAL E INDUSTRIAL

27. Véase [DGPC]

10. PROHIBICIÓN DE RESERVICIO CON O SIN REVENTA

28. El *Servicio cualificado 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.

29. 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

30. Véase [DGPC]

12. MODIFICACIÓN DE LA PST Y DPST

31. Véase [DGPC]

13. POLÍTICA DE SELLADO DE TIEMPO DE FNMT

13.1. IDENTIFICACIÓN

32. La presente *Política del Servicio cualificado de Sellado de Tiempo* de la FNMT-RCM para la expedición de *Sellos cualificados de Tiempo electrónicos* tiene la siguiente identificación:

Tabla 1 Identificación Política del Servicio cualificado FNMT de Sellado de Tiempo

Nombre	*Política del Servicio cualificado de Sellado de Tiempo* de FNMT
Referencia/OID	0.4.0.2023.1.1
Versión	1.1
Localización	http://www.cert.fnmt.es/dpcs/

DPC relacionada	Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica de la FNMT-RCM
Localización	http://www.cert.fnmt.es/dpcs/

33. 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 cualificado de Sellado de Tiempo* y se encuentra identificada y referenciada por el *OID* 0.4.0.2023.1.1 correspondiente a best-practices-ts-policy definido en el estándar europeo ETSI EN 319 421.

34. El *Servicio cualificado de Sellado de Tiempo* que provee la FNMT-RCM, como *Prestador cualificado de Servicios de Confianza*, se presta de conformidad con los requisitos del Reglamento eIDAS y el estándar europeo ETSI EN 319 401 "General Policy Requirements for Trust Service Providers".

13.2. COMUNIDAD Y ÁMBITO DE APLICACIÓN

35. La presente política es de aplicación en la expedición de *Sellos cualificados de Tiempo electrónico* 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 EN 319 421].
- Son emitidos con base en los criterios establecidos para tales en la normativa técnica EESSI [ETSI EN 319 422] y [RFC 3161]
- Están firmados electrónicamente con los *Datos de Creación de Firma* / *Sello* de la FNMT-RCM, concretamente bajo la *Cadena de Certificación* de la *Autoridad de Certificación* raíz con CN=AC RAIZ FNMT-RCM.
- La política definida a través del campo "policy" del propio *Sello cualificado de tiempo electrónico* expresa la adhesión a la política general del estándar europeo ETSI EN 319 421 (best practices policy for time-stamp).
- 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

36. 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 electrónico* de los mismos.

37. Por otra parte, con la finalidad de que un tercero pueda depositar la confianza en un *Sello de tiempo electrónico* emitido 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.

38. Por tanto, sin haber hecho las comprobaciones pertinentes, no se debe confiar en un *Sello de tiempo electrónico* 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 este servicio.

39. 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.

40. 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 del *Sello electrónico* conjunto de dichos datos y dicha referencia temporal con un *Certificado* cuyo titular es la FNMT-RCM, prestador del *Servicio cualificado 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 *Sello electrónico* probará la existencia de estos en un instante de tiempo.

13.4. RESPONSABILIDADES Y OBLIGACIONES DE LAS PARTES

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

13.4.1. Responsabilidades de las partes

42. Para poder solicitar la emisión de *Sellos de tiempo electrónicos* 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)

43. La FNMT-RCM se responsabiliza 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, que introduce en los *Sellos de tiempo electrónicos* en el momento de la solicitud, más no de la veracidad ni de los contenidos representados por los datos electrónicos remitidos por las entidades usuarias del servicio, que son el objeto del *Sello de tiempo electrónico* emitido.

44. La FNMT-RCM no será responsable de los daños y perjuicios y/o funcionamiento defectuoso que los *Sellos de tiempo electrónicos* 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.

45. La FNMT-RCM no responderá ante personas cuyo comportamiento en la utilización del *Servicio cualificado de Sellado de Tiempo* y/o los propios *Sellos de tiempo electrónicos* 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 Prácticas del *Servicio Cualificado 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.

46. 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-RCM podrá establecer cláusulas de limitación de responsabilidad adicionales a las recogidas en este documento.

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

48. 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 Servicios de Confianza y de Certificación electrónica* de aplicación y en la Ley.

49. 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

50. Salvo contratación de esta obligación con la FNMT-RCM, es responsabilidad de la *Entidad Usuaria* la verificación de los *Sellos Electrónicos* empleados para la emisión de los *Sellos de tiempo electrónicos*, así como de la comprobación del estado de los *Certificados* existentes en la *Cadena de certificación*, no cabiendo, en ningún caso, presumir la autenticidad de los *Sellos* o *Certificados* sin dichas comprobaciones.

51. Será responsabilidad del *Solicitante* y poseedor de los *Sellos de tiempo electrónicos,* el refirmado o resellado de los datos anejos en el *Sello de tiempo electrónico* en los casos en los que el *Certificado* empleado para la construcción de dicho *Sello de tiempo* haya perdido su validez (por ejemplo por caducidad, revocación o algoritmia obsoleta), anulando así su carácter probatorio y veraz.

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

53. Asimismo, será responsabilidad de la *Entidad Usuaria* observar lo dispuesto en la *Política y Prácticas* del *Servicio Cualificado 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 electrónicos* en sus correspondientes políticas.

13.4.1.3. Responsabilidades de las partes confiantes

54. Será responsabilidad de las partes confiantes, salvo contratación de esta obligación con la FNMT-RCM, la verificación de los *Sellos Electrónicos* empleados para la emisión de los *Sellos de tiempo electrónicos*, así como el estado de revocación de los *Certificados* existentes en la *Cadena de certificación*, no cabiendo en ningún caso presumir la autenticidad de los *Sellos* o *Certificados* sin dicha verificación.

55. No podrá considerarse que la parte confiante ha actuado con la mínima diligencia debida si confía en un *Sello Electrónico* basado en un *Certificado* emitido por la FNMT-RCM sin haber observado lo dispuesto en las *Políticas y Declaraciones de Prácticas de Servicios de Confianza y de Certificación electrónica* de aplicación y comprobado que dicho *Sello Electrónico* puede ser verificado por referencia a una *Cadena de certificación* válida.

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

13.4.2. Obligaciones de la partes

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

57. La FNMT-RCM como prestador del *Servicio Cualificado 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 declaración de Política y Prácticas del *Servicio Cualificado de Sellado de Tiempo,* así como en la [DGPC].
- Mantener y calibrar la referencia temporal empleada para la emisión de *Sellos de tiempo electrónicos* con una desviación que no supere el tiempo definido en el apartado correspondiente a la precisión de la sincronización para la emisión del *Sello de tiempo electrónico* respecto de la referencia temporal proporcionada por la Sección de Hora del Real Instituto y Observatorio de la Armada.
- Incluir en los *Sellos de tiempo electrónicos* que emite los elementos necesarios para determinar la fecha y hora en la que el *Sello* en cuestión se ha emitido así como la representación de los datos a fechar, recibida de la *Entidad Usuaria*, sin realizar alteración o modificación alguna sobre la misma.
- Gestionar las *Claves Privadas* empleadas para la emisión de *Sellos de tiempo electrónicos* 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 Confianza*" 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 electrónicos.*
- 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 del *Servicio Cualificado 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 electrónicos* con una TSU cuyo Certificado electrónico no esté vigente, ya sea por caducidad o por revocación del mismo, así como en el caso de expirado el periodo de tiempo de uso de la *Clave privada*.
- No emitir *Sellos de tiempo electrónicos* en caso de que exista, o se tenga sospecha del compromiso de las operaciones del *Servicio Cualificado 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 electrónicos* 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

58. Las partes que realizan uso del S*ervicio Cualificado 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 electrónicos* 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 electrónicos*:

1) Verificar que el *Sello electrónico* que acompaña a los *Sellos de tiempo electrónicos* es el de la FNMT-RCM y no otro y que además es correcto.

2) Comprobar la validez de los *Certificados* empleados para la emisión del *Sello de tiempo electrónico* 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 electrónicos* dentro de los límites y ámbito descritos en las presentes Políticas y Prácticas del *Servicio Cualificado de Sellado de Tiempo*.
- No hacer valer los *Sellos de tiempo electrónicos* como referencia temporal en caso de que el *Prestador de Servicios de Confianza* 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 electrónicos* en los casos en los que los *Datos de Creación de Sello* 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 de tiempo electrónico*.
- No hacer valer los *Sellos de tiempo electrónicos* 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

59. Las partes que confían en un *Sello de tiempo electrónico* emitido por la FNMT-RCM tienen la obligación de:

- Con carácter general, seguir los procedimientos y directrices expresadas en la presente declaración de Política y Prácticas del *Servicio Cualificado de Sellado de Tiempo.*
- Como paso previo al depósito de la confianza en los *Sellos de tiempo electrónicos*,

  1) Verificar que el *Sello electrónico* que acompaña a los *Sellos de tiempo electrónicos* es el de la FNMT-RCM y no otro y que además es correcto.

  2) Comprobar la validez de los *Certificados* empleados para la emisión del *Sello de tiempo electrónico* 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 electrónicos* dentro de los límites y ámbito descritos en las presentes Políticas y Prácticas del *Servicio Cualificado de Sellado de Tiempo*.

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

60. Con objeto de la prestación del *Servicio Cualificado 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 Confianza" de la [DGPC].

61. Los *Sellos de tiempo electrónicos* emitidos bajo esta política son *sellados* 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.

62. 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].

63. Los *Datos de Creación de Sello* de la unidad de *Sellado de Tiempo* están vinculados al siguiente *Certificado.*

14. CERTIFICADO DE LA TSU

64. El *Certificado* electrónico de la TSU para prestar el *Servicio cualificado de Sellado de Tiempo* es expedido por la FNMT – RCM con el OID de política 1.3.6.1.4.1.5734.3.9.20, con la *Autoridad de Certificación* "AC Componentes informáticos", que opera de conformidad con el estándar europeo ETSI EN 319 411-1. Dicho *Certificado* y las prácticas y políticas de certificación particulares de la *Autoridad de Certificación* "AC Componentes informáticos" están disponibles para su descarga y consulta en http://www.ceres.fnmt.es/dpcs.

65. El citado *Certificado electrónico* de la TSU incluye, siguiendo las recomendaciones de las normas ETSI EN 319 421 y ETSI EN 319 422, la extensión privateKeyUsage, que limita el uso de la *Clave privada* estableciendo una fecha de caducidad anterior a la de la clave pública, de manera que se asegure un tiempo suficiente para la renovación de los sellados emitidos por una TSU antes de la caducidad de su certificado.

66. Las características de dicho *Certificado* son las siguientes:

Subject: CN=AUTORIDAD DE SELLADO DE TIEMPO FNMT-RCM - TSU 2016, organizationIdentifier=VATES-Q2826004J, OU=CERES, O=FÁBRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA, C=ES

Issuer: "AC Componentes"

Algoritmo y longitud de la clave: RSA 3072

Validez: 6 años. Hasta el 25 de noviembre de 2022.

Periodo de uso de la clave privada: 5 años. Hasta el 25 de noviembre de 2021.

67. Los *Datos de Creación de sello* de la *Unidad de Sellado de Tiempo* están vinculados al *Certificado* de la *Autoridad de Sellado de Tiempo,* de conformidad con el estándar X.509 versión 3, cuyo perfil puede ser consultado en la página http://www.cert.fnmt.es/dpcs/.

15. PRACTICA DEL SERVICIO CUALIFICADO DE SELLADO DE TIEMPO

15.1. PROVISIÓN Y DISPONIBILIDAD DEL SERVICIO CUALIFICADO DE SELLADO DE TIEMPO

68. La emisión de *Sellos de tiempo electrónicos* se realizará ante la petición de la *Entidad Usuaria*. Cuando esta desea obtener un *Sello de tiempo electrónico* 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 electrónico* correspondiente.

69. Este *Sello de tiempo electrónico* vinculará, a través del *Sello electrónico* de la FNMT-RCM, los datos recibidos y la fecha y hora de la recepción.

70. Hay que señalar que la FNMT-RCM decidirá si el algoritmo hash utilizado para representar los datos a sellar 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-256
- SHA-384
- SHA-512

71. 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 electrónico* 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.

72. El *Servicio Cualificado 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.

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

15.2. PETICIÓN DE UN SELLO DE TIEMPO ELECTRÓNICO

74. Para solicitar un *Sello de tiempo electrónico*, 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.

75. Como paso previo a la realización de solicitudes, la *Entidad Usuaria* deberá obtener un *Certificado* de los admitidos por FNMT-RCM para tal fin, que empleará como mecanismo de identificación y autenticación en cada solicitud de *Sellado de Tiempo.*

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

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

78. 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. En este caso, el OID utilizado es 0.4.0.2023.1.1 correspondiente a best-practices-ts-policy definido en el estándar europeo ETSI EN 319 421.

`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.

15.3. RESPUESTA A UNA PETICIÓN DE SELLADO DE TIEMPO

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

80. 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 *Sellado de Tiempo* (TSTInfo) sellado por la *Autoridad de Sellado de Tiempo*.

81. El *Certificado* de la *Autoridad de Sellado de Tiempo* es emitido por la CA con la extensión id-kp-timestamping que indica que este certificado se utilizará con el fin exclusivo de expedir *Sellos de tiempo electrónicos*.

```
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 *Sellado de Tiempo* y el *Sello electrónico* del mismo. Incluye los *Certificados* de la *Autoridad de Sellado de Tiempo* 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 correspondiente a best-practices-ts-policy definido en el estándar europeo ETSI EN 319 421 (OID 0.4.0.2023.1.1).

`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 TSU al *Sellado de Tiempo* 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 *Sellados de Tiempo* 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` Identificador de la TSA que coincide con el subject del certificado de la *Autoridad de Sellado de Tiempo*.

`extensions` Extensiones de la respuesta. Se incluye la extensión QCStatements identificando así el *Sello de tiempo electrónico* como cualificado, según lo especificado en el estándar ETSI EN 319 422.

82. Los *Sellos de tiempo electrónicos* emitidos bajo esta política están sellados electrónicamente por los *Datos de Creación de Sello* de la FNMT-RCM haciendo uso de los siguientes algoritmos:

- SHA-256
- RSA 3072

15.4. VALIDACIÓN DEL SELLO DE TIEMPO ELECTRÓNICO

83. Para validar un sello de tiempo, las partes confiantes verificarán el *Sello electrónico* que acompaña a los *Sellos de tiempo electrónicos* haciendo uso del campo "messageImprint" descrito en el apartado anterior, así como el estado de validez del *Certificado* de la TSU a través del *Servicio de información y consulta del estado de los certificados* (protocolo OCSP) de conformidad con los procedimientos indicados en las Políticas y Prácticas de Certificación Particulares correspondientes a dicho *Certificado* (Política y Prácticas de Certificación Particulares de los Certificados de Componente "AC Componentes informáticos"), que se puede consultar en www.cert.fnmt.es/dpcs.

16. AUDITORÍAS

84. En este apartado será de aplicación general lo descrito en la Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica, y adicionalmente lo especificado en el presente apartado.

85. El *Servicio Cualificado de Sellado de Tiempo* ofrecido por la FNMT-RCM está sujeto a auditorías periódicas, según el esquema de certificación correspondiente a los *Prestadores de Servicios de Confianza*, en cuanto al cumplimiento de los requisitos definidos por los estándares europeos ETSI EN 319 401 "General Policy Requirements for Trust Service Providers", ETSI EN 319 421 "Trust Service Providers issuing Time-Stamps" y ETSI EN 319 422 "Time-stamping protocol and time-stamp token profiles".

86. Las auditorías mencionadas en el apartado anterior son realizadas anualmente por un organismo acreditado para tal fin.

17. TARIFAS

87. FNMT-RCM aplicará a las Administraciones Públicas las tarifas aprobadas por la Subsecretaría de la cual depende para la prestación de los servicios de confianza o, en su defecto, las tarifas acordadas en el convenio o encomienda de gestión formalizado para tal efecto.

88. Las tarifas a aplicar al sector privado se rigen por el contrato suscrito para la provisión del *Servicio Cualificado de Sellado de Tiempo*. Adicionalmente, la FNMT – RCM podrá establecer las tarifas y los medios de pago que considere oportunos en cada momento. El precio y condiciones de pago podrán ser consultados en la página web de la FNMT – RCM o bien serán facilitados por el área comercial correspondiente bajo petición a la dirección de correo electrónico comercial.ceres@fnmt.es.

89. Los requisitos de política definidos en el presente documento no implican ninguna restricción en el cobro del *Servicio Cualificado de Sellado de Tiempo.*