



Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

**DECLARACIÓN DE PRÁCTICAS Y POLÍTICAS DE CERTIFICACIÓN DE
CERTIFICADOS DE COMPONENTES “AC COMPONENTES
INFORMÁTICOS”**

	NOMBRE	FECHA
Elaborado por:	FNMT-RCM	26/04/2022
Revisado por:	FNMT-RCM	27/04/2022
Aprobado por:	FNMT-RCM	28/07/2022

Versión	Fecha	Descripción
1.0	21/11/2013	Primera versión
1.1	07/03/2014	Eliminación de la Suspensión
1.2	22/10/2014	Revisión conforme WebTrust
1.3	23/03/2015	Inclusión del OID del certificado para uso de Unidades de Sellado de Tiempo
1.4	24/06/2016	Eliminación de componentes de personas físicas y actualización de perfiles: inclusión de campo Locality
1.5	03/01/2017	Adaptación al reglamento eIDAS
1.6	09/10/2017	Incorporación de requisitos CAB/Forum
1.7	21/09/2018	Incorporación de requisitos CAB/Forum
1.8	5/03/2019	Incorporación de requisitos CAB/Forum en materia de validación de dominios.
1.9	30/05/2019	Actualización métodos de validación de dominios conforme a CA/Browser Forum Baseline Requirements.
1.10	18/11/2019	Incorporación de referencia explícita al identificador de dominio a los efectos de las comprobaciones con el registro AAC



Versión	Fecha	Descripción
2.0	19/06/2020	Revisión general y adaptación a RFC 3647
2.1	31/08/2020	Reducción del periodo de validez de los certificados SSL a 12 meses.
2.2	01/10/2020	Incorporación del ECU “Autenticación de cliente” a los certificados de autenticación de sitios web
2.3	28/04/2021	Revisión anual y revisión Política Mozilla v.2.7.1 Se incluye información acerca de los métodos para comunicar un compromiso de claves
2.4	30/09/2021	Revisión general conforme a Mozilla Root Store Policy v.2.7.1, Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v.1.8.0. y EV Guidelines v.1.7.8. Se incorporan detalles en relación al ballot SC48.
2.5	28/07/2022	Incorporación de un nuevo certificado de autenticación de sitio web con perfil QNCP-w

Referencia: DPC/PC-DPC-ACCOMP_0205/SGPSC/2022

Documento clasificado como: *Público*



Índice de contenidos

1. Introducción.....	10
1.1. Objeto	10
1.2. Nombre del documento e identificación	11
1.3. Partes intervinientes	12
1.3.1. Autoridad de Certificación.....	13
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	15
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.....	19
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
3.2.2.1 Identidad	22
3.2.2.2 Nombre comercial o marca registrada	23
3.2.2.3 Verificación del país	23
3.2.2.4 Validación de la autorización y control sobre el dominio	23
3.2.2.5 Autenticación para una dirección IP	24



3.2.2.6 Validación de dominio wildcard	25
3.2.2.7 Fiabilidad de las fuentes de datos.....	25
3.2.2.8 Registro AAC.....	25
3.2.3. Autenticación de la identidad de la persona física solicitante.....	25
3.2.4. Información no verificada del Suscriptor.....	25
3.2.5. Validación de la capacidad de representación	25
3.2.6. Criterios de interoperación.....	26
3.3. <i>Identificación y autenticación para peticiones de renovación de claves</i>	26
3.3.1. Identificación y autenticación para renovación rutinaria de claves.....	26
3.3.2. Identificación y autenticación para renovación de claves después de una revocación.....	26
3.4. <i>Identificación y autenticación para peticiones de revocación</i>	26
4. Requisitos operativos del ciclo de vida de los certificados	27
4.1. <i>Solicitud de Certificados</i>	27
4.1.1. Quién puede solicitar un Certificado	27
4.1.2. Proceso de registro y responsabilidades.....	27
4.2. <i>Procedimiento de solicitud de certificados</i>	28
4.2.1. Realización de las funciones de identificación y autenticación	28
4.2.2. Aprobación o rechazo de la solicitud del certificado	28
4.2.3. Tiempo en procesar la solicitud	29
4.3. <i>Emisión del certificado</i>	29
4.3.1. Acciones de la AC durante la emisión	29
4.3.2. Notificación de emisión de certificado	29
4.4. <i>Aceptación del certificado</i>	30
4.4.1. Proceso de aceptación.....	30
4.4.2. Publicación del certificado por la AC	30
4.4.3. Notificación de la emisión a otras entidades.....	30
4.5. <i>Par de claves y uso del certificado</i>	30
4.5.1. Clave privada del suscriptor y uso del certificado	30
4.5.2. Uso del certificado y la clave pública por terceros que confían.....	30
4.6. <i>Renovación del certificado</i>	31
4.6.1. Circunstancias para la renovación del certificado.....	31
4.6.2. Quién puede solicitar la renovación del certificado	31
4.6.3. Procesamiento de solicitudes de renovación del certificado	31
4.6.4. Notificación de la renovación del certificado	31
4.6.5. Conducta que constituye la aceptación de la renovación del certificado	31
4.6.6. Publicación del certificado renovado	31
4.6.7. Notificación de la renovación del certificado a otras entidades.....	32
4.7. <i>Renovación con regeneración de las claves del certificado</i>	32
4.7.1. Circunstancias para la renovación con regeneración de claves.....	32
4.7.2. Quién puede solicitar la renovación con regeneración de claves.....	32
4.7.3. Procesamiento de solicitudes de renovación con regeneración de claves	32
4.7.4. Notificación de la renovación con regeneración de claves	32
4.7.5. Conducta que constituye la aceptación de la renovación con regeneración de claves	32
4.7.6. Publicación del certificado renovado	32
4.7.7. Notificación de la renovación con regeneración de claves a otras entidades	32



4.8.	<i>Modificación del certificado</i>	33
4.8.1.	Circunstancias para la modificación del certificado	33
4.8.2.	Quién puede solicitar la modificación del certificado.....	33
4.8.3.	Procesamiento de solicitudes de modificación del certificado.....	33
4.8.4.	Notificación de la modificación del certificado	33
4.8.5.	Conducta que constituye la aceptación de la modificación del certificado	33
4.8.6.	Publicación del certificado modificado.....	33
4.8.7.	Notificación de la modificación del certificado a otras entidades.....	33
4.9.	<i>Revocación y suspensión del certificado</i>	33
4.9.1.	Circunstancias para la revocación.....	34
4.9.1.1	Causas de revocación de un Certificado de entidad final	34
4.9.1.1	Causas de revocación de un Certificado de CA subordinada.....	36
4.9.2.	Quién puede solicitar la revocación	37
4.9.3.	Procedimiento de solicitud de la revocación.....	37
4.9.4.	Periodo de gracia de la solicitud de revocación	38
4.9.5.	Plazo de tiempo para procesar la solicitud de revocación	38
4.9.6.	Obligación de verificar las revocaciones por las partes que confían	39
4.9.7.	Frecuencia de generación de CRLs.....	39
4.9.8.	Periodo máximo de latencia de las CRLs	39
4.9.9.	Disponibilidad del sistema de verificación online del estado de los certificados	39
4.9.10.	Requisitos de comprobación en línea de la revocación.....	39
4.9.11.	Otras formas de aviso de revocación disponibles	40
4.9.12.	Requisitos especiales de revocación de claves comprometidas	40
4.9.13.	Circunstancias para la suspensión.....	40
4.9.14.	Quién puede solicitar la suspensión	40
4.9.15.	Procedimiento para la petición de la suspensión.....	40
4.9.16.	Límites sobre el periodo de suspensión	40
4.10.	<i>Servicios de información del estado de los certificados</i>	40
4.10.1.	Características operativas.....	41
4.10.2.	Disponibilidad del servicio	41
4.10.3.	Características opcionales.....	41
4.11.	<i>Finalización de la suscripción</i>	41
4.12.	<i>Custodia y recuperación de claves</i>	41
4.12.1.	Prácticas y políticas de custodia y recuperación de claves	41
4.12.2.	Prácticas y políticas de protección y recuperación de la clave de sesión	41
5.	Controles de seguridad física, de procedimientos y de personal	41
5.1.	<i>Controles de Seguridad Física</i>	41
5.1.1.	Ubicación de las instalaciones	42
5.1.2.	Acceso Físico.....	42
5.1.3.	Electricidad y Aire Acondicionado.....	42
5.1.4.	Exposición al agua	42
5.1.5.	Prevención y Protección contra incendios	42
5.1.6.	Almacenamiento de Soportes	42
5.1.7.	Eliminación de Residuos.....	42
5.1.8.	Copias de Seguridad fuera de las instalaciones.....	42
5.2.	<i>Controles de Procedimiento</i>	42
5.2.1.	Roles de Confianza	42



5.2.2.	Número de personas por tarea.....	42
5.2.3.	Identificación y autenticación para cada rol.....	43
5.2.4.	Roles que requieren segregación de funciones	43
5.3.	<i>Controles de Personal</i>	43
5.3.1.	Conocimientos, cualificación, experiencia y requerimientos acreditativos	43
5.3.2.	Procedimientos de verificación de antecedentes	43
5.3.3.	Requisitos de formación	43
5.3.4.	Requisitos y frecuencia de actuación formativa.....	43
5.3.5.	Secuencia y frecuencia de rotación laboral.....	43
5.3.6.	Sanciones por acciones no autorizadas	43
5.3.7.	Requisitos de contratación de personal	43
5.3.8.	Suministro de documentación al personal.....	43
5.4.	<i>Procedimientos de auditoría</i>	44
5.4.1.	Tipos de eventos registrados	44
5.4.2.	Frecuencia de procesamiento de registros	44
5.4.3.	Periodo de conservación de los registros	44
5.4.4.	Protección de los registros	44
5.4.5.	Procedimientos de copias de seguridad de los registros auditados	44
5.4.6.	Sistemas de recolección de registros.....	44
5.4.7.	Notificación al sujeto causante de los eventos	44
5.4.8.	Análisis de vulnerabilidades	44
5.5.	<i>Archivado de registros</i>	44
5.5.1.	Tipos de registros archivados.....	44
5.5.2.	Periodo de retención del archivo.....	45
5.5.3.	Protección del archivo	45
5.5.4.	Procedimientos de copia de respaldo del archivo	45
5.5.5.	Requisitos para el sellado de tiempo de los registros of Records	45
5.5.6.	Sistema de archivo	45
5.5.7.	Procedimientos para obtener y verificar la información archivada.....	45
5.6.	<i>Cambio de claves de la AC</i>	45
5.7.	<i>Gestión de incidentes y vulnerabilidades</i>	45
5.7.1.	Gestión de incidentes y vulnerabilidades.....	45
5.7.2.	Actuación ante datos y software corruptos	45
5.7.3.	Procedimiento ante compromiso de la clave privada de la AC.....	45
5.7.4.	Continuidad de negocio después de un desastre	46
5.8.	<i>Cese de la actividad del Prestador de Servicios de Confianza</i>	46
6.	Controles de seguridad técnica	46
6.1.	<i>Generación e instalación de las Claves</i>	46
6.1.1.	Generación del par de claves	46
6.1.1.1	Generación del par de Claves de la CA.....	46
6.1.1.2	Generación del par de Claves de la RA.....	46
6.1.1.3	Generación del par de Claves de los Suscriptores.....	46
6.1.2.	Envío de la clave privada al suscriptor	46
6.1.3.	Envío de la clave pública al emisor del certificado.....	46
6.1.4.	Distribución de la clave pública de la AC a las partes que confían	46
6.1.5.	Tamaños de claves y algoritmos utilizados.....	47
6.1.6.	Parámetros de generación de la clave pública y verificación de la calidad.....	47



6.1.7.	Usos admitidos de las claves (KeyUsage field X.509v3)	47
6.2.	<i>Protección de la clave privada y controles de los módulos criptográficos</i>	47
6.2.1.	Estándares para los módulos criptográficos	47
6.2.2.	Control multi-persona (n de m) de la clave privada.....	48
6.2.3.	Custodia de la clave privada	48
6.2.4.	Copia de seguridad de la clave privada.....	48
6.2.5.	Archivado de la clave privada.....	48
6.2.6.	Transferencia de la clave privada a/o desde el módulo criptográfico	48
6.2.7.	Almacenamiento de la clave privada en el módulo criptográfico	48
6.2.8.	Método de activación de la clave privada	48
6.2.9.	Método de desactivación de la clave privada.....	48
6.2.10.	Método de destrucción de la clave privada	48
6.2.11.	Clasificación de los módulos criptográficos	48
6.3.	<i>Otros aspectos de la gestión del par de claves</i>	49
6.3.1.	Archivo de la clave pública.....	49
6.3.2.	Periodos operativos del certificado y periodos de uso del par de claves.....	49
6.4.	<i>Datos de activación</i>	49
6.4.1.	Generación e instalación de datos de activación	49
6.4.2.	Protección de datos de activación	49
6.4.3.	Otros aspectos de los datos de activación	49
6.5.	<i>Controles de seguridad informática</i>	49
6.5.1.	Requisitos técnicos específicos de seguridad informática	49
6.5.2.	Evaluación del nivel de seguridad informática	50
6.6.	<i>Controles técnicos del ciclo de vida</i>	50
6.6.1.	Controles de desarrollo de sistemas	50
6.6.2.	Controles de gestión de la seguridad.....	50
6.6.3.	Controles de seguridad del ciclo de vida	50
6.7.	<i>Controles de seguridad de red</i>	50
6.8.	<i>Fuente de tiempo</i>	50
7.	Perfiles de los certificados, CRLs y OCSP	50
7.1.	<i>Perfil del certificado</i>	50
7.1.1.	Número de versión.....	51
7.1.2.	Extensiones del certificado	51
7.1.3.	Identificadores de objeto de algoritmos	51
7.1.4.	Formatos de nombres.....	51
7.1.5.	Restricciones de nombres	51
7.1.6.	Identificador de objeto de política de certificado.....	52
7.1.7.	Empleo de la extensión restricciones de política	52
7.1.8.	Sintaxis y semántica de los calificadores de política	52
7.1.9.	Tratamiento semántico para la extensión “Certificate policy”.....	52
7.2.	<i>Perfil de la CRL</i>	52
7.2.1.	Número de versión.....	52
7.2.2.	CRL y extensiones	52
7.3.	<i>Perfil de OCSP</i>	53
7.3.1.	Número de versión.....	53



7.3.2.	Extensiones del OCSP	53
8.	Auditorías de cumplimiento	53
8.1.	<i>Frecuencia de las auditorías</i>	<i>54</i>
8.2.	<i>Cualificación del auditor</i>	<i>54</i>
8.3.	<i>Relación del auditor con la empresa auditada</i>	<i>55</i>
8.4.	<i>Elementos objetos de auditoría</i>	<i>55</i>
8.5.	<i>Toma de decisiones frente a detección de deficiencias</i>	<i>55</i>
8.6.	<i>Comunicación de los resultados</i>	<i>55</i>
8.7.	<i>Autoevaluación</i>	<i>55</i>
9.	Otros asuntos legales y de actividad	55
9.1.	<i>Tarifas</i>	<i>55</i>
9.1.1.	Tarifas de emisión o renovación de certificados	55
9.1.2.	Tarifas de acceso a los certificados	55
9.1.3.	Tarifas de acceso a la información de estado o revocación	55
9.1.4.	Tarifas para otros servicios	56
9.1.5.	Política de reembolso	56
9.2.	<i>Responsabilidad financiera</i>	<i>56</i>
9.2.1.	Seguro de responsabilidad civil	56
9.2.2.	Otros activos	56
9.2.3.	Seguros y garantías para entidades finales	56
9.3.	<i>Confidencialidad de la información</i>	<i>56</i>
9.3.1.	Alcance de la información confidencial	56
9.3.2.	Información no incluida en el alcance	56
9.3.3.	Responsabilidad para proteger la información confidencial	56
9.4.	<i>Protección de datos de carácter personal</i>	<i>57</i>
9.4.1.	Plan de privacidad	57
9.4.2.	Información tratada como privada	57
9.4.3.	Información no considerada privada	57
9.4.4.	Responsabilidad de proteger la información privada	57
9.4.5.	Aviso y consentimiento para usar información privada	57
9.4.6.	Divulgación conforme al proceso judicial o administrativo	57
9.4.7.	Otras circunstancias de divulgación de información	57
9.5.	<i>Derechos de propiedad intelectual</i>	<i>57</i>
9.6.	<i>Obligaciones y garantías</i>	<i>57</i>
9.6.1.	Obligaciones de la AC	57
9.6.2.	Obligaciones de la AR	59
9.6.3.	Obligaciones de los Suscriptores	59
9.6.4.	Obligaciones de las partes que confían	61
9.6.5.	Obligaciones de otros participantes	61
9.7.	<i>Renuncia de garantías</i>	<i>61</i>
9.8.	<i>Límites de responsabilidad</i>	<i>62</i>



9.9.	<i>Indemnizaciones</i>	62
9.9.1.	Indemnización de la CA.....	62
9.9.2.	Indemnización de los Suscriptores.....	62
9.9.3.	Indemnización de las partes que confían	62
9.10.	<i>Periodo de validez de este documento</i>	62
9.10.1.	Plazo	62
9.10.2.	Terminación.....	62
9.10.3.	Efectos de la finalización	62
9.11.	<i>Notificaciones individuales y comunicación con los participantes</i>	62
9.12.	<i>Modificaciones de este documento</i>	63
9.12.1.	Procedimiento para las modificaciones.....	63
9.12.2.	Periodo y mecanismo de notificación	63
9.12.3.	Circunstancias bajo las cuales debe cambiarse un OID	63
9.13.	<i>Reclamaciones y resolución de disputas</i>	63
9.14.	<i>Normativa de aplicación</i>	63
9.15.	<i>Cumplimiento de la normativa aplicable</i>	63
9.16.	<i>Estipulaciones diversas</i>	64
9.16.1.	Acuerdo íntegro	64
9.16.2.	Asignación	64
9.16.3.	Severabilidad	64
9.16.4.	Cumplimiento	64
9.16.5.	Fuerza Mayor.....	64
9.17.	<i>Otras estipulaciones</i>	64

Índice de tablas

Tabla 1 – Certificado de la AC RAIZ FNMT-RCM	13
Tabla 2 – Certificado de la AC subordinada Componentes Informáticos	13
Tabla 3 – Perfil de la CRL.....	52



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 por el que se deroga la Directiva 1999/93/CE, a través de una entidad independiente y en el marco de un esquema de certificación, 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 de Componentes* 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 dichos *Certificados*, las condiciones aplicables a la solicitud, emisión, uso y extinción de la vigencia de los mismos, y
 - 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.
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.



1.2. NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

7. El presente documento se denomina “*Políticas y Prácticas de certificación particulares de los Certificados de Componentes – AC Componentes Informáticos*”, y en adelante será citado en este documento y con el ámbito descrito en el mismo como “*Declaración de Prácticas y Políticas Particulares*” o por su acrónimo “*DPPP*”.
8. 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*.
9. 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.
10. La presente *Política de Certificación* de la FNMT-RCM para la expedición de *Certificados de Componentes* se descompone en las identificadas a continuación:

Denominación general: *Política de Certificación de Certificados de componente de la FNMT-RCM (AC Componentes Informáticos)*

Nombre: *Política de Certificación de Certificados de componente de firma de código*

Referencia / OID: 1.3.6.1.4.1.5734.3.9.4

Nombre: *Política de Certificación de Certificados de componente para su uso en las Unidades de Sellado de Tiempo*

Referencia / OID: 1.3.6.1.4.1.5734.3.9.14

Nombre: *Política de Certificación de Certificado de componente de sello de entidad*

Referencia / OID: 1.3.6.1.4.1.5734.3.9.19

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

Nombre: *Política de Certificación de Certificado de componente como Unidad de Sellado de Tiempo del Servicio cualificado de Sellado de Tiempo de la FNMT – RCM*

Referencia / OID: 1.3.6.1.4.1.5734.3.9.20

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

Nombre: *Política de Certificación de Certificado de autenticación de sitio web estándar*

Referencia / OID: 1.3.6.1.4.1.5734.3.9.16

Tipo de política asociada: OVCP. OID: 0.4.0.2042.1.7

Nombre: *Política de Certificación de Certificado de autenticación de sitio web wildcard*

Referencia / OID: 1.3.6.1.4.1.5734.3.9.17

Tipo de política asociada: OVCP. OID: 0.4.0.2042.1.7



Nombre: Política de Certificación de *Certificado de autenticación de sitio web multidominio (SAN/UCC)*

Referencia / OID: 1.3.6.1.4.1.5734.3.9.18

Tipo de política asociada: OVCP. OID: 0.4.0.2042.1.7

Nombre: Política de Certificación de *Certificado cualificado de autenticación de sitio web estándar*

Referencia / OID: 1.3.6.1.4.1.5734.3.9.21

Tipo de política asociada: OVCP. OID: 0.4.0.2042.1.7

Organization identity Validation OID: 2.23.140.1.2.2

QNCP-w OID: 0.4.0.194112.1.5

Versión: 2.5

Fecha de aprobación: 28/07/2022

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/>

11. En el párrafo anterior, se identifica un OID de política para cada perfil de *Certificado*, aunque todas ellas se describen conjuntamente en este mismo documento. La razón de ello es doble, por un lado, se permite diferenciar de manera automatizada la estructura de campos a interpretar en cada tipo de *Certificado*, y por el otro, se unifican las reglas de aplicación de los *Certificados* a una misma comunidad y con los mismos requisitos de seguridad. Cada una de las políticas se ha relacionado con el tipo de *Certificado*.

1.3. PARTES INTERVINIENTES

12. 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

13. 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. 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

Certificado de la AC RAIZ FNMT-RCM	
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) Autoridades de Certificación subordinadas: expiden los *Certificados* de entidad final objeto de la presente *DPPP*. Los certificados de dichas Autoridades vienen identificados por la siguiente información:

Tabla 2 – Certificado de la AC subordinada Componentes Informáticos

Certificado de la AC subordinada Componentes Informáticos	
Sujeto	OU=AC Componentes Informáticos, O=FNMT-RCM, C=ES
Emisor	OU = AC RAIZ FNMT-RCM, O = FNMT-RCM, C = ES



Certificado de la AC subordinada Componentes Informáticos	
Número de serie (hex)	34:C6:AB:04:4E:36:99:12:51:C8:25:0B:6C:94:D6:C0
Validez	No antes: 24 de junio de 2013 No después: 24 de junio de 2028
Longitud clave pública	RSA 2048
Algoritmo de firma	RSA - SHA256
Identificador de clave	19 F8 58 2F 14 D6 A6 CC 9B 04 98 08 0D 4C D7 AB 00 A7 83 65

1.3.2. Autoridad de Registro

14. 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 de autenticación de sitio web* se le expide al *Suscriptor* que tiene el control del nombre de dominio que se incorpora al *Certificado*
 - El *Certificados de Sello de entidad* se le expide al *suscriptor* que ha creado el mismo.

1.3.3. Suscriptores de los certificados

15. Los *Suscriptores* son las personas jurídicas a quienes se expide este tipo de *Certificados* y que están legalmente obligados por un acuerdo que describe los términos de uso del *Certificado*.

1.3.4. Partes que confían

16. Terceras partes que confían en los *Certificados* emitidos bajo esta *Política de Certificación*: son las personas que voluntariamente confían en dichos *Certificados* en virtud de la confianza depositada en la FNMT – RCM, como Prestador de Servicios de Confianza.
17. Adicionalmente, para el caso particular de los *Certificado de autenticación de sitio web*, las partes que confían son aquellos usuarios de Internet que establecen conexiones a sitios web mediante el uso de protocolos TLS/SSL que incorporan este tipo de *Certificados* y deciden confiar en ellos.



1.3.5. Otros participantes

18. No estipulado.

1.4. USO DE LOS CERTIFICADOS

1.4.1. Usos permitidos de los certificados

19. Los *Certificados de autenticación de sitios web* expedidos bajo esta *Política de Certificación* se consideran válidos como medio por el que puede garantizarse a la persona que visita un sitio web que existe una entidad, la FNMT-RCM, auténtica y legítima, que respalda la existencia de dicho sitio web.
20. El *Certificado cualificado de autenticación de sitio web* estándar con políticas de Organization Validation (OV) expedidos bajo la presente *Política de Certificación* son *Certificados Cualificados* conforme al 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 (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” y ETSI EN 319 412-4 “Certificate profile for web site certificates”.
21. El *Certificado de componente de sello de entidad* y el *Certificado de componente como Unidad de Sellado de Tiempo del Servicio cualificado de Sellado de Tiempo* de la FNMT – RCM, son *Certificados cualificados* 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.

1.4.2. Restricciones en el uso de los certificados

22. 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*.
23. La FNMT-RCM prohíbe el uso de los *Certificados* emitidos bajo la presente *DPPP* para la interceptación ilegal o descifrado de comunicaciones cifradas (MITM), inspección profunda de paquetes (DPI), etc.
24. No se podrá emplear este tipo de *Certificados* para:
- Firmar otro *Certificado*, salvo supuestos expresamente autorizados previamente.
 - Firmar software o componentes – a excepción de los *Certificados de componente de firma de código*.



- Generar *Sellos de Tiempo* para procedimientos de *Sellado de Tiempo* –a excepción de los *Certificados* expedidos por la FNMT-RCM para *Unidades de Sellado de Tiempo*.
- Prestar servicios a título gratuito u oneroso, salvo supuestos expresamente autorizados previamente, como serían a título enunciativo y no limitativo:
 - Prestar servicios de *OCSP*.
 - Prestar servicios de facturación electrónica.
 - Generar *Listas de Revocación*.
 - Prestar servicios de notificación

1.5. ADMINISTRACIÓN DE POLÍTICAS

1.5.1. Entidad responsable

25. 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 Prácticas y Políticas de Certificación*, y responsable de su mantenimiento.

1.5.2. Datos de contacto

26. 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
28071 – MADRID
E-mail: ceres@fnmt.es
Teléfono: 902 181 696

27. 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

28. 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

29. La FNMT-RCM gestiona sus servicios de certificación y emite certificados de conformidad con la última versión de los "Requisitos base para la emisión y gestión de certificados de confianza", requisitos establecidos por la entidad CA/Browser forum y que pueden consultarse en la siguiente dirección <https://cabforum.org/baseline-requirements-documents/>
30. La FNMT-RCM revisará sus políticas y prácticas de certificación y actualizará anualmente la presente Declaración de la Política de Certificados para mantenerla acorde a la última versión de los referidos requisitos, incrementando el número de versión y agregando una entrada de registro de cambios con fecha, incluso si no se realizaron otros cambios en el documento.
31. Las actualizaciones tanto para las Prácticas de Certificación Particulares, como para la Política de Certificación se ponen a disposición de las partes, publicando nuevas versiones en [https:// https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion](https://https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion)

1.6. DEFINICIONES Y ACRÓNIMOS

1.6.1. Definiciones

32. A las definiciones dispuestas en la *DGPC*, para la interpretación del presente documento se añaden las siguientes:
 - *Certificado de autenticación de sitio web*: Es un *Certificado de Componente* que permite autenticar un sitio web, establecer comunicaciones seguras utilizando el protocolo SSL/TSL y vincular el sitio web con la persona física o jurídica a quien se ha expedido el *Certificado*. Son *Certificados de autenticación de sitios web*:
 - *Certificado de autenticación de sitio web* estándar
 - *Certificado de autenticación de sitio web* multidominio
 - *Certificado de autenticación de sitio web* wildcard
 - *Certificado cualificado de autenticación de sitio web* estándar
 - *Certificado de autenticación de sitio web* multidominio (SAN/UCC): Es el *Certificado de autenticación de sitio web* que garantiza la seguridad de un conjunto de dominios independientes entre sí.
 - *Certificado de autenticación de sitio web* wildcard Es el *Certificado de autenticación de sitio web* que garantiza la seguridad de un conjunto de subdominios ilimitado, a partir del tercer nivel, con un único *Certificado de autenticación de sitio web*.
 - *Certificado de Componente*: *Certificado* empleado por un *Componente* informático en una infraestructura de clave pública.
 - *Certificado de componente* de firma de código: Permite firmar software y garantizar la identidad del propietario y la integridad del código.

- *Certificado de componente* de sello de entidad: Se utiliza para la automatización de procesos de firma y autenticación entre componentes informáticos. Además, se permite al usuario elegir el uso extendido de claves del *Certificado* (autenticación de cliente, protección de correo electrónico).
- *Certificado de componente* para su uso en las *Unidades de Sellado de Tiempo*: Es utilizado por *Autoridades de Sellado de Tiempo* de terceros.
- *Certificado de componente* para su uso en la *Unidad de Sellado de Tiempo* de la FNMT-RCM: Es utilizado por *Autoridades de Sellado de Tiempo* de la FNMT-RCM para prestar el Servicio cualificado de Sellado de Tiempo de dicha Entidad, como Prestador cualificado de Servicios de Confianza. En todo lo relativo a dicho servicio, puede consultarse la Política y Declaración de Prácticas del Servicio de Sellado de Tiempo en la siguiente dirección: <http://www.cert.fnmt.es/dpcs/>
- *Certificate Transparency (CT)*: es un marco abierto para la supervisión de *Certificados de autenticación de sitio web*, de forma que cuando se expide uno de estos *Certificados*, se publica en registros CT, posibilitando así que los propietarios de dominios puedan supervisar la emisión de los mismos para sus dominios y detectar *Certificados* emitidos erróneamente.
- *Componente*: Conjunto de elementos informáticos interrelacionados entre sí para transmitir o tratar información y con capacidad de firmarla o cifrarla de manera autónoma.
- *Informe de incidencia con un certificado*: queja de sospecha de compromiso clave, mal uso del certificado u otros tipos de fraude, compromiso, mal uso o conducta inapropiada relacionada con los certificados.
- *Non-Reserved LDH Label*: De RFC 5890: “Conjunto de etiquetas LDH válidas que no tienen “-” en la tercera y cuarta posición.”
- *P-Label*: Etiqueta “XN” que contiene una salida válida del algoritmo Punycode (como se define en RFC 3492, Sección 6.3) a partir de la quinta posición y siguientes.
- *Registro AAC (CAA records)*: Registro de recursos DNS (Sistema de Nombres de Dominio) de Autorización de Autoridad de Certificación (AAC). Permite a un titular de nombre de dominio DNS especificar las Autoridades de Certificación (AC) autorizadas para emitir certificados para ese dominio. La publicación de los registros de recursos de AAC permite a un titular de nombres de dominio implementar controles adicionales para reducir el riesgo de que se produzca una emisión no autorizada de un *Certificado de autenticación de sitio web* para su nombre de dominio.
- *Representante*: Administrador, cargo público o apoderado general del *Suscriptor* cuando este es una persona jurídica, órgano u organismo público y que actúa en nombre del *Suscriptor*. Es también la persona física a la que se reconoce la capacidad de autorizar al *Solicitante*.
- *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 y se referencia en el Sujeto en el Certificado. Es el titular y responsable del uso del Certificado que posee el control exclusivo y la capacidad de decisión sobre el *Componente*.



(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

33. 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 por el que se deroga la Directiva 1999/93/CE.

EV: Validación extendida (Extended Validation).

ETSI: European Telecommunications Standards Institute

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)

OV: Validación de Organización (Organizational Validation).

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

PIN: Número de identificación personal (Personal Identification Number).

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

TLS/SSL: Protocolos que proporcionan cifrado de datos y autenticación entre aplicaciones y servidores (Transport Layer Security/Secure Socket Layer protocol).

UTC: Tiempo coordinado universal (Coordinated Universal Time).

2. PUBLICACIÓN Y REPOSITORIOS

2.1. REPOSITORIO

34. La FNMT-RCM, 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

35. La información relativa a la expedición de *Certificados* electrónicos objeto de la presente *DPPP*, accesible a través de la sede electrónica de la FNMT-RCM (<https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion>), incluye las siguientes informaciones:

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

36. 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

37. 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*.

38. 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.

39. 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

40. 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

41. 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

42. 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). La FNMT-RCM cumple con los requisitos X.500, RFC 5280 y CA/Browser Forum a este respecto.
43. El campo Common Name define al titular de Certificado.

3.1.2. Significado de los nombres

44. 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

45. 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

46. 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

47. 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

48. Los suscriptores no podrán solicitar *Certificados* con ningún contenido que infrinja los derechos de propiedad intelectual de un tercero. Véase el apartado correspondiente en la *DGPC*.

3.2. VALIDACIÓN INICIAL DE LA IDENTIDAD

49. La FNMT-RCM realiza el proceso de validación de la información incluida en el *Certificado* de conformidad con los "Requisitos base para la emisión y gestión de certificados de confianza", requisitos establecidos por la entidad CA/Browser forum y que pueden consultarse en la dirección <https://cabforum.org/baseline-requirements-documents/>.
50. La FNMT-RCM registra todas las confirmaciones realizadas en esta sección para los procesos periódicos de auditoría tanto interna como independiente.

3.2.1. Métodos para probar la posesión de la clave privada

51. La FNMT-RCM recibe una solicitud de *Certificado*, en formato PKCS#10, firmada digitalmente por la *Clave privada* generada por el *Representante del Suscriptor* en su entorno. Antes de proceder a la expedición del *Certificado*, la FNMT-RCM verifica dicha firma, garantizando que la *Clave pública* incluida en la solicitud se corresponde con la *Clave privada* generada por el *Responsable del Certificado*.

3.2.2. Autenticación de la identidad de la Organización

3.2.2.1 Identidad

52. La FNMT-RCM verifica la existencia legal, la dirección y la identidad de la organización suscriptora del *Certificado* mediante diferentes métodos, en función del tipo de organización (privada, pública o de negocio).
53. Cuando el *Suscriptor* es una entidad privada, se verificará su existencia, dirección e identidad, 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.
54. 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.
55. Si la naturaleza del *Suscriptor* fuera distinta de los dos casos anteriores, las verificaciones relativas a la existencia legal, dirección y la identidad se realizará mediante consulta directa al registro oficial correspondiente.
56. La lista de las fuentes de consulta de Agencias de Registro es publicada en la web de la FNMT-RCM (<https://www.cert.fnmt.es/registro/utilidades>).
57. La FNMT-RCM no expide *Certificados* bajo la presente *DPPP* cuyo *Suscriptor* sea una persona física.
58. La FNMT-RCM verifica que el nombre, dirección y número de identificación fiscal de la organización suscriptora del *Certificado* incorporados a la solicitud del mismo coinciden con el nombre, dirección y número de identificación fiscal inscritos formalmente en los registros consultados según se describe en los apartados anteriores.

3.2.2.2 Nombre comercial o marca registrada

59. La FNMT – RCM no asume compromiso alguno sobre el uso de marcas comerciales en la emisión de los *Certificados* expedidos bajo la presente *Política de Certificación*. No se permite el uso de signos distintivos cuyo derecho de uso no sea propiedad del *Titular* o esté debidamente autorizado, por lo que la FNMT–RCM no está obligada a verificar previamente la titularidad o registro de marcas registradas y demás signos distintivos antes de la emisión de los *Certificados*, aunque figuren en registros públicos.

3.2.2.3 Verificación del país

60. El país se verificará utilizando cualquiera de los métodos indicados en la Sección 3.2.2.1

3.2.2.4 Validación de la autorización y control sobre el dominio

61. Para validar el dominio de los *Certificados de autenticación de sitios web*, la FNMT-RCM utiliza alguno de los siguientes métodos descritos en el documento CA/Browser Forum's Baseline Requirements: “3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact”, “3.2.2.4.4 Constructed Email to Domain Contact” o “3.2.2.4.7 DNS Change “. Para cada uno de los métodos empleado, la FNMT-RCM; seguirá un proceso documentado y mantendrá registros que indiquen los métodos utilizados para cada emisión. El resto de los métodos descritos en CA/Browser Forum's Baseline Requirements no se emplea para la validación de dominios.

- 3.2.2.4.2 Email, Fax, SMS, o correo postal al Contacto de Dominio:

Confirmar el control del solicitante sobre el FQDN enviando un código aleatorio por correo electrónico y recibiendo una respuesta de confirmación utilizando dicho código aleatorio. El código aleatorio se enviará a una dirección de correo electrónico identificada como contacto de dominio.

Cada correo electrónico puede confirmar el control de varios nombres de dominio.

FNMT-RCM podrá enviar el correo electrónico identificado en esta sección a más de un destinatario siempre que el Registrador de nombres de dominio identifique a cada destinatario como representante del Registrante de nombres de dominio para cada FQDN que se verifica mediante el correo electrónico.

El código aleatorio será único en cada correo electrónico.

FNMT-RCM puede reenviar el correo electrónico en su totalidad, incluida la reutilización del código aleatorio, siempre que el contenido completo de la comunicación y los destinatarios permanezcan sin cambios.

El valor aleatorio seguirá siendo válido para su uso en una respuesta de confirmación durante no más de 30 días desde su creación.

- 3.2.2.4.4 Correo electrónico al contacto del Dominio:

Confirmar el control del Solicitante sobre el FQDN solicitado (i) enviando un correo electrónico a una o más direcciones creadas usando 'admin', 'administrador', 'webmaster', 'hostmaster' o 'postmaster' como parte local, seguido del signo de arroba ("@"), seguido

de un Nombre de dominio, (ii) que incluye un código aleatorio en el correo electrónico y (iii) recibe una respuesta de confirmación utilizando dicho código aleatorio.

Cada correo electrónico puede confirmar el control de varios FQDN, siempre que el nombre de dominio utilizado en el correo electrónico sea un nombre de dominio para cada FQDN que se confirma.

El código aleatorio será único en cada correo electrónico.

FNMT-RCM puede reenviar el correo electrónico en su totalidad, incluida la reutilización del código aleatorio, siempre que el contenido completo de la comunicación y los destinatarios permanezcan sin cambios.

El valor aleatorio seguirá siendo válido para su uso en una respuesta de confirmación durante no más de 30 días desde su creación.

- 3.2.2.4.7 Cambio en DNS:

Confirmar el control del Solicitante sobre el FQDN solicitado al confirmar la presencia de un código aleatorio en un registro TXT o CAA de DNS para 1) un Nombre de dominio; o 2) un nombre de dominio que tiene como prefijo una etiqueta que comienza con un carácter de subrayado.

FNMT-RCM proporcionará un código aleatorio exclusivo para la solicitud del certificado y no utilizará el código aleatorio después de 30 días.

62. La FNMT-RCM confirma que el Representante del Suscriptor posee el control sobre los nombres completos de los dominios o FQDN (siglas en inglés de Fully Qualified Domain Name) que son incorporados a los *Certificados de autenticación de sitio web* que expide. Para ello, la FNMT-RCM consulta, a través de la aplicación que registra las solicitudes de estos Certificados, la identidad del Representante del Suscriptor y el nombre del citado FQDN. A continuación, verifica que la solicitud proviene del contacto que tiene el control sobre dicho dominio (según los métodos definidos en el apartado anterior) o tiene autorización por parte de este. Adicionalmente se comprueba que la solicitud del Certificado ha sido realizada con posterioridad al alta en dichos registros.
63. Antes de la emisión de un *Certificado de autenticación de sitios web*, se verifica que el dominio a incluir en el Certificado es público (no es un dominio interno) y se consulta a registros públicos para verificar que no es un dominio de alto riesgo (por ejemplo, el registro de Google creado para este fin, como es Safe Browsing site status).
64. Para aquellos *Certificados* que incorporen más de un nombre de dominio (*Certificados multidominio*), se realizarán las comprobaciones correspondientes para todos y cada uno de los nombres de dominio incorporados al *Certificado*. Si alguno de dichos nombres de dominio no cumpliera con los requisitos que se verifican con las comprobaciones realizadas, no se expedirá el *Certificado*.

3.2.2.5 Autenticación para una dirección IP

65. Bajo la presente *DPPP*, no se emiten certificados para identificar direcciones IP.

3.2.2.6 Validación de dominio wildcard

66. La RA, verificará que todo el espacio de nombres de dominio en los *Certificados Wildcard OV* es controlado legítimamente por el *Suscriptor*.
67. Si un wildcard cayera dentro de la etiqueta inmediatamente a la izquierda de un sufijo público o un registro controlado, la FNMT_RCM rechazará la emisión de dicho *Certificado* a menos que el *Solicitante* demuestre el control legítimo de todo el espacio de nombres de dominio (p. ej., no se emitirá “*.co.uk” o “*.local”, pero se puede emitir “*.example.com” a Example Co.). Para ello consultará la “Public Suffix List” disponible en <https://publicsuffix.org/> y que se descargará periódicamente.

3.2.2.7 Fiabilidad de las fuentes de datos

68. Antes de utilizar cualquier fuente de datos como fuente de datos confiable, la RA evaluará la fuente en cuanto a su confiabilidad, precisión y resistencia a la alteración o falsificación

3.2.2.8 Registro AAC

69. La FNMT-RCM comprueba si hay un Registro AAC para cada nombre de dominio que incluye en un *Certificado de autenticación de sitios web* emitido, de acuerdo con el procedimiento establecido en RFC 8659 y siguiendo las instrucciones de procesamiento establecidas en RFC 8659 para cualquier registro encontrado. Si existe dicho Registro AAC, no emitirá dicho *Certificado* a menos que determine que la solicitud del *Certificado* es consistente con el conjunto de registro de recursos AAC aplicable. El identificador de dominio reconocido como propio asociado a la autoridad de certificación de la FNMT se ha establecido en “fnmt.es”.

3.2.3. Autenticación de la identidad de la persona física solicitante

70. La AR de la FNMT-RCM comprueba que el *Representante del Suscriptor* coincide con la persona física que solicita un *Certificado*, mediante la firma electrónica del formulario de solicitud utilizando un *Certificado* cualificado de firma electrónica, garantizando así la autenticidad de su identidad.

3.2.4. Información no verificada del Suscriptor

71. 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

72. 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.

73. Cuando el citado formulario se firma mediante un *Certificado* cualificado diferente de los mencionados en el párrafo 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

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

3.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE RENOVACIÓN DE CLAVES

3.3.1. Identificación y autenticación para renovación rutinaria de claves

75. Los *Suscriptores* de los *Certificados* deberían solicitar la renovación de los mismos antes de que expire su período de vigencia. Las condiciones de autenticación de una petición de renovación se desarrollan en el apartado de esta *DPPP* correspondiente al proceso de renovación de *Certificados* (véase apartado 4.6 del presente documento).

3.3.2. Identificación y autenticación para renovación de claves después de una revocación

76. La FNMT-RCM no renueva *Certificados* que han sido revocados. El proceso de renovación del *Certificado* tras la revocación del mismo será el mismo que el que se sigue en la emisión inicial de dicho *Certificado*.

3.4. IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE REVOCACIÓN

77. 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

4.1. SOLICITUD DE CERTIFICADOS

4.1.1. Quién puede solicitar un Certificado

78. Únicamente podrán solicitar *Certificados* los *Representantes del Suscriptor*, o personas debidamente autorizados a solicitar el *Certificado* en nombre del *Suscriptor*,
79. Para la solicitud de *Certificados de autenticación de sitio web*, además de lo estipulado en el párrafo anterior, tendrán que acreditar tener el control sobre el nombre del dominio a incluir en el *Certificado*. El citado control sobre el nombre del dominio será verificado por la FNMT-RCM según se describe en el apartado “3.2 Validación inicial de la identidad” de la presente *DPPP*.

4.1.2. Proceso de registro y responsabilidades

80. Cada *Solicitante* deberá presentar una solicitud de *Certificado* y la información requerida antes de emitir un *Certificado*. La FNMT-RCM autentica y protege todas las comunicaciones frente a modificaciones con el *Solicitante*.
81. El proceso de registro incluye las siguientes fases:
- Enviar una solicitud de *Certificado* completa y aceptar los términos y condiciones aplicables. Con esta aceptación, los *Suscriptores* garantizan que toda la información contenida en la solicitud de *Certificado* es correcta.
 - Generar un par de claves,
 - Entregar la clave pública del par de claves a la CA y
 - Pagar cuando proceda las tarifas aplicables.
82. La AR de la FNMT-RCM realiza la verificación de la identidad de la Organización suscriptora y del *Representante del Suscriptor*, y comprueba que la solicitud del *Certificado* es correcta completa y debidamente autorizada, de conformidad con los requisitos definidos en el apartado “3.2 Validación inicial de la identidad” del presente documento. FNMT-RCM podrá realizar comprobaciones adicionales a los procesos de validación descritos en el citado apartado.
83. FNMT-RCM recopilará las evidencias correspondientes a las comprobaciones realizadas y quedarán almacenadas en un repositorio.
84. El apartado 9.6 “Obligaciones y garantías” 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

85. El *Representante del Suscriptor* remite a la AR de la FNMT-RCM un formulario, firmado electrónicamente con un *Certificado* electrónico cualificado, que recoge toda la información a incorporar en el *Certificado*. A partir de dicha información, la AR de la FNMT-RCM lleva a cabo las comprobaciones descritas en el apartado “3.2 Validación inicial de la identidad” de la presente *DPPP*.
86. 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.
87. La firma electrónica generada para la suscripción del contrato será verificada por la FNMT-RCM.
88. El empleo de los datos o la documentación de validación previa, obtenidos de una fuente de las especificadas en la sección 3.2, no se puede utilizar más de 12 meses después de que se validasen dichos datos o documentación.

4.2.2. Aprobación o rechazo de la solicitud del certificado

89. La AR que actúa en el proceso de expedición de *Certificados* es siempre la propia FNMT-RCM y, por tanto, no delega la validación a ninguna otra AR.
90. La AR de la FNMT-RM realiza las comprobaciones relativas a la prueba de posesión de la *Clave privada* por parte del *Representante del Suscriptor*, la autenticación de la identidad de la Organización y de la persona que solicita el *Certificado*, así como la validación del dominio para *Certificados de autenticación de sitios web*, según se describe en el apartado “3.2 Validación inicial de la identidad” de la presente *DPPP*, que darán como resultado la aprobación o el rechazo de la solicitud del mismo.
91. La FNMT-RCM mantiene una base de datos interna de todos los *Certificados* revocados y de todas las solicitudes de *Certificados* rechazadas previamente debido a sospecha de phishing u otro uso fraudulento. Esta información es tomada en cuenta para identificar posteriores solicitudes de *Certificados* sospechosos antes de proceder a la aprobación de la expedición de los mismos.
92. Adicionalmente, FNMT-RCM desarrolla, mantiene e implementa procedimientos documentados que identifican y requieren actividad de verificación adicional para las solicitudes de *Certificados de autenticación de sitios web* de alto riesgo antes de la aprobación de la expedición del *Certificado*, según sea razonablemente necesario para garantizar que dichas solicitudes se verifican adecuadamente según estos requisitos.
93. Si alguna de estas validaciones no ha podido ser confirmada, la FNMT-RCM rechazará la solicitud del *Certificado de autenticación de sitios web*, reservándose el derecho de no revelar los motivos de dicha denegación. El *Representante del Suscriptor* cuya solicitud haya sido rechazada podrá volver a solicitarlo posteriormente.



94. Adicionalmente, la FNMT-RCM comprueba si hay un *Registro AAC* para cada nombre de dominio que incluye en un *Certificado de autenticación de sitios web* emitido, de acuerdo con el procedimiento establecido en RFC 8659 y siguiendo las instrucciones de procesamiento establecidas en RFC 8659 para cualquier registro encontrado. Si existe dicho *Registro AAC*, no emitirá dicho *Certificado* a menos que determine que la solicitud del *Certificado* es consistente con el conjunto de registro de recursos AAC aplicable. El identificador de dominio reconocido como propio asociado a la autoridad de certificación de la FNMT se ha establecido en “fnmt.es”.

4.2.3. Tiempo en procesar la solicitud

95. El plazo de tiempo en procesar la solicitud de un *Certificado* depende en gran medida de que el *Representante del Suscriptor* proporcione la información y la documentación necesarias de la forma prevista en los procedimientos aprobados por la FNMT-RCM para este fin. No obstante, la FNMT-RCM hará el esfuerzo necesario para que el proceso de validación que dará como resultado la aceptación o el rechazo de la solicitud no exceda de dos (2) días hábiles, tras la recepción de toda la información necesaria.
96. Este periodo de tiempo podrá, ocasionalmente, ser superado por motivos fuera del control de la FNMT-RCM. En estos casos, hará lo posible por mantener informado al *Representante del Suscriptor* que realizó la solicitud de las causas de tales retrasos.

4.3. EMISIÓN DEL CERTIFICADO

4.3.1. Acciones de la AC durante la emisión

97. Una vez aprobada la solicitud del *Certificado* por parte de la AR de la FNMT-RCM, el sistema de generación de certificados cuenta con una serie de controles previos a la emisión del certificado que verifican el cumplimiento de requisitos de la RFC 5280 y CA/Browser Forum (BRs y, si aplica, EVGs). Tras esta verificación se procede a expedir el *Certificado* conforme al perfil aprobado para cada tipo de *Certificado*.
98. Así mismo, la FNMT-RCM monitoriza periódicamente posibles desviaciones en los certificados emitidos.
99. Los procesos relativos a la emisión de *Certificados* garantizan que todas las cuentas que intervienen en los mismos tienen autenticación multi-factor.

4.3.2. Notificación de emisión de certificado

100. Una vez emitido el *Certificado*, FNMT-RCM envía una comunicación a la dirección de correo electrónico consignada en el formulario de solicitud firmado por el *Representante del Suscriptor*, informando que está disponible dicho *Certificado* para su descarga.



4.4. ACEPTACIÓN DEL CERTIFICADO

4.4.1. Proceso de aceptación

101. En el proceso de solicitud del *Certificado*, el *Representante del 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

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

4.4.3. Notificación de la emisión a otras entidades

103. Antes de la expedición de *Certificados de autenticación de sitio web* se envía un pre-certificado a los registros del servicio *Certificate Transparency* de aquellos proveedores con los que la FNMT-RCM mantiene un acuerdo para tal fin.
104. Para el resto de *Certificados* emitidos bajo la presente *DPPP*, la FNMT-RCM no realiza ninguna notificación sobre la emisión de *Certificados* a otras entidades.

4.5. PAR DE CLAVES Y USO DEL CERTIFICADO

4.5.1. Clave privada del suscriptor y uso del certificado

105. La FNMT-RCM no genera ni almacena las *Claves Privadas* asociadas a los *Certificados* expedidos bajo la presente *Política de Certificación*. Corresponde la condición de custodio y el control de las claves del *Certificado* a los *Representantes del Suscriptor*. Por tanto, la *Clave Privada* asociada a la *Clave Pública* estará bajo la responsabilidad de dicho custodio y actuará como representante de la Entidad que tiene la titularidad, gestión y administración de la dirección electrónica correspondiente.

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

106. Los terceros que confían en los *Certificados* se atenderán a las obligaciones y responsabilidades definidas en la presente *DPPP*.
107. Las entidades usuarias y terceros que confían utilizarán software que sea compatible con los estándares aplicables al uso de *Certificados* electrónicos (X.509, IETF, RFCs...). Si la conexión al sitio web requiriese de adicionales medidas de aseguramiento, dichas medidas han de ser obtenidas por las entidades usuarias.
108. Los terceros que confían en el establecimiento de una conexión segura garantizada por un *Certificado de autenticación de sitios web* deben cerciorarse de que dicha conexión fue creada durante el periodo de validez del *Certificado*, que dicho *Certificado* está siendo usado con el propósito para el que se expidió de acuerdo con la presente *DPPP*, así como verificar que en ese momento el *Certificado* está activo, mediante la comprobación de su estado de revocación



en la forma y condiciones que se expresan en el apartado “4.10 Servicios de información del estado de los certificados” del presente documento.

4.6. RENOVACIÓN DEL CERTIFICADO

109. La renovación de un *Certificado* consiste en la emisión de un nuevo *Certificado* sin cambiar ninguna información del *Firmante*, *Clave pública* o cualquier otra información que aparezca en el mismo.

110. Bajo las presentes *Políticas de Certificación*, la FNMT-RCM no renueva *Certificados* manteniendo la *Clave pública* del mismo, sino que, en todo caso, la renovación de *Certificados* se realiza renovando las *Claves criptográficas*, según se define en el apartado “4.7 Renovación con regeneración de las claves del certificado” del presente documento.

4.6.1. Circunstancias para la renovación del certificado

111. Bajo las presentes Políticas de Certificación, la FNMT-RCM no renueva *Certificados* manteniendo la *Clave pública* del mismo.

4.6.2. Quién puede solicitar la renovación del certificado

112. Bajo las presentes Políticas de Certificación, la FNMT-RCM no renueva *Certificados* manteniendo la *Clave pública* del mismo.

4.6.3. Procesamiento de solicitudes de renovación del certificado

113. Bajo las presentes Políticas de Certificación, la FNMT-RCM no renueva *Certificados* manteniendo la *Clave pública* del mismo.

4.6.4. Notificación de la renovación del certificado

114. Bajo las presentes Políticas de Certificación, la FNMT-RCM no renueva *Certificados* manteniendo la *Clave pública* del mismo.

4.6.5. Conducta que constituye la aceptación de la renovación del certificado

115. Bajo las presentes Políticas de Certificación, la FNMT-RCM no renueva *Certificados* manteniendo la *Clave pública* del mismo.

4.6.6. Publicación del certificado renovado

116. Bajo las presentes Políticas de Certificación, la FNMT-RCM no renueva *Certificados* manteniendo la *Clave pública* del mismo.



4.6.7. Notificación de la renovación del certificado a otras entidades

117. Bajo las presentes Políticas de Certificación, la FNMT-RCM no renueva *Certificados* manteniendo la *Clave pública* del mismo.

4.7. RENOVACIÓN CON REGENERACIÓN DE LAS CLAVES DEL CERTIFICADO

118. La renovación con regeneración de claves de los *Certificados* emitidos bajo la presente *DPPP* se realiza siempre emitiendo nuevas claves públicas y privadas, 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

119. Las claves de los *Certificados* se renovarán bajo los siguientes supuestos:
- Por caducidad próxima de las actuales claves a petición del solicitante de la renovación.
 - Por compromiso de las claves u otra circunstancia de las recogidas en el apartado “4.9 *Revocación y suspensión del certificado*” de la presente *DPPP*.

4.7.2. Quién puede solicitar la renovación con regeneración de claves

120. 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

121. 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

122. 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

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

4.7.6. Publicación del certificado renovado

124. 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

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



4.8. MODIFICACIÓN DEL CERTIFICADO

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

4.8.1. Circunstancias para la modificación del certificado

127. No se estipula la modificación.

4.8.2. Quién puede solicitar la modificación del certificado

128. No se estipula la modificación.

4.8.3. Procesamiento de solicitudes de modificación del certificado

129. No se estipula la modificación.

4.8.4. Notificación de la modificación del certificado

130. No se estipula la modificación.

4.8.5. Conducta que constituye la aceptación de la modificación del certificado

131. No se estipula la modificación.

4.8.6. Publicación del certificado modificado

132. No se estipula la modificación.

4.8.7. Notificación de la modificación del certificado a otras entidades

133. No se estipula la modificación.

4.9. REVOCACIÓN Y SUSPENSIÓN DEL CERTIFICADO

134. Los *Certificados* emitidos bajo la presente *DPPP* 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.
135. 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*.
136. 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.
137. La FNMT-RCM, como *Prestador de Servicios de Confianza*, se reserva el derecho de no expedir o revocar este tipo de *Certificados* si el *Suscriptor* que tiene el control de los datos de Datos de Creación de Firma o del nombre de dominio del sitio web incluido en el *Certificado* no hace un uso adecuado del mismo, conculcando derechos de propiedad industrial o intelectual de terceros sobre las aplicaciones o sitios web que se desean proteger con tales *Certificados*, o su uso se presta a engaño o confusión sobre la titularidad de tales aplicaciones o sitios web y, por tanto, de sus contenidos. En especial, tal reserva de derechos se podrá ejecutar por la FNMT-RCM cuando en la utilización de tales *Certificados* se atente contra los siguientes principios:
- a) La salvaguarda del orden público, la investigación penal, la seguridad pública y la defensa nacional.
 - b) La protección de la salud pública o de las personas físicas que tengan la condición de consumidores o usuarios, incluso cuando actúen como inversores.
 - c) El respeto a la dignidad de la persona y al principio de no discriminación por motivos de raza, sexo, religión, opinión, nacionalidad, discapacidad o cualquier otra circunstancia personal o social, y
 - d) La protección de la juventud y de la infancia.
138. La FNMT-RCM, se mantendrá indemne por parte de los titulares o responsables de los equipos, aplicaciones o sitios web que incumplan lo previsto en este apartado y que tengan relación con el *Certificado*, quedando exonerada de cualquier reclamación o reivindicación por el uso inadecuado de tales *Certificados*.

4.9.1. Circunstancias para la revocación

4.9.1.1 Causas de revocación de un Certificado de entidad final

139. Adicionalmente a lo previsto en el apartado anterior, serán causas de revocación de un *Certificado* de los emitidos bajo las presentes *DPPP*:
- 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*.
 - La no aceptación de las nuevas condiciones que puedan suponer la emisión de nuevas *Declaraciones de Prácticas de Certificación*, durante el periodo de un mes tras su publicación.
- b) Resolución judicial o administrativa que así lo ordene.
- c) Extinción, disolución o cierre del sitio web identificado por el *Certificado*.
- d) Extinción o disolución de la personalidad jurídica del *Suscriptor*.
- e) Terminación de la forma de representación del representante del *Suscriptor* del *Certificado*.
- f) Incapacidad sobrevenida, total o parcial, del representante del *Suscriptor*.
- g) Inexactitudes en los datos aportados por el *Representante del 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.
- h) Contravención de una obligación sustancial de esta *Declaración de Prácticas de Certificación* por parte del *Suscriptor*, del *Representante del Suscriptor* o de una *Oficina de Registro* si, en este último caso, hubiese podido afectar al procedimiento de emisión del *Certificado*.
- i) Utilizar el *Certificado* con el propósito de generar dudas a los usuarios sobre la procedencia de los productos o servicios ofertados, haciendo ver que su origen es distinto del realmente ofertado. Para ello, se seguirán los criterios sobre actividad infractora de las normas sobre consumidores y usuarios, comercio, competencia y publicidad.
- j) Solicitar para el Sujeto del certificado signos distintivos, denominaciones o derechos de propiedad industrial o intelectual de las que el *Suscriptor* no sea titular, licenciatario o usuario autorizado
- k) Resolución del contrato suscrito entre el *Suscriptor* o su *Representante*, y la FNMT-RCM, o el impago de los servicios prestados.
- l) 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.
- m) 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*.
140. En ningún caso se debe entender que la FNMT-RCM asume obligación alguna de comprobar los extremos mencionados en las letras c) a j) del presente apartado.



141. 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 *Representante del Suscriptor* siguiendo el procedimiento establecido para este tipo de *Certificados*.
 - Que la revocación se debiera haber efectuado por haberse extinguido el contrato suscrito con el *Suscriptor*.
 - Que la solicitud de revocación o la causa que la motiva, le haya sido notificada mediante resolución judicial o administrativa.
 - Que en las causas c) a g) del presente apartado le sean acreditados dichos extremos fehacientemente, previa identificación del *Solicitante* de la revocación.
142. 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.
143. Todas las solicitudes de revocación de certificados de entidad final, son procesadas en el plazo máximo de 24 horas desde la recepción de la misma.

4.9.1.1 Causas de revocación de un Certificado de CA subordinada

144. La CA emisora revocará el certificado de la CA subordinada en el plazo de 7 días si en cualquiera de las siguientes situaciones:
- a) La CA subordinada solicita la revocación por escrito;
 - b) La CA subordinada notifica a la CA emisora que la solicitud de certificado original no fue autorizada y no otorga autorización retroactivamente;
 - c) La CA emisora obtiene evidencia de que la *Clave privada* de la CA subordinada correspondiente a la *Clave pública* en el *Certificado* sufrió un compromiso de clave o ya no cumple con los requisitos de las secciones 6.1.5 y 6.1.6,
 - d) La CA emisora obtiene evidencia de que el *Certificado* fue mal utilizado;
 - e) La CA emisora es consciente de que el *Certificado de autenticación de sitios web* no se emitió de acuerdo, o que la CA subordinada no ha cumplido con los requisitos establecidos por la entidad CA/Browser fórum para este tipo de *Certificados*, o esta *DPPP*;
 - f) La CA emisora determina que cualquiera de la información que aparece en el Certificado es inexacta o engañosa;
 - g) La CA emisora o CA subordinada cesa sus operaciones por cualquier motivo y no ha hecho arreglos para que otra CA brinde apoyo de revocación para el Certificado;
 - h) El derecho de la CA emisora o de la CA subordinada a emitir Certificados según los requisitos establecidos por la entidad CA/Browser fórum vence o se revoca o finaliza, a menos que la CA emisora haya hecho arreglos para continuar manteniendo el repositorio de CRL / OCSP; o

- i) La *DPPP* de la CA emisora requiere la revocación.

4.9.2. Quién puede solicitar la revocación

145. La CA, la RA y los *Suscriptor* puede iniciar la revocación de un certificado
146. La revocación de un *Certificado* de los emitidos bajo las presentes *DPPP* solamente podrá ser solicitada por la persona con facultades de representación del *Suscriptor* al que se ha expedido el *Certificado*.
147. Adicionalmente, estarán legitimados para solicitar la revocación de dicho *Certificado*:
- El órgano directivo, organismo o entidad pública *Suscriptora* del *Certificado* o persona en quien delegue.
 - La *Oficina de Registro*, —a través de su responsable— que esté designada a tal efecto, por la Administración, organismo o entidad de derecho público, *Suscriptora* del *Certificado* a revocar, cuando detecte que alguno de los datos consignados en el *Certificado*
 - es incorrecto, inexacto o haya variado respecto a lo consignado en el *Certificado*, o
 - la persona física, custodio del *Certificado*, no se corresponda con el responsable máximo o designado para la gestión y administración de la dirección electrónica consignada en el *Certificado* objeto de la revocaciónsiempre en el marco de los términos y condiciones aplicables a la revocación de este tipo de *Certificados*.
148. Adicionalmente, los suscriptores, las partes confiables, los proveedores de software de aplicaciones y otros terceros pueden informar a la CA emisora de una causa razonable para revocar el certificado, enviando un *Informe de incidencia con un certificado*.
149. No obstante, la FNMT-RCM podrá revocar de oficio los *Certificados* emitidos bajo las presentes *DPPP* en los supuestos recogidos en la presente *Declaración de Prácticas y Políticas de Certificación*.

4.9.3. Procedimiento de solicitud de la revocación

150. Existe un servicio de atención telefónica, en horario 24 x 7, en el teléfono 902 200 616, al que se pueden dirigir las solicitudes de revocación de *Certificados*. La comunicación quedará grabada y registrada, sirviendo de soporte y garantía de la aceptación de la solicitud de revocación solicitada.
151. Para solicitar una revocación telefónica de un *Certificado*, el *Solicitante* de la misma debe ser el *Suscriptor* o su representante en el caso de personas jurídicas u organismos públicos, y debe aparecer como tal en el certificado a revocar. En el caso del representante, este debe ser la misma persona que actuó como tal en la solicitud de expedición del certificado objeto de la revocación.
152. Adicionalmente, es posible dirigir la solicitud de revocación al Área de Registro de la FNMT-RCM, siguiendo el siguiente procedimiento:

1. Solicitud del *Suscriptor*

El *Representante del Suscriptor* enviará a la FNMT-RCM el formulario de solicitud de revocación, cumplimentado y firmado electrónicamente con alguno de los *Certificados* admitidos para la solicitud y por los canales electrónicos habilitados por esta Entidad.

2. Tramitación de la solicitud por la FNMT-RCM

El registrador de la FNMT-RCM recibirá el contrato de revocación y realizará las mismas comprobaciones relativas a la identidad y capacidad del Representante del Suscriptor que para el caso de la solicitud de expedición y, si procediera, tramitará la revocación del Certificado.

153. 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 la causa de revocación. El *Representante del Suscriptor* recibirá, a través de la dirección de correo electrónico consignada en la solicitud, la notificación del cambio de estado de vigencia del *Certificado*.

154. La FNMT – RCM, aunque no haya recibido la solicitud de revocación por parte del *Suscriptor*, procederá a revocar aquellos *Certificados* de los que obtenga evidencias de estar incluidos en alguna de las causas de revocación previstas en la presente *Declaración de Políticas y Prácticas de Certificación Particulares*.

4.9.4. Periodo de gracia de la solicitud de revocación

155. 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

156. En las 24 horas posteriores a la recepción de un *CPR*, la FNMT-RCM investigará los hechos y circunstancias relacionados y proporcionará un informe preliminar tanto al *Suscriptor* como a la entidad que lo presentó.

157. Después de revisar los hechos y circunstancias, la CA trabajará con el *Suscriptor* y cualquier entidad que genere un *CPR* u otro aviso relacionado con la revocación, para establecer si el *Certificado* será revocado o no y, de ser así, la fecha en la que la CA lo revocará. El período desde la recepción del *CPR* o el aviso relacionado con la revocación hasta la revocación publicada no excederá el plazo establecido en la sección 4.9.1.1.

158. La fecha seleccionada por la CA considerará los siguientes criterios:

1. La naturaleza del presunto problema (alcance, contexto, gravedad, magnitud, riesgo de daño);
2. Las consecuencias de la revocación (impactos directos y colaterales a los Suscriptores y Partes que Confían);
3. El número de CPR recibidos sobre un Certificado o Suscriptor en particular;
4. La entidad que presenta la queja ; y

5. Legislación relevante.

159. La FNMT – RCM procede a la revocación inmediata del *Certificado de autenticación de sitios web* 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

160. Las terceras partes que confían y aceptan el uso de los *Certificados* emitidos por la FNMT – RCM están obligadas a verificar:
- la *Firma Electrónica Avanzada* o 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

161. 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

162. 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

163. 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

164. La comprobación en línea del estado de revocación de los *Certificados* emitidos bajo la presente *DPPP* 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

165. No definidas.

4.9.12. Requisitos especiales de revocación de claves comprometidas

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

4.9.13. Circunstancias para la suspensión

167. No se contempla la suspensión de certificados.

4.9.14. Quién puede solicitar la suspensión

168. No se contempla la suspensión de certificados.

4.9.15. Procedimiento para la petición de la suspensión

169. No se contempla la suspensión de certificados.

4.9.16. Límites sobre el periodo de suspensión

170. No se contempla la suspensión de certificados.

4.10. SERVICIOS DE INFORMACIÓN DEL ESTADO DE LOS CERTIFICADOS

171. 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.
172. Será responsabilidad de la Entidad usuaria contar con un *Cliente OCSP* para operar con el servidor OCSP puesto a disposición por la FNMT-RCM.
173. 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

174. 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

175. 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.
176. 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

177. No estipuladas.

4.11. FINALIZACIÓN DE LA SUSCRIPCIÓN

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

4.12. CUSTODIA Y RECUPERACIÓN DE CLAVES

4.12.1. Prácticas y políticas de custodia y recuperación de claves

179. La FNMT-RCM no genera las *Claves privadas* de los *Certificados* emitidos bajo la presente *DPPP* y, por tanto, no las custodia ni puede recuperarlas.

4.12.2. Prácticas y políticas de protección y recuperación de la clave de sesión

180. No estipulado.

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

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

5.1. CONTROLES DE SEGURIDAD FÍSICA

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



5.1.1. Ubicación de las instalaciones

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

5.1.2. Acceso Físico

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

5.1.3. Electricidad y Aire Acondicionado

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

5.1.4. Exposición al agua

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

5.1.5. Prevención y Protección contra incendios

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

5.1.6. Almacenamiento de Soportes

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

5.1.7. Eliminación de Residuos

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

5.1.8. Copias de Seguridad fuera de las instalaciones

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

5.2. CONTROLES DE PROCEDIMIENTO

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

5.2.1. Roles de Confianza

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

5.2.2. Número de personas por tarea

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



5.2.3. Identificación y autenticación para cada rol

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

5.2.4. Roles que requieren segregación de funciones

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

5.3. CONTROLES DE PERSONAL

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

5.3.1. Conocimientos, cualificación, experiencia y requerimientos acreditativos

197. Véase el apartado correspondiente en la *DGPC*

5.3.2. Procedimientos de verificación de antecedentes

198. Véase el apartado correspondiente en la *DGPC*

5.3.3. Requisitos de formación

199. Véase el apartado correspondiente en la *DGPC*

5.3.4. Requisitos y frecuencia de actuación formativa

200. Véase el apartado correspondiente en la *DGPC*

5.3.5. Secuencia y frecuencia de rotación laboral

201. Véase el apartado correspondiente en la *DGPC*

5.3.6. Sanciones por acciones no autorizadas

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

5.3.7. Requisitos de contratación de personal

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

5.3.8. Suministro de documentación al personal

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



5.4. PROCEDIMIENTOS DE AUDITORÍA

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

5.4.1. Tipos de eventos registrados

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

5.4.2. Frecuencia de procesamiento de registros

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

5.4.3. Periodo de conservación de los registros

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

5.4.4. Protección de los registros

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

5.4.5. Procedimientos de copias de seguridad de los registros auditados

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

5.4.6. Sistemas de recolección de registros

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

5.4.7. Notificación al sujeto causante de los eventos

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

5.4.8. Análisis de vulnerabilidades

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

5.5. ARCHIVADO DE REGISTROS

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

5.5.1. Tipos de registros archivados

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



5.5.2. Periodo de retención del archivo

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

5.5.3. Protección del archivo

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

5.5.4. Procedimientos de copia de respaldo del archivo

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

5.5.5. Requisitos para el sellado de tiempo de los registros of Records

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

5.5.6. Sistema de archivo

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

5.5.7. Procedimientos para obtener y verificar la información archivada

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

5.6. CAMBIO DE CLAVES DE LA AC

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

5.7. GESTIÓN DE INCIDENTES Y VULNERABILIDADES

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

5.7.1. Gestión de incidentes y vulnerabilidades

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

5.7.2. Actuación ante datos y software corruptos

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

5.7.3. Procedimiento ante compromiso de la clave privada de la AC

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



5.7.4. Continuidad de negocio después de un desastre

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

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

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

6. CONTROLES DE SEGURIDAD TÉCNICA

229. 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

230. 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*, véase el apartado correspondiente en la *DGPC*.

6.1.1.2 Generación del par de Claves de la RA

231. No estipulado

6.1.1.3 Generación del par de Claves de los Suscriptores

232. Las *Claves privadas* de los *Certificados* emitidos bajo la presente *DPPP* son generadas y custodiadas por el *Suscriptor* del *Certificado*.

6.1.2. Envío de la clave privada al suscriptor

233. No existe ninguna generación ni entrega de la *Clave privada* al *Titular* por parte de la *CA*.

6.1.3. Envío de la clave pública al emisor del certificado

234. 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

235. La FNMT-RCM distribuye las *Claves públicas*, tanto de la AC raíz como de las AC Subordinadas que expiden los *Certificados* emitidos bajo la presente *DPPP*, a través de varios



medios, como son mediante publicación en su sede electrónica (www.sede.fnmt.gob.es) o mediante información pública a través del presente documento, en el apartado “1.3.1. Autoridad de Certificación”.

6.1.5. Tamaños de claves y algoritmos utilizados

236. El algoritmo utilizado es RSA with SHA-256.

237. En cuanto al tamaño de las claves, dependiendo de cada caso, es:

- Claves de la AC FNMT raíz: RSA 4.096 bits.
- Claves de las AC Subordinadas: RSA 2.048 bits.
- Claves de los *Certificados finales emitidos bajo la presente DPPP*: RSA 2.048 bits.

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

238. Las *Claves públicas* de los *Certificados* están codificadas de acuerdo con RFC5280 y PKCS#1.

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

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

240. 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* finales emitidos bajo la presente *DPPP* tienen habilitado exclusivamente el uso para firmar/sellar *Certificados* de usuario final y CRLs.

241. El *Certificado de autenticación de sitios web* tiene habilitado el uso de firma digital (digital Signature). Adicionalmente, estos *Certificados* cuentan con el uso extendido de clave de autenticación de servidor (server authentication) y autenticación de cliente (client authentication).

242. El *Certificado de componente de Sello de Entidad* tiene habilitados los usos de firma y cifrado y cuentan con el uso extendido de autenticación y protección de correo.

243. Los *Certificados de componente para su uso en las Unidades de Sellado de Tiempo*, tienen habilitados los usos de firma y cifrado y cuentan con el uso extendido propio del sellado de tiempo.

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

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

6.2.1. Estándares para los módulos criptográficos

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



6.2.2. Control multi-persona (n de m) de la clave privada

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

6.2.3. Custodia de la clave privada

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

6.2.4. Copia de seguridad de la clave privada

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

6.2.5. Archivado de la clave privada

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

6.2.6. Transferencia de la clave privada a/o desde el módulo criptográfico

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

6.2.7. Almacenamiento de la clave privada en el módulo criptográfico

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

6.2.8. Método de activación de la clave privada

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

6.2.9. Método de desactivación de la clave privada

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

6.2.10. Método de destrucción de la clave privada

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

6.2.11. Clasificación de los módulos criptográficos

255. 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

256. Los *Certificados* emitidos bajo la presente *DPPP* y, por tanto, sus *Claves públicas* asociadas, son conservadas por la FNMT-RCM durante el periodo de tiempo exigido por la legislación vigente, que actualmente es de 15 años.

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

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

- *Certificado* de la AC raíz y su par de *Claves*: véase el apartado “1.3.1. Autoridad de Certificación” de la presente *DPPP*.
- El *Certificado* de la AC subordinada que expide los *Certificados* de entidad final y su par de *Claves*: véase el apartado “1.3.1. Autoridad de Certificación” de la presente *DPPP*.
- Los *Certificados de autenticación de sitios web* y su par de *Claves*: el periodo máximo de vigencia de los *Certificados* y su par de *Claves* es de 12 meses.
- Los *Certificados de componente de Sello de Entidad*: el periodo máximo de vigencia de los *Certificados* y su par de *Claves* es de 36 meses.
- Los *Certificados de componente para su uso en las Unidades de Sellado de Tiempo*: el periodo máximo de vigencia de los *Certificados* y su par de *Claves* 7 años.

6.4. DATOS DE ACTIVACIÓN

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

6.4.1. Generación e instalación de datos de activación

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

6.4.2. Protección de datos de activación

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

6.4.3. Otros aspectos de los datos de activación

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

6.5. CONTROLES DE SEGURIDAD INFORMÁTICA

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

6.5.1. Requisitos técnicos específicos de seguridad informática

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



6.5.2. Evaluación del nivel de seguridad informática

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

6.6. CONTROLES TÉCNICOS DEL CICLO DE VIDA

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

6.6.1. Controles de desarrollo de sistemas

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

6.6.2. Controles de gestión de la seguridad

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

6.6.3. Controles de seguridad del ciclo de vida

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

6.7. CONTROLES DE SEGURIDAD DE RED

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

6.8. FUENTE DE TIEMPO

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

7. PERFILES DE LOS CERTIFICADOS, CRLs Y OCSP

7.1. PERFIL DEL CERTIFICADO

271. Los *Certificados de autenticación de sitios web* son emitidos de conformidad con el estándar europeo ETSI EN 319 412-4 “Certificate profile for web site certificates” y con las políticas OV identificada con el OID 0.4.0.2042.1.7. y 2.23.140.1.2.2

272. Los *Certificados de componente de sello de entidad* son emitidos de conformidad con el estándar europeo ETSI EN 319 411-2 “Requirements for trust service providers issuing EU qualified certificates” y ETSI EN 319 412-3 “Certificate profile for certificates issued to legal persons” y contienen el identificador de política 0.4.0.194112.1.1



7.1.1. Número de versión

273. Los *Certificados* emitidos bajo la presente *DPPP* son conformes con el estándar X.509 versión 3.

7.1.2. Extensiones del certificado

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

7.1.3. Identificadores de objeto de algoritmos

275. El identificador de objeto (OID) correspondiente al algoritmo criptográfico utilizado (Sha256withRsaEncryption) es 1.2.840.113549.1.1.11.

7.1.4. Formatos de nombres

276. A la fecha de emisión, toda la información del titular es precisa y se han verificado todos los atributos presentes en el campo *Subject* del certificado.
277. La codificación de los *Certificados* emitidos bajo la presente *DPPP* 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.
278. Los *Certificados de autenticación de sitios web* deben contener una extensión Subject Alternative Name (SAN) válida y completa. La entrada *dNSName* en la extensión SAN debe contener o bien un FQDN o un nombre de dominio Wildcard que la CA haya previamente validado conforme a la sección 3.2.2.4.
279. Los *Certificados de autenticación de sitios web* no deben contener metadatos como ".", "-", y "" (es decir, espacio) o cualquier indicación de que un valor o campo está ausente, incompleto o no sea de aplicación.
280. Los *Certificados de autenticación de sitios web* no deben contener el carácter ("_") en las entradas *dNSName*.
281. Los campos OU quedan restringidos a la información del *Subscriber* que ha sido verificada conforme a la sección 3 de la presente *DPC*.
282. Los nombres de dominio Wildcard deben ser validados de conformidad con lo establecido en la sección 3.2.2.6. no pudiendo contener un nombre interno.
283. El FQDN o la parte del FQDN de un *Certificado Wildcard* sólo puede contener etiquetas *P-Labels* o *Non-Reserved LDH Labels*.

7.1.5. Restricciones de nombres

284. Las CAs subordinadas que emiten los certificados bajo la presente *DPPP* no están restringidas técnicamente.



7.1.6. Identificador de objeto de política de certificado

285. El identificador de objeto (OID) de la política de los emitidos bajo la presente *DPPP* 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

286. La extensión “Policy Constrains” del *Certificado* raíz de la AC no es utilizado.

7.1.8. Sintaxis y semántica de los calificadores de política

287. 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”

288. 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

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

7.2.2. CRL y extensiones

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

Tabla 3 – Perfil de la CRL

Campos y extensiones	Valor
Versión	V2
Algoritmo de firma	Sha256WithRSAEncryption
Número de CRL	Valor incremental

Campos y extensiones	Valor
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)
Identificador de la clave de Autoridad	Hash de la clave del emisor
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

291. El perfil de los mensajes OCSP emitidos por la FNMT-RCM, cumple con las especificaciones contenidas en el IETF RFC 6960 Internet X.509 PKI Online Certificate Status Protocol (OCSP) profile.

7.3.1. Número de versión

292. Los *Certificados* utilizados por el *Servicio de información y consulta sobre el estado de validez de los certificados*, vía OCSP, son conformes con el estándar X.509 versión 3.

7.3.2. Extensiones del OCSP

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

8. AUDITORÍAS DE CUMPLIMIENTO

294. 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”.

295. Así mismo, los *Certificados* que tienen la consideración de cualificados, son sometidos a la auditoría que garantiza el cumplimiento con los requisitos establecidos en los estándares



- Europeos ETSI EN 319 411-2 “Requirements for trust service providers issuing EU qualified certificates”.
296. El sistema de expedición de *Certificados* es sometido a otras auditorías adicionales:
- Auditoría del Sistema de Gestión de la Seguridad de la Información conforme a UNE-ISO/IEC 27001 “Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos”.
 - Auditoría según lo dictaminado en el Esquema Nacional de Seguridad (Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica).
 - Auditoría del Sistema de Gestión de la Calidad con arreglo a ISO 9001.
 - Auditoría del Sistema de Gestión de la Responsabilidad Social en correspondencia con IQNet SR10.
 - Auditoría del Plan de continuidad de negocio según ISO 22301.
 - Auditoría conforme el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (RGPD / LOPD-GDD).
297. También se llevan a cabo análisis de riesgos, de acuerdo a lo dictado en el Sistema de Gestión de la Seguridad de la Información.
- 8.1. FRECUENCIA DE LAS AUDITORÍAS**
298. Periódicamente se elaborarán los correspondientes planes de auditorías.
299. La *Autoridad de Certificación* que expide los *Certificados* está sujeta a auditorías periódicas, de conformidad con el estándar europeo ETSI EN 319 401 “General Policy Requirements for Trust Service Providers”, ETSI EN 319 411-1 “Policy and security requirements for Trust Service Providers issuing certificates”, 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” and ETSI EN 319 412- 4 “Certificate profile for web site certificates” según proceda. La auditoría es realizada anualmente por una empresa externa acreditada.
300. La frecuencia del resto de auditorías adicionales, será conforme a lo estipulado en la normativa vigente correspondiente y con CAB Forum’s Baseline Requirements.
- 8.2. CUALIFICACIÓN DEL AUDITOR**
301. Véase el apartado correspondiente en la *DGPC*.



8.3. RELACIÓN DEL AUDITOR CON LA EMPRESA AUDITADA

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

8.4. ELEMENTOS OBJETOS DE AUDITORÍA

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

8.5. TOMA DE DECISIONES FRENTE A DETECCIÓN DE DEFICIENCIAS

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

8.6. COMUNICACIÓN DE LOS RESULTADOS

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

8.7. AUTOEVALUACIÓN

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

9. OTROS ASUNTOS LEGALES Y DE ACTIVIDAD

9.1. TARIFAS

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

9.1.1. Tarifas de emisión o renovación de certificados

308. La determinación de tarifas aplicables a la emisión o renovación de *Certificados* seguirá lo establecido en el apartado “9.1 Tarifas” del presente documento.

9.1.2. Tarifas de acceso a los certificados

309. No estipulado.

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

310. 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

311. La determinación de tarifas aplicables a otros servicios seguirá lo establecido en el apartado “9.1 Tarifas” del presente documento.

9.1.5. Política de reembolso

312. 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

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

9.2.1. Seguro de responsabilidad civil

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

9.2.2. Otros activos

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

9.2.3. Seguros y garantías para entidades finales

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

9.3. CONFIDENCIALIDAD DE LA INFORMACIÓN

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

9.3.1. Alcance de la información confidencial

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

9.3.2. Información no incluida en el alcance

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

9.3.3. Responsabilidad para proteger la información confidencial

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



9.4. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

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

9.4.1. Plan de privacidad

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

9.4.2. Información tratada como privada

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

9.4.3. Información no considerada privada

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

9.4.4. Responsabilidad de proteger la información privada

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

9.4.5. Aviso y consentimiento para usar información privada

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

9.4.6. Divulgación conforme al proceso judicial o administrativo

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

9.4.7. Otras circunstancias de divulgación de información

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

9.5. DERECHOS DE PROPIEDAD INTELECTUAL

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

9.6. OBLIGACIONES Y GARANTÍAS

9.6.1. Obligaciones de la AC

330. 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 Prácticas y Políticas de Certificación*.



331. 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.
332. La FNMT-RCM emite los *Certificados de autenticación de sitios web* de conformidad con los "Requisitos base para la emisión y gestión de certificados de confianza", requisitos establecidos por la entidad CA/Browser forum y que pueden consultarse en la dirección <https://cabforum.org/>. Asimismo, adaptará sus prácticas de expedición de dichos *Certificados* a la versión vigente de los citados requisitos. En caso de cualquier incoherencia entre la presente *DPPP* y la citada versión, dichos requisitos prevalecerán sobre este documento.
333. 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:
334. 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* 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.



9.6.2. Obligaciones de la AR

335. Véase el apartado correspondiente en la *DGPC*.
336. Las actividades relativas a la AR serán realizadas exclusivamente por la FNMT-RCM, a través de su Área de Registro.
337. 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*.
 - Para los *Certificados de autenticación de sitios web*, comprobar que la titularidad del nombre de dominio se corresponde con la identidad del *Suscriptor* o, en su caso, obtener la autorización de éste, que se asociará al *Certificado de autenticación de sitios web*, por los medios a su alcance que, razonablemente, permitan acreditar tal titularidad, de conformidad con el estado de la técnica.
 - Para los *Certificados de autenticación de sitios web*, recoger expresamente la manifestación del *Suscriptor* en relación con la titularidad del dominio del *Certificado de autenticación de sitios web*, manifestando que tiene el poder único de decisión sobre el mismo.
 - 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*.

9.6.3. Obligaciones de los Suscriptores

338. Véase el apartado correspondiente en la *DGPC*.
339. En cuanto a los *Certificados de autenticación de sitios web*, los *Suscriptores* han de tener el control del nombre de dominio de sitio web incluido en dichos *Certificados* y mantener bajo su uso exclusivo las *Claves privadas* asociadas.
340. El *Solicitante* y el *Suscriptor* de los *Certificados* expedidos bajo la presente *DPPP*, 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, licenciataria 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 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.
 - Devolver o destruir el *Certificado* cuando así lo exija la FNMT-RCM, y no usarlo con propósito de firmar o identificarse electrónicamente cuando el *Certificado* caduque, o sea revocado.
341. Será en todo caso 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.
342. 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.
343. 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.
344. 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

345. Será responsabilidad de la Entidad usuaria y de los terceros que confían en los *Certificados* la verificación y comprobación del estado de los *Certificados*, no cabiendo en ningún caso presumir la validez de los Certificados sin dichas comprobaciones.
346. Cuando se trate de un *Certificado Cualificado*, verificar que el identificador del servicio es el que se encuentra publicado en la correspondiente *Trusted Service List*, accesibles a través del siguiente enlace:
<https://esignature.ec.europa.eu/intl-comp-tl-browser/#/screen/trusted-list-provider/ES>
347. Si las circunstancias indican necesidad de garantías adicionales, la Entidad Usuaria deberá obtener garantías adicionales para que dicha confianza resulte razonable.
348. Asimismo, será responsabilidad de la Entidad Usuaria observar lo dispuesto en la Declaración de Prácticas de Certificación y sus posibles modificaciones futuras, con especial atención a los límites de uso establecidos para los *Certificados* en esta Política de Certificación.
349. Véase el apartado correspondiente en la *DGPC*.

9.6.5. Obligaciones de otros participantes

350. No estipulado.

9.7. RENUNCIA DE GARANTÍAS

351. No estipulado.



9.8. LÍMITES DE RESPONSABILIDAD

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

9.9. INDEMNIZACIONES

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

9.9.1. Indemnización de la CA

354. No estipulado.

9.9.2. Indemnización de los Suscriptores

355. No estipulado.

9.9.3. Indemnización de las partes que confían

356. No estipulado.

9.10. PERIODO DE VALIDEZ DE ESTE DOCUMENTO

9.10.1. Plazo

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

9.10.2. Terminación

358. 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

359. 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

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



9.12. MODIFICACIONES DE ESTE DOCUMENTO

9.12.1. Procedimiento para las modificaciones

361. Las modificaciones de la presente *Declaración de Prácticas y Políticas de Certificación* serán aprobadas por la Dirección del departamento Ceres, que quedarán reflejadas en la correspondiente acta del Comité de Gestión del Prestador, de conformidad con el procedimiento interno aprobado mediante el documento “Procedimiento de revisión y mantenimiento de las políticas de certificación y declaración de prácticas de servicios de confianza”.

9.12.2. Periodo y mecanismo de notificación

362. Cualquier modificación en la presente *Declaración de Prácticas y Políticas de Certificación* será publicada de forma inmediata en la URL de acceso a las mismas.
363. Si las modificaciones a realizar no conllevan cambios significativos en cuanto al régimen de obligaciones y responsabilidades de las partes o relativos a una modificación de las políticas de prestación de los servicios, la FNMT-RCM no informará previamente a los usuarios, limitándose a publicar una nueva versión de la declaración afectada en su página web.

9.12.3. Circunstancias bajo las cuales debe cambiarse un OID

364. Las modificaciones significativas de las condiciones de los servicios, régimen de obligaciones y responsabilidades o limitaciones de uso pueden ocasionar un cambio de política del servicio y su identificación (OID), así como el enlace a la nueva declaración de política del servicio. En este caso, la FNMT-RCM podrá establecer un mecanismo de información de los cambios propuestos y, en su caso, de recogida de opiniones de las partes afectadas.

9.13. RECLAMACIONES Y RESOLUCIÓN DE DISPUTAS

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

9.14. NORMATIVA DE APLICACIÓN

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

9.15. CUMPLIMIENTO DE LA NORMATIVA APLICABLE

367. La FNMT-RCM manifiesta su compromiso de cumplimiento de la normativa y de los requisitos de aplicación a cada tipo de *Certificado de autenticación de sitios web*, incluyendo



las consideraciones establecidas en el apartado “1.5.4. Procedimiento de aprobación de la DPC” del presente documento de *DPPP*.

9.16. ESTIPULACIONES DIVERSAS

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

9.16.1. Acuerdo íntegro

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

9.16.2. Asignación

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

9.16.3. Severabilidad

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

9.16.4. Cumplimiento

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

9.16.5. Fuerza Mayor

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

9.17. OTRAS ESTIPULACIONES

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