Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

DECLARACIÓN DE POLÍTICAS Y PRÁCTICAS DE CERTIFICACIÓN DE CERTIFICADOS DE CREACIÓN DE SELLOS DE TIEMPO ELECTRÓNICOS

	NOMBRE	FECHA
Elaborado por:	FNMT-RCM	25/09/2025
Revisado por:	FNMT-RCM	01/10/2025
Aprobado por:	FNMT-RCM	05/10/2025

Versión	Fecha	Descripción
1.0	5/03/2019	Creación del documento
1.1	19/06/2020	Revisión general
1.2	28/04/2021	Revisión general Se contempla que el tamaño de las claves de los certificados de entidad final sea de 3072 ó 4096 bits
1.3	22/12/2023	Se añade la nueva TSU 2023
1.4	03/02/2025	Revisión general
1.5	23/06/2025	Se eliminan referencias a TSU 2020
1.6	01/09/2025	Inclusión jerarquía de curva elíptica. Se añade nueva TSU 2025
1.7	07/10/2025	Sección 6.1.5, uso de claves RSA de al menos 3072 bits
1.8	05/10/2026	Revisión general.

Referencia: DPC/DPCTSU_0108/SGPSC/2026

Documento clasificado como: *Público*

Índice de contenidos

1. Introducción 8

1.1. Objeto 8

1.2. Nombre del documento e identificación 9

1.3. Partes intervinientes 10
1.3.1. Autoridad de Certificación 10
1.3.2. Autoridad de Registro 14
1.3.3. Suscriptores de los certificados 14
1.3.4. Partes que confían 14
1.3.5. Otros participantes 14

1.4. Uso de los certificados 15
1.4.1. Usos permitidos de los certificados 15
1.4.2. Restricciones en el uso de los certificados 15

1.5. Administración de Políticas 16
1.5.1. Entidad responsable 16
1.5.2. Datos de contacto 16
1.5.3. Responsables de adecuación de la DPC 16
1.5.4. Procedimiento de aprobación de la DPC 17

1.6. Definiciones y Acrónimos 17
1.6.1. Definiciones 17
1.6.2. Acrónimos 18

2. Publicación y repositorios 19

2.1. Repositorio 19

2.2. Publicación de información de certificación 20

2.3. Frecuencia de publicación 20

2.4. Control de acceso a los repositorios 20

3. Identificación y autenticación 21

3.1. Denominación 21
3.1.1. Tipos de nombres 21
3.1.2. Significado de los nombres 21
3.1.3. Seudónimos 21
3.1.4. Reglas utilizadas para interpretar varios formatos de nombres 21
3.1.5. Unicidad de los nombres 21
3.1.6. Reconocimiento y autenticación de marcas registradas 21

3.2. Validación inicial de la identidad 22
3.2.1. Métodos para probar la posesión de la clave privada 22
3.2.2. Autenticación de la identidad de la Organización 22
3.2.3. Autenticación de la identidad de la persona física solicitante 23
3.2.4. Información no verificada del Suscriptor 23

3.2.5. Validación de la capacidad de representación 23
3.2.6. Criterios de interoperación 23

3.3. Identificación y autenticación para peticiones de renovación de claves 23

3.4. Identificación y autenticación para peticiones de revocación 24

4. Requisitos operativos del ciclo de vida de los certificados 24

4.1. Solicitud de Certificados 24
4.1.1. Quién puede solicitar un Certificado 24
4.1.2. Proceso de registro y responsabilidades 24

4.2. Procedimiento de solicitud de certificados 25
4.2.1. Realización de las funciones de identificación y autenticación 25
4.2.2. Aprobación o rechazo de la solicitud del certificado 25
4.2.3. Tiempo en procesar la solicitud 25

4.3. Emisión del certificado 26
4.3.1. Acciones de la AC durante la emisión 26
4.3.2. Notificación de la emisión 27

4.4. Aceptación del certificado 27
4.4.1. Proceso de aceptación 27
4.4.2. Publicación del certificado por la AC. 27
4.4.3. Notificación de la emisión a otras entidades 27

4.5. Par de claves y uso del certificado 27
4.5.1. Clave privada del suscriptor y uso del certificado 27
4.5.2. Uso del certificado y la clave pública por terceros que confían 28

4.6. Renovación del certificado 28

4.7. Renovación con regeneración de las claves del certificado 28
4.7.1. Circunstancias para la renovación con regeneración de claves 28
4.7.2. Quién puede solicitar la renovación con regeneración de claves 29
4.7.3. Procesamiento de solicitudes de renovación con regeneración de claves 29
4.7.4. Notificación de la renovación con regeneración de claves 29
4.7.5. Conducta que constituye la aceptación de la renovación con regeneración de claves 29
4.7.6. Publicación del certificado renovado 29
4.7.7. Notificación de la renovación con regeneración de claves a otras entidades 29

4.8. Modificación del certificado 29

4.9. Revocación y suspensión del certificado 30
4.9.1. Circunstancias para la revocación 30
4.9.1.1 Circunstancias para la revocación del certificado del suscriptor 30
4.9.1.2 Circunstancias para la revocación del certificado de la CA subordinada 31
4.9.2. Quién puede solicitar la revocación 32
4.9.3. Procedimiento de solicitud de la revocación 32
4.9.4. Periodo de gracia de la solicitud de revocación 33
4.9.5. Plazo de tiempo para procesar la solicitud de revocación 33
4.9.6. Obligación de verificar las revocaciones por las partes que confían 33
4.9.7. Frecuencia de generación de CRLs 33

4.9.8. Periodo máximo de latencia de las CRLs 33
4.9.9. Disponibilidad del sistema de verificación online del estado de los certificados 33
4.9.10. Requisitos de comprobación en línea de la revocación 34
4.9.11. Otras formas de aviso de revocación disponibles 34
4.9.12. Requisitos especiales de revocación de claves comprometidas 34
4.9.13. Circunstancias para la suspensión 34
4.9.14. Quién puede solicitar la suspensión 34
4.9.15. Procedimiento para la petición de la suspensión 34
4.9.16. Límites sobre el periodo de suspensión 34

4.10. Servicios de información del estado de los certificados 34
4.10.1. Características operativas 35
4.10.2. Disponibilidad del servicio 35
4.10.3. Características opcionales 35

4.11. Finalización de la suscripción 35

4.12. Custodia y recuperación de claves 35
4.12.1. Políticas y prácticas de custodia y recuperación de claves 35
4.12.2. Políticas y prácticas de protección y recuperación de la clave de sesión 35

5. Controles de seguridad física, de procedimientos y de personal 36

5.1. Controles de Seguridad Física 36

5.2. Controles de Procedimiento 36

5.3. Controles de Personal 36

5.4. Procedimientos de auditoría 36

5.5. Archivado de registros 36

5.6. Cambio de claves de la AC 36

5.7. Gestión de incidentes y vulnerabilidades 36

5.8. Cese de la actividad del Prestador de Servicios de Confianza 36

6. Controles de seguridad técnica 37

6.1. Generación e instalación de las Claves 37
6.1.1. Generación del par de claves 37
6.1.1.1 Generación del par de Claves de la CA 37
6.1.1.2 Generación del par de Claves de la RA 37
6.1.1.3 Generación del par de Claves de los Suscriptores 37
6.1.2. Envío de la clave privada al suscriptor 37
6.1.3. Envío de la clave pública al emisor del certificado 37
6.1.4. Distribución de la clave pública de la AC a las partes que confían 37
6.1.5. Tamaños de claves y algoritmos utilizados 37
6.1.6. Parámetros de generación de la clave pública y verificación de la calidad 38
6.1.7. Usos admitidos de las claves (KeyUsage field X.509v3) 38

6.2. Protección de la clave privada y controles de los módulos criptográficos 38

6.3. Otros aspectos de la gestión del par de claves *38*
6.3.1. Archivo de la clave pública 38
6.3.2. Periodos de operación del certificado y periodos de uso del par de claves 38
6.4. Datos de activación *39*
6.5. Controles de seguridad informática *39*
6.6. Controles técnicos del ciclo de vida *39*
6.7. Controles de seguridad de red *39*
6.8. Fuente de tiempo *39*
6.9. Otros controles adicionales *39*

7. Perfiles de los certificados, CRLs y OCSP 39

7.1. Perfil del certificado *39*
7.1.1. Número de versión 39
7.1.2. Extensiones del certificado 40
7.1.3. Identificadores de objeto de algoritmos 40
7.1.4. Formatos de nombres 40
7.1.5. Restricciones de nombres 40
7.1.6. Identificador de objeto de política de certificado 40
7.1.7. Empleo de la extensión restricciones de política 40
7.1.8. Sintaxis y semántica de los calificadores de política 40
7.1.9. Tratamiento semántico para la extensión "Certificate policy" 41
7.2. Perfil de la CRL *41*
7.2.1. Número de versión 41
7.2.2. CRL y extensiones 41
7.3. Perfil de OCSP *42*
7.3.1. Número de versión 42
7.3.2. Extensiones del OCSP 42

8. Auditorías de cumplimiento 42

8.1. Frecuencia de las auditorías *43*
8.2. Cualificación del auditor *43*
8.3. Relación del auditor con la empresa auditada *43*
8.4. Elementos objetos de auditoría *43*
8.5. Toma de decisiones frente a detección de deficiencias *43*
8.6. Comunicación de los resultados *43*

9. Otros asuntos legales y de actividad 43

9.1. Tarifas *43*
9.1.1. Tarifas de emisión o renovación de certificados 43
9.1.2. Tarifas de acceso a los certificados 43

9.1.3. Tarifas de acceso a la información de estado o revocación 44
9.1.4. Tarifas para otros servicios 44
9.1.5. Política de reembolso 44

9.2. Responsabilidad financiera 44

9.3. Confidencialidad de la información 44

9.4. Protección de datos de carácter personal 44

9.5. Derechos de propiedad intelectual 44

9.6. Obligaciones y garantías 44
9.6.1. Obligaciones de la AC 44
9.6.2. Obligaciones de la AR 46
9.6.3. Obligaciones de los Suscriptores 46
9.6.4. Obligaciones de las partes que confían 48
9.6.5. Obligaciones de otros participantes 48

9.7. Renuncia de garantías 48

9.8. Limitaciones de responsabilidad 48

9.9. Indemnizaciones 48

9.10. Periodo de validez de este documento 49
9.10.1. Plazo 49
9.10.2. Terminación 49
9.10.3. Efectos de la finalización 49

9.11. Notificaciones individuales y comunicación con los participantes 49

9.12. Modificaciones de este documento 49
9.12.1. Procedimiento para las modificaciones 49
9.12.2. Periodo y mecanismo de notificación 49
9.12.3. Circunstancias bajo las cuales debe cambiarse un OID 49

9.13. Reclamaciones y resolución de disputas 49

9.14. Normativa de aplicación 50

9.15. Cumplimiento de la normativa aplicable 50

9.16. Estipulaciones diversas 50

9.17. Otras estipulaciones 50

Índice de tablas

Tabla 1 – Certificado de la AC RAIZ FNMT-RCM 11

Tabla 2 – Certificado de la AC subordinada Unidades de Sellado de Tiempo 11

Tabla 3 – Certificado de la AC RAIZ FNMT-RCM TSA 12

Tabla 4 – Certificado de la AC TSA FNMT 13
Tabla 5 – Certificado de la AC TSA CLIENTES 13
Tabla 6 – Perfil de la CRL..... 41

1. INTRODUCCIÓN

1. La Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, de aquí en adelante FNMT-RCM, con NIF Q2826004-J, es una entidad pública empresarial de las previstas en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que, como organismo público, tiene personalidad jurídica pública diferenciada, patrimonio y tesorería propios, y autonomía de gestión en los términos de dicha ley.

2. Está adscrita al Ministerio de Hacienda, el cual, a través de la Subsecretaría de Hacienda, ejercerá la dirección estratégica y el control de eficacia de la Entidad en los términos previstos en la citada Ley 40/2015.

3. La FNMT-RCM cuenta con una larga trayectoria histórica en la realización de sus actividades industriales, así como el respaldo del Estado. Desde la entrada en vigor del artículo 81, de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social y sus modificaciones, ha contribuido a impulsar la extensión de los servicios a los que ha sido facultada y ha alcanzado un destacado puesto en la prestación de los servicios de confianza.

4. Asimismo, la FNMT-RCM, a través del Departamento CERES (CERtificación ESpañola), acredita ser un *Prestador Cualificado de Servicios de Confianza*, 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 modificado por el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024 (en adelante, Reglamento eIDAS), de conformidad con el estándar europeo ETSI EN 319 401 "General Policy Requirements for Trust Service Providers".

1.1. OBJETO

5. El presente documento tiene por objeto la información pública de las condiciones y características de los servicios de confianza dirigidos a los usuarios de los *Certificados TSU* por parte de la FNMT-RCM como *Prestador de Servicios de Confianza*, recogiendo en concreto las obligaciones que se compromete a cumplir en relación con

   - la gestión de los *Certificados TSU*, las condiciones aplicables a la solicitud, emisión, uso y extinción de la vigencia de los mismo, que se expiden para la prestación del *Servicio de Sellado de Tiempo*,
   - la prestación del servicio de consulta del estado de validez de los *Certificados*, así como las condiciones aplicables al uso del servicio y garantías ofrecidas, y
   - La emisión de certificados cualificados para firma digital de sellos de tiempo.

6. Además, en el presente documento se recogen, bien directamente o con referencias a la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica de la FNMT-RCM* de la que depende la presente Declaración, los detalles del régimen de responsabilidad aplicable a las partes usuarias y/o que confían en los servicios mencionados

en el párrafo anterior, los controles de seguridad aplicados a sus procedimientos e instalaciones en aquello que pueda ser publicado sin perjudicar la eficacia de los mismos, y las normas de secreto y confidencialidad, así como cuestiones relativas a la propiedad de sus bienes y activos, a la protección de datos de carácter personal, y demás cuestiones de tipo informativo que considere interesante poner a disposición del público.

7. 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. La declaración de *Políticas y Prácticas del Servicio de Sellado de Tiempo* está perfectamente identificada con su correspondiente OID (0.4.0.2023.1.1) y está disponible para su consulta en www.cert.fnmt.es/dpcs.

1.2. NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

8. El presente documento se denomina "*Declaración de Políticas y Prácticas de certificación de certificados de sello electrónicos*", y en adelante será citado en este documento y con el ámbito descrito en el mismo como "*Declaración de Políticas y Prácticas Particulares*" o por su acrónimo "*DPPP*".

9. Las presentes *Políticas de Certificación y Prácticas de Certificación Particulares* forman parte de la *Declaración de Prácticas de Certificación* y tendrán prelación sobre lo dispuesto en el cuerpo principal de la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica*.

10. En caso de que existiera contradicción entre el presente documento y lo dispuesto en la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica*, tendrá preferencia lo aquí articulado.

11. La presente *Política de Certificación* de la FNMT-RCM se descompone en las identificadas a continuación:

Nombre: *Política de Certificación de Certificado TSU 2023*

Referencia / OID de política: 1.3.6.1.4.1.5734.3.18.2

Tipo de política asociada: QCP-l. OID: 0.4.0.194112.1.1

Nombre: Política de Certificación de *Certificado TSU 2025*

Referencia / OID de política: 1.3.6.1.4.1.5734.3.28.1.0

Tipo de política asociada: QCP-l. OID: 0.4.0.194112.1.1

Nombre: Política de Certificación de *Certificados cualificados de sello electrónico de TSU CLIENTES*

Referencia / OID de política: 1.3.6.1.4.1.5734.3.27.1.0

Tipo de política asociada: QCP-l. OID: 0.4.0.194112.1.1

Versión: 1.8

Fecha de expedición: 05/10/2026

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/

12. Los *Certificados TSU* emitidos bajo esta política, son un tipo de certificado que se expide para la prestación del Servicio de Sellado de Tiempo.

1.3. PARTES INTERVINIENTES

13. Las partes que intervienen en la gestión y uso de los *Servicios de Confianza* descritos en la presente *DPPP* son las siguientes:

1. Autoridad de Certificación
2. Autoridad de Registro
3. Suscriptores o titulares de los *Certificados*
4. Partes que confían
5. Otros participantes

1.3.1. Autoridad de Certificación

14. La FNMT-RCM es la *Autoridad de Certificación* que expide los Certificados electrónicos objeto de la presente *DPPP*. A estos efectos, existen las siguientes *Autoridades de Certificación*:

a) Autoridad de Certificación raíz (Jerarquía RSA). Dicha Autoridad expide exclusivamente *Certificados* de Autoridades de Certificación subordinadas. El certificado raíz de esta AC viene identificado por la siguiente información:

Tabla 1 – Certificado de la AC RAIZ FNMT-RCM

Campo	Valor
Sujeto	OU = AC RAIZ FNMT-RCM, O = FNMT-RCM, C = ES
Emisor	OU = AC RAIZ FNMT-RCM, O = FNMT-RCM, C = ES
Número de serie (hex)	5D:93:8D:30:67:36:C8:06:1D:1A:C7:54:84:69:07
Validez	No antes: 29 de octubre de 2008. No después: 1 de enero de 2030
Longitud clave pública	RSA 4.096 bits
Algoritmo de firma	RSA – SHA256
Identificador de clave	F7 7D C5 FD C4 E8 9A 1B 77 64 A7 F5 1D A0 CC BF 87 60 9A 6D

b) Autoridad de Certificación subordinada a la raíz de RSA: expide los *Certificados TSU* objeto de la presente *DPPP*. El certificado de dicha Autoridad viene identificado por la siguiente información:

Tabla 2 – Certificado de la AC subordinada Unidades de Sellado de Tiempo

Campo	Valor
Sujeto	CN = AC Unidades de Sellado de Tiempo, serialNumber = Q2826004J, OU = CERES, O = FNMT-RCM, C = ES
Emisor	OU = AC RAIZ FNMT-RCM, O = FNMT-RCM, C = ES
Número de serie (hex)	2C:ED:1A:5E:02:80:5B:BC:5D:DF:8A:3A:EC:AA:98:5A
Validez	No antes: 28 de noviembre de 2019. No después: 28 de noviembre de 2029.

Campo	Valor
Longitud clave pública	RSA 4096 bits
Algoritmo de firma	RSA – SHA256
Identificador de clave	40 B9 55 04 A8 4F 7F 60 90 ED 11 95 25 C3 25 FA 5A F4 85 D5

c) Autoridad de Certificación raíz (Jerarquía Curva Elíptica). Dicha Autoridad expide exclusivamente Certificados de Autoridades de Certificación subordinadas con algoritmia de curva elíptica. El certificado raíz de esta AC vienen identificado por la siguiente información:

Tabla 3 – Certificado de la AC RAIZ FNMT-RCM TSA

Campo	Valor
Sujeto	CN = AC RAIZ FNMT-RCM TSA, Org_ID = VATES-Q2826004J, O = FNMT-RCM, C = ES
Emisor	CN = AC RAIZ FNMT-RCM TSA, Org_ID = VATES-Q2826004J, O = FNMT-RCM, C = ES
Número de serie (hex)	5197B0DC756F57727C8E41DFC036DEBB883E05EF
Validez	No antes:10 Octubre 2024 No después: 04 Octubre 2049
Longitud clave pública	EC 384 bits (P-384)
Algoritmo de firma	SHA-384 with ECDSA
Identificador de clave	8F18 753B 8043 DC18 C16E E3B4 B66A ACF7 3766 0901

d) Autoridad de Certificación subordinada a la raíz de curva elíptica: expide los Certificados TSU objeto de la presente DPPP con algoritmia de curva elíptica. El Certificado de dicha Autoridad viene identificado por la siguiente información:

Tabla 4 – Certificado de la AC TSA FNMT

Campo	Valor
Sujeto	CN = AC TSA FNMT, ORG_ID = VATES-Q2826004J, O = FNMT-RCM,C = ES
Emisor	CN = AC RAIZ FNMT-RCM TSA, ORG_ID = VATES-Q2826004J, O= FNMT-RCM, C = ES
Número de serie (hex)	6F0E2C683FDBD98B4ABD6E25FD6C665296D60487
Validez	No antes:10 Octubre 2024 No después: 07 Octubre 2039
Longitud clave pública	EC 384 bits (P-384)
Algoritmo de firma	SHA-384 with ECDSA
Identificador de clave	4802 BE75 7431 DE28 BF6C 8B89 8DA2 D8A5 67E5 1D64

e) Autoridad de Certificación subordinada a la raíz de curva elíptica: expide los certificados cualificados para firma digital de sellos de tiempo objeto de la presente DPPP con algoritmia de curva elíptica. El Certificado de dicha Autoridad viene identificado por la siguiente información:

Tabla 5 – Certificado de la AC TSA CLIENTES

Campo	Valor
Sujeto	CN = AC TSA CLIENTES, ORG_ID = VATES-Q2826004J, O = FNMT-RCM,C = ES
Emisor	CN = AC RAIZ FNMT-RCM TSA, ORG_ID = VATES-Q2826004J, O= FNMT-RCM, C = ES
Número de serie (hex)	5CD7A6AD9FF9BDB06B430636442C0391825218C5

Campo	Valor
Validez	No antes:10 Octubre 2024 No después: 07 Octubre 2039
Longitud clave pública	EC 384 bits (P-384)
Algoritmo de firma	SHA-384 with ECDSA
Identificador de clave	8F18 753B 8043 DC18 C16E E3B4 B66A ACF7 3766 0901

1.3.2. Autoridad de Registro

15. La FNMT-RCM es la única *Autoridad de Registro* que actúa en el proceso de expedición de este tipo de *Certificados*. Realiza las tareas de identificación y comprobación, con el fin principal de garantizar que el *Certificado* se le expide al *Suscriptor* que tiene el control del nombre de dominio que se incorpora al *Certificado*.

1.3.3. Suscriptores de los certificados

16. El suscriptor de los *Certificados TSU* para la prestación del Servicio de Sellado de Tiempo, será la persona jurídica a quien se expide este tipo de *Certificados* y que suscribe un acuerdo que describe los términos de uso del *Certificado.*

1.3.4. Partes que confían

17. Las partes que confían son aquellas personas físicas o jurídicas, diferentes del Suscriptor, que reciben y / o usan *Certificados* expedidos por la FNMT-RCM. Será responsabilidad de la Entidad usuaria, de los terceros que confían en los *Certificados* y, en general de los miembros de la *Comunidad Electrónica*, la verificación y comprobación del estado de los *Certificados*, no cabiendo en ningún caso presumir la validez de los *Certificados* sin dichas comprobaciones

1.3.5. Otros participantes

18. *Autoridad de Sellado de Tiempo*: La FNMT-RCM es la Autoridad de Sellado de Tiempo cuando provee el Servicio de Confianza de creación de Sellos de tiempo electrónicos, bajo su correspondiente Declaración de Prácticas Particulares, o, en su caso, aquellos terceros a los que se expide este tipo de certificados, como prestadores de su propio servicio de sellado de tiempo.

1.4. USO DE LOS CERTIFICADOS

1.4.1. Usos permitidos de los certificados

19. El uso de los *Certificados TSU* expedidos bajo esta *Política de Certificación,* es el propio para crear sellos de tiempo electrónicos.

20. Los *Certificados TSU* expedidos bajo esta *Política de Certificación* a la propia FNMT-RCM es el empleado para proveer el *Servicio de Sellado de Tiempo* cualificado, de conformidad con la Declaración de Política y Prácticas de Sellado de Tiempo, que puede consultarse en http://www.cert.fnmt.es/dpcs/

21. El Certificado que utiliza la FNMT-RCM para crear los Sellos de Tiempo electrónicos mediante su Servicio de Sellado de Tiempo puede descargarse desde la sede electrónica:

    https://www.sede.fnmt.gob.es/descargas/certificados-raiz-de-la-fnmt

22. Todos los *Certificados TSU* son *Certificados Cualificados* conforme al Reglamento eIDAS y de conformidad con los requisitos establecidos en los estándares europeos ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates", ETSI EN 319 421 "Policy and Security Requirements for Trust Service Providers issuing Time-Stamps" y ETSI EN 319 422 "Time stamping protocol and time-stamp token profiles".

1.4.2. Restricciones en el uso de los certificados

23. Los citados *Certificados TSU* incluyen, siguiendo las recomendaciones de las normas ETSI EN 319 421 y ETSI EN 319 422, la extensión privateKeyUsagePeriod, 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.

24. Si una *Entidad usuaria* o un tercero desean confiar en estos *Certificados* sin acceder al *Servicio de información y consulta sobre el estado de validez de los certificados* expedidos bajo esta *Política de Certificación*, no se obtendrá cobertura de las presentes *Políticas y Prácticas de Certificación Particulares*, 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*.

25. No se podrá emplear este tipo de *Certificados* para:

    - Firmar o sellar otro *Certificado*, salvo supuestos expresamente autorizados previamente.
    - Usos particulares o privados, salvo para relacionarse con las Administraciones cuando éstas lo admitan.
    - Firmar o sellar software o componentes.

- Prestar servicios a título gratuito u oneroso, salvo supuestos expresamente autorizados previamente, como por ejemplo serían a título enunciativo:
    - Prestar servicios de *OCSP*.
    - Generar *Listas de Revocación.*
    - Prestar servicios de notificación
- Cualquier uso que exceda de la finalidad de este tipo de Certificados sin la autorización previa de la FNMT-RCM.

1.5. ADMINISTRACIÓN DE POLÍTICAS

1.5.1. Entidad responsable

26. La Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, con NIF Q2826004-J, es la *Autoridad de Certificación* que expide los certificados a los que aplica la presente *Declaración de Políticas y Prácticas de Certificación*.

1.5.2. Datos de contacto

27. La dirección de contacto de la FNMT-RCM como *Prestador de Servicios de Confianza* es la siguiente:

Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda

Dirección de Sistemas de Información - Departamento CERES

C/ Jorge Juan, 106

28009– MADRID

E-mail: ceres@fnmt.es

Teléfono: +34 91 740 69 82

28. Para informar problemas de seguridad relacionados con un certificado, tales como sospecha de compromiso clave, uso indebido o fraude, envíenos un Informe de incidencia sobre certificado a la cuenta de correo electrónico: incidentes.ceres@fnmt.es.

1.5.3. Responsables de adecuación de la DPC

29. La Dirección de la FNMT-RCM dispone, dentro de sus competencias, de capacidad para especificar, revisar y aprobar los procedimientos de revisión y mantenimiento, tanto para las Prácticas de Certificación Particulares, como para la Política de Certificación correspondiente.

1.5.4. Procedimiento de aprobación de la DPC

30. La FNMT – RCM, a través de su Comité de Gestión del Prestador de Servicios de Confianza, vela por el cumplimiento de las Declaraciones de Políticas y Prácticas de Certificación, las aprueba y realiza el pertinente proceso de revisión de las mismas, con una periodicidad anual

1.6. DEFINICIONES Y ACRÓNIMOS

1.6.1. Definiciones

31. A los efectos de lo dispuesto en la presente *DPPP*, cuando los términos comiencen con letra mayúscula y estén en cursiva, se tendrán en cuenta de forma general las definiciones expresadas en la *DGPC* y, en particular, las expresadas a continuación:

- *Autoridad de Sellado de Tiempo (AST o TSA –en inglés-)*: Sistema de confianza, gestionado por un *Prestador de Servicios de Confianza*, responsable de emitir *Sellos de tiempo electrónico*. Jurídicamente es un caso particular de *Prestador de Servicios de Confianza* y por extensión se denomina al prestador *Autoridad de Sellado de Tiempo*.
- *Certificado TSU:* Certificado de sello electrónico empleado para la creación de *Sellos de tiempo electrónicos* en la prestación del *Servicio de Sellado de Tiempo*.
- *Declaración de Prácticas de Certificación (DPC):* Declaración puesta a disposición del público de manera fácilmente accesible, por vía electrónica y de forma gratuita por parte de la FNMT-RCM. Tiene la consideración de documento de seguridad en el que se detallan, en el marco eIDAS, las obligaciones que los *Prestadores de Servicios de Confianza* se comprometen a cumplir en relación con la gestión de los *Datos de creación y verificación de firma* y de los *Certificados electrónicos*, las condiciones aplicables a la solicitud, expedición, uso y extinción de la vigencia de los *Certificados*, las medidas de seguridad técnicas y organizativas, los perfiles y los mecanismos de información sobre la vigencia de los *Certificados.*
- *Declaración de Políticas y Prácticas Particulares (DPPP): DPC* particular que aplica a la expedición de un conjunto determinado de *Certificados* expedidos por la FNMT-RCM bajo las condiciones particulares recogidas en dicha Declaración, y que le son de aplicación las Políticas particulares definidas en la misma.
- *Organismo de supervisión:* organismo designado por un Estado miembro como responsable de las funciones de supervisión en materia de prestación de servicios de confianza, de conformidad con el Reglamento eIDAS.
- *Política de Sellado de Tiempo (particular)*: Documento que establece el conjunto de reglas que indica la aplicabilidad de un determinado tipo de *Sellado de Tiempo* a la *Comunidad Electrónica* y/o clase de aplicación con requisitos de seguridad comunes.
- *Prestador de Servicios de Sellado de Tiempo*: Es aquella persona física o jurídica que, de conformidad con la normativa sobre *Sellado de Tiempo* expide *Sellos de tiempo electrónicos*.

- *Representante del Suscriptor*: es la persona física representante legal, o persona autorizada por éste, de la organización *Suscriptora* del *Certificado*, para la solicitud y uso de dicho *Certificado*.
- *Sellado de Tiempo (Time Stamping en inglés)*: Consignación de la fecha y hora en un documento electrónico mediante procedimientos criptográficos indelebles, basándose en las especificaciones *Request For Comments*: 3161 – *"Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)",* que logra fechar el documento de forma objetiva.
- *Sello de tiempo electrónico:* Datos en formato electrónico que vinculan otros datos en formato electrónico con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante.
- *Servicio de Sellado de Tiempo:* Servicio prestado bajo demanda por la FNMT-RCM a los interesados que lo soliciten, que basándose en las especificaciones Request For Comments: RFC 3161 – "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)" y ETSI EN 319 421 "Policy and Security Requirements for Trust Service Providers issuing Time-Stamps", data los documentos de forma objetiva logrando que, de forma indubitada se pueda atribuir un momento temporal a la existencia de un documento electrónico. La FNMT-RCM sólo prestará este servicio para determinadas entidades y sus límites de uso, obligaciones y responsabilidades de las partes vendrán descritas en las correspondientes políticas y prácticas particulares del servicio.
- *Suscriptor*: Persona jurídica, órgano u organismo público destinatario de las actividades de la FNMT-RCM como *Prestador de Servicios de Confianza*, que suscribe los términos y condiciones del servicio. Bajo las presentas *Políticas de Certificación*, dicho servicio consiste en la expedición de *Certificados TSU*. El *Suscriptor* se referencia en el campo *Sujeto* del *Certificado* y es el titular y responsable de su uso y posee el control exclusivo y la capacidad de decisión sobre el mismo.
- *Tiempo Universal Coordinado* o UTC (Coordinated Universal Time): Es el tiempo de la zona horaria de referencia respecto a la cual se calculan todas las otras zonas del mundo. Es la escala de tiempo sucesora de GMT y que, a diferencia de este, se basa en referencias atómicas.
- *Unidad de Sellado de Tiempo (TSU –en inglés-):* Conjunto de hardware y software gestionado de forma independiente y que en cada momento sólo tiene activa una clave de sello para la emisión de *Sellos de tiempo electrónicos*.

(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)

1.6.2. Acrónimos

32. A los efectos de lo dispuesto en la presente *DPPP*, son de aplicación los siguientes acrónimos, cuyo significado es acorde con el estándar europeo ETSI EN 319 411 "Policy and security requirements for Trust Service Providers issuing certificates":

AC: Autoridad de Certificación

AR: Autoridad de Registro

ARL: Lista de Revocación de Autoridades de Certificación

CN: Nombre común (Common Name)

CRL: Lista de *Certificados* revocados

DN: Nombre distintivo (Distinguished Name)

DPC: Declaración de Prácticas de Certificación

eIDAS: Reglamento 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 modificado por el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024 (en adelante, Reglamento eIDAS).

ENISA: Agencia de la Unión Europea para la Ciberseguridad

ETSI: European Telecommunications Standards Institute

EUCC: Esquema europeo de certificación de la ciberseguridad basado en los criterios comunes.

HSM: Módulo de seguridad criptográfico (Hardware Security Module). Es un dispositivo de seguridad que genera y protege claves criptográficas.

OCSP: Protocolo de internet usado para obtener el estado de un certificado en línea (Online Certificate Status Protocol)

OID: Identificador de Objeto (Object IDentifier)

PDS: Declaración informativa de la PKI (PKI Disclosure Statement).

PKCS: Estándares PKI desarrollados por Laboratorios RSA (Public Key Cryptography Standards).

UTC: Tiempo coordinado universal (Coordinated Universal Time).

2. PUBLICACIÓN Y REPOSITORIOS

2.1. REPOSITORIO

33. La FNMT-RCM, como como *Prestador de Servicios de Confianza*, mantiene un repositorio de información pública, disponible en horario 24x7, todos los días del año, con las características que se exponen en los siguientes apartados y con acceso a través de la dirección:

https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion

2.2. PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN

34. La información relativa a la expedición de *Certificados* electrónicos objeto de la presente *DPPP* incluye las siguientes informaciones:

- Declaraciones de políticas y prácticas de Certificación.
- Perfiles de los *Certificados*.
- Las declaraciones informativas de la PKI (PDS).
- Los términos y condiciones de uso de los *Certificados*, como instrumento jurídico vinculante.

35. Adicionalmente, se puede acceder a la descarga de los Certificados raíz y de AC subordinadas de la FNMT-RCM, así como a información adicional, a través de la dirección:

https://www.sede.fnmt.gob.es/descargas/

2.3. FRECUENCIA DE PUBLICACIÓN

36. La FNMT-RCM revisará sus políticas y prácticas de certificación y actualizará anualmente la presente *DPPP*, siguiendo las pautas establecidas en el apartado "1.5.4. Procedimiento de aprobación de la DPC" del presente documento de *DPPP*.

37. Cualquier modificación en la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica* o en las *Políticas* y *Prácticas de Certificación Particulares* será publicada de forma inmediata en la URL de acceso a las mismas.

38. En cuanto a la frecuencia de publicación de CRL, se define en el apartado "4.9.7 Frecuencia de generación de CRLs", de la *DGPC*.

2.4. CONTROL DE ACCESO A LOS REPOSITORIOS

39. Todos los repositorios anteriormente citados son de acceso libre para la consulta y, en su caso, descarga de la información. Así mismo, la FNMT-RCM ha establecido controles para impedir que personas no autorizadas puedan añadir, modificar o borrar información incluida en sus repositorios y para proteger la autenticidad e integridad de dicha información.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. DENOMINACIÓN

40. La codificación de los *Certificados* sigue el estándar RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". Todos los campos definidos en el perfil de los *Certificados* en las *Políticas de Certificación* y *Prácticas de Certificación Particulares,* excepto en los campos que específicamente se exprese lo contrario, emplean la codificación UTF8String.

3.1.1. Tipos de nombres

41. Los *Certificados* electrónicos de entidad final objeto de la presente *DPPP* contienen un nombre distintivo (*DN*) en el campo Subject Name, que se componen según se describe en la información relativa al perfil del Certificado (apartado 7.1 del presente documento).

42. El campo Common Name contiene la denominación del sistema o de la aplicación del proceso automático para el que se expide el *Certificado*.

3.1.2. Significado de los nombres

43. Todos los nombres distintivos (*DN*) del campo Subject Name son significativos. La descripción de los atributos asociados al *Suscriptor* del *Certificado* es legible por humanos (véase el apartado 7.1.4 Formato de nombres del presente documento).

3.1.3. Seudónimos

44. Bajo la presente *Política de Certificación* la FNMT – RCM no admite el uso de seudónimos.

3.1.4. Reglas utilizadas para interpretar varios formatos de nombres

45. Se aplican los requisitos definidos por el estándar X.500 de referencia en la norma ISO/IEC 9594.

3.1.5. Unicidad de los nombres

46. El nombre distintivo (*DN*) asignado al *Suscriptor* del *Certificado* dentro del dominio del *Prestador de Servicios de Confianza* será único.

3.1.6. Reconocimiento y autenticación de marcas registradas

47. Véase el apartado correspondiente en la *DGPC*.

3.2. VALIDACIÓN INICIAL DE LA IDENTIDAD

3.2.1. Métodos para probar la posesión de la clave privada

48. La FNMT-RCM no genera ni almacena el par de Claves asociado a los *Certificados TSU* expedidos bajo la presente Política de Certificación a terceros, poniendo todos los mecanismos necesarios durante el proceso de Solicitud del *Certificado* para garantizar que el Suscriptor se encuentran en posesión de la Clave Privada asociada a la Clave Pública que se certificará.

49. Las Claves que la FNMT-RCM necesita para la prestación de su *Servicio de Sellado de Tiempo*, serán generadas por ella misma dentro de su propia infraestructura en un entorno físico seguro.

3.2.2. Autenticación de la identidad de la Organización

50. La FNMT-RCM verifica la existencia legal y la identidad de la organización suscriptora del *Certificado* mediante diferentes métodos, en función del tipo de organización. Con carácter previo al establecimiento de cualquier relación institucional con los *Suscriptores*, la FNMT-RCM informa, a través de los medios y direcciones web citadas en estas *Prácticas de Certificación Particulares* y, subsidiariamente, en la *DGPC*, acerca de las condiciones del servicio, así como de las obligaciones, garantías y responsabilidades de las partes implicadas en la expedición y uso de los *Certificados* por ella emitidos en su labor como *Prestador de Servicios de Confianza.*

51. Las actividades de comprobación de la identidad del *Suscriptor* del *Certificado TSU*, serán realizadas por el personal autorizado de las Oficinas de Registro de la FNMT-RCM, garantizando la identidad de la organización.

52. Cuando el *Suscriptor* es una entidad privada, se verificará su existencia, que está legalmente reconocida, activa en ese momento e inscrita formalmente, mediante consulta directa de la AR de la FNMT-RCM al servicio que el Registro Mercantil dispone para este fin.

53. En el caso de entidades públicas, dicha verificación se realizará mediante consulta directa de la AR de la FNMT-RCM al inventario de entes del sector público de la Intervención General de la Administración del Estado, dependiente del Ministerio de Hacienda, o al Boletín Oficial correspondiente.

54. Si la naturaleza del *Suscriptor* fuera distinta de los dos casos anteriores, las verificaciones relativas a la existencia legal y la identidad se realizará mediante consulta directa al registro oficial correspondiente.

55. La FNMT-RCM verifica que el nombre y número de identificación fiscal de la organización suscriptora del *Certificado* incorporados a la solicitud del mismo coinciden con el nombre y número de identificación fiscal inscritos formalmente en los registros consultados según se describe en los apartados anteriores.

3.2.3. Autenticación de la identidad de la persona física solicitante

56. Las operaciones de verificación de la identidad, son realizadas por personal de la FNMT-RCM con los debidos conocimientos y autorizaciones, manteniendo en todo momento las necesarias medidas de seguridad, en un entorno altamente seguro. El Solicitante de los *Certificados TSU* se corresponderá con el representante del Suscriptor o persona debidamente autorizada por éste.

3.2.4. Información no verificada del Suscriptor

57. Toda la información incorporada al *Certificado* electrónico es verificada por la *Autoridad de Registro*, por tanto, no se incluye información no verificada en el campo "Subject" de los certificados expedidos.

3.2.5. Validación de la capacidad de representación

58. La Autoridad de Registro verifica que el *Solicitante* de un *Certificado TSU* expedido bajo la presente *DPPP* ha sido previamente autorizado por el *Suscriptor* para llevar a cabo dicha solicitud. Estas comprobaciones se llevarán a cabo siempre ante cualquier solicitud de un nuevo *Certificado TSU*.

59. La AR de la FNMT-RCM verifica que el *Solicitante* tiene suficiente capacidad de representación mediante la firma electrónica del formulario de solicitud, según se describe en el apartado 3.2.3 de la presente *DPPP*, aceptando el uso de un *Certificado* cualificado de representante de administrador único o solidario de la persona jurídica suscriptora o un *Certificado* cualificado de *Personal al servicio de la Administración Pública*, para cuya expedición ha sido acreditada la capacidad de representación.

60. Cuando el citado formulario se firma mediante un *Certificado* cualificado diferente de los mencionados en el apartado anterior, la AR de la FNMT-RCM comprueba la facultad de representación del firmante de la solicitud mediante consulta a registros oficiales (Registro Mercantil, Boletines Oficiales, etc. en función de la naturaleza de la representación). Si del resultado de estas consultas no se obtuvieran evidencias de representación suficiente, la AR de la FNMT-RCM se pondrá en contacto con el *Suscriptor* para recabar dichas evidencias.

3.2.6. Criterios de interoperación

61. No existen relaciones de interactividad con Autoridades de Certificación externas a FNMT-RCM.

3.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE RENOVACIÓN DE CLAVES

62. Bajo las presentes Políticas de Certificación, la FNMT-RCM no contempla ningún proceso de regeneración de claves.

63. Las condiciones de autenticación de una petición de renovación se desarrollan en el apartado correspondiente al proceso de renovación de Certificados de este documento.

3.4. IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE REVOCACIÓN

64. Las condiciones de autenticación de una petición de revocación se desarrollan en el apartado de esta *DPPP* correspondiente al proceso de revocación de *Certificados* (véase apartado 4.9 del presente documento).

4. REQUISITOS OPERATIVOS DEL CICLO DE VIDA DE LOS CERTIFICADOS

65. Las Claves que la FNMT-RCM necesita para el desarrollo del servicio de Sellado de Tiempo, en su actividad como *Prestador de Servicios de Confianza*, serán generadas por ella misma dentro de su propia infraestructura en un entorno físico seguro y al menos por dos personas autorizadas para ello.

66. El procedimiento para la generación de claves, denominado "Ceremonia de generación de claves", se encuentra documentado en el procedimiento interno "Gestión del ciclo de vida de las claves de la FNMT-RCM como prestador de servicios de certificación y sellado".

4.1. SOLICITUD DE CERTIFICADOS

4.1.1. Quién puede solicitar un Certificado

67. Únicamente podrán solicitar *Certificados TSU* emitidos bajo esta política, el representante del Suscriptor, autorizado a tal efecto. Con carácter previo a la solicitud, el *Suscriptor* del *Certificado*, a través de su representante, formalizará el acuerdo que recoge los términos de uso, obligaciones y responsabilidades sobre el mismo.

4.1.2. Proceso de registro y responsabilidades

68. El Solicitante, a través de un formulario de solicitud de *Certificados TSU* aportará los datos identificativos, tales como el NIF, primer apellido, NIF del organismo suscriptor, entre otros.

69. La FNMT-RCM, tras recibir esta información, comprobará la validez de la información de la solicitud firmada, así como el tamaño de las claves generadas.

70. FNMT-RCM recopilará las evidencias correspondientes a las comprobaciones realizadas y quedarán almacenadas en un repositorio.

71. Para la emisión del *Certificado TSU* que la FNMT-RCM necesita para la prestación de su *Servicio de Sellado de Tiempo*

a. La AR de la FNMT-RCM verificará que el personal de la FNMT-RCM responsable de llevar a cabo las tareas de solicitud y registro del *Certificado TSU* cuenta con la autorización necesaria y que se documenta en el procedimiento interno "Gestión del ciclo de vida de las claves de la FNMT-RCM como prestador de servicios de certificación y sellado"

b. FNMT-RCM recopilará las evidencias correspondientes a las comprobaciones realizadas y quedarán almacenadas en un repositorio. Todo el proceso quedará documentado como parte de la "Ceremonia de generación de claves"

72. El apartado 9.8 "Responsabilidades" del presente documento establece las responsabilidades de las partes en este proceso.

4.2. PROCEDIMIENTO DE SOLICITUD DE CERTIFICADOS

4.2.1. Realización de las funciones de identificación y autenticación

73. La FNMT-RCM comprobará la veracidad de los datos incluidos en la solicitud y, en su caso, la capacidad del *Representante* a través de las verificaciones correspondientes y conservando las evidencias oportunas.

4.2.2. Aprobación o rechazo de la solicitud del certificado

74. La AR que actúa en el proceso de expedición de *Certificados TSU* es siempre la propia FNMT-RCM.

75. La AR de la FNMT-RM realiza las comprobaciones relativas a la prueba de posesión de la *Clave privada*, la autenticación de la identidad de la Organización y de la persona que solicita el *Certificado*.

76. Si alguna de estas validaciones no ha podido ser confirmada, la FNMT-RCM rechazará la solicitud del *Certificado*, reservándose el derecho de no revelar los motivos de dicha denegación.

4.2.3. Tiempo en procesar la solicitud

77. Para los *Certificados TSU*, se establece un tiempo máximo aproximado para procesar la solicitud, de 72 horas desde la recepción por parte de la *Oficina de Registro* de la FNMT – RCM, de toda la documentación necesaria para realizar las comprobaciones requeridas de forma previa a la expedición del *Certificado*.

4.3. EMISIÓN DEL CERTIFICADO

4.3.1. Acciones de la AC durante la emisión

78. Una vez aprobada la solicitud del *Certificado* por parte de la AR de la FNMT-RCM, el sistema realiza algunas comprobaciones, como el tamaño de la *Clave pública* generada, y procede a expedir el *Certificado* conforme al perfil aprobado para cada tipo de *Certificado*.

79. La emisión de *Certificados* de la FNMT-RCM sólo puede realizarla ella misma, en calidad de *Prestador de Servicios de Confianza*, no existiendo ninguna otra entidad u organismo con capacidad de emisión de los mismos. La *Autoridad de Certificación* de la FNMT-RCM solo acepta solicitudes de generación de *Certificados* provenientes de fuentes autorizadas. Todos los datos contenidos en cada solicitud están protegidos contra alteraciones a través de mecanismos de *Firma Electrónica* o *Sello Electrónicos*. En cualquier caso, la FNMT-RCM actuará eficazmente para:

- Comprobar la correspondencia entre la Clave Privada y la Clave Pública.
- Lograr que la información incluida en el *Certificado* se base en la información proporcionada por la Oficina de Registro correspondiente.
- No ignorar hechos notorios que puedan afectar a la fiabilidad del *Certificado*.
- Lograr que el DN (nombre distintivo) del Sujeto asignado en el Certificado sea único en el ámbito de la presente *DPPP*.

80. Para la emisión del *Certificado* se seguirán los siguientes pasos:

1. Composición de la estructura de datos que conforman el *Certificado*.

   Con los datos recogidos durante el proceso de solicitud del *Certificado*, se procede a componer el nombre distintivo (DN) conforme al estándar X.500, asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedades.

   El atributo CN contiene la denominación del sistema o de la aplicación del proceso automático para el que se expide el *Certificado*.

2. Generación del Certificado conforme al perfil del Certificado correspondiente.

81. El formato de los *Certificados*, expedidos por la FNMT-RCM bajo la presente *Política de Certificación*, en consonancia con la norma UIT-T X.509 versión 3 y de acuerdo con la normativa legalmente aplicable en materia de *Certificados Cualificados*, puede consultarse en la página http://www.cert.fnmt.es/dpcs/

82. No se permitirán las emisiones basadas en el algoritmo SHA1, ya que se considera un algoritmo inseguro, obsoleto y no recomendado por ENISA ni autorizado por las guías actuales del Centro Criptológico Nacional.

4.3.2. Notificación de la emisión

83. Una vez emitido el *Certificado TSU*, la FNMT-RCM informará al *Suscriptor* sobre la disponibilidad del *Certificado*.

4.4. ACEPTACIÓN DEL CERTIFICADO

4.4.1. Proceso de aceptación

84. En el proceso de solicitud del *Certificado TSU*, el Suscriptor acepta las condiciones de uso y expresa su voluntad de obtener el *Certificado*, como requisitos necesarios para la generación del mismo.

4.4.2. Publicación del certificado por la AC.

85. Los *Certificados* generados son almacenados en un repositorio seguro de la FNMT-RCM.

4.4.3. Notificación de la emisión a otras entidades

86. No se realizan notificaciones de emisión a otras entidades.

4.5. PAR DE CLAVES Y USO DEL CERTIFICADO

4.5.1. Clave privada del suscriptor y uso del certificado

87. La FNMT-RCM no genera ni almacena las Claves Privadas asociadas a los *Certificados TSU* expedidos a suscriptores distintos a la FNMT-RCM bajo la presente Política de Certificación.

88. Las Claves que la FNMT-RCM necesita para la prestación de su Servicio de Sellado de Tiempo, serán generadas por ella misma dentro de su propia infraestructura, en dispositivos criptográficos certificados, en un entorno físico seguro y al menos por dos personas autorizadas para ello.

89. Las claves privadas de la TSU utilizada por el Servicio cualificado de Sellado de Tiempo de la FNMT-RCM son generadas por personal designado con el rol de confianza correspondiente y custodiadas por un dispositivo criptográfico que cumple los requisitos de seguridad conforme a Common Criteria (ISO/IEC 15408), con nivel de aseguramiento EAL4+ incluyendo el componente ALC_FLR.2 y AVA_VAN.5. , 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 y acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad y publicados por ENISA. 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.

90. 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*.

91. 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.

92. 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.

4.5.2. Uso del certificado y la clave pública por terceros que confían

93. Los terceros que confían en los *sellos electrónicos* realizados con las *Claves privadas* asociadas al *Certificado TSU* se atendrán a las obligaciones y responsabilidades definidas en la presente *DPPP*.

4.6. RENOVACIÓN DEL CERTIFICADO

94. Bajo las presentes *Políticas de Certificación*, la FNMT-RCM no renueva *Certificados* manteniendo la *Clave pública* del mismo según se define en el apartado "4.7 Renovación con regeneración de las claves del certificado" del presente documento.

4.7. RENOVACIÓN CON REGENERACIÓN DE LAS CLAVES DEL CERTIFICADO

95. La renovación con regeneración de claves de los *Certificados TSU* se realiza siempre emitiendo nuevas claves, siguiendo el mismo proceso que el descrito para la emisión de un *Certificado* nuevo.

4.7.1. Circunstancias para la renovación con regeneración de claves

96. Las claves de una unidad de sellado de la FNMT-RCM se renovarán bajo los siguientes supuestos:

- Por caducidad próxima de las actuales claves
- Por incumplimientos del certificado asociado a la clave privada con la normativa o legislación vigente o que vaya a entrar en vigor

- Por incompatibilidades del certificado asociado a la clave privada con productos comerciales o que supongan un obstáculo para el desarrollo del negocio de la Autoridad de Sellado
- Siempre y cuando el CGPSC estime conveniente desde un punto de vista técnico o comercial la creación de una nueva unidad de sellado con nuevas características
- Por obsolescencia de los algoritmos criptográficos, de forma que la seguridad de los mismos se prevea que pueda ser comprometida en un tiempo anterior al de caducidad del certificado asociado. En los casos en los que esta previsión llegue a materializarse, se activará adicionalmente el Plan de Compromiso de Claves de la Autoridad de Sellado, bajo el supuesto de compromiso de algoritmos.
- Por compromiso de las claves, supuesto en el que se actuará de acuerdo con lo dispuesto en el Plan de Compromiso de Claves de Sellado

4.7.2. Quién puede solicitar la renovación con regeneración de claves

97. Se seguirá el mismo proceso que el descrito para la emisión de un *Certificado* nuevo.

4.7.3. Procesamiento de solicitudes de renovación con regeneración de claves

98. Se seguirá el mismo proceso que el descrito para la emisión de un *Certificado* nuevo.

4.7.4. Notificación de la renovación con regeneración de claves

99. Se seguirá el mismo proceso que el descrito para la emisión de un *Certificado* nuevo.

4.7.5. Conducta que constituye la aceptación de la renovación con regeneración de claves

100. Se seguirá el mismo proceso que el descrito para la emisión de un *Certificado* nuevo.

4.7.6. Publicación del certificado renovado

101. Se seguirá el mismo proceso que el descrito para la emisión de un *Certificado* nuevo.

4.7.7. Notificación de la renovación con regeneración de claves a otras entidades

102. Se seguirá el mismo proceso que el descrito para la emisión de un *Certificado* nuevo.

4.8. MODIFICACIÓN DEL CERTIFICADO

103. No es posible realizar modificaciones de los *Certificados* expedidos. Por tanto, cualquier necesidad de modificación conlleva la expedición de un nuevo *Certificado*.

4.9. REVOCACIÓN Y SUSPENSIÓN DEL CERTIFICADO

104. Los *Certificados TSU* emitidos por la FNMT-RCM quedarán sin efecto en los siguientes casos:

a) Terminación del período de validez del *Certificado.*

b) Cese en la actividad como *Prestador de Servicios de Confianza* de la FNMT-RCM, salvo que, previo consentimiento expreso del *Suscriptor*, los *Certificados* expedidos por la FNMT-RCM hayan sido transferidos a otro *Prestador de Servicios de Confianza*.

En estos dos casos [a) y b)], la pérdida de eficacia de los *Certificados* tendrá lugar desde que estas circunstancias se produzcan.

c) Revocación del *Certificado* por cualquiera de las causas recogidas en el presente documento.

105. Los efectos de la revocación del *Certificado*, esto es, la extinción de su vigencia, surtirán desde la fecha en que la FNMT-RCM tenga conocimiento cierto de cualquiera de los hechos determinantes y así lo haga constar en su *Servicio de información y consulta sobre el estado de los certificados*.

106. La FNMT-RCM pone a disposición de los *Suscriptores*, terceros que confían, proveedores de software y terceras partes una vía de comunicación a través de la sede electrónica de la FNMT-RCM

https://www.sede.fnmt.gob.es/

con instrucciones claras, para permitirles reportar cualquier asunto relacionado con este tipo de *Certificados*, en cuanto a un supuesto compromiso de *Clave Privada*, uso indebido de los *Certificados* u otros tipos de fraude, compromiso, mal uso o conducta inapropiada.

107. Se atenderá asimismo a lo dispuesto en el "Plan de Actuación ante Compromiso de Unidades de Sellado de la FNMT-RCM "

4.9.1. Circunstancias para la revocación

4.9.1.1 Circunstancias para la revocación del certificado del suscriptor

108. La solicitud de revocación de los *Certificados* podrá efectuarse durante el período de validez que consta en el *Certificado.*

109. Serán causas de revocación de un *Certificado TSU*:

a) La solicitud de revocación por parte de las personas autorizadas. En todo caso deberá dar lugar a esta solicitud:

- La pérdida del soporte del *Certificado*.
- La utilización por un tercero de la *Clave Privada* asociada al *Certificado*.

- La violación o puesta en peligro del secreto de la *Clave Privada* asociada al *Certificado*.

b) Resolución judicial o administrativa que así lo ordene.

c) Extinción o disolución de la personalidad jurídica del *Suscriptor*.

d) Inexactitudes en los datos aportados por el *Suscriptor* para la obtención del *Certificado*, o alteración de los datos aportados para la obtención del *Certificado* o modificación de las circunstancias verificadas para la expedición del *Certificado*, de manera que éste ya no fuera conforme a la realidad.

e) Contravención de una obligación sustancial de esta *Declaración de Prácticas de Certificación* por parte del *Suscriptor*, o de una *Oficina de Registro* si, en este último caso, hubiese podido afectar al procedimiento de emisión del *Certificado*.

f) Violación o puesta en peligro del secreto de los *Datos de Creación de Firma* / *Sello* de la FNMT-RCM, con los que firma / sella los *Certificados* que emite.

g) Incumplimiento de los requisitos definidos por los esquemas de auditorías a los que se somete la *Autoridad de Certificación* que expide los *Certificados* cubiertos por la presente *DPPP*, con especial atención a los de algoritmia y tamaños de clave, que supongan un riesgo inaceptable por parte de las partes que confían en estos *Certificados*.

110. La FNMT-RCM únicamente será responsable de las consecuencias que se desprendan de no haber revocado un *Certificado* en los siguientes supuestos:

- Que la revocación le haya sido solicitada por el *Suscriptor* siguiendo el procedimiento establecido para este tipo de *Certificados.*
- Que la solicitud de revocación o la causa que la motiva, le haya sido notificada mediante resolución judicial o administrativa.

111. Las actuaciones constitutivas de delito o falta de las que no tenga conocimiento la FNMT-RCM que se realicen sobre los datos o el *Certificado*, las inexactitudes sobre los datos o falta de diligencia en su comunicación a la FNMT-RCM, producirán la exoneración de responsabilidad de la FNMT-RCM.

112. La revocación de los *Certificados* implica, además de su extinción y la imposibilidad de seguir utilizando los *Datos de creación de firma* o claves privadas asociados, la finalización de la relación y régimen de uso de dicho *Certificado* y su *Clave privada* con la FNMT-RCM.

4.9.1.2 Circunstancias para la revocación del certificado de la CA subordinada

113. Se atenderá a lo dispuesto en el "Plan de Actuación ante Compromiso de la Infraestructura de Clave Pública de FNMT-RCM"

4.9.2. Quién puede solicitar la revocación

114. La revocación de un *Certificado TSU* sólo podrá ser solicitada por el *Suscriptor* a través de su representante, o personas en quien deleguen.

115. Además, la FNMT-RCM podrá revocar de oficio los *Certificados* en los supuestos recogidos en la presente Declaración de Políticas y Prácticas de Certificación.

4.9.3. Procedimiento de solicitud de la revocación

116. La solicitud de revocación de un *Certificado TSU*, se podrá iniciar a través del teléfono habilitado para tal fin (previa identificación del Solicitante) cuyo número se hace público en la web de la FNMT – RCM y que estará operativo en horario 24x7.

117. El proceso de revocación puede realizarse de forma ininterrumpida 24x7, a través del Servicio de Revocación telefónica puesto a disposición de los usuarios para esta finalidad, asegurando la revocación del *Certificado* en un plazo inferior a 24h.

118. Durante la revocación telefónica, el solicitante de la revocación tendrá que confirmar los datos que se le soliciten, y aportar aquellos que sean imprescindibles para la validación de forma inequívoca de su capacidad para solicitar dicha revocación.

119. Adicionalmente, se puede solicitar la revocación de cualquier *Certificado* a través de la *Oficina de Registro*. Los datos personales y su tratamiento quedarán sometidos a la legislación específica. Para ello, el solicitante de la revocación remitirá a la *Oficina de Registro* de la FNMT-RCM el formulario creado a tal efecto, debidamente cumplimentado y firmado. Una vez la *Oficina de Registro* reciba la documentación, comprobará y validará la información, así como la capacidad del solicitante para pedir la revocación, procediendo a revocar el *Certificado* si todo es correcto.

120. Si la persona solicitante no puede aportar los datos requeridos o se determina que no está capacitada para solicitar la revocación, la solicitud de revocación será desestimada.

121. Tan pronto la revocación sea efectiva, serán notificados a través de la dirección de correo electrónico facilitada, tanto el *Suscriptor* del certificado como el *Representante del Suscriptor* que solicita la revocación.

122. Una vez que la FNMT-RCM ha procedido a la revocación del *Certificado*, se publicará en el *Directorio* seguro la correspondiente *Lista de Certificados Revocados,* conteniendo el número de serie del *Certificado* revocado, así como la fecha, hora y causa de revocación. Una vez que un *Certificado* ha sido revocado, su vigencia queda definitivamente extinguida, sin posibilidad de revertir su estado.

123. La revocación de un *Certificado TSU* emitido a la FNMT-RCM se llevará a cabo atendiendo a lo descrito en el procedimiento “Gestión del ciclo de vida de las claves de la FNMT-RCM como prestador de servicios de certificación y sellado”.

4.9.4. Periodo de gracia de la solicitud de revocación

124. No existe periodo de gracia asociado a este proceso, pues la revocación se realiza de forma inmediata a la recepción verificada de la solicitud de revocación.

4.9.5. Plazo de tiempo para procesar la solicitud de revocación

125. La FNMT – RCM procede a la revocación inmediata del *Certificado TSU* en el momento de realizar las comprobaciones descritas anteriormente o, en su caso, una vez comprobada la veracidad de la solicitud realizada mediante resolución judicial o administrativa.

4.9.6. Obligación de verificar las revocaciones por las partes que confían

126. Las terceras partes que confían y aceptan el uso de los *Certificados* emitidos por la FNMT – RCM están obligadas a verificar:

- el *Sello Electrónico Avanzado* del *Prestador de Servicios de Confianza* emisor del *Certificado,*
- que el *Certificado* continúa vigente y activo, y
- el estado de los *Certificados* incluidos en la *Cadena de Certificación.*

4.9.7. Frecuencia de generación de CRLs

127. Las *Listas de Revocación* (*CRL*) de los certificados de entidad final se emiten al menos cada 12 horas, o cuando se produce una revocación y tienen un periodo de validez de 24 horas. Las *CRL* de los certificados de *Autoridad* se emiten cada 6 meses, o cuando se produce una revocación de una *Autoridad de Certificación* subordinada y tienen un periodo de validez de 6 meses.

4.9.8. Periodo máximo de latencia de las CRLs

128. La publicación de las *Listas de Revocación* se realiza en el momento de generación de dichas Listas, por lo que el periodo de latencia entre la generación de la CRL y su publicación es nulo.

4.9.9. Disponibilidad del sistema de verificación online del estado de los certificados

129. La información relativa al estado de los certificados estará disponible en línea las 24 horas del día, los 7 días de la semana. En caso de fallo del sistema se pondrá en marcha el Plan de continuidad de negocio para solventar el incidente a la mayor brevedad posible.

4.9.10. Requisitos de comprobación en línea de la revocación

130. La comprobación en línea del estado de revocación del *Certificado TSU* puede realizarse mediante el *Servicio de información del estado de los certificados*, ofrecido a través de OCSP según se describe en el apartado 4.10 del presente documento. El interesado en utilizar dicho servicio deberá:

- Comprobar la dirección contenida en la extensión AIA (Authority Information Access) del certificado.
- Comprobar que la respuesta OCSP está firmada / sellada.

4.9.11. Otras formas de aviso de revocación disponibles

131. No definidas.

4.9.12. Requisitos especiales de revocación de claves comprometidas

132. Se atenderá a lo dispuesto en el "Plan de Actuación ante Compromiso de la Infraestructura de Clave Pública de FNMT-RCM"

133. Véase el apartado correspondiente en la *DGPC*.

4.9.13. Circunstancias para la suspensión

134. No se contempla la suspensión de certificados.

4.9.14. Quién puede solicitar la suspensión

135. No se contempla la suspensión de certificados.

4.9.15. Procedimiento para la petición de la suspensión

136. No se contempla la suspensión de certificados.

4.9.16. Límites sobre el periodo de suspensión

137. No se contempla la suspensión de certificados.

4.10. SERVICIOS DE INFORMACIÓN DEL ESTADO DE LOS CERTIFICADOS

138. El funcionamiento del *Servicio de información y consulta del estado de los certificados* es el siguiente: el servidor OCSP recibe la petición OCSP efectuada por un *Cliente OCSP* y comprueba el estado de vigencia de los *Certificados* incluidos en la misma. En caso de que la petición sea válida, se emitirá una respuesta de OCSP informando acerca del estado en el que se encuentran en ese momento los *Certificados* incluidos en la petición. Dicha respuesta es

firmada / sellada con los *Datos de Creación de Firma* / *Sello* de la FNMT-RCM garantizando así la integridad y la autenticidad de la información suministrada sobre el estado de revocación de los *Certificados* consultados.

139. Será responsabilidad de la Entidad usuaria contar con un *Cliente OCSP* para operar con el servidor OCSP puesto a disposición por la FNMT-RCM.

140. La FNMT-RCM opera y mantiene sus capacidades de mantenimiento de sus CRL y servicio OCSP con recursos suficientes para proporcionar un tiempo de respuesta máximo de diez segundos bajo condiciones normales de operación.

4.10.1. Características operativas

141. La información relativa a la validación de los *Certificados* electrónicos objeto de la presente *DPPP* es accesible a través de los medios descritos en la *DGPC*.

4.10.2. Disponibilidad del servicio

142. La FNMT-RCM garantiza el acceso a este servicio, en horario 24x7, por parte de los usuarios, titulares y las partes que confían en los *Certificados*, de forma segura, rápida y gratuita.

143. En el caso de indisponibilidad del servicio por operaciones de mantenimiento, la FNMT-RCM notificará esta circunstancia en la dirección http://www.ceres.fnmt.es, si es posible con al menos cuarenta y ocho (48) horas de antelación, y tratará de solventarla en un periodo no superior a veinticuatro (24) horas.

4.10.3. Características opcionales

144. No estipuladas.

4.11. FINALIZACIÓN DE LA SUSCRIPCIÓN

145. La suscripción finalizará en el momento de extinción de la vigencia del *Certificado TSU*, ya sea por expiración del periodo de vigencia o por revocación del mismo.

4.12. CUSTODIA Y RECUPERACIÓN DE CLAVES

4.12.1. Políticas y prácticas de custodia y recuperación de claves

146. La FNMT-RCM no recuperará las *Claves privadas* de los *Titulares* de los *Certificados*.

4.12.2. Políticas y prácticas de protección y recuperación de la clave de sesión

147. No estipulado.

5. CONTROLES DE SEGURIDAD FÍSICA, DE PROCEDIMIENTOS Y DE PERSONAL

148. Véase el apartado correspondiente en la *DGPC*.

5.1. CONTROLES DE SEGURIDAD FÍSICA

149. Véase el apartado correspondiente en la *DGPC*.

5.2. CONTROLES DE PROCEDIMIENTO

150. Véase el apartado correspondiente en la *DGPC*.

5.3. CONTROLES DE PERSONAL

151. Véase el apartado correspondiente en la *DGPC*.

5.4. PROCEDIMIENTOS DE AUDITORÍA

152. Véase el apartado correspondiente en la *DGPC*.

5.5. ARCHIVADO DE REGISTROS

153. Véase el apartado correspondiente en la *DGPC*.

5.6. CAMBIO DE CLAVES DE LA AC

154. Véase el apartado correspondiente en la *DGPC*.

5.7. GESTIÓN DE INCIDENTES Y VULNERABILIDADES

155. Véase el apartado correspondiente en la *DGPC*.

5.8. CESE DE LA ACTIVIDAD DEL PRESTADOR DE SERVICIOS DE CONFIANZA

156. Véase el apartado correspondiente en la *DGPC*.

6. CONTROLES DE SEGURIDAD TÉCNICA

157. Véase el apartado correspondiente en la *DGPC*.

6.1. GENERACIÓN E INSTALACIÓN DE LAS CLAVES

6.1.1. Generación del par de claves

6.1.1.1 Generación del par de Claves de la CA

158. En relación con la información de las *Claves* que la FNMT-RCM necesita para el desarrollo de su actividad como *Prestador de Servicios de Confianza de Sellado de Tiempo,* generará las Claves de los *Certificados TSU* atendiendo a lo descrito en el procedimiento de "Gestión del ciclo de vida de las claves de la FNMT-RCM como prestador de servicios de certificación y sellado". Véase el aparatado correspondiente en la *DGPC*.

6.1.1.2 Generación del par de Claves de la RA

159. No estipulado

6.1.1.3 Generación del par de Claves de los Suscriptores

160. En relación a la generación de las *Claves* para un *Suscriptor* distinto de la FNMT-RCM, se garantiza que éstas sean generadas y custodias por el propio *Suscriptor* del *Certificado*.

6.1.2. Envío de la clave privada al suscriptor

161. No existe ninguna entrega de la *Clave privada* al *Titular*.

6.1.3. Envío de la clave pública al emisor del certificado

162. La *Clave pública,* generada junto a la *Clave privada* sobre el dispositivo de generación y custodia de claves, es entregada a la Autoridad de Certificación mediante el envío de una solicitud de certificación en formato PKCS#10.

6.1.4. Distribución de la clave pública de la AC a las partes que confían

163. Véase el apartado correspondiente en la *DGPC*.

6.1.5. Tamaños de claves y algoritmos utilizados

164. Los algoritmos utilizados bajo el ámbito de la presente DPPP son

- RSA con SHA-256.
- ECDSA con SHA-384

165. En cuanto al tamaño de las claves, son:

- de al menos 3.072 bits en el caso de claves RSA
- de al menos 256 bits en el caso de claves ECDSA

6.1.6. Parámetros de generación de la clave pública y verificación de la calidad

166. Véase el apartado correspondiente en la *DGPC*.

6.1.7. Usos admitidos de las claves (KeyUsage field X.509v3)

167. Los *Certificados* FNMT incluyen la extensión Key Usage y, según el caso, Extended Key Usage, indicando los usos habilitados de la *Claves*.

168. El *Certificado* raíz de la AC tiene habilitados los usos de *Claves* para firmar/sellar los *Certificados* de las AC Subordinadas y las ARLs. Los *Certificados* de las AC Subordinadas que expiden los *Certificados TSU* tienen habilitado exclusivamente el uso para firmar/sellar *Certificados* de usuario final (*Certificados TSU*) y CRLs.

169. El *Certificado TSU* tiene habilitado exclusivamente el uso de autenticación y firma digital.

6.2. PROTECCIÓN DE LA CLAVE PRIVADA Y CONTROLES DE LOS MÓDULOS CRIPTOGRÁFICOS

170. Véase el apartado correspondiente en la *DGPC*.

6.3. OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

6.3.1. Archivo de la clave pública

171. Véase el apartado correspondiente en la *DGPC*.

6.3.2. Periodos de operación del certificado y periodos de uso del par de claves

172. Los periodos de operación de los *Certificados* y sus *Claves* asociadas son:

- Los *Certificado* de AC raíz y su par de *Claves*: véase el apartado "1.3.1. Autoridad de Certificación" de la presente *DPPP*.
- Los *Certificados* de AC subordinadas que expiden los *Certificados TSU* y su par de *Claves*: véase el apartado "1.3.1. Autoridad de Certificación" de la presente *DPPP*.
- Los *Certificados TSU* y su par de *Claves:* el periodo máximo de vigencia de los *Certificados* y su par de *Claves:* no superior a 5 años.

6.4. DATOS DE ACTIVACIÓN

173. Véase el apartado correspondiente en la *DGPC*.

6.5. CONTROLES DE SEGURIDAD INFORMÁTICA

174. Véase el apartado correspondiente en la *DGPC*.

6.6. CONTROLES TÉCNICOS DEL CICLO DE VIDA

175. Véase el apartado correspondiente en la *DGPC*.

6.7. CONTROLES DE SEGURIDAD DE RED

176. Véase el apartado correspondiente en la *DGPC*.

6.8. FUENTE DE TIEMPO

177. Véase el apartado correspondiente en la *DGPC*.

6.9. OTROS CONTROLES ADICIONALES

178. Véase el apartado correspondiente en la *DGPC*.

7. PERFILES DE LOS CERTIFICADOS, CRLS Y OCSP

7.1. PERFIL DEL CERTIFICADO

179. Los *Certificados TSU* emitidos bajo esta política son de conformidad con el estándar X.509 versión 3, RFC 5280 y con los estándares europeos ETSI EN 319 411-2 “Requirements for trust service providers issuing EU qualified certificates”, ETSI EN 319 412-3 “Certificate profile for certificates issued to legal persons”, ETSI EN 319 421 “Policy and Security Requirements for Trust Service Providers issuing Time-Stamps” y ETSI EN 319 422 “Time stamping protocol and time-stamp token profiles”.

7.1.1. Número de versión

180. Los *Certificados TSU* son conformes con el estándar X.509 versión 3.

7.1.2. Extensiones del certificado

181. En la página http://www.cert.fnmt.es/dpcs/ se publica el documento que describe el perfil de los *Certificados TSU*, incluyendo todas sus extensiones.

7.1.3. Identificadores de objeto de algoritmos

182. El identificador de objeto (OID) correspondiente al algoritmo de firma criptográfico utilizado puede ser:

- 1.2.840.113549.1.1.11 - SHA-256 with RSA Encryption.
- 1.2.840.10045.4.3.3 - SHA-384 with ECDSA Encryption.
- 1.2.840.10045.4.3.2 - SHA-256 with ECDSA Encryption.

183. El identificador de objeto (OID) correspondiente al algoritmo de clave pública puede ser:

- 1.2.840.113549.1.1.1 - rsaEncryption
- 1.2.840.10045.2.1 - EcPublicKey

7.1.4. Formatos de nombres

184. La codificación de los *Certificados* TSU sigue la recomendación RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". Todos los campos definidos en el perfil de estos *Certificados,* excepto en los campos que específicamente se exprese lo contrario, emplean la codificación UTF8String.

7.1.5. Restricciones de nombres

185. El nombre distintivo (*DN*) asignado al *Suscriptor* del *Certificado* dentro del dominio del *Prestador de Servicios de Confianza* será único y con la composición definida en el perfil del *Certificado*.

7.1.6. Identificador de objeto de política de certificado

186. El identificador de objeto (OID) de la política del *Certificados TSU* es la definida en el apartado "1.2 Nombre del documento e identificación" del presente documento.

7.1.7. Empleo de la extensión restricciones de política

187. La extensión "Policy Constrains" del *Certificado* raíz de la AC no es utilizado.

7.1.8. Sintaxis y semántica de los calificadores de política

188. La extensión "Certificate Policies" incluye dos campos de "Policy Qualifiers":

- CPS Pointer: contiene la URL donde se publican las *Políticas de Certificación* y *Prácticas de Servicios de confianza* aplicables a este servicio.
- User notice: contiene el texto que puede ser desplegado en la pantalla del usuario del *Certificado* durante la verificación del mismo.

7.1.9. Tratamiento semántico para la extensión "Certificate policy"

189. La extensión "Certificate Policy" incluye el campo OID de política, que identifica la política asociada al *Certificado* por parte de la FNMT–RCM, así como los dos campos relacionados en el apartado anterior.

7.2. PERFIL DE LA CRL

7.2.1. Número de versión

190. El perfil de las CRL son conformes con el estándar X.509 versión 2.

7.2.2. CRL y extensiones

191. El perfil de las CRL sigue la siguiente estructura:

Tabla 6 – Perfil de la CRL

Campos y extensiones	Valor
Versión	V2
Algoritmo de firma	Sha256WithRSAEncryption o Sha384WithECDSAEncryption.
Número de CRL	Valor incremental
Emisor	DN del emisor
Fecha de emisión	Tiempo UTC de emisión.
Fecha de próxima actualización	Fecha de emisión + 24 horas (salvo la ARL que es Fecha de emisión + 1 año)

Campos y extensiones	Valor
Punto de distribución	URLs del punto de distribución y ámbito de las CRLs
ExpiredCertsOnCRL	NotBefore de la CA
Certificados revocados	Lista de certificados revocados, conteniendo al menos para cada entrada, número de serie y fecha de revocación

7.3. PERFIL DE OCSP

7.3.1. Número de versión

192. Véase el apartado correspondiente en la *DGPC*.

7.3.2. Extensiones del OCSP

193. Véase el apartado correspondiente en la *DGPC*.

8. AUDITORÍAS DE CUMPLIMIENTO

194. El sistema de expedición de *Certificados* es sometido anualmente a un proceso de auditoría conforme a los estándares europeos ETSI EN 319 401 "General Policy Requirements for Trust Service Providers" y ETSI EN 319 411-1 "Policy and security requirements for Trust Service Providers issuing certificates".

195. En el caso de los *Certificados* con la consideración de cualificados la auditoría garantiza adicionalmente el cumplimiento con los requisitos establecidos en los estándares europeos ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates", ETSI EN 319 421 "Policy and Security Requirements for Trust Service Providers issuing Time-Stamps" y ETSI EN 319 422 "Time stamping protocol and electronic time-tamp profiles".

196. Véase el apartado correspondiente en la *DGPC*.

8.1. FRECUENCIA DE LAS AUDITORÍAS

197. Véase el apartado correspondiente en la *DGPC*.

8.2. CUALIFICACIÓN DEL AUDITOR

198. Véase el apartado correspondiente en la *DGPC*.

8.3. RELACIÓN DEL AUDITOR CON LA EMPRESA AUDITADA

199. Véase el apartado correspondiente en la *DGPC*.

8.4. ELEMENTOS OBJETOS DE AUDITORÍA

200. Véase el apartado correspondiente en la *DGPC*.

8.5. TOMA DE DECISIONES FRENTE A DETECCIÓN DE DEFICIENCIAS

201. Véase el apartado correspondiente en la *DGPC*.

8.6. COMUNICACIÓN DE LOS RESULTADOS

202. Véase el apartado correspondiente en la *DGPC*.

9. OTROS ASUNTOS LEGALES Y DE ACTIVIDAD

9.1. TARIFAS

203. Véase el apartado correspondiente en la *DGPC*.

9.1.1. Tarifas de emisión o renovación de certificados

204. Véase el apartado correspondiente en la *DGPC*.

9.1.2. Tarifas de acceso a los certificados

205. No estipulado.

9.1.3. Tarifas de acceso a la información de estado o revocación

206. La FNMT-RCM ofrece los servicios de información del estado de los certificados a través de del protocolo OCSP de forma gratuita.

9.1.4. Tarifas para otros servicios

207. Véase el apartado correspondiente en la *DGPC*.

9.1.5. Política de reembolso

208. La FNMT – RCM cuenta con una política de devolución que permite la solicitud de reembolso dentro del período de desistimiento establecido, aceptando que este hecho llevará consigo la revocación automática del certificado. El procedimiento se publica en la sede electrónica de la FNMT – RCM.

9.2. RESPONSABILIDAD FINANCIERA

209. Véase el apartado correspondiente en la *DGPC*.

9.3. CONFIDENCIALIDAD DE LA INFORMACIÓN

210. Véase el apartado correspondiente en la *DGPC*.

9.4. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

211. Véase el apartado correspondiente en la *DGPC*.

9.5. DERECHOS DE PROPIEDAD INTELECTUAL

212. Véase el apartado correspondiente en la *DGPC*.

9.6. OBLIGACIONES Y GARANTÍAS

9.6.1. Obligaciones de la AC

213. Las obligaciones y responsabilidades de la FNMT-RCM, como *Prestador de Servicios de Confianza*, con el *Suscriptor* del *Certificado* y, en su caso, con las partes usuarias y terceros que confían, quedarán determinadas, principalmente, por el documento relativo a las

condiciones de utilización o el contrato de expedición del *Certificado*, y, subsidiariamente, por la presente *Declaración de Políticas y Prácticas de Certificación*.

214. La FNMT – RCM cumple los requisitos de las especificaciones técnicas de la norma ETSI EN 319 411 para la emisión de *Certificados* y se compromete a continuar cumpliendo con dicha norma o aquellas que la sustituyan.

215. Sin perjuicio de lo dispuesto en la normativa de aplicación a este tipo de *Certificados*, así como las obligaciones descritas en el apartado correspondiente de la *DGPC*, el *Prestador de Servicios de Confianza* se obliga a:

216. Con carácter previo a la expedición del *Certificado*

- Comprobar la identidad y circunstancias personales del *Solicitante* del *Certificado* y del *Suscriptor* y/o su *Representante* y recoger la manifestación de que el *Solicitante* está autorizado por el *Suscriptor* para realizar la solicitud.

  La identificación se realizará a través de *Certificados* cualificados de firma electrónica admitidos en los procesos de FNMT-RCM.

- En el proceso de registro, comprobar los datos relativos a la personalidad jurídica del *Suscriptor* y a la capacidad del *Representante*. Todas estas comprobaciones se realizarán según lo dispuesto en las *Prácticas de Certificación Particulares* expresadas en este documento y según los protocolos y procedimientos de registro de la FNMT-RCM.

  En los procesos de comprobación de los extremos antes señalados anteriormente la FNMT-RCM podrá realizar verificaciones mediante la intervención de terceros que ostenten facultades fedatarias o de registros públicos o privados.

- Verificar que toda la información contenida en la solicitud del *Certificado* se corresponde con la aportada por el *Solicitante*.

- Comprobar que el *Solicitante* está en posesión de la *Clave Privada* asociada a la *Clave Pública* que se incorpora al *Certificado* a emitir.

- Garantizar que los procedimientos seguidos aseguran que las *Claves Privadas* correspondientes a los *Certificados TSU* son generadas sin que se realicen copias ni se produzca el almacenamiento de los mismos por parte de la FNMT-RCM.

- Realizar la comunicación de información al *Suscriptor, Representante* y *Solicitante* de tal forma que se procure su *Confidencialidad*.

- Poner a disposición del *Solicitante, Suscriptor, Representante* y demás interesados (http://www.ceres.fnmt.es) la *Declaración de Prácticas de Certificación* y cuanta información sea relevante para el desarrollo de los procedimientos relacionados con el ciclo de vida de los *Certificados* objeto de esta *Política de Certificación* y *Prácticas de Certificación Particulares* de conformidad con la normativa aplicable.

217. Véase el apartado correspondiente en la *DGPC*.

9.6.2. Obligaciones de la AR

218. Las actividades relativas a la AR serán realizadas exclusivamente por la FNMT-RCM, a través de su Área de Registro.

219. La AR, a través del Área de Registro de la FNMT-RCM, tiene las siguientes obligaciones:

- Con carácter general, seguir los procedimientos establecidos por la FNMT-RCM en la *Política y Prácticas de Certificación* de aplicación en el desempeño de sus funciones de gestión, expedición y revocación de *Certificados* y no alterar dicho marco de actuación.
- En particular, comprobar la identidad, y cualesquiera circunstancias personales relevantes para la finalidad asignada, de los *Solicitantes* de los *Certificados*, *Suscriptores* y sus *Representantes*, utilizando cualquiera de los medios admitidos en Derecho y conforme a lo previsto con carácter general en la *DGPC* y con carácter particular en la presente *DPPP*.
- Conservar toda la información y documentación relativa a los *Certificados*, cuya solicitud, renovación o revocación gestiona durante quince (15) años.
- Realizar la recepción y gestión de las solicitudes y los contratos de expedición (formulario pdf) de *Certificados* con el *Suscriptor* de los mismos.
- Comprobar diligentemente las causas de revocación que pudieran afectar a la vigencia de los *Certificados*.

220. Véase el apartado correspondiente en la *DGPC*.

9.6.3. Obligaciones de los Suscriptores

221. En cuanto a los *Certificados TSU* han de mantener bajo su uso exclusivo las *Claves privadas* asociadas.

222. El *Solicitante* y el *Suscriptor* de los *Certificados* expedidos bajo la presente *DPP*, tienen la obligación de:

- No usar el *Certificado* fuera de los límites especificados en la presente *Política y Prácticas de Certificación* particulares.
- No usar el *Certificado* en caso de que el *Prestador de Servicios de Confianza* haya cesado su actividad como Entidad emisora de *Certificados* que expidió el certificado en cuestión, especialmente en los casos en los que los *Datos de Creación de Sello* del prestador puedan estar comprometidos, y así se haya comunicado.
- Aportar información veraz en la solicitud de los *Certificados* y mantenerla actualizada, suscribiendo los contratos por persona con capacidad suficiente.

- No solicitar para el *Sujeto* del certificado signos distintivos, denominaciones o derechos de propiedad industrial o intelectual de las que no sea titular, licenciatario o cuente con autorización demostrable para su uso.
- Actuar con diligencia respecto de la custodia y conservación de los *Datos de creación de Firma / Sello* o cualquier otra información sensible como *Claves*, códigos de activación del *Certificado*, palabras de acceso, números de identificación personal, etc., así como de los soportes de los *Certificados,* lo que comprende en todo caso, la no revelación de ninguno de los datos mencionados.
- Conocer, aceptar y cumplir las condiciones de utilización de los *Certificados* previstas en las condiciones de uso y en la *Declaración de Prácticas de Certificación* y en particular, las limitaciones de uso de los *Certificados*
- Conocer y cumplir las modificaciones que se produzcan en la *Declaración de Prácticas de Certificación*.
- Solicitar la revocación del correspondiente *Certificado*, según el procedimiento descrito en el presente documento, notificando diligentemente a la FNMT-RCM las circunstancias para la revocación o sospecha de pérdida de la *Confidencialidad*, la divulgación, modificación o uso no autorizado de las *Claves privadas* asociadas,
- Revisar la información contenida en el *Certificado*, y notificar a la FNMT-RCM cualquier error o inexactitud.
- Verificar con carácter previo a confiar en los *Certificados,* la *Firma electrónica* o el *Sello electrónico* avanzados del *Prestador de Servicios de Confianza* emisor del *Certificado.*
- Notificar diligentemente a la FNMT-RCM cualquier modificación de los datos aportados en la solicitud del *Certificado*, solicitando, cuando consecuentemente fuere pertinente, la revocación del mismo.

223. Será responsabilidad del *Suscriptor* utilizar de manera adecuada y custodiar diligentemente el *Certificado*, según el propósito y función para el que ha sido expedido, así como informar a la FNMT-RCM acerca de cualquier variación de estado o información respecto de lo reflejado en el *Certificado*, para su revocación y nueva expedición.

224. Asimismo, será el *Suscriptor* quien deba responder, en todo caso, ante la FNMT-RCM, las *Entidades usuarias* y, en su caso, ante terceros, del uso indebido del *Certificado*, o de la falsedad o errores de las manifestaciones en él recogidas, o actos u omisiones que provoquen daños y perjuicios a la FNMT-RCM o a terceros.

225. Será responsabilidad y, por tanto, obligación del *Suscriptor* no usar el *Certificado* en caso de que el *Prestador de Servicios de Confianza* haya cesado en la actividad como Entidad emisora de *Certificados* que realizó la expedición del *Certificado* en cuestión y no se hubiera producido la subrogación prevista en la ley. En todo caso, el *Suscriptor* no usará el *Certificado* 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.

226. Solicitar la revocación del *Certificado TSU* emitido bajo esta política cuando alguno de los datos referidos al *Suscriptor* sean incorrectos, inexactos o hayan variado respecto a lo consignado en el *Certificado,* o no se correspondan con el titular y contactos establecidos en las bases de datos correspondientes para la gestión y administración de la dirección electrónica consignada en el *Certificado* objeto de la revocación.

227. Las relaciones de la FNMT-RCM y el *Suscriptor* quedarán determinadas principalmente, a los efectos del régimen de uso de los *Certificados,* a través del documento relativo a las condiciones de utilización o en su caso, contrato de emisión del *Certificado* y atendiendo a los acuerdos, convenios o documento de relación entre la FNMT-RCM y la Entidad Pública correspondiente.

9.6.4. Obligaciones de las partes que confían

228. Véase el apartado correspondiente en la *DGPC*.

9.6.5. Obligaciones de otros participantes

229. No estipulado.

9.7. RENUNCIA DE GARANTÍAS

230. No estipulado.

9.8. LIMITACIONES DE RESPONSABILIDAD

231. En relación a los *Certificados TSU* pertenecientes a Autoridades de Sellado de Tiempo de terceros, se hace constar que la FNMT-RCM no tendrá responsabilidad alguna, ni garantizará, ningún aspecto del servicio de Sellado de Tiempo que puedan ofrecer las entidades titulares de tales *Certificados* y Autoridades de Sellado de Tiempo. En especial la exención de responsabilidad alcanzará a la gestión de cualquiera de los aspectos relacionados con los sistemas de información empleados por dichos *Certificados* o Autoridades, así como la validez de las fuentes de tiempo, o su sincronismo, empleadas en el servicio.

232. Véase el apartado correspondiente en la *DGPC*.

9.9. INDEMNIZACIONES

233. Véase el apartado correspondiente en la *DGPC*.

9.10. PERIODO DE VALIDEZ DE ESTE DOCUMENTO

9.10.1. Plazo

234. La presente *Declaración de Practicas y Políticas de Certificación* entrará en vigor en el momento de su publicación.

9.10.2. Terminación

235. La presente *Declaración de Practicas y Políticas de Certificación* será derogada en el momento que una nueva versión del documento sea publicada. La nueva versión sustituirá íntegramente al documento anterior. La FNMT – RCM se compromete a someter dicha Declaración a un proceso de revisión anual.

9.10.3. Efectos de la finalización

236. Para los certificados vigentes emitidos bajo una *Declaración de Practicas y Políticas de Certificación* anterior, la nueva versión prevalecerá a la anterior en todo lo que no se oponga a ésta.

9.11. NOTIFICACIONES INDIVIDUALES Y COMUNICACIÓN CON LOS PARTICIPANTES

237. Véase el apartado correspondiente en la *DGPC*.

9.12. MODIFICACIONES DE ESTE DOCUMENTO

9.12.1. Procedimiento para las modificaciones

238. Véase el apartado correspondiente en la *DGPC*.

9.12.2. Periodo y mecanismo de notificación

239. Véase el apartado correspondiente en la *DGPC*.

9.12.3. Circunstancias bajo las cuales debe cambiarse un OID

240. Véase el apartado correspondiente en la *DGPC*.

9.13. RECLAMACIONES Y RESOLUCIÓN DE DISPUTAS

241. Véase el apartado correspondiente en la *DGPC*.

9.14. NORMATIVA DE APLICACIÓN

242. Véase el apartado correspondiente en la *DGPC*.

9.15. CUMPLIMIENTO DE LA NORMATIVA APLICABLE

243. La FNMT-RCM manifiesta el cumplimiento de la normativa de aplicación.

9.16. ESTIPULACIONES DIVERSAS

244. Véase el apartado correspondiente en la *DGPC*.

9.17. OTRAS ESTIPULACIONES

245. Véase el apartado correspondiente en la *DGPC*.