Política de Certificación de certificados de Servidor Seguro SSL, Servidor Seguro SSL con Validación Extendida (SSL EV), Sede Electrónica y Sede Electrónica con Validación Extendida (Sede EV)

	Esta especificación ha sido preparada por ANF AC para liberar a terceras partes.	**NIVEL DE SEGURIDAD** DOCUMENTO PÚBLICO

ÍNDICE

1. INTRODUCCIÓN

ANF Autoridad de Certificación, (en adelante ANF AC), es una entidad jurídica, constituida al amparo de la Ley Orgánica 1/2002 del 22 de marzo e inscrita en el Ministerio del Interior con el número nacional 171.443 y CIF G-63287510.

ANF AC tiene asignado el código privado de empresa (SMI Network Management Private Enterprise Codes) 18332 por la organización internacional IANA -Internet Assigned Numbers Authority-, bajo la rama iso.org.dod.internet.private.enterprise (1.3.6.1.4.1 -IANA –Registered Private Enterprise-).*[1]

El prefijo del OID de esta Política es 1.3.6.1.4.1.18332.55.1.1, se le añade una extensión de formato X.Y que recoge la versión de la PC.

El presente documento es la Política de Certificación correspondiente a los certificados emitidos por ANF AC del tipo Servidor Seguro SSL, Servidor Seguro SSL con Validación Extendida (EV), Sede Electrónica nivel medio y nivel alto, y Sede Electrónica con Validación Extendida (EV) nivel medio y nivel alto. Esta documentación contiene las reglas a las que se sujeta el uso de los certificados definidos en esta política. Se describen los papeles, responsabilidades y relaciones entre el usuario final y ANF Autoridad AC y las reglas de solicitud, adquisición gestión y uso de los certificados. Este documento detalla y complementa lo definido de forma genérica en la Declaración de Prácticas de Certificación de ANF AC.

La presente Política de se ha estructurado conforme a lo dispuesto por el grupo de trabajo PKIX del IETF (Internet Engineering Task Force), en su documento de referencia RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" propuesto por Network Working Group para este tipo de documentos. Se ha incluido un apartado de Buenas Prácticas asumidas por ANF AC, y que atienden la Publicación de Mozilla sobre Prácticas Problemáticas de CA.*[2]

Esta política de certificación ha tenido en consideración y se ha inspirado en lo definido en el Esquema nacional de identificación y firma electrónica de las Administraciones Públicas Bloque I, Política de Certificación v1.2.1 OID 1.3.6.1.4.1.14862.1.4; en conformidad con el Real Decreto 4/2010 del Gobierno de España; y la guía de Perfiles de Certificados Electrónicos v.1.7.6 publicada por el Consejo Superior de Administración Electrónica.

Esta Política de Certificación asume que el lector conoce los conceptos de PKI, certificado y firma electrónica; en caso contrario se recomienda al lector que se

forme en el conocimiento de los anteriores conceptos antes de continuar con la lectura del presente documento.

*[1] Información que puede ser consultada en:

http://www.iana.org/assignments/enterprise-numbers

*[2] http://wiki.mozilla.org/CA:Problematic_Practices

1.1. Descripción de los certificados

ANF AC en el marco de su Servicio de Certificación Digital emite certificados de carácter técnico del tipo:

- **Servidor Seguro SSL**

  El fin de este certificado es establecer comunicaciones de datos vía TLS/SSL en servicios y aplicaciones informáticas, especialmente para:

  1. La identificación de la organización titular del dominio, proporcionando una garantía razonable al usuario de un navegador de Internet de que el sitio web al que accede es titularidad de la Organización identificada en el certificado a través de su nombre y dirección.

  2. La encriptación de las comunicaciones entre el usuario y el sitio web, facilitando el intercambio de las claves de cifrado necesarias para el cifrado de la información a través de Internet.

  La validez de estos certificados es de 2 años.

- **Servidor Seguro SSL con Validación Extendida (EV)**

  Además de las utilidades proporcionadas por el certificado SSL, la Validación Extendida (EV) tiene como objetivo proporcionar un mejor nivel de autenticación de las Organizaciones, para asegurar las transacciones en sus sitios Web.

  El objetivo de los Certificados SSL EV es su utilización en protocolos TLS / SSL con la finalidad de garantizar la validez de la constitución de la organización identificada en el certificado evitando casos de phishing u otros casos de fraude de identidad on- line.

ANF AC cumple lo indicado en las guías del CAB Forum publicadas en www.cabforum.org, incluyendo la aceptación de los programas de auditoría especificados en las mismas.

La validez de estos certificados es de 2 años.

En el ámbito de la Ley 11/2007 de España, de 22 de junio de acceso electrónico de los ciudadanos a los servicios públicos, ANF AC emite certificados del tipo,

- **Sede electrónica**

  El fin de este certificado es establecer comunicaciones de datos vía TLS/SSL en servicios y aplicaciones informáticas, especialmente para:

  1. La identificación de la Administración Pública, órgano o entidad administrativa titular del dominio.

  2. La encriptación de las comunicaciones entre el usuario y el sitio web, facilitando el intercambio de las claves de cifrado necesarias para el cifrado de la información a través de Internet.

  Se trata de un certificado emitido con la consideración legal de reconocido en el que se identifica a la Administración Pública, órgano o entidad administrativa titular de la sede.

  La validez de estos certificados es de 2 años.

- **Sede electrónica con EV**

  Además de las utilidades proporcionadas por el certificado de Sede Electrónica la Validación Extendida (EV) tiene como objetivo proporcionar un mejor nivel de autenticación de la Administración Pública, órgano o entidad administrativa para asegurar las transacciones en sus sitios Web evitando casos de phishing u otros casos de fraude de identidad on-line.

- Además, ANF AC cumple lo indicado en las guías del CAB Forum publicadas en www.cabforum.org, incluyendo la aceptación de los programas de auditoría especificados en las mismas.

- La validez de estos certificados es de 2 años.

1.2. Identificación

Nombre del documento	Política de Certificación de Certificados reconocidos de sede electrónica en soporte software
Versión	1.1
Estado de la política	APROBADO
Referencia del documento / OID	1.3.6.1.4.1.18332.55.1.1
Fecha de emisión	2 de diciembre de 2010
Fecha de expiración	No es aplicable
CPS relacionada	Declaración de Prácticas de Certificación (CPS) de ANF AC OID: 1.3.6.1.4.1. 18332.1.9 Disponible en https://www.anf.es/AC/documentos/
Localización	https://www.anf.es/AC/documentos/

Con el objeto de identificar los certificados, ANF AC les ha asignado los siguientes identificadores de objeto (OID).

CERTIFICADO – CERTIFICATE	OID
Servidor Seguro SSL	1.3.6.1.4.1.18332.55.2.1
Servidor Seguro SSL EV	1.3.6.1.4.1.18332.55.3.1
Sede Electrónica	1.3.6.1.4.1.18332.55.4.1
Sede Electrónica EV Nivel Medio	1.3.6.1.4.1.18332.55.5.1
Sede Electrónica EV Nivel Alto	1.3.6.1.4.1.18332.55.6.1
Sede Electrónica EV Nivel Medio	1.3.6.1.4.1.18332.55.7.1

Los certificados emitidos con la consideración de reconocidos incorporan adicionalmente el identificador de objeto (OID) definido por el TS 101 862, del Instituto

Europeo de Normas de Telecomunicaciones, sobre perfiles de certificados reconocidos: 0.4.0.1862.1.1. Más información en punto 7.1 de este documento.

1.3. Tipo de Soporte

Los certificados de Servidor Seguro SSL, Servidor Seguro SSL con EV, Sede Electrónica, Sede Electrónica con EV se emiten en tres tipos de soporte en función de dónde se cree y resida el par de claves:

- Token criptográfico por software.

  Los datos de creación de firma están contenidos en un token criptográfico en formato PKCS#15. Este token está construido siguiendo el formato PKCS#15v.1.1. Solo son token criptográficos autorizados por ANF AC, aquellos que figuran publicados en www.anf.es

- Soporte hardware criptográfico.

  Con soporte en un dispositivo seguro de creación de firma (HSM)

- Soporte hardware criptográfico con captura de valores biométricos.

  Con soporte en un dispositivo seguro de creación de firma (HSM)

La presente política, en cuanto a los certificados del tipo Sede Electrónica, sigue las definiciones de los niveles de aseguramiento de los Perfiles de certificados electrónicos, en su versión V1.7.6 del 16/07/2010, publicado por el Consejo Superior de Administración Electrónica del Gobierno de España.

Se definen dos niveles de aseguramiento:

Nivel medio:

- Este nivel corresponde a una configuración de mecanismos de seguridad apropiada para la mayoría de aplicaciones.
- El riesgo previsto por este nivel (siguiendo la recomendación de la OCDE):
  - Infracción de seguridad (ej: el robo de identidad)
  - Puede producir pérdidas económicas moderadas
  - Pérdida de información sensible o crítica.
  - Refutación de una transacción con impacto económico significativo.
- Asimismo, el riesgo previsto por este nivel corresponde al nivel 3 de garantía previsto en la Política Básica de Autenticación de IDABC*[1].

Los mecanismos de seguridad aceptables incluyen los certificados X.509 en software. En los casos de certificados emitidos a personas, se corresponde con el de un "certificado reconocido", como se define en la Ley 59/2003, de firma electrónica, para firma electrónica avanzada, sin dispositivo seguro de creación de firma.

Nivel alto:

Este nivel corresponde a una configuración de mecanismos de seguridad apropiada para las aplicaciones que precisan medidas adicionales, en atención al análisis de riesgo realizado.

- El riesgo previsto por este nivel (siguiendo la recomendación de la OCDE):

- Infracción de seguridad
- Puede producir pérdidas económicas importantes
- Pérdida de información altamente sensible o crítica.
- Refutación de una transacción con impacto económico muy significativo.
- Asimismo, el riesgo previsto por este nivel corresponde al nivel 4 de garantía previsto en la Política Básica de Autenticación de IDABC.
- Los mecanismos de seguridad aceptables incluyen los certificados X.509 en hardware. En los casos de certificados emitidos a personas, se corresponde con el de "firma electrónica reconocida", como se define en la Ley 59/2003, de firma electrónica. El soporte tiene que estar homologado por ANF Autoridad de Certificación.

De acuerdo con lo especificado, en los certificados de nivel medio las claves son creadas y almacenadas en soporte software. En los certificados de nivel alto las claves son creadas y almacenadas en soporte HSM.

ANF AC dispone de un servicio de sellado de fecha y hora, según determina la ETSI TS 102 023, conforme a DPC OID 1.3.6.1.4.1.18332.5.1 de ANF Autoridad de Sellado de Tiempo.

*[1] Decisión 2004/387/CE del Parlamento Europeo y del Consejo, de 21 de abril de 2004, relativa a la prestación interoperable de servicios paneuropeos de administración electrónica al sector público, las empresas y los ciudadanos (IDABC) [Diario Oficial L 144 de 30.4.2004]

Cuando el soporte elegido por el suscriptor sea por software, los sistemas donde se almacenen las claves privadas deben cumplir una serie de requisitos relativos a la seguridad física y lógica de los mismos. ANF AC podrá, de manera discrecional, solicitar al suscriptor que evidencie los mecanismos utilizados para el bastionado de dichos sistemas.

En la revisión que efectúe ANF AC sobre estos sistemas, seguirá las recomendaciones publicadas por el CCN (Centro Criptológico Nacional) de España, dentro de su serie CCN-STIC, orientadas específicamente a garantizar la seguridad de los sistemas de las tecnologías de la información y lax comunicaciones.

1.4. Comunidad de usuarios y ámbito de aplicación

1.4.1. Autoridades de Certificación

Esta PC hace referencia a los certificados del tipo Servidor Seguro SSL, Servidor Seguro SSL con Validación Extendida (EV), Sede Electrónica nivel medio y alto y Sede Electrónica con Validación Extendida (EV) nivel medio y alto, son emitidos por la CA Subordinada "ANF AC SSLSede CA1" de ANF AC.

- AC Raíz: Autoridad de Certificación de primer nivel. Esta AC sólo emite certificados para sí misma y sus AC Subordinadas. Únicamente está en funcionamiento durante la realización de las operaciones para las que se establece.

Sus datos más relevantes son:

Nombre distintivo	CN = ANF Server CA, O=ANF Autoridad de Certificación, C=ES
Número de serie	01 34 4b
Nombre distintivo del emisor	CN = ANF Server CA, O=ANF Autoridad de Certificación, C=ES
Periodo de validez	Desde 2009-12-01 1:00:00 hasta 2021-12-01 1:00:00
Huella digital (SHA-1)	12 61 25 c5 7d b7 7b 9d a8 47 d9 0d 6c 3e 9f 8a d0 f7 c0 1e

- ANF SSLSede CA1: Autoridad de Certificación subordinada de la AC Raíz. Su función es la emisión de certificados para los usuarios finales de esta PKI de ANF AC. Sus datos más relevantes son:

Nombre distintivo	CN = ANF SSLSede CA1, O= ANF Autoridad de Certificación, C=ES
Número de serie	
Nombre distintivo del emisor	CN = ANF Server CA, O=ANF Autoridad de Certificación, C=ES
Periodo de validez	Desde hasta
Huella digital (SHA-1)	

1.4.2. Autoridades de Registro

1.4.2.1 Autoridades de Registro Reconocidas

Las Autoridades de Registro que gestionan este tipo de certificados pertenecen a la Red Nacional de Proximidad de Autoridades de Registro Reconocidas por ANF AC.

Las Autoridades de Registro Reconocidas son personas físicas o jurídicas a las que ANF AC ha dotado con certificados específicos que les habilitan para intervenir como "Autoridad de Registro Reconocida". Concretamente tienen activados en su certificado los siguientes OID:

1.3.6.1.4.1.18332.42.1 Código del Identificador operador AR responsable de la solicitud.

1.3.6.1.4.1.18332.42.2 Código del Identificador de ARR si se trata de Nivel 1.

1.3.6.1.4.1.18332.42.4 Código del Identificador de ARR si se trata de Nivel 2.

1.3.6.1.4.1.18332.42.6 URL de las Actas elaboradas para la emisión del certificado.

La tramitación de la petición siempre se realizará de forma personal y presencial, acompañando documentos originales de identificación y suscribiendo el correspondiente contrato de petición de emisión.

ANF AC verifica la capacidad legal del solicitante para tramitar la petición, comprueba la identidad y la titularidad del dominio solicitado, y determina la adecuación de la emisión solicitada. ANF AC se reserva el derecho de rechazar o solicitar ampliación de acreditación en todos los casos que considere oportuno.

1.4.2.2 Autoridades de Registro Colaboradoras

ANF AC aceptará los trámites de identificación y autentificación que los solicitantes hayan llevado a cabo ante entidades, instituciones o profesionales que dentro del ordenamiento jurídico español, las capacite para asumir estas funciones.

Cabe apuntar, a modo meramente enunciativo, alguna de las entidades ante las que se puede realizar este trámite:

- Consulados y embajadas españolas.
- Notarios.
- Secretarios judiciales.
- Secretarios de Ayuntamientos.

1.4.3. Usuarios Finales

Cabe distinguir los siguientes usuarios finales:

1.4.3.1. Suscriptor del certificado

El grupo de usuarios que pueden solicitar certificados definidos por esta política, está limitado exclusivamente al compuesto por legítimos propietarios de dominios cuya denominación no conlleve a confusión con otras entidades que, teniendo denominaciones similares o idénticas ya están presentes en la Red.

Si la propiedad del dominio es de una persona jurídica, o una Administraciones Pública, órgano o entidad de derecho público, la solicitud del certificado tiene que ser realizada por una persona física con suficiente capacidad legal para realizar esta petición.

Certificados de Servidor Seguro SSL y Servidor Seguro SSL con EV.

Tienen la consideración de suscriptor:

- **Solicitante del certificado**

  El certificado debe ser solicitado por una persona física en su propio nombre como titular del dominio, o con capacidad legal suficiente para asumir la representación del titular del dominio.

- **Responsable del certificado**

  Es la persona física así identificada en el objeto "Identidad Administrativa" dentro de la extensión SubjectAltName, que el suscriptor identifica como el responsable para custodiar y activar el Certificado de Órgano Administrativo.

- **Suscriptor del certificado**

  Los suscriptores son las personas, físicas o jurídicas, así identificadas en el campo "Subject" del certificado.

Certificados de Sede Electrónica con o sin extensión EV, Nivel Alto y Nivel Medio.

Tienen la consideración de suscriptor:

De acuerdo con la Ley 11/2007 (LAECSP), la Ley 59/2003 (LFE) y la normativa administrativa correspondiente,

- **Solicitante del certificado**

  El certificado debe ser solicitado por una persona física con capacidad legal suficiente para asumir la representación del suscriptor.

- **Responsable del certificado**

  Es la persona física Es la persona física así identificada en el objeto "Identidad Administrativa" dentro de la extensión SubjectAltName.

- **Suscriptor del certificado**

  Los suscriptores son las Administraciones Públicas, órganos o entidades de derecho público.

  En el certificado de Sello Electrónico, dentro del campo "Subject" (concretamente en el atributo Common Name) también se identifica el dispositivo o servidor.

1.4.3.2. Terceros que confían en los certificados

- Los usuarios de clientes de aplicaciones en el ámbito de la verificación de la identidad del servidor o de las sedes electrónicas a la que se conectan y del cifrado del canal de los datos transmitidos entre ellos.
- Las aplicaciones y servicios con capacidades de soporte SSL y/o TLS, en el ámbito de verificación de la identidad del servidor o de las sedes electrónicas a las que se conectan, y del cifrado del canal de los datos transmitidos entre ellos.

1.5. Uso de los certificados

1.5.1. Usos Permitidos

1.5.1.1. Suscriptor del certificado

El titular sólo puede utilizar la clave privada y el certificado para los usos autorizados en esta PC y de acuerdo con lo establecido en los campos 'Key Usage' y 'Extended Key Usage' del certificado. Del mismo modo, el titular solo podrá utilizar el par de claves y el certificado tras aceptar las condiciones de uso establecidas en la DPC y PC y sólo para lo que éstas establezcan.

Los certificados emitidos por ANF AC bajo esta Política de Certificación, pueden utilizarse para dotar a las sedes electrónicas de capacidades SSL/TLS. Asimismo y en el caso de sedes electrónicas, pueden utilizarse como mecanismo de

identificación de estas sedes de forma inequívoca ante servicios y aplicaciones informáticas.

1.5.1.2. Terceros que confían en los certificados

Los Terceros que confían sólo pueden depositar su confianza en los certificados para aquello que establece esta PC y de acuerdo con lo establecido en el campo 'Key Usage' del certificado. Los Terceros que confían han de realizar las operaciones de clave pública de manera satisfactoria para confiar en el certificado, así como asumir la responsabilidad de verificar el estado del certificado utilizando los medios que se establecen en la DPC y en esta PC. Asimismo, se obligan a las condiciones de uso establecidas en estos documentos.

1.5.2. Usos restringidos

Pueden ser utilizados de forma restringida por el Responsable del Certificado, y con supervisión del suscriptor, en conformidad con las normas administrativas y organizativas que determine el suscriptor.

1.5.3. Usos prohibidos

Los certificados se utilizarán únicamente conforme a la función y finalidad que tengan establecida en la presente Política de Certificación, y con arreglo a la normativa vigente.

1.6. Política de Administración de ANF AC

1.6.1. Especificación de la Organización Administradora

Nombre	ANF Autoridad de Certificación
Dirección de email	fdiaz@anf.es
Dirección	Calle Orense, 85
	Madrid - 28020 - España
Número de teléfono	+34·902 902 172
Número de fax	+34·93 303 16 11

1.6.2. Persona de Contacto

Nombre	ANF Autoridad de Certificación
Dirección de email	fdiaz@anf.es
Dirección	Calle Orense, 85
	Madrid - 28020 - España
Número de teléfono	+34·902 902 172
Número de fax	+34·93 303 16 11

1.6.3. Competencia para determinar la adecuación de esta Política a la CPS de ANF AC

Las modificaciones propuestas o las nuevas aportaciones a incluir sobre esta Política, deben, previa a su aprobación por parte de la Junta Rectora de la PKI de ANF AC, ser contrastadas con las restantes Políticas de Certificación y Políticas de Firma que ANF AC tenga publicadas, a fin de asegurar que las Políticas soportan

estos cambios. Las modificaciones están recogidas en un documento de actualización de Políticas cuyo mantenimiento esta garantizado por ANF AC y publicado en www.anf.es

Desde el punto de vista de la norma X.509 v3, una Política de Certificación es un conjunto de reglas que definen la emisión, gestión, la aplicabilidad o uso de un certificado en una comunidad de usuarios, sistemas o clase particular de aplicaciones que tengan en común una serie de requisitos de seguridad.

En esta Política de Certificación detalla y completa lo estipulado en la "Declaración de Prácticas de Certificación" (DPC) de la PKI ANF AC, conteniendo las reglas a las que se sujeta el uso de los certificados definidos en esta política, así como el ámbito de aplicación y las características técnicas de este tipo de certificados.

Básicamente la Política de Certificación determina qué requerimientos de seguridad son necesarios para la emisión de cada tipo de certificado, mientras que la DPC informa de cómo se cumplen.

Las versiones actualizadas de la documentación específica pueden ser consultadas en www.anf.es

1.6.4. Procedimiento de Publicación

ANF AC publica la Política de Certificación y CPS en el repositorio público accesible a todos los ciudadanos en www.anf.es

1.7. Definiciones y Acrónimos

1.7.1. Definiciones

- Bastionado: es el proceso mediante el cual se implementa una política de seguridad específica sobre una instalación de un sistema operativo. El bastionado de un equipo intenta reducir el nivel de exposición de un equipo y, por tanto, los riesgos y vulnerabilidades asociados a éste.
- Dispositivo Seguro de Creación de Firma Electrónica: es un dispositivo que se encuentra certificado con un nivel de seguridad igual o equivalente a ITSEC EAL 4 +, y soporta los estándares PKCS#11 y CSP.

1.7.2. Acrónimos

SSL: Secure Sockets Layer

TLS: Transport Security Layer

2. Publicación de información y repositorio de certificados

2.1. Repositorio de certificados

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

Cabe destacar que el servicio de Repositorio está disponible durante las 24 horas de los 7 días de la semana, y, en caso de fallo del sistema y que éste quede fuera de control, ANF AC dispone de un Plan de Contingencias que posibilita la reactivación en un tiempo prudencial.

ANF AC mantiene en su repositorio de informaciones:

a) La documentación de servicio exigible, debidamente actualizada.

b) Todas las versiones anteriores de la citada documentación, con indicación de los periodos y certificados en que resultaron aplicables.

Dicha documentación se mantiene durante un período mínimo de quince años después de la revocación del certificado. El periodo queda reseñado en el certificado, en la extensión QcRetentionPeriod con valor 15 años.

Además ANF AC cumple con las obligaciones de registro y archivo de informaciones adecuadas a la duración de los diferentes tipos de documentos y expedientes electrónicos empleados por la Administración.

En cualquier caso, ANF AC mantiene la justificación documental que acredita la aceptación del certificado emitido de forma permanente.

2.2. Publicación

ANF AC publica en su repositorio:

- Los certificados emitidos, incluidos los certificados de Entidades de Certificación: CA Raíz, CA Subordinadas y CAs intermedias.

- Las listas de certificados revocados y otras informaciones de estado de revocación de los certificados.

- La política general de certificación de la Administración General del Estado, así como cualesquiera políticas específicas de certificados dictadas por el prestador de servicios de certificación para desarrollar ulteriores requisitos, dentro del marco de esta política.
- Las Declaraciones de Prácticas de Certificación.
- En su caso, los documentos de condiciones generales vinculantes con suscriptores y terceros que confían en los certificados.

2.3. Frecuencia de actualizaciones

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

La información de estado de revocación de certificados se publicará de acuerdo con lo establecido en las secciones 4.9.7 y 4.9.9 de esta política.

2.4. Controles de acceso al repositorio de certificados.

ANF AC no limita el acceso de lectura a las informaciones establecidas en el punto 2.2 de esta sección.

Con el fin de proteger la integridad y autenticidad de la información de estado de revocación, solo personal autorizado y debidamente autenticado puede añadir, modificar o borrar registros del Repositorio.

ANF AC aplica la correspondiente política de seguridad, con el fin de garantizar que:

- Únicamente personas autorizadas puedan hacer anotaciones y modificaciones.
- Pueda comprobarse la autenticidad de la información.
- Los certificados sólo estén disponibles para consulta si el suscriptor o responsable del certificado ha prestado su consentimiento.
- Pueda detectarse cualquier cambio técnico que afecte a los requisitos de seguridad.

3. Identificación y Autenticación

3.1. Registro de nombres

3.1.1. Tipos de nombres

Todos los certificados del tipo Servidor Seguro SSL y Sede Electrónica, contienen un nombre distintivo (DN) que identifica al dominio DNS y a la persona u organización titular del mismo. De acuerdo con lo previsto en la Recomendación ITUT X.501 y contenido en el campo Subject, incluyendo un componente Common Name.

El atributo CN (Common Name) del DN ha de hacer referencia al nombre dominio DNS.

Las circunstancias personales y atributos de las personas y organizaciones identificadas en los certificados se incluyen en atributos predefinidos en normas y especificaciones técnicas de reconocimiento general.

3.1.2. Normalización e Identidad Administrativa

ANF AC para los certificados del tipo Sede Electrónica, en cualquiera de sus modalidades, utiliza el esquema de nombres normalizado publicado por el Consejo Superior de Administración Electrónica "Esquema de identificación y firma electrónica Bloque I: Perfiles de certificados electrónicos v.1.7.6".

El perfil de este tipo de certificados incorpora la "Identidad Administrativa".

CERTIFICADO	CAMPOS "IDENTIDAD ADMINISTRATIVA" FIJOS
SEDE ELECTRÓNICA	• Tipo de certificado
	• Nombre de la entidad suscriptora
	• NIF entidad suscriptora
	• Nombre descriptivo de la sede electrónica
	• Denominación de nombre de dominio

3.1.3. Significado de los nombres

El campo Subject Name representa la identidad de la persona o entidad que recibe el certificado.

El nombre contenido en el Subject Name adopta la forma de un Nombre Distinguido, de acuerdo con la Recomendación ITU-T X.501

En la extensión Subject Alternative Name se incluyen identidades alternativas del titular del certificado.

La especificación IETF RFC 5280 prevé el empleo de los siguientes tipos de datos:

- Identidad basada en correo electrónico.

- Identidad basada en nombre diferenciado (DN), que se suele emplear para construir un nombre alternativo basado en atributos propietarios, que no resultan ambiguos en ningún caso (por ejemplo, ANFAC, ANFSubCA1,u otros).

- Identidad basada en nombre de dominio de Internet (DNS).

- Identidad basada en dirección IP.

- Identidad basada en identificador de recurso universal (URI).

De todos ellos se puede contener más de una instancia (por ejemplo, diversas direcciones de correo electrónico).

Todos esos nombres son verificados por ANF AC.

Los nombres de los certificados serán comprensibles e interpretados de acuerdo con la legislación aplicable a los nombres de las personas físicas y jurídicas titulares de los certificados.

Los nombres incluidos en los certificados serán tratados de acuerdo con las recomendaciones indicadas en la sección 7 del apartado "**Guía de cumplimentación de campos de los certificados"** de este documento.

3.1.4. Uso de anónimos y seudónimo

No se permiten

3.1.5. Interpretación de formatos de nombres

Se seguirá lo con las recomendaciones indicadas en el apartado 7.1.12 de este documento

3.1.6. Unicidad de los nombres

Los nombres de los suscriptores de certificados serán únicos, para cada servicio de generación de certificados operado por ANF AC y para cada tipo de certificado, es decir, una persona podrá tener a su nombre certificados de tipos diferentes expedidos por este Prestador de Servicios de Certificación.

3.1.7. Resolución de conflictos relativos a nombres

Los solicitantes de certificados no incluirán nombres en las solicitudes que puedan suponer infracción, por el suscriptor, de derechos de tercero.

ANF AC se reserva el derecho de rehusar una solicitud de certificado por causa de conflicto de nombre.

ANF AC comprobará si el nombre de dominio solicitado puede conducir a error con otro nombre ya existente en la Red, y en caso de existir, determinará bajo su exclusivo criterio sobre la conveniencia de emitir o denegar la emisión del certificado solicitado.

3.1.8. Reconocimiento, autenticación y función de las marcas registradas.

Los nombres distintivos son propiedad de las personas que sustentan los derechos de marca correspondiente sobre los mismos, de existir. Si no se conoce esta circunstancia, ANF AC empleará el nombre propuesto por el usuario, bajo la entera responsabilidad de éste.

3.2. Validación inicial de la identidad

3.2.1. Métodos de prueba de posesión de la clave privada.

El método de demostración de posesión de la clave privada será mediante solicitudes basadas en el estándar PKCS #10, otra prueba criptográfica equivalente o cualquier otro método fiable aprobado por el prestador de servicios de certificación.

3.2.2. Autenticación de la identidad de una organización, su representante legal , y responsable del certificado.

La petición debe de realizarse mediante personación del representante legal de la Organización y del responsable del certificado ante una Autoridad de Registro autorizada por ANF AC, mostrando documentación original de identidad. Como mínimo compuesta por:

a) Cedula de identificación o pasaporte en caso de ciudadanos nacionales.

b) En caso de ciudadanos extranjeros, se requerirá:

I. Miembro de la Unión Europea o de Estados parte del Espacio Económico Europeo, será exigible,

- Documento nacional de identidad o equivalente en su país de origen o pasaporte
- Y certificado emitido por el Registro de Ciudadanos Miembros de la Unión.

II. En relación a ciudadanos extracomunitarios

- Pasaporte y
- Tarjeta de residencia y permiso de trabajo.

Podrá prescindirse de la personación ante la Autoridad de Registro si los formularios correspondientes han sido debidamente cumplimentados, y la firma del representante legal del suscriptor y la del responsable del certificado han sido legitimadas en presencia notarial, adjuntado copias compulsadas de los documentos de identidad, autorización y representación legal. En el caso de entidades de derecho público, la figura notarial podrá ser sustituida por la presencia de un funcionario con atribuciones de fedatario público, según normativa legal al efecto.

En el caso de personas jurídicas se requiere:

- Cedula de identificación fiscal de la Entidad.
- En el caso de certificados del tipo:
  - SSL y SSL EV,
    - Las sociedades mercantiles y demás personas jurídicas cuya inscripción sea obligatoria en el Registro Mercantil, acreditarán la válida constitución mediante la aportación de:

      - Si *SSL,* nota simple del Registro Mercantil relativo a los datos de constitución y personalidad jurídica de las mismas.

      - Si *SSL EV,* original o copia auténtica de un certificado del Registro Mercantil relativo a los datos de constitución y personalidad jurídica de las mismas. Dicho certificado deberá haber sido expedido durante los quince días hábiles anteriores a la fecha de solicitud del certificado.

    - Las Asociaciones, Fundaciones y Cooperativas acreditarán la válida constitución mediante la aportación de original o copia auténtica de un certificado del registro público donde consten inscritas, relativo a su constitución. Dicho certificado deberá

haber sido expedido durante los quince días hábiles anteriores a la fecha de solicitud del certificado.

- Las sociedades civiles y demás personas jurídicas, aportarán original o copia auténtica del documento público que acredite su constitución de manera fehaciente.
- Las Administraciones Públicas y entidades pertenecientes al sector público,
- Entidades cuya inscripción sea obligatoria en un Registro, acreditarán la válida constitución mediante la aportación de original o copia auténtica de un certificado relativo a los datos de constitución y personalidad jurídica de las mismas. Dicho certificado deberá haber sido expedido durante los quince días hábiles anteriores a la fecha de solicitud del certificado.
- Entidades creadas por norma, aportarán referencia a la norma de creación.

  - Sede y Sede EV,

- La titularidad de la Administración, órgano o entidad administrativa sobre la dirección electrónica y/o dominio consignado en el certificado.

  Podrá acreditarse a través de la normativa de creación de la sede electrónica.

Documentación acreditativa del poder suficiente del solicitante

- *SSL EV,*
  - Además de los administradores y representantes legales, se considera que tienen capacidad suficiente para realizar la tramitación de solicitud, los representantes voluntarios siempre y cuando acrediten poder suficiente para la realización de actos de administración o celebración de contratos en nombre de la entidad.

    No será necesario obtener la justificación documental de las facultades de representación de quien actúa en su nombre, siempre que estén reguladas por

Norma legal.

- *Sede y Sede EV,*
  - La legitimidad y competencia del *Solicitante* se acreditará a través de su condición de representante legal del titular de la sede electrónica y vigencia en el cargo.

La Autoridad de Registro obtiene copia digital certificada mediante su firma electrónica, de todos los documentos originales que el solicitante del certificado y el responsable del certificado ha utilizado para identificarse. Además suscribe junto con el solicitante del certificado, de forma manuscrita, el contrato de solicitud de certificado y prestación de servicios de certificación.

ANF AC verificará en los registros oficiales que la organización está legalmente constituida y en plena operatividad, comprobando la vigencia del poder de representación legal utilizado por la persona física solicitante del certificado.

ANF AC comprobará que el solicitante es propietario de la sede electrónica y la posesión del dominio al que hace referencia. Así mismo identificará a las personas autorizadas inscritas en el servidor WHOIS de dominios correspondiente, y la dirección de email de contacto inscrito en el mismo.

ANF AC enviará un correo electrónico informativo del trámite iniciado a la dirección de email de las personas de contacto inscritas en el Servidor WHOIS, y el trámite continuará cuando al menos una de las personas de contacto dé su conformidad a la emisión del certificado solicitado.

ANF AC comprobará todos datos utilizando para ello la información disponible de registros oficiales y de dominio, requiriendo al solicitante o a la Organización a la que representa las aclaraciones o documentos adicionales que considere necesarios.

3.2.3. Autenticación de la identidad de una persona física

La petición debe de realizarse mediante personación física del representante legal de la Organización solicitante de emisión del certificado, ante una Autoridad de Registro autorizada por ANF AC, mostrando documentación original de identidad. Como mínimo compuesta por:

c) Cedula de identificación o pasaporte en caso de ciudadanos nacionales.

d) En caso de ciudadanos extranjeros, se requerirá:

I. Miembro de la Unión Europea o de Estados parte del Espacio Económico Europeo, será exigible,

- Documento nacional de identidad o equivalente en su país de origen o pasaporte
- Y certificado emitido por el Registro de Ciudadanos Miembros de la Unión.

II. En relación a ciudadanos extracomunitarios

- Pasaporte y
- Tarjeta de residencia y permiso de trabajo.

Podrá prescindirse de la personación ante la Autoridad de Registro, si los formularios correspondientes han sido debidamente cumplimentados, y la firma del representante legal del suscriptor, y en su caso la del responsable del certificado han sido legitimadas en presencia notarial, adjuntado copias compulsadas de los documentos de identidad, autorización y representación legal.

En el caso de personas jurídicas se requiere:

- Cedula de identificación fiscal de la Entidad.
- Documentación acreditativa del poder suficiente del solicitante

La Autoridad de Registro obtiene copia digital certificada mediante su firma electrónica, de todos los documentos originales que el solicitante del certificado ha utilizado para identificarse. Todas las partes, autoridad de registro, solicitante del certificado y representante legal, suscriben de forma manuscrita, el contrato de solicitud de certificado y prestación de servicios de certificación.

ANF AC verificará en los registros oficiales que la organización está legalmente constituida y en plena operatividad, comprobando la vigencia del poder de representación legal utilizado por la persona física solicitante del certificado.

En el supuesto de que el suscriptor utilice para generar y almacenar sus claves un soporte con sistema de captura de datos biométricos, el proceso de autenticación de identidad deberá realizarse necesariamente de forma presencial ante una Autoridad de Registro de ANF AC.

3.2.4. Validación.

En el caso de certificados del tipo,

- *SSL*,

ANF AC comprobará la documentación mediante consulta a la base de datos *whois*, verificará que el dominio está registrado, consultando registradores válidos.

Se adjuntará copia impresa de la consulta whois al acta de validación.

- *Sede,*

ANF AC comprobará la norma de creación de la Sede y el titular de la misma.

- *SSL EV y Sede EV,*

ANF AC validará la documentación aportada por el solicitante y no iniciará el proceso de emisión de certificados hasta que la documentación requerida haya sido entregada y validada.

La validación se realizará por la Asesoría Jurídica y por el Área Técnica/Responsable de Seguridad. Esta última revisará y validará la petición técnica.

Con la finalidad de validar la documentación, se podrán utilizar los siguientes medios.

- De forma general, se admitirá como válido y no será necesario comprobar la validez de documentos que hayan sido certificados por un notario.
- Boletines Oficiales de ámbito nacional o regional de los organismos públicos a los que pertenecen organismos y empresas públicas.
- Registros públicos en los que legalmente deben estar registradas las entidades, determinando su vigencia y la inscripción de los poderes ostentados por el representante legal que tramitó la solicitud, así como su capacidad de obrar de forma independiente o mancomunada.
- Con respecto a dominios y direcciones de Internet, ANF AC consultará únicamente en registradores asignados por ICANN/IANA los nombres de dominio y direcciones asociadas al certificado.

- ANF AC en la medida de sus posibilidades, comprobará en empresa privada que el dominio no sea similar a otros dominios que están operando en la Red, analizando especialmente si el certificado solicitado tiene como fin simular la dirección de otra entidad, en especial de entidades de reconocido prestigio.

La Asesoría Jurídica y el Área Técnica/Responsable de Seguridad comprobarán la documentación aportada, y como mínimo:

- Se verifica que dominio no consta en los listados como de riesgo, en las bases de datos internas de ANF AC y/o en el AntiphisingWorkGroup.
- Dirección postal: se comprobará si los datos comprobados en la documentación analizada coinciden con la documentación aportada.
- En el caso de que las direcciones no sean coincidentes, ANF AC verificará que la dirección que consta en la solicitud corresponde a una ubicación en la que la Organización solicitante opera de manera estable. Esta verificación se podrá llevar a cabo mediante declaración firmada o justificantes del pago de impuestos, incluso remitiendo correo certificado con acuse de recibo
- Teléfono: ANF AC deberá comprobar que el teléfono (deberá ser un teléfono fijo, no móvil) pertenece a la entidad solicitante (consulta en el registro en páginas amarillas y posterior comprobación mediante llamada
- Consulta a la base de datos *whois*, verificar que el dominio está registrado, consultando registradores válidos. Se adjuntará copia impresa de la consulta whois al acta de validación.
- Existe un listado de registradores admitidos por tipo de dominio (http://www.iana.org/domains/root/db/) ya sean genéricos (gTLD's) o de país (*country- code*, ccTLDs) que indica cual es el registrador oficial delegado para cada tipo de dominio. En concreto, *se puede consultar el whois para los más habituales en:*

Dominios .com, .net, .org, .info, .biz	http://www.networksolutions.com http://www.whois.net http://www.who.is http://whois.domaintools.com Registradores de dominio locales

Dominos .es	http://www.nic.es
Dominios .eu	http://www.eurid.eu
Domicios .ec	http://www.nic.ec
Domicios .pa	http://www.nic.pa

- Se comprobará que el titular (*registrant*) coincide con la organización solicitante. En caso de no coincidir, el solicitante deberá aportar documentación que justifique el derecho de uso por parte del titular. ANF AC contactará con el titular que figure en el *whois* para verificar que el solicitante tiene el derecho de uso del dominio o subdominio.
- Validación del Código de cuenta corriente en empresa privada.
- ANF AC en la medida de sus posibilidades, comprobará en empresa privada que el dominio no sea similar a otros dominios que están operando en la Red, analizando especialmente si el certificado solicitado tiene como fin simular la dirección de otra entidad, en especial de entidades de reconocido prestigio.

ANF se reserva el derecho de requerir al solicitante las aclaraciones o documentos adicionales que considere necesarios.

3.2.5. Buenas prácticas

Claves privadas generadas en archivos PKCS#12

Se tiene conocimiento de que algunas entidades emisoras generan el par de claves para sus suscriptores, y posteriormente entregan el certificado validado SSL en un archivo PKCS#12. Esto es considerado como una práctica insegura, y tal como queda reseñada en esta Política de Certificación de ANF AC, esta entidad emisora de certificados no genera las claves de sus suscriptores, son los propios suscriptores los que en cualquiera de las modalidades de soporte de certificado, software o hardware, se generan su propio par de claves. ANF AC en ningún caso tiene acceso a la clave privada de sus usuarios.

Dominios validados

ANF AC tiene como buena práctica validar los dominios de las personas físicas o entidades que solicitan un certificado SSL o de Sede en cualquiera de sus modalidades, de tal forma que los datos de los certificados se encuentran válidos y actualizados.

Larga vida de Certificados Validados

Aunque el periodo de vigencia de un certificado de entidad final emitido por ANF AC no supera los 2 años, es posible que el titular tramite una renovación automática y, por lo tanto, la vida del certificado sea de larga duración.

No obstante existe la posibilidad de que una persona haya adquirido un dominio, que hasta determinada fecha era propiedad de otra persona. Si el anterior propietario tenía un certificado de Dominio Validado SSL que aun sigue vigente, cabe la posibilidad de que el propietario anterior, con el certificado válido y una suplantación de DNS, pueda dar acceso seguro a un sitio malicioso.

Para evitar este supuesto, ANF AC comprueba que los datos que se incluyen en el certificado son válidos y actualizados a intervalos de tiempo de 24 meses.

Dominios comodines

Algunas entidades emisoras de certificados de dominio validados, emiten certificados que pueden funcionar como certificados de comodines, por ejemplo, un certificado para *. example.com donde el CA verifica sólo la propiedad y el control del dominio example.com. Esto posibilita que un suscriptor pueda establecer un sitio web malicioso con protección SSL, y cuyo objetivo es imitar sitios legítimos como por ejemplo, paypal.example.com, y todo ello sin el conocimiento de la CA.

ANF AC tiene como buena práctica NO emitir certificados que pueden ser utilizados como dominios comodines.

Prefijos de Dirección de correo electrónico de Certificados de Dominio Validado.

ANF AC limita el conjunto de direcciones de verificación por correo electrónico a las siguientes:

- admin @ dominio
- administrador @ dominio
- webmaster @ dominio
- hostmaster @ dominio
- postmaster @ dominio
- Así como cualquier dirección que aparece en el campo de contacto técnico o administrativo de registro del dominio WHOIS, independientemente de los dominios de las direcciones '.

No se impone a los suscriptores requerimientos de discriminación de mayúsculas minúsculas respecto a la lista especificada anteriormente.

Delegación de validación de correos a terceros

ANF AC valida directamente la identificación de los correos electrónicos inscritos en el WHOIS, evitando así la delegación a terceros de la identificación

Expedición directamente de la entidad final desde la raíz

ANF AC emite los certificados SSL desde una autoridad subordinada por lo que no compromete la clave privada de la raíz, delegando la expedición a una CA subordinada.

Permitir a entidades externas operar con CA subornidas

Los certificados de CA subordinada emitidos por ANF AC, son gestionados directamente y de forma exclusiva por ANF AC , en ningún caso cede las operaciones a entidades externas.

Certificados a nombre de HOST o direcciones IP privadas

ANF AC sólo expide certificados SSL a dominios que se pueden resolver en internet, y son públicos. Evitando la emisión de certificados a IP privadas que pueden utilizar los certificados para una organización o red domestica y a dominios que no se pueden resolver por DNS.

Tamaños mínimos de clave

ANF AC mantiene un seguimiento de los algoritmos utilizados y longitudes de claves seguras, para que estén en conformidad con las recomendaciones publicadas por el NIST o lugares como https://wiki.mozilla.org/CA:MD5and1024

3.3. Identificación y autenticación de las solicitudes de renovación del par de claves.

3.3.1. Identificación y autenticación de las solicitudes de renovación rutinarias.

La identificación y autenticación para la renovación del certificado se puede realizar utilizando las técnicas para la autenticación e identificación inicial (descrita en el punto 3.2.3)O bien tramitando la solicitud de renovación telemáticamente cumplimentando el formulario correspondiente que puede ser obtenido en https://www.anf.es/formularios/renovacion y firmándolo electrónicamente con un certificado emitido con la calificación de Reconocido, y figurando como titular la Organización suscriptora del certificado del que se solicita renovación.

Y de conformidad con lo establecido en el art. 13.4 b) de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, la renovación del certificado mediante solicitudes firmadas digitalmente, exigirá que haya transcurrido un período de tiempo desde la identificación personal menor a los cinco años.

3.3.2. Validación para la renovación de certificados después de la revocación

No se podrán renovar certificados que hayan sido revocados.

3.3.3. Identificación y autenticación de las solicitudes de renovación de clave después de una revocación – Clave no comprometida.

No se autoriza la renovación de certificados caducados, ni revocados.

3.4. Identificación y autenticación de las solicitudes de revocación del par de claves

La política de identificación para las solicitudes de revocación acepta los siguientes métodos de identificación:

- **Telemática**. Mediante la firma electrónica de la solicitud de revocación (https://www.anf.es/formularios/revocacion/

  por parte del solicitante del certificado o del responsable del mismo en la fecha de la solicitud de revocación.

- **Telefónica**. Mediante la respuesta a las preguntas realizadas desde el servicio de soporte telefónico disponible en el número 902 902 172.

- **De forma presencial**. Personándose el suscriptor o el representante legal del titular del certificado en alguna de las oficinas de ANF AC publicadas en:

  http://www.anf.es/anf/corporacion/infraestructura.html.

  Acreditando su identidad mediante documentación original, y firmando de forma manuscrita el formulario correspondiente.

ANF AC o cualquiera de las Autoridades de Registro que componen su Red Nacional de Proximidad pueden solicitar de oficio la revocación de un certificado si tuvieran el conocimiento o sospecha del compromiso de la clave privada asociada al certificado, o cualquier otro hecho que recomendará emprender dicha acción.

ANF AC deberá autenticar las peticiones e informes relativos a la revocación de un certificado, comprobando que provienen de una persona autorizada.

Dichas peticiones e informes serán confirmados cumpliendo los procedimientos establecidos en la Declaración de Prácticas de Certificación.

3.5. Autenticación de una petición de suspension

No se autorizan solicitudes de suspensión.

4. El ciclo de vida de los certificados.

Las especificaciones contenidas en este apartado complementan lo previsto en la Declaración de Prácticas de Certificación (CPS) de la ANF AC.

4.1. Solicitud de emisión de certificado

4.1.1. Legitimación para solicitar la emission

Antes de la emisión y entrega de un certificado, debe existir una solicitud previa, que será a instancia de parte.

4.1.1.1. Especificaciones para los certificados de sede electronic

Será necesaria la identificación de la persona que actúa como responsable del certificado. Será necesario la comprobación de la existencia y titularidad del servidor y nombre de Dominio.

4.1.2. Procedimiento de alta; Responsabilidades

La entidad de registro debe asegurarse de que las solicitudes de certificado son completas, precisas y están debidamente autorizadas. Además informará al suscriptor a través de su representante legal y al responsable del certificado de los términos y condiciones aplicables al certificado. La citada información se comunicará en soporte duradero, en papel o electrónicamente, y en lenguaje fácilmente comprensible.

La solicitud se deberá acompañar con la documentación justificativa de la identidad y otras circunstancias del suscriptor y de su representante legal, de acuerdo con lo establecido en las secciones 3.2.2 y 3.2.3 de esta política de certificación.

4.2. Procesamiento de la solicitud de certificación

Una vez haya tenido lugar una petición de certificado, ANF AC verificará la información proporcionada, conforme a la sección correspondiente de esta política y su DPC.

La valoración del proceso seguido, tanto de la documentación como del resultado de la valoración efectuada, es analizada por el Responsable de Dictamen de Emisión. ANF AC ha dotado con certificados específicos a los responsables para la emisión de dictámenes, estos certificados incluyen la extensión 1.3.6.1.4.1.18332.42.3 con el valor "Responsable Dictamen de emisión".

Tanto el dictamen como la notificación al usuario, son firmados por el responsable que se ha encargado de realizar las comprobaciones.

Si la información no es correcta, se denegará la petición. En caso que los datos se verifiquen correctamente, se aprobará la emisión del certificado.

4.2.1. Especificaciones para los certificados de tipo Sede Electrónica

Una vez aprobada la solicitud del certificado, ANF AC, o su Autoridad de Registro Reconocida, se pondrá en contacto con el responsable de la instalación del certificado, a fin determinar el mecanismo de remisión de la clave pública a certificar, de acuerdo con lo establecido en la sección correspondiente.

Después de la recepción, en condiciones de seguridad, de la clave pública se procederá a la emisión del certificado y a su entrega.

4.3. Emisión de certificados

Una vez validada la documentación por ANF AC, el Responsable del Área Técnica se pondrá en contacto con el Responsable Técnico indicado en la Solicitud de Emisión para que genere la petición técnica y la remita por email.

ANF AC no es responsable de la monitorización, investigación o confirmación de la exactitud de la información contenida en el certificado con posterioridad a su

emisión. En el caso de recibir información sobre la inexactitud o la no aplicabilidad actual de la información contenida en el certificado, éste puede ser revocado.

La emisión del certificado tendrá lugar una vez que se hayan llevado a cabo las verificaciones necesarias para validar la solicitud de certificación y el Responsable de Dictámenes de Emisión haya emitido acta de aprobación. El mecanismo por el que determina la naturaleza y la forma de realizar dichas comprobaciones es esta Política de Certificación.

El mecanismo por el que determina la naturaleza y la forma de realizar dichas comprobaciones es esta Política de Certificación.

4.3.1. Acciones de la Entidad de Certificación durante el proceso de emission

Después de la aprobación de la solicitud de certificación se procederá a la emisión del certificado, de forma segura y se pondrá el certificado a disposición del suscriptor o responsable del certificado, para la aceptación de este, de acuerdo con lo establecido en la sección correspondiente.

Los procedimientos establecidos en esta sección también se aplicarán en caso de renovación de certificados, ya que ésta implica la emisión de un nuevo certificado.

Concretamente:

- El procedimiento de generación de certificados de ANF AC vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada. Detalle en la DPC de ANF AC.

- ANF AC no genera las claves del suscriptor.

- ANF AC aplica la correspondiente Política de Seguridad a fin de mantener la confidencialidad e integridad de los datos de registro, especialmente en caso de que sean intercambiados con el suscriptor o responsable del certificado.

- ANF AC publica en el repositorio los certificados emitidos con un usuario de escritura específicamente habilitado a dicho fin, con los permisos granulares de acceso y controles de seguridad regulados y necesarios para ello, garantizando la seguridad de las comunicaciones.

Adicionalmente, ANF AC:

- Incluye en el certificado las informaciones establecidas en el artículo 11.2 de la Ley 59/2003.

- Especifica la fecha y la hora en las que se expidió un certificado.

- Los Dispositivos Seguros de Creación de Firma Electrónica, son entregados personalmente al suscriptor o responsable del certificado por la Autoridad de Registro Reconocida de ANF AC.

- ANF AC utiliza sistemas y productos fiables que estan protegidos contra toda alteración y que garantizan la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.

4.3.2. Notificación de la emisión al suscriptor

ANF AC notifica al solicitante la aprobación o denegación de la solicitud.

También se notificará al suscriptor que se ha creado el certificado, se encuentra disponible y la forma de obtenerlo.

4.4. Aceptación, entrega y devolución de certificados

4.4.1. Responsabilidades de la Entidad de Certificación

ANF AC pone a disposición del suscriptor, previo a la entrega del certificado:

- El dispositivo criptográfico de firma, verificación de firma, cifrado o descifrado.
- Información básica sobre la política y uso del certificado, incluyendo especialmente información sobre ANF AC y su Declaración de Prácticas de Certificación aplicable, así como sus obligaciones, facultades y responsabilidades.
- Información sobre el certificado y el dispositivo criptográfico.
- Información sobre las obligaciones del responsable del certificado.
- Información sobre la responsabilidad del responsable del certificado.
- Información del método de imputación exclusiva al responsable de su clave privada y de sus datos de activación del certificado y, en su caso, del dispositivo criptográfico.

En el acto de entrega del certificado, se procede a :

- El suscriptor firma una hoja de entrega del certificado.
- Se deja constancia de la fecha del acto de entrega y aceptación.

4.4.2. Conducta que constituye aceptación del certificado

La aceptación de los certificados por parte de los suscriptores se produce en el momento de la firma del Contrato de Solicitud de Certificado asociado a cada Política de Certificación. La aceptación del contrato implica el conocimiento y aceptación por parte del suscriptor de la Política de Certificación asociada.

El Contrato de Certificación es un documento que debe ser firmado por el suscriptor y cuyo fin es vincular a la persona que solicita el certificado, con el conocimiento de las normas de uso y con la veracidad de los datos presentados. El formulario del Contrato de Prestación de Servicios de Certificación Electrónica se recoge en el Anexo I de esta Política de Certificación.

Entrega

ANF AC entrega el certificado, por un medio seguro (por ejemplo, correo electrónico firmado, descarga de por web mediante identificación segura, entrega presencial. etc.), al Responsable Técnico que conste en la *Solicitud de Emisión.*

Devolución

La organización dispone de un plazo de 15 días, desde la entrega del certificado, para comprobar el correcto funcionamiento del mismo y en caso de que fuera necesario devolverlo a ANF AC.

Si la devolución se debiese a defectos de funcionamiento por causas técnicas (entre otras, mal funcionamiento del soporte del certificado, problemas de compatibilidad de programas, error técnico en el certificado, etc.) o a errores en los datos contenidos en el certificado, ANF AC revocará el certificado emitido y procederá a emitir un nuevo certificado.

4.4.3 Publicación del certificad

Los certificados se podrán publicar, en todo caso, sin el consentimiento previo de los responsables de certificado.

4.4.4. Notificación de la emisión a tercero

No es aplicable.

4.5. Uso del par de claves y del certificado.

4.5.1. Requisitos generales de uso

Los certificados se utilizarán de acuerdo con su función propia y finalidad establecida, sin que puedan utilizarse en otras funciones y con otras finalidades. De la misma forma, los certificados tendrán que utilizarse únicamente de acuerdo con la ley aplicable, especialmente teniendo en cuenta las restricciones de importación y exportación existentes en cada momento.

Las extensiones Key Usage y Extended KeyUsage se utilizará para establecer límites técnicos a los usos que puede darse a una clave privada correspondiente a una clave pública listada en un certificado X.509 v3.

Los certificados podrán utilizarse con un dispositivo seguro de creación de firma electrónica, que cumpla los requisitos establecidos por el artículo 24 de la Ley 59/2003, de 19 de diciembre, con esta política y con las correspondientes condiciones adicionales.

4.5.2. Uso por los suscriptores

Las subscriptores deberán:

- Proteger sus claves privadas en todo momento, conforme a lo establecido en esta política, y tal y como se estipule en su acuerdo de aceptación del certificado. En especial, los suscriptores de un certificado deben ser

especialmente diligentes en la custodia de su dispositivo seguro de creación de firma, con la finalidad de evitar usos no autorizados.

- Utilizar el par de claves exclusivamente para los usos autorizados reseñados en esta política. Ateniéndose a todos los términos, condiciones y restricciones exigidos en el uso de sus claves privadas y certificados.

- Notificar de forma diligente la sospecha de compromiso de clave o su pérdida. Esta notificación deberá realizarse directamente o indirectamente por mecanismos previstos en la Declaración de Prácticas de Certificación de ANF AC.

El suscriptor genera sus propias claves, se obliga a:

- Generar sus claves de suscriptor utilizando el algoritmo reconocido como aceptable para la firma electrónica reconocida., de los homologados por ANF AC.

- Crear, en su caso, las claves dentro del dispositivo seguro de creación de firma suministrado por ANF AC.

- Utilizar longitudes y algoritmos de clave reconocidos como aceptables para la firma electrónica reconocida.

4.5.3. Uso por un tercero que confía en los certificados

Es obligación de aquellas terceras partes que confían en los certificados emitidos por una Entidad de Certificación tal y como se describe en la presente política:

- Utilizar los certificados para los propósitos para los cuales fueron emitidos, tal y como se detalla en la información del certificado (por ejemplo, lo definido en la extensión "key usage").

- Controlar que cada certificado que se utilice es válido según lo establecido en los estándares X.509 y RFC 5280.

- Establecer la confianza en la Entidad de Certificación que ha emitido el certificado verificando la cadena de certificación de acuerdo con las recomendaciones del estándar X.509 versión 3 y la RFC 5280.

- Utilizar los certificados de Sede Electrónica, emitidos bajo esta política de certificación, sólo para aquellas transacciones que estén sujetas a lo indicado en la Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP) o la Declaración de Prácticas de Certificación de la entidad emisora.

4.6. Renovación de certificados sin renovación de claves.

Cuando se solicite la renovación de un certificado sin renovación del par de claves, la ANC AC previamente a su emisión, determinará que este par de claves aun es criptográficamente confiable. En caso que así se considere, se procederá a verificar que los datos de registro continúan siendo válidos y, si algún dato ha cambiado éste deberá ser verificado, guardado y el suscriptor deberá estar de acuerdo con él, tal y como se especifica en la sección correspondiente de esta política.

Si las condiciones jurídicas de prestación del servicio han variado desde la emisión del certificado, ANF AC informará de este hecho al solicitante.

El procedimiento aplicable a la renovación sin renovación de claves requerirá la recuperación segura de los dispositivos criptográficos donde residen las claves, antes de, en su caso, proceder al borrado seguro del dispositivo y a la nueva generación del certificado.

El procedimiento aplicable a la renovación sin renovación de claves de estos certificados podrá basarse en la existencia previa de un certificado vigente, siempre que el par de claves de este certificado sea criptográficamente fiable para el nuevo plazo de vigencia del nuevo certificado, y que no exista la sospecha del compromiso de la clave privada del suscriptor o del responsable del certificado.

En ANEXO II se incluye formulario de solicitud de Renovación.

4.7. Renovación de certificados con renovación de claves

En el supuesto de que el motivo de la solicitud de renovación sea:

- Claves comprometidas o pérdida de fiabilidad de las mismas.

La renovación se realizará siempre con cambio de claves.

Cuando se solicite la renovación de un certificado con renovación del par de claves, se verificará que los datos de registro continúan siendo válidos y, si algún dato ha cambiado éste deberá ser verificado, guardado y el suscriptor deberá estar de acuerdo con él, tal y como se especifica en la sección correspondiente de esta política.

Si las condiciones jurídicas de prestación del servicio han variado desde la emisión del certificado, ANF AC, o la Autoridad de Registro Reconocida, informará de este hecho al solicitante.

4.8. Tramitación de las peticiones de renovación de certificados con cambio de claves.

El procedimiento aplicable a la renovación del certificado será el mismo que para la emisión de un certificado completamente nuevo.

En cualquier caso la renovación de un certificado está supeditada a:

- Que lo solicite en debido tiempo y forma, siguiendo las instrucciones y normas que se establecen en la DPC de ANF AC.

- Que ANF AC o la AR que intervino en su tramitación de solicitud, no hayan tenido conocimiento cierto de la concurrencia de ninguna causa de revocación del certificado.

- Que la solicitud de renovación de servicios de prestación se refiera al mismo tipo de certificado emitido inicialmente.

4.9. Modificación de certificados.

No está autorizado.

4.10. Revocación y suspensión de certificados.

4.10.1. Causas para la revocación

Además de lo previsto en la Declaración de Prácticas de Certificación, en el caso de certificados del tipo,

- *SSL EV,*
- *Sede EV (en cualquiera de sus niveles de seguridad)*

ANF AC deberá,

1. Presentar al suscriptor, a terceras partes y a los navegadores de Internet instrucciones claras para la presentación de denuncias o sospechas de compromiso de la clave privada, de mal uso de certificados o de otros tipos de fraude, compromiso, mal uso, o conducta impropia en relación con los Certificados.

2. ANF AC investigará los informes de problemas dentro de las veinticuatro horas siguientes a su recepción y decidirá sobre la revocación, como mínimo atendiendo a los siguientes criterios:

- La naturaleza del supuesto problema;
- El número de informes recibidos de problemas de un certificado o página web.
- La identidad de los denunciantes.
- La legislación vigente.

Y como regla general en todos los certificados emitidos en el ámbito de esta Política de Certificación, se procederá a la revocación por:

1. Circunstancias que afecten la información contenida en el certificado

- Modificación de alguno de los datos contenidos en el certificado.
- Descubrimiento que alguno de los datos aportados en la solicitud de certificado es incorrecto, así como la alteración o modificación de las circunstancias verificadas para la expedición del certificado.

- Descubrimiento que alguno de los datos contenidos en el certificado es incorrecto.

2. Circunstancias que afectan la seguridad de la clave o del certificado

- Compromiso de la clave privada o de la infraestructura o sistemas de la Entidad de Certificación que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de este incidente.
- Infracción, por la Entidad de Certificación, de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en la DPC de la Entidad de Certificación.
- Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado del suscriptor o del responsable de certificado.
- Acceso o utilización no autorizada, por un tercero, de la clave privada del suscriptor o del responsable de certificado.
- El uso irregular del certificado por el suscriptor o del responsable de certificado, o falta de diligencia en la custodia de la clave privada.

3. Circunstancias que afectan la seguridad del dispositivo criptográfico

- Compromiso o sospecha de compromiso de la seguridad del dispositivo criptográfico.
- Pérdida o inutilización por daños del dispositivo criptográfico.
- Acceso no autorizado, por un tercero, a los datos de activación del suscriptor o del responsable de certificado.

4. Circunstancias que afectan el suscriptor o responsable del certificado.

- Finalización de la relación entre el suscriptor y el responsable del certificado.
- Modificación o extinción de la relación jurídica subyacente o causa que provocó la emisión del certificado al suscriptor o responsable del certificado.
- Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud de éste.
- Infracción por el suscriptor o responsable del certificado, de sus obligaciones, responsabilidad y garantías, establecidas en el instrumento

jurídico correspondiente o en la Declaración de Prácticas de Certificación de la Entidad de Certificación que le emitió el certificado.

- La incapacidad sobrevenida o la muerte del suscriptor o responsable del certificado.

- La extinción de la persona jurídica suscriptora del certificado, así como la finalidad de la autorización del suscriptor al responsable del certificado o la finalización de la relación entre suscriptor y responsable del certificado.

- Solicitud del suscriptor de revocación del certificado, de acuerdo con lo establecido en la sección 3.4 de esta política.

5. Otras circunstancias:

- La suspensión del certificado digital por un periodo superior al establecido en la sección 1.1.1 y sección 4.9.16 de esta política.

- La finalización del servicio de este prestador de servicios de certificación electrónica, de acuerdo con lo establecido en la sección 5.8 de esta política.

El instrumento jurídico que vincula a la Entidad de Certificación con el suscriptor establecerá que el suscriptor tendrá que solicitar la revocación del certificado en caso de tener conocimiento de alguna de las circunstancias indicadas anteriormente.

4.10.2. Entidad que puede solicitar la revocación

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

Y en general podrán solicitar la revocación de un certificado:

- El suscriptor a cuyo nombre fue emitido el certificado.
- Un representante autorizado por el suscriptor.
- El responsable del certificado
- La Entidad de Registro que tramitó la solicitud del certificado.

4.10.3. Procedimiento de solicitud de revocación

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

La entidad que necesite revocar un certificado tiene que solicitarlo a ANF AC o, en su caso, a la Autoridad de Registro ante la que tramitó la solicitud del certificado.

La solicitud de revocación deberá contener como mínimo la siguiente información:

- Fecha de solicitud de la revocación.
- Identidad del suscriptor.
- Razón detallada para la petición de revocación.
- Nombre y título de la persona que pide la revocación.
- Información de contacto de la persona que pide la revocación.

La solicitud de revocación será procesada a su recepción.

La solicitud tiene que estar autenticada, de acuerdo con los requisitos establecidos en la sección correspondiente de esta política, antes de proceder a la revocación.

ANF AC una vez autenticada la petición, podrá revocar directamente el certificado.

Se informa al suscriptor y, en su caso, al responsable del certificado sobre el cambio de estado del certificado revocado.

ANF AC no reactivará el certificado, una vez revocado.

Todos los certificados revocados se incluirán en todas las publicaciones de las CRL hasta que el periodo de validez de los certificados haya expirado.

Nota: Un certificado revocado no puede volver a utilizarse; esto quiere decir que no puede levantarse la revocación, ni anularse de ninguna otra forma: es un estado definitivo del certificado.

En ANEXO III se incluye formulario de solicitud de Revocación.

Medios de tramitación de la solicitud:

4.10.3.1. Telemático

Accediendo al Área de Gestión de certificados en https://www.anf.es el usuario puede revocar los certificados que ha solicitado o de los que tiene permiso para ello.

4.10.3.2. Telefónico

Mediante llamada telefónica al número de soporte telefónico de la ANF AC 902 902 172.

4.10.3.3. Presencial

Personándose en cualquiera de las oficinas de ANF AC, publicadas en:

http://www.anf.es/anf/corporacion/infraestructura.html

4.10.4. Periodo de gracia de la solicitud de revocación

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

Las solicitudes de revocación se remitirán de forma razonablemente inmediata cuando se tenga conocimiento de la causa de revocación

4.10.5. Plazo máximo de procesamiento de la solicitud de revocación

Las solicitudes de revocación se tramitarán de forma razonablemente inmediata cuando se tenga conocimiento de la causa de revocación y se haya autenticado al solicitante, y comprobado su capacidad de obrar.

4.10.6. Obligación de consulta de información de revocación de certificados

Los terceros que confían deben comprobar el estado de aquellos certificados en los que deseen confiar.

ANF AC pone a disposición de los terceros que confían un servicio de información de estado de los certificados basados en el protocolo OCSP y, al menos, otra forma de acceso y descarga de las listas de certificados revocados (CRL) (en conformidad con el Apartado 2.7 "Esquema Nacional de identificación y firma electrónica de las Administraciones públicas. Bloque III: Propuestas de condiciones generales adicionales en la AGE"). Estos dos métodos están operativos sin coste adicional.

4.10.7. Frecuencia de emisión de listas de revocación de certificados (CRLs)

En cada certificado se especificará la dirección de la CRL que le corresponda, mediante la extensión cRLDistributionPoints.

ANF AC emite una CRL diaria, incluso cuando no haya cambios o actualizaciones, para así asegurar la vigencia de la información publicada (en conformidad con el Apartado 2.7 "Esquema de identificación y firma electrónica de las Administraciones públicas. Bloque III: Propuestas de condiciones generales adicionales en la AGE").

En la CRL se específica el momento programado como límite para la emisión de una nueva CRL.

4.10.8. Periodo máximo de publicación de CRLs

El cambio de estado de la vigencia de un certificado debe indicarse en la CRL transcurridos menos de cinco minutos desde que se produjo dicho cambio (en conformidad con el Apartado 2.7 "Esquema de identificación y firma electrónica de las Administraciones públicas. Bloque III: Propuestas de condiciones generales adicionales en la AGE").

4.10.9. Disponibilidad de servicios de comprobación de estado de certificados.

Los terceros que confían podrán consultar los certificados publicados en el Repositorio de ANF AC, por medio de un servicio de información de estado de los certificados basado en el protocolo OCSP.

4.10.10. Obligación de consulta de servicios de comprobación de estado de certificados

Los terceros que confían deberán comprobar el estado de aquellos certificados en los que deseen confiar.

Una forma por la que se puede verificar el estado de los certificados es consultando la CRL más reciente emitida por la Entidad de Certificación que expidió el certificado en el que se desea confiar.

ANF AC dará soporte a los terceros de confianza en cómo y dónde encontrar los servicios de comprobación de estado de certificados basados en OCSP o la CRL correspondiente (en conformidad con el Apartado 3.2 "Esquema de identificación y firma electrónica de las Administraciones públicas. Bloque III: Propuestas de condiciones generales adicionales en la AGE").

Si por cualquier circunstancia no fuera factible obtener información del estado de un certificado, el sistema que deba utilizarlo deberá desestimar su uso, o en función del riesgo, del grado de responsabilidad y de las consecuencias que se pudieran producir, utilizarlo sin garantizar su autenticidad en los términos y estándares que se recogen en esta política.

4.10.11. Otras formas de información de revocación de certificados

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

4.10.12. Requisitos especiales en caso de compromiso de la clave privada

El compromiso de la clave privada de ANF AC será notificado, en la medida posible, a todos los participantes.

4.10.13. Causas de suspensión de certificados

No autorizado

4.10.14. Legitimación para solicitar la suspensión

No autorizado

4.10.15. Procedimiento de solicitud de suspensión

No autorizado

4.10.16. Periodo máximo de suspensión de un certificado

No autorizado

4.11. Servicios de comprobación de estado de certificados

4.11.1. Características de operación de los servicios

Las CRL serán descargadas desde el Repositorio de ANF AC e instaladas por los terceros de confianza.

De forma alternativa, los verificadores podrán consultar los certificados publicados en el Repositorio de ANF AC, a través de una interfaz web.

4.11.2. Disponibilidad de los servicios

Los sistemas de distribución de CRLs y de consulta en línea del estado de los certificados deberán estar disponibles las 24 horas de los 7 días de la semana.

En caso de fallo de los sistemas de comprobación de estado de certificados por causas fuera del control ANF AC realizará sus mejores esfuerzos para asegurar que este servicio se mantiene inactivo el mínimo tiempo posible. Siendo el periodo máximo de 5 horas en el que el servicio tendrá que volver a operar. Y en caso contrario activará el Plan de Contingencias que prevé una reactivación del servicio en un tiempo máximo de 6 horas.

ANF AC facilitar soporte e información a los terceros de confianza sobre el funcionamiento del servicio de información de estado de certificados

4.12. Finalización de la suscripción

La extinción de la validez de un certificado se produce en los siguientes casos:

- Revocación anticipada del certificado por cualquiera de las causas recogidas en el presente documento.
- Expiración de la vigencia del certificado.

Si no se solicita la renovación del certificado, la extinción de su validez supondrá la extinción

de la relación entre el suscriptor y la Entidad de Certificación.

4.13. Depósito y recuperación de claves.

ANF AC no realiza depósito de claves.

4.14. Caducidad de las claves de certificado de CA.

ANF AC evitará generar certificados que caduquen con posterioridad a los certificados de CA. Para ello no se emitirán cuyo periodo de validez exceda el del certificado de CA en cuestión y se generarán con el nuevo certificado de CA, con el fin de evitar la notificación a los subscriptores para que procedan a la renovación de su certificado, en el supuesto que el certificado de CA caducara con anterioridad.

5. Controles de seguridad física, de gestión y de operaciones

5.1. Controles de Seguridad Física

5.1.1. Ubicación y construcción

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

5.1.2. Acceso físico

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

5.1.3. Alimentación eléctrica y aire acondicionado

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

5.1.4. Exposición al agua

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

5.1.5. Protección y prevención de incendios

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

5.1.6. Sistema de almacenamiento

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

5.1.7. Eliminación de residuos

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

5.1.8. Backup remoto

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

5.2. Controles de procedimientos

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

5.2.1. Papeles de confianza

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

5.2.2. Número de personas requeridas por tarea

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

5.2.3. Identificación y autenticación para cada papel

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

5.3. Controles de seguridad de personal

Este apartado refleja el contenido del documento Controles de Seguridad del Personal de ANF AC.

5.3.1. Requerimientos de antecedentes, calificación, experiencia, y acreditación

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

5.3.2. Procedimientos de comprobación de antecedentes

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

5.3.3. Requerimientos de formación

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

5.3.4. Requerimientos y frecuencia de actualización de la formación

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

5.3.5. Frecuencia y secuencia de rotación de tareas

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

5.3.6. Sanciones por acciones no autorizadas

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

5.3.7. Requerimientos de contratación de personal

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

5.3.8. Documentación proporcionada al personal

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

5.3.9. Controles periódicos de cumplimiento

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

5.3.10. Finalización de los contratos

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

5.4. Procedimientos de Control de Seguridad

5.4.1. Auditorias e incidentes

ANF AC mantiene los siguientes criterios con relación a la información disponible para auditorías y análisis de incidentes que pueda haber con los certificados emitidos y el tratamiento de los mismos. Los usuarios de certificados pueden comunicar a ANF AC quejas o sugerencias a través de los siguientes medios:

- Vía telefónica: 902 902 172
- Vía mail: soporte@anf.es
- Presencial: Dirección de sedes:

  http://www.anf.es/anf/corporacion/infraestructura,html
- Mediante la cumplimentación del formulario disponible en la dirección www.anf.es
- Cumplimentando los formularios de quejas o reclamaciones disponibles en los puestos de registro.

- Existe un registro interno de incidentes que se hayan producido con los certificados emitidos (incidentes de seguridad gestionados por el Comité de Seguridad de ANF AC). Estos incidentes se registran, analizan y solucionan según los procedimientos del SGSI de ANF AC.
- En la planificación anual de auditorías se audita específicamente la operativa de emisión de los certificados con una muestra mínima del 2% de los certificados emitidos.
- En la DPC se define el periodo de conservación de la documentación.

5.4.2. Tipos de eventos registrados

En conformidad con lo especificado en la DPC de ANF AC, este Prestador de Servicios de Certificación guarda registro, al menos, de los siguientes eventos relacionados con la seguridad de la PKI:

- Encendido y apagado de los sistemas.
- Inicio y terminación de la aplicación de autoridad de certificación o de autoridad de registro central.
- Intentos de crear, borrar, cambiar contraseñas o permisos de los usuarios dentro del sistema.
- Generación y cambios en las claves del prestador de servicios de certificación.
- Cambios en las políticas de emisión de certificados.
- Intentos de entrada y salida del sistema.
- Intentos no autorizados de entrada en la red del prestador de servicios de certificación.
- Intentos no autorizados de acceso a los ficheros del sistema.
- Intentos fallidos de lectura en un certificado, y de lectura y escritura en el Repositorio de certificados.
- Eventos relacionados con el ciclo de vida del certificado, como solicitud, emisión, revocación y renovación de un certificado.
- Eventos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación del mismo.

Ya sea manual o electrónicamente, ANF AC guarda la siguiente información:

- La ceremonia de generación de claves y las bases de datos de gestión de claves.
- Los registros de acceso físico.
- Mantenimientos y cambios de configuración del sistema.
- Cambios en el personal.
- Informes de compromisos y discrepancias.

- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal.

- Posesión de datos de activación, para operaciones con la clave privada del prestador de servicios de certificación.

Para todos los eventos identificados en esta sección, el registro de auditoría deberá contener al menos:

- El tipo de evento registrado.
- La fecha y hora en que se ha producido.
- Para los mensajes de las Autoridades de Registro solicitando acciones de la Entidad de

Certificación, la identificación del origen del mensaje, el destinatario y el contenido.

- Para las solicitudes de emisión o revocación de los certificados, un indicador de la concesión o la denegación de la petición.
- Para las acciones realizadas directamente por un operador, la identidad del equipo desde el que se realiza la acción.

5.4.3. Frecuencia de tratamiento de registros de auditoría

Los registros de auditoría se examinan por lo menos una vez a la semana en busca de actividad sospechosa o no habitual.

El procesamiento de los registros de auditoría consiste en una revisión de los registros, verificando que estos no han sido manipulados, una inspección aleatoria de todas las entradas de registro y una investigación más profunda de cualquier alerta o irregularidad en los registros.

Las incidencias detectadas son documentadas, detallando las medidas adoptadas, y el personal implicado en la toma de decisiones.

5.4.4. Periodo de retención para los logs de auditoría

Los registros de auditoría son retenidos en el recinto, después de ser procesados, durante un mínimo de tres meses. A partir de ese momento se archivan de acuerdo con la sección 5.5.2 de esta política.

5.4.5. Protección de los logs de auditoría

Los ficheros de registros, tanto manuales como electrónicos, son protegidos de lecturas, modificaciones, borrados o cualquier otro tipo de manipulación no autorizada, aplicando controles de acceso lógico y físico. Estas medidas de protección imposibilitan la eliminación de los registros de auditoría antes de que haya expirado su periodo de almacenamiento,

5.4.6. Procedimientos de backup de los registros de auditoría

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

5.4.7. Sistema de recogida de información de auditoría (interno vs externo)

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

5.4.8. Notificación al sujeto causa del evento

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

5.4.9. Análisis de vulnerabilidades

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

5.5. Archivo de informaciones y registros

Toda la información relativa a los certificados se guarda durante un período de tiempo apropiado, según lo establecido en la sección 5.5.2 de esta política

5.5.1. Tipo de informaciones y eventos registrados

ANF AC guarda todos los eventos que tengan lugar durante el ciclo de vida de un certificado, incluyendo la renovación del mismo.

El prestador de servicios de certificación tiene que guardar un registro de, al menos, la siguiente información:

- Tipo de documento presentado en la solicitud del certificado.
- Número de identificación único proporcionado por el documento anterior.
- Identidad de la entidad que acepta la solicitud de certificado.
- La ubicación de las copias de solicitudes de certificados y del documento firmado por el suscriptor.
- La documentación relativa a la recepción de dispositivos seguros de creación de firma.

5.5.2. Periodo de retención para el archivo.

ANF AC guarda todos los registros especificados en la sección anterior de esta política sin pérdida, por un periodo de 15 años como mínimo.

5.5.3. Protección del archivo.

ANF AC asume la obligación de:

- Mantener la integridad y la confidencialidad del archivo que contiene los datos referentes a los certificados emitidos.
- Archivar los datos anteriormente citados de forma completa y confidencial.
- Mantener la privacidad de los datos de registro del suscriptor.

5.5.4. Procedimientos de backup del archivo.

ANF AC realiza copias de respaldo incrementales diarias de todos sus documentos electrónicos, según se indica en la sección 5.5.1 de esta política. Debe, además, realizar copias de respaldo completas semanalmente para casos de recuperación de datos, de acuerdo con la sección 5.7 de esta política.

Además, guarda los documentos en papel, según se indica en la sección 5.5.1, en un lugar fuera de sus instalaciones habituales de trabajo para casos de recuperación de datos, de acuerdo con la sección 5.7 de esta política.

5.5.5. Requerimientos para el sellado de tiempo de los registros.

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC y DPC de ANF TSA.

5.5.6. Sistema de recogida de información de auditoría (interno vs externo).

ANF AC dispone de un sistema de mantenimiento de datos de archivo fuera de sus propias instalaciones, tal y como se especifica en la sección 5.5.4 de esta política.

5.5.7. Procedimientos para obtener y verificar información archivada

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

5.6. Renovación de claves de una Entidad de Certificación

La validez del certificado empleado por ANF AC para la emisión de certificados de CAs subordinadas o entidades finales, es superior al periodo de validez de los certificados que emite, de tal manera que no se pueden expedir certificados cuyo periodo de vigencia superen la validez del propio certificado de la CA raíz o CA subordinada.

Tras la renovación de las claves de un certificado de CA, el proceso de renovación de un par de claves de suscriptor será igual que el realizado anteriormente (con las claves antiguas de la CA emisora), tal y como se especifica en la sección 4.7 de esta política.

5.7. Recuperación en caso de compromiso de una clave o de desastre

5.7.1. Alteración de los recursos hardware, software y/o datos

Cuando tenga lugar un evento de corrupción de recursos, aplicaciones o datos se activa un procedimiento que permite iniciar las gestiones necesarias, de acuerdo con el Plan de Seguridad, el Plan de Contingencia y el Plan de Auditoría, o los documentos que los sustituyan, para hacer que el sistema vuelva a su estado normal de funcionamiento.

5.7.2. La clave pública de una entidad se revoca

En caso de revocación de una de las jerarquías de certificación de ANF AC, se llevará a cabo lo siguiente:

- Notificar este hecho, cuando se produzca, a la Administración General del Estado.

- Informar del hecho publicando una CRL, según lo establecido en la sección 4.10.7 de esta política.

- Realizar todos los esfuerzos necesarios para informar de la revocación a todos los suscriptores a los cuales el prestador de servicios de certificación emitió certificados, así como a los terceros que deseen confiar en esos certificados.

- Realizar una renovación de claves, en caso de que la revocación no haya sido debida a la terminación del servicio por parte del prestador de servicios de certificación, según lo establecido en la sección 5.6 de esta política.

Las causas de revocación contempladas en el presente apartado pueden ser por compromiso de clave, por causas técnicas, por razones organizativas o por desastre.

5.7.3. Compromiso de la clave privada de la CA

El plan de continuidad de negocio de ANF AC contempla el compromiso o la sospecha de compromiso de su clave privada como un desastre.

En caso de compromiso, el prestador de servicios de certificación debe realizar como mínimo las siguientes acciones:

- Informar a todos los suscriptores y verificación del compromiso.

- Indicar que los certificados y la información del estado de revocación que han sido entregados usando la clave de este prestador de servicios de certificación ya no son válidos.

5.7.4. Instalación de seguridad después de un desastre natural u otro tipo de desastre

El Plan de Contingencias de ANF AC desarrolla, mantiene, contempla la posibilidad de probar y, si es necesario, ejecutar un plan de emergencia para el caso de que ocurra un desastre, ya sea por causas naturales o causado por el hombre, sobre las instalaciones, el cual indica cómo restaurar los servicios de los sistemas de información.

La ubicación de los sistemas de recuperación de desastres dispone de las protecciones físicas de seguridad detalladas en el Plan de Seguridad.

El Plan de Contingencia de ANF AC establece la capacidad de restaurar la operación normal de los servicios de revocación y, en su caso, de suspensión, en las 24 horas siguientes al desastre, pudiendo, como mínimo, ejecutarse las siguientes acciones:

- Suspensión de certificados.
- En su caso, revocación de certificados.
- Publicación de información de revocación.

La base de datos de recuperación de desastres utilizada por el prestador de servicios de certificación debe estar sincronizada con la base de datos de producción, dentro de los límites temporales especificados en el plan de seguridad del prestador.

Los equipos de recuperación de desastres del prestador de servicios de certificación tienen las medidas de seguridad físicas especificadas en el plan de seguridad

5.8. Cese de una CA

ANF AC manifiesta que las posibles interrupciones a los suscriptores y a terceras partes son mínimas como consecuencia del cese de sus servicios y, en particular, asegurar un mantenimiento continuo de los registros requeridos a fin de proporcionar evidencia de los certificados emitidos y de otros servicios ofrecidos, en caso de investigación civil o criminal.

Antes de terminar sus servicios, ANF AC ejecutará, como mínimo, los siguientes procedimientos:

- Informar a todos los suscriptores y terceros que confían en los certificados que ha emitido.

- Retirar toda autorización de subcontrataciones que actúan en nombre del prestador de servicios de certificación en el proceso de emisión de certificados.

- Ejecutar las tareas necesarias para transferir las obligaciones de mantenimiento de la información de registro y los archivos de registro de eventos durante los períodos de tiempo respectivos indicados al suscriptor y a los terceros que confían en los certificados.

- Destruir las claves privadas del prestador de servicios de certificación o retirarlas del uso.

El prestador de servicios de certificación debe declarar en sus prácticas las previsiones que tiene para el caso de terminación del servicio. Estas deben incluir:

- Notificación a las entidades afectadas.

- Transferencia de las obligaciones del prestador de servicios de certificación a otras personas.

- Cómo se tratará el estado de revocación de los certificados emitidos que aún no han expirado.

6. Controles de seguridad técnica

ANF AC emplea sistemas y productos fiables, que están protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.

Para el desarrollo de su actividad como Prestador de Servicios de Certificación, ANF AC cuenta con un Departamento de I+D+i, y una sección criptográfica que determina el estado de seguridad de todos los elementos criptográficos utilizados en su PKI.

6.1. Generación e Instalación del par de claves

En este punto se hace siempre referencia a las claves generadas para los certificados emitidos bajo el ámbito de la presente Política de Certificación. La información sobre las claves de las entidades que componen la Autoridad de Certificación se encuentra en la Declaración de Prácticas de Certificación (CPS) de ANF AC.

El par de claves para el certificado emitido bajo el ámbito de la presente Política de Certificación, se generan por el propio suscriptor del certificado. ANF AC no tiene acceso en ningún momento a la clave privada del suscriptor.

6.1.2. Entrega de la clave privada a la entidad

No aplicable. ANF AC no genera claves de sus usuarios finales.

6.1.3. Entrega de la clave pública al emisor del certificado

La clave pública a ser certificada es generada por el suscriptor y es entregada a la Autoridad de Certificación mediante el envío de una solicitud de certificación en formato CSR Certificate Signing Request que sigue la especificación PKCS#10.

6.1.4. Entrega de la clave pública de la CA a los usuarios

La clave pública de la CA Raíz y CAs subordinadas están a disposición los terceros que confían en los certificados, asegurando la integridad de la clave y autenticando su origen.

La clave pública del prestador de servicios de certificación raíz se publica en el Repositorio, en forma de certificado autofirmado en el caso de CA Raíz, y certificado emitido por la CA Raíz en caso de CAs subordinadas, junto a una declaración que especifica que la clave autentica a ANF AC.

Se incluyen medidas adicionales para confiar en el certificado autofirmado, como la comprobación de la huella digital del certificado.

Los usuarios pueden acceder al Repositorio para obtener las claves públicas ANF AC.

6.1.5. Tamaño de las claves

El tamaño de las claves para los certificados emitidos bajo el ámbito de la presente Política de Certificación tiene que ser de 1024 bits de longitud mínima y en conformidad con lo reseñado en el Apartado 7.1 de este documento.

6.1.6. Parámetros de generación de la clave pública

Los parámetros de clave pública son generados conforme a PKCS#1, utilizándose como segunda pareja de la clave pública, FERMAT 4. Conforme a las recomendaciones de la RFC 3447 que define el formato de cifrado RSA.

6.1.7. Comprobación de la calidad de los parámetros

Se utilizan los parámetros definidos en la suite criptográfica 001 especificada en el documento de ETSI TS 102 176-1 "Electronic Signatures and Infrastructures (ESI);

Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms". Y se tiene en cuenta el informe ECRYPT2 D.SPA.x *1

*1 D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010), de fecha 30 de marzo de 2010

(http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

6.1.8. Renovación de claves de una Entidad de Certificación

La validez del certificado empleado por ANF AC para la emisión de certificados de CAs subordinadas o entidades finales, es superior al periodo de validez de los certificados que emite, de tal manera que no se pueden expedir certificados cuyo periodo de vigencia superen la validez del propio certificado de la CA raíz o CA subordinada.

Tras la renovación de las claves de un certificado de CA, el proceso de renovación de un par de claves de suscriptor será igual que el realizado anteriormente (con las claves antiguas de la CA emisora), tal y como se especifica en la sección 4.7 de esta política.

6.1.9. Fines del uso del par de claves

Las claves se generan en hardware criptográfico que cumpla los niveles de seguridad indicados en el apartado 6.2.1.

Las claves de firma electrónica de los usuarios finales se generan en dispositivos criptográficos que cumplan los niveles de seguridad indicados en el apartado 6.2.1.

6.2. Protección de la Clave Privada

En este punto se hace siempre referencia a las claves generadas para los certificados emitidos bajo el ámbito de la presente Política de Certificación. La

información sobre las claves de las entidades que componen la Autoridad de Certificación se encuentra en la Declaración de Prácticas de Certificación (CPS) de A NF Autoridad de Certificación.

6.2.1. Estándares para los módulos criptográficos

Los dispositivos empleados en la emisión de los certificados correspondientes a adscritos a esta Política de Certificación deben respetar la especificación ISO 15408 Common Criteria EAL 4+.

6.2.2. Características del servidor bastionado

Los sistemas donde se almacenen las claves privadas deben cumplir una serie de requisitos relativos a la seguridad física y lógica de los mismos. ANF AC podrá, de manera discrecional, solicitar al organismo suscriptor que evidencie los mecanismos utilizados para el bastionado de dichos sistemas.

Se recomienda seguir las guías generadas por el CCN (Centro Criptológico Nacional) dentro de su serie CCN-STIC, orientadas específicamente a garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración.

6.2.3. Control multipersona de la clave privada

Las claves privadas para los certificados emitidos bajo el ámbito de la presente Política de Certificación se encuentran bajo el control exclusivo de una única persona: el responsable del certificado.

Las claves privadas empleadas por ANF AC para la emisión de certificados, requieren la presencia de al menos dos operadores autorizados. Más información en DPC de ANF AC.

6.2.4. Introducción de la clave privada en el módulo criptográfico

Las claves privadas se generan directamente en los módulos criptográficos que están en posesión del titular del certificado, y que es además utilizado como dispositivo de firma.

6.2.5. Método de activación de la clave privada.

La clave privada utilizada por ANF AC para la emisión de certificados, se activa mediante la ejecución del correspondiente procedimiento de inicio seguro del módulo criptográfico, por las personas indicadas en la sección 6.2.2

La clave privada del suscriptor se activa mediante la introducción del PIN en el dispositivo criptográfico o aplicación de firma.

6.2.6. Método de desactivación de la clave privada

Para certificados en tarjeta con la consideración de dispositivo seguro de creación de firma, cuando la misma se retire del dispositivo lector, o la aplicación que la utilice finalice la sesión, será necesaria nuevamente la introducción del PIN.

6.2.7. Método de destrucción de la clave privada

Las claves privadas serán destruidas en una forma que impida su robo, modificación, divulgación no autorizada o uso no autorizado.

6.3. Custodia, copia y recuperación de claves

6.3.1. Política y prácticas de custodia, copia y recuperación de claves

Las claves privadas de la CA Raíz y CAs subordinadas se almacenan en espacios ignífugos y protegidos por controles de acceso físico dual (al menos dos personas simultáneamente).

ANF AC dispone de una copia de seguridad de estas claves, la cual se encuentra custodiada en una caja de seguridad bancaria. El acceso está restringido a personal expresamente autorizado por la Junta Rectora de ANF AC.

La copia de las claves privadas se encuentra almacenada en un módulo hardware de proceso dedicado, y con el nivel de seguridad adecuado para imposibilitar su extracción del dispositivo.

En el caso de los suscriptores, no es posible generar copias de seguridad de las claves y la clave almacenada en el dispositivo (HSM) no puede ser extraída del mismo.

6.3.2. Archivo de la clave privada

Las claves privadas de ANF AC son archivadas al final de su periodo de operación, de forma permanente.

Dado que ANF AC no tiene acceso a las claves privadas de sus usuarios, no es posible archivas estas claves una vez finalizado su periodo de operaciones.

6.3.3. Periodo de uso para las claves públicas y privadas

Los certificados de usuario final emitidos al amparo de la presente política tienen una validez de dos (2) años.

6.4. Otros aspectos de gestión del par de claves

6.4.1. Archivo de la clave pública

ANF AC archivar sus claves públicas, de acuerdo con lo establecido en la sección 5.5 de esta política.

6.4.2. Periodos de utilización de las claves pública y privada

Los periodos de utilización de las claves serán los determinados por la duración del certificado, transcurrido el cual no podrán continuar utilizándose.

Como excepción, la clave privada podrá continuar empleándose para el descifrado de documentos, incluso tras la expiración del certificado.

6.5. Datos de Activación

6.5.1. Generación de los datos de activación

El titular del certificado es el responsable de generar los datos de activación.

6.5.2. Protección de los datos de activación

El responsable del certificado es el responsable de la protección de los datos de activación de su clave privada.

6.5.3. Otros aspectos de los datos de activación

No estipulado.

6.6. Controles de Seguridad informática

6.6.1. Requisitos técnicos específicos de seguridad informática

El acceso los sistemas está limitado a personas debidamente autorizadas. En particular:

- ANF AC cuenta con una Política de Seguridad que permite una administración efectiva del nivel de acceso de los usuarios (operadores, administradores, así como cualquier usuario con acceso directo al sistema) para mantener la seguridad del sistema, incluyendo gestión de cuentas de usuarios, auditoría y modificaciones o denegación de acceso oportunas.

- El acceso a los sistemas de información y aplicaciones se restringe de acuerdo a lo establecido en la política de control de acceso, así como que los sistemas proporcionan los controles de seguridad suficientes para implementar la segregación de funciones, incluyendo la separación de funciones de administración de los sistemas de seguridad y de los operadores. En concreto, el uso de programas de utilidades del sistema estará restringido y estrechamente controlado. Todo ello queda detallado en la DPC y ANEXOS de ANF AC.

- El personal de ANF AC es identificado y reconocido antes de utilizar aplicaciones críticas relacionadas con el ciclo de vida del certificado.

- El personal del prestador será responsable y deberá poder justificar sus actividades, por ejemplo mediante un archivo de eventos.

- Deberá evitarse la posibilidad de revelación de datos sensibles mediante la reutilización de objetos de almacenamiento (por ejemplo ficheros borrados) que queden accesibles a usuarios no autorizados.

- Los sistemas de seguridad y monitorización deben permitir una rápida detección, registro y actuación ante intentos de acceso irregular o no autorizado a sus recursos (por ejemplo, mediante sistema de detección de intrusiones, monitorización y alarma).

- El acceso a los repositorios públicos de la información del prestador (por ejemplo, certificados o información de estado de revocación) deberá contar con un control de accesos para modificaciones o borrado de datos.

6.6.2. Evaluación del nivel de seguridad informática

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

6.7. Controles técnicos del ciclo de vida

6.7.1. Controles de desarrollo de sistemas

ANF AC realiza análisis de requisitos de seguridad durante las fases de diseño y especificación de requisitos de cualquier componente empleado en las aplicaciones de esta PKI, a fin de garantizar que los sistemas son seguros.

Se emplean procedimientos de control de cambios para las nuevas versiones, actualizaciones y parches de emergencia, de dichos componentes.

6.7.2. Controles de gestión de seguridad

ANF AC mantiene un inventario de todos los activos de información y realizará una clasificación de los mismos, de acuerdo con sus necesidades de protección, coherente con el análisis de riesgos efectuado.

La configuración de los sistemas se auditará de forma periódica, de acuerdo con lo establecido en la sección 9.1 de esta política.

Se realiza un seguimiento de las necesidades de capacidad, y se planificarán procedimientos para garantizar suficiente disponibilidad electrónica y de almacenamiento para los activos informativos.

6.8. Controles de seguridad de red

El acceso a las diferentes redes de ANF AC está limitado a personal debidamente autorizado. En particular:

- Se implementan controles para proteger la red interna de dominios externos accesibles por terceras partes. Los cortafuegos están configurados de forma que se

impiden accesos y protocolos que no sean necesarios para las operaciones de servicio.

- Los datos sensibles son cifrados cuando se intercambian a través de redes no seguras (incluyendo como tales los datos de registro del suscriptor).

- Se garantiza que los componentes locales de red están ubicados en entornos seguros, así como la auditoría periódica de sus configuraciones.

6.9. Controles de seguridad de los módulos criptográficos

Las claves de la CA Raíz y CAs Subordinadas son generadas en dispositivos criptográficos seguros, operados por personal de confianza y en un entorno seguro bajo control dual (al menos dos personas simultáneamente).

Estos dispositivos cumplen los estándares criptográficos de seguridad, que se han indicado en las secciones anteriores.

Los algoritmos de generación de claves están aceptados para el uso de la clave a que estén destinados (en conformidad con los diferentes tipos de certificados que se definen).

7. Perfiles de certificados y listas de certificados revocados

Usos previstos: firma, cliente ssl, s/mime, scl, vpn, cifrado (sin recuperación de claves).

7.1. Perfil de Certificado

El certificado incorpora información estructurada conforme con el estándar X.509 v3 de la IETF, tal y como se especifica en la norma RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL).

Los certificados que son emitidos con la calificación de Certificados Electrónicos Reconocidos (cualificados), cumplen los estándares:

- ETSI TS 101 862 v.1.2: Qualified Certificate Profile
- RFC 3739 Internet X.509 Public Key Infrastructure: Qualified Certificates Profile

Dentro de los certificados existen campos comunes a los ya estandarizados, ej: commonName (cuyo objectId es 2.5.4.3) o serialNumber (cuyo objectId es 2.5.4.5). También incluyen un conjunto de campos "propietarios" llamados Identidad Administrativa, la cual aporta información relativa del suscriptor, o del representante legal, o del responsable del certificado, o de todos ellos. Toda esta información se almacena dentro de un único campo: SubjectAlternativeName.

Para el objeto Identidad Administrativa, al tratarse de un conjunto de campos propietarios, se han asignado ObjectIds unívocos a nivel internacional. Concretamente:

> Los campos referenciados con el OID 1.3.6.1.4.1.18332.x.x.*1, son extensiones propietarias de ANF AC. Los campos con el ISO/IANA del MPR 2.16.724.1.3.5.xx*1, son extensiones propietarias requeridas en el Esquema de identificación y firma electrónica v.1.7.6 publicado por el Consejo Superior de Administración Electrónica.

Dentro de los certificados además de los campos comunes ya estandarizados, p.ej: commonName (cuyo objectId es 2.5.4.3) o serialNumber (cuyo objectId es 2.5.4.5). También incluyen un conjunto de campos "propietarios" asociados al

objeto Identidad Administrativa, la cual aporta información relativa del suscriptor, o del representante legal, o del responsable del certificado, o de todos ellos. Toda esta información se almacena dentro de un único campo: SubjectAlternativeName.

Los certificados que son expedidos con la calificación de reconocidos están identificados en la extensión OID 1.3.6.1.5.5.7.1.3 que indica la existencia de una lista de "QCStatements", conforme al ETSI TS 101 862 v.1.2.1. Concretamente:

- La inclusión 0.4.0.1862.1.1. del valor « QcCompliance» establece la calificación con la que se ha realizado la emisión «Certificado reconocido»
- Los certificados cuyo soporte es un dispositivo hardware criptográficos (HSM) tienen activada la extensión "QcSSCD" , el valor es «QCWithSSCD»
- La inclusión del valor «QCForLegalPerson» identifica «Certificado expedido a una persona jurídica».
- Qualified Certificate Policy (QCP) contiene los OID de las Políticas a las que se somete el certificado. Y en la extensión CertificatePolicies en los campos "Policy Identifier" y "Policy Qualifier ID"
- QcEuRetentionPeriod: determina el periodo de conservación de toda la información relevante para el uso de un certificado, tras la caducidad de este. En el caso de ANF AC, es de 15 años.
- QcLimitValue: Informa del límite monetario que asume la CA como responsabilidad en la pérdida de transacciones a ella imputables. Además en el caso de ANF AC, este valor de límite de responsabilidad se incluye en la extensión propietaria del OID 1.3.6.1.4.1.18332.40.1.

Además en la extensión CertificatePolicies "User Notice" se específica si el certificado es emitido con la calificación de reconocido, y en caso de tratarse de un perfil de certificado de Administración Pública especifica el nivel de seguridad, medio o alto.

Periodo de validez del certificado, esta reseñado en Tiempo Coordinado Universal, y codificado conforme a la RFC 3280.

La Clave pública del Sujet, está codificada de acuerdo con RFC 5280.

La Firma, generada y codificada de acuerdo con RFC 5280.

*[1] http://www.oid-info.com/get/

7.1.1. Certificado Servidor Seguro SSL

Perfil del Certificado de Servidor Seguro SSL		
Campos de X509v1		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
1. Versión	V3	
2. Serial Number	Número secuencial único.	
3. Signature Algorithm	SHA1WithRSAEncryption	
4. Issuer (emisor)	Igual al campo subject del certificado de la CA emisora	
5. Validez NotBefore notAfter	2 años Válido desde Válido hasta	
6. Subject	CN = Dominio DNS OU = **Certificado Servidor Seguro SSL** O = Nombre de la organización L = Localidad ST = Provincia C = País (Código de país de dos dígitos según ISO 3166-1). serialNumber = Cédula Identificación Fiscal	

7. Subject Public Key Info OID 1.3.14.3.2.26	Algoritmo: RSA Encryption Longitud clave: 1024 mínimo	
Campos de X509v3		
1. Subject Key Identifier	Derivada de utilizar la función de hash sobre la clave pública del sujeto	**NO**
2. Authority Key Identifier	Derivada de utilizar la función de hash sobre la clave pública de la CA emisora	**NO**
3. KeyUsage	Digital Signature = 1	**SI**
	Non Repudiation *[1] = 0	
	Key Encipherment = 1	
	Data Encipherment = 0	
	Key Agreement = 1	
	Key Certificate Signature = 0	
	CRL Signature = 0	
4. extKeyUsage	Autenticación TLS webServer	**SI**
5. Certificate Policies Policy Identifier Policy Qualifier ID Policy CPS Location userNotice	 1.3.6.1.4.1.18332.55.4.1 1.3.6.1.4.1.18332.55.1.1 https://www.anf.es/AC/documentos/ Este es un certificado reconocido de Servidor Seguro SSL. ANF Autoridad de Certificación es un emisor de certificados electrónicos reconocidos, conforme a lo establecido en la Ley 29/2003 de firma electrónica de España. Consulte las condiciones de uso en URL de la DPC	**NO**

6. Subject Alternate Names	Dirección email según RFC 822 dnsName = Nombre de Dominio DNS	**NO**
Directory Name	**Identidad Administrativa**	
1.3.6.1.4.1.18332.29.1.	Nombre del responsable del certificado	
1.3.6.1.4.1.18332.29.2.	Primer Apellido del Responsable del Certificado	
1.3.6.1.4.1.18332.29.3.	Segundo Apellido del Responsable del Certificado	
1.3.6.1.4.1.18332.29.4.	Cédula de Identificación Personal Responsable	
1.3.6.1.4.1.18332.29.5.	Correo electrónico del Responsable del Certificado	
1.3.6.1.4.1.18332.29.7.	Departamento al que está adscripto Responsible	
1.3.6.1.4.1.18332.10.1.	Nombre del Representante legal	
1.3.6.1.4.1.18332.10.2.	Primer del Representante legal	
1.3.6.1.4.1.18332.10.3.	Segundo Apellido del Representante legal	
1.3.6.1.4.1.18332.10.4.	Cédula de Identificación Personal Representante legal	
1.3.6.1.4.1.18332.10.5.	Titulo acreditativo del Representante legal	
1.3.6.1.4.1.18332.10.6.	Si la capacidad es mancomunada	
1.3.6.1.4.1.18332.10.7.	Dirección correo electrónico	
7. Issuer Alternate Names	Igual a la extensión subjectAltName del certificado de la CA emisora	
. dNSName	URL dominio organización	**NO**
. rfc822Name	Correo electrónico de contacto de la Entidad de Certificación emisora	

8. Basic Constraints Entidad final	CA: FALSE	**SI**
9. CRLDistributionPoints	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=https://www.anf.es/anf/certificacion/certificados-electonicos/gestion/200.1.33.html [2]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=https://crl.anf.es/AC/ANFServerCA.crl	**NO**
10. Auth. Information Access authorityInfoAccess	http://ocsp.anf.es:8094	**NO**
11. QcStatements QcRetentionPeriod *OID 0.4.0.1862.1.3* QcCompliance *OID 0.4.0.1862.1.1* QcLimitValue *OID 0.4.0.1862.1.2*	15 años Certificado reconocido Importe límite de responsabilidad asumido por el emisor	**NO**
12. Subject	Street = Calle y número (opcional) postalCode = Código Postal (opcional) serialNumber = Cédula Identificación Fiscal entidad GivenName = Nombre del Responsable del Certificado. (como constan en el DNI) SurName = Apellidos del Responsable del	**NO**

	Certificado. (como constan en el DNI) T, Title = Cargo del Responsable del Certificado. EmailAddress (EA) = Dirección correo del titular del certificado	
13. dNSName	Dominio DNS	

*[1] Non Repudiation (Content Commitment)

7.1.2. Certificado de Servidor Seguro SSL con EV (con SHA-1)

Perfil del Certificado de Servidor Seguro SSL con EV		
Campos de X509v1		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
1. Versión	V3	
2. Serial Number	Número secuencial único.	
3. Signature Algorithm	SHA1WithRSAEncryption	
4. Issuer (emisor)	Igual al campo subject del certificado de la CA emisora	
5. Validez NotBefore notAfter	2 años Válido desde Válido hasta	
6. Subject	CN = Dominio DNS OU = Certificado Servidor Seguro SSL con EV O = Nombre de la organización L = Localidad ST = Provincia C = País (Código de país de dos dígitos según ISO 3166-1).	

7. Subject Public Key Info OID 1.3.14.3.2.26	Algoritmo: RSA Encryption Longitud clave: 1024 mínimo	
Campos de X509v3		
1. Subject Key Identifier	Derivada de utilizar la función de hash sobre la clave pública del sujeto	**NO**
2. Authority Key Identifier	Derivada de utilizar la función de hash sobre la clave pública de la CA emisora	**NO**
3. KeyUsage	Digital Signature = 1	**SI**
	Non Repudiation *[1] = 0	
	Key Encipherment = 1	
	Data Encipherment = 0	
	Key Agreement = 1	
	Key Certificate Signature = 0	
	CRL Signature = 0	
4. extKeyUsage	Autenticación TLS webServer	**SI**
5. Certificate Policies Policy Identifier Policy Qualifier ID Policy CPS Location userNotice	 1.3.6.1.4.1.18332.55.4.1 1.3.6.1.4.1.18332.55.1.1 https://www.anf.es/AC/documentos/ Este es un certificado reconocido de Servidor Seguro SSL con EV. ANF Autoridad de Certificación es un emisor de certificados electrónicos reconocidos, conforme a lo establecido en la Ley 29/2003 de firma electrónica de España. Consulte las condiciones de uso en URL de	**NO**

	la DPC	
6. Subject Alternate Names	CN = Dominio DNS Dirección email según RFC 822	**NO**
Directory Name 1.3.6.1.4.1.18332.29.1. 1.3.6.1.4.1.18332.29.2. 1.3.6.1.4.1.18332.29.3. 1.3.6.1.4.1.18332.29.4. 1.3.6.1.4.1.18332.29.5. 1.3.6.1.4.1.18332.29.7.	**Identidad Administrativa** Nombre del responsable del certificado Primer Apellido del Responsable del Certificado Segundo Apellido del Responsable del Certificado Cédula de Identificación Personal Responsable Correo electrónico del Responsable del Certificado Departamento al que está adscripto Responsable	
1.3.6.1.4.1.18332.10.1. 1.3.6.1.4.1.18332.10.2. 1.3.6.1.4.1.18332.10.3. 1.3.6.1.4.1.18332.10.4. 1.3.6.1.4.1.18332.10.5. 1.3.6.1.4.1.18332.10.6. 1.3.6.1.4.1.18332.10.7.	Nombre del Representante legal Primer del Representante legal Segundo Apellido del Representante legal Cédula de Identificación Personal Representante legal Titulo acreditativo del Representante legal Si la capacidad es mancomunada Dirección correo electrónico	
7. Issuer Alternate Names . dNSName . rfc822Name	Igual a la extensión subjectAltName del certificado de la CA emisora URL dominio organización Correo electrónico de contacto de la Entidad de Certificación emisora	**NO**

8. Basic Constraints Entidad final	CA: FALSE	**SI**
9. CRLDistributionPoints	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=https://www.anf.es/anf/certificacion/certificados-electonicos/gestion/200.1.33.html [2]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=https://crl.anf.es/AC/ANFServerCA.crl	**NO**
10. Auth. Information Access authorityInfoAccess	http://ocsp.anf.es:8094	**NO**
11. QcStatements QcRetentionPeriod *OID 0.4.0.1862.1.3* QcCompliance *OID 0.4.0.1862.1.1* QcLimitValue *OID 0.4.0.1862.1.2*	15 años Certificado reconocido Importe límite de responsabilidad asumido por el emisor	**NO**
12. Subject Directory Attributes	Street = Calle y número (opcional) postalCode = Código Postal (opcional) serialNumber = Cédula Identificación Fiscal entidad GivenName = Nombre del Responsable del Certificado. (como constan en el DNI)	**NO**

	SurName = Apellidos del Responsable del Certificado. (como constan en el DNI) T, Title = Cargo del Responsable del Certificado. EmailAddress (EA) = Dirección correo del titular certificado	
13. businessCategory	[OID.2.5.4.15] Valores posibles: -"PrivateOrganization" para Organización privada -"GovernmentEntity" para Entidad pública -"Business Entity" para Empresa -"Non-comercial Entity" para Entidad no comercial	**NO**
14. jurisdictionOfIncorporationLocalityName	[OID: 1.3.6.1.4.1.311.60.2.1.1] Localidad en la que está registrada la empresa (Opcional)	**NO**
15. jurisdictionOfIncorporationStateOrProvinceName	[OID: 1.3.6.1.4.1.311.60.2.1.2] Provincia en la que está registrada la empresa	**NO**
16. jurisdictionOfIncorporationCountryName	[OID: 1.3.6.1.4.1.311.60.2.1.3] País en el que está registrada la empresa	**NO**
17. dNSName	Dominios DNS adicionales (Opcional)	**NO**

*[1] Non Repudiation (Content Commitment)

7.1.3. Certificado de Servidor Seguro SSL con EV (SHA-256)

Perfil del Certificado de Servidor Seguro SSL con EV		
Campos de X509v1		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
1. Versión	V3	
2. Serial Number	Número secuencial único.	
3. Signature Algorithm	sha256WithRSAEncryption	
4. Issuer (emisor)	Igual al campo subject del certificado de la CA emisora	
5. Validez notBefore notAfter	2 años Válido desde Válido hasta	
6. Subject	CN = Dominio DNS OU = Certificado Servidor Seguro SSL con EV O = Nombre de la organización L = Localidad ST = Provincia C = País (Código de país de dos	

	dígitos según ISO 3166-1).	
7. Subject Public Key Info OID 1.3.14.3.2.26	Algoritmo: RSA Encryption Longitud clave: 2048 mínimo	
Campos de X509v3		
1. Subject Key Identifier	Derivada de utilizar la función de hash sobre la clave pública del sujeto	**NO**
2. Authority Key Identifier	Derivada de utilizar la función de hash sobre la clave pública de la CA emisora	**NO**
3. KeyUsage	Digital Signature = 1	**SI**
	Non Repudiation *[1] = 0	
	Key Encipherment = 1	
	Data Encipherment = 0	
	Key Agreement = 1	
	Key Certificate Signature = 0	
	CRL Signature = 0	
4. extKeyUsage	Autenticación TLS webServer	**SI**
5. Certificate Policies Policy Identifier Policy Qualifier ID Policy CPS Location userNotice	 1.3.6.1.4.1.18332.55.4.1 1.3.6.1.4.1.18332.55.1.1 https://www.anf.es/AC/documentos/ Este es un certificado reconocido de Servidor Seguro SSL con EV. ANF Autoridad de Certificación es un emisor de certificados electrónicos reconocidos, conforme a lo establecido en la Ley	**NO**

	29/2003 de firma electrónica de España. Consulte las condiciones de uso en la CPS.	
6. Subject Alternate Names	CN = Dominio DNS Dirección email según RFC 822	**NO**
Directory Name 1.3.6.1.4.1.18332.29.1. 1.3.6.1.4.1.18332.29.2. 1.3.6.1.4.1.18332.29.3. 1.3.6.1.4.1.18332.29.4. 1.3.6.1.4.1.18332.29.5. 1.3.6.1.4.1.18332.29.7.	**Identidad Administrativa** Nombre del responsable del certificado Primer Apellido del Responsable del Certificado Segundo Apellido del Responsable del Certificado Cédula de Identificación Personal Responsable Correo electrónico del Responsable del Certificado Departamento al que está adscripto Responsable	
1.3.6.1.4.1.18332.10.1. 1.3.6.1.4.1.18332.10.2. 1.3.6.1.4.1.18332.10.3. 1.3.6.1.4.1.18332.10.4. 1.3.6.1.4.1.18332.10.5. 1.3.6.1.4.1.18332.10.6. 1.3.6.1.4.1.18332.10.7.	Nombre del Representante legal Primer del Representante legal Segundo Apellido del Representante legal Cédula de Identificación Personal Representante legal Titulo acreditativo del Representante legal Si la capacidad es mancomunada Dirección correo electrónico	
7. Issuer Alternate Names . dNSName . rfc822Name	Igual a la extensión subjectAltName del certificado de la CA emisora URL dominio organización Correo electrónico de contacto de la	**NO**

	Entidad de Certificación emisora	
8. Basic Constraints Entidad final	CA: FALSE	**SI**
9. CRLDistributionPoints	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=https://www.anf.es/anf/certificacion/certificados-electonicos/gestion/200.1.33.html [2]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=https://crl.anf.es/AC/ANFServerCA.crl	**NO**
10. Auth. Information Access authorityInfoAccess	http://ocsp.anf.es:8094	**NO**
11. QcStatements QcRetentionPeriod *OID 0.4.0.1862.1.3* QcCompliance *OID 0.4.0.1862.1.1* QcLimitValue *OID 0.4.0.1862.1.2*	15 años Certificado reconocido Importe límite de responsabilidad asumido por el emisor	**NO**
12. Subject	Street = Calle y número (opcional) postalCode = Código Postal (opcional) serialNumber = Cédula Identificación Fiscal entidad GivenName = Nombre del Responsable del Certificado. (como constan en el DNI)	**NO**

	SurName = Apellidos del Responsable del Certificado. (como constan en el DNI) T, Title = Cargo del Responsable del Certificado. EmailAddress (EA) = Dirección correo del titular	
13. businessCategory	[OID.2.5.4.15] Valores posibles: -"PrivateOrganization" para Organización privada -"GovernmentEntity" para Entidad pública -"Business Entity" para Empresa -"Non-comercial Entity" para Entidad no comercial	**NO**
14. jurisdictionOfIncorporationLocalityName	[OID: 1.3.6.1.4.1.311.60.2.1.1] Localidad en la que está registrada la empresa (Opcional)	**NO**
15. jurisdictionOfIncorporationStateOrProvinceName	[OID: 1.3.6.1.4.1.311.60.2.1.2] Provincia en la que está registrada la empresa	**NO**
16. jurisdictionOfIncorporationCountryName	[OID: 1.3.6.1.4.1.311.60.2.1.3] País en el que está registrada la empresa	**NO**
17. dNSName	Dominios DNS adicionales (Opcional)	**NO**

*[1] Non Repudiation (Content Commitment)

7.1.4. Certificado de Sede Electrónica

Perfil del Certificado de Sede Electrónica		
Campos de X509v1		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
1. Versión	V3	
2. Serial Number	Número secuencial único.	
3. Signature Algorithm	SHA1WithRSAEncryption	
4. Issuer (emisor)	Igual al campo subject del certificado de la CA emisora	
5. Validez notBefore notAfter	2 años Válido desde Válido hasta	
6. Subject	CN = Dominio DNS OU = Sede Electrónica O = Entidad suscriptora L = Localidad ST = Provincia C = País (Código de país de dos dígitos según ISO 3166-1). serialNumber = Cédula Identificación Fiscal	

7. Subject Public Key Info OID 1.3.14.3.2.26	Algoritmo: RSA Encryption Longitud clave: 1024 mínimo	
Campos de X509v3		
1. Subject Key Identifier	Derivada de utilizar la función de hash sobre la clave pública del sujeto	**NO**
2. Authority Key Identifier	Derivada de utilizar la función de hash sobre la clave pública de la CA emisora	**NO**
3. KeyUsage	Digital Signature = 1	**SI**
	Non Repudiation *[1] = 0	
	Key Encipherment = 1	
	Data Encipherment = 0	
	Key Agreement = 1	
	Key Certificate Signature = 0	
	CRL Signature = 0	
4. extKeyUsage	Autenticación TLS webServer	**SI**
5. Certificate Policies Policy Identifier Policy Qualifier ID Policy CPS Location userNotice	 1.3.6.1.4.1.18332.55.4.1 1.3.6.1.4.1.18332.55.1.1 https://www.anf.es/AC/documentos/ Certificado reconocido de sede electrónica, nivel medio. ANF Autoridad de Certificación es un emisor de certificados electrónicos reconocidos, conforme a lo establecido en la Ley 29/2003 de firma electrónica de España. Consulte las condiciones de uso en URL de la DPC	**NO**

6. Subject Alternate Names	CN = Dominio DNS Dirección email según RFC 822	**NO**
Directory Name *Tipo de certificado* **OID:** **2.16.724.1.3.5.1.2.1** *Nombre entidad suscriptora* **OID:** **2.16.724.1.3.5.1.2.2** *NIF entidad suscriptora* **OID:** **2.16.724.1.3.5.1.2.3** *Nombre descriptivo sede* **OID:** **2.16.724.1.3.5.1.2.4** *Denominación dominio* **OID:** **2.16.724.1.3.5.1.2.5**	***Identidad Administrativa*** Sede Electrónica Propietaria del certificado NIF Célula FIscal Breve descripción de la Sede indicando un nombre Dominio al que pertenece la Sede	
1.3.6.1.4.1.18332.29.1. 1.3.6.1.4.1.18332.29.2. 1.3.6.1.4.1.18332.29.3. 1.3.6.1.4.1.18332.29.4. 1.3.6.1.4.1.18332.29.5. 1.3.6.1.4.1.18332.29.7.	Nombre del responsable del certificado Primer Apellido del Responsable del Certificado Segundo Apellido del Responsable del Certificado Cédula de Identificación Personal Responsable Correo electrónico del Responsable del Certificado Departamento al que está adscripto Responsable	
1.3.6.1.4.1.18332.10.1.	Nombre del Representante legal	

1.3.6.1.4.1.18332.10.2. 1.3.6.1.4.1.18332.10.3. 1.3.6.1.4.1.18332.10.4. 1.3.6.1.4.1.18332.10.5. 1.3.6.1.4.1.18332.10.6. 1.3.6.1.4.1.18332.10.7.	Primer del Representante legal Segundo Apellido del Representante legal Cédula de Identificación Personal Representante legal Titulo acreditativo del Representante legal Si la capacidad es mancomunada Dirección correo electrónico	
7. Issuer Alternate Names . dNSName . rfc822Name	Igual a la extensión subjectAltName del certificado de la CA emisora URL dominio organización Correo electrónico de contacto de la Entidad de Certificación emisora	**NO**
8. Basic Constraints Entidad final	CA: FALSE	**SI**
9. CRLDistributionPoints	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=https://www.anf.es/anf/certificacion/certificados-electonicos/gestion/200.1.33.html [2]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=https://crl.anf.es/AC/ANFServerCA.crl	**NO**
10. Auth. Information Access authorityInfoAccess	http://ocsp.anf.es:8094	**NO**

11. QcStatements QcCompliance *OID 0.4.0.1862.1.1* QcLimitValue *OID 0.4.0.1862.1.2* QcRetentionPeriod *OID 0.4.0.1862.1.3* QCForLegalPerson	 Certificado reconocido Importe límite de responsabilidad asumido por el emisor 15 años Certificado emitido a persona jurídica	**NO**
12. Subject	Street = Calle y número (opcional) postalCode = Código Postal (opcional) serialNumber = Cédula Identificación Fiscal titular. GivenName = Nombre del Responsable del Certificado (como constan en el DNI) SurName = Nombre del Responsable del Certificado (como constan en el DNI) T, Title = Cargo Nombre del Responsable del Certificado EmailAddress (EA) = Dirección correo electrónico organización	**NO**
13. dNSName	Dominio DNS	

*[1] Non Repudiation (Content Commitment)

7.1.5. Certificado de Sede Electrónica con EV (SHA-1)

Perfil del Certificado de Sede Electrónica con EV		
Campos de X509v1		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
1. Versión	V3	
2. Serial Number	Número secuencial único.	
3. Signature Algorithm	SHA1WithRSAEncryption	
4. Issuer (emisor)	Igual al campo subject del certificado de la CA emisora	
5. Validez notBefore notAfter	2 años Válido desde Válido hasta	
6. Subject	CN = Dominio DNS OU = Sede Electrónica con EV O = Entidad suscriptora L = Localidad ST = Provincia C = País (Código de país de dos dígitos según ISO 3166-1).	
7. Subject Public Key Info	Algoritmo: RSA Encryption Longitud clave: 1024 mínimo	

Campos de X509v3		
1. Subject Key Identifier	Derivada de utilizar la función de hash sobre la clave pública del sujeto	**NO**
2. Authority Key Identifier	Derivada de utilizar la función de hash sobre la clave pública de la CA emisora	**NO**
3. KeyUsage	Digital Signature = 1	**SI**
	Non Repudiation *[1] = 0	
	Key Encipherment = 1	
	Data Encipherment = 0	
	Key Agreement = 1	
	Key Certificate Signature = 0	
	CRL Signature = 0	
4. extKeyUsage	Autenticación TLS webServer	**SI**
5. Certificate Policies Policy Identifier Policy Qualifier ID Policy CPS Location userNotice	 1.3.6.1.4.1.18332.55.4.1 1.3.6.1.4.1.18332.55.1.1 https://www.anf.es/AC/documentos/ Certificado reconocido de sede electrónica, nivel medio. ANF Autoridad de Certificación es un emisor de certificados electrónicos reconocidos, conforme a lo establecido en la Ley 29/2003 de firma electrónica de España. Consulte las condiciones de uso en URL de la DPC	**NO**
6. Subject Alternate Names	CN = Dominio DNS Dirección email según RFC 822	**NO**

Directory Name *Tipo de certificado* **OID: 2.16.724.1.3.5.1.1.1** *Nombre entidad suscriptora* **OID: 2.16.724.1.3.5.1.1.2** *NIF entidad suscriptora* **OID: 2.16.724.1.3.5.1.1.3** *Nombre descriptivo sede* **OID: 2.16.724.1.3.5.1.1.4** *Denominación dominio* **OID: 2.16.724.1.3.5.1.1.5**	***Identidad Administrativa*** Sede Electrónica Propietaria del certificado NIF Célula Fiscal Breve descripción de la Sede indicando un nombre Dominio al que pertenece la Sede	
1.3.6.1.4.1.18332.29.1. 1.3.6.1.4.1.18332.29.2. 1.3.6.1.4.1.18332.29.3. 1.3.6.1.4.1.18332.29.4. 1.3.6.1.4.1.18332.29.5. 1.3.6.1.4.1.18332.29.7.	Nombre del responsable del certificado Primer Apellido del Responsable del Certificado Segundo Apellido del Responsable del Certificado Cédula de Identificación Personal Responsable Correo electrónico del Responsable del Certificado Departamento al que está adscripto Responsable	
1.3.6.1.4.1.18332.10.1. 1.3.6.1.4.1.18332.10.2. 1.3.6.1.4.1.18332.10.3. 1.3.6.1.4.1.18332.10.4. 1.3.6.1.4.1.18332.10.5. 1.3.6.1.4.1.18332.10.6.	Nombre del Representante legal Primer del Representante legal Segundo Apellido del Representante legal Cédula de Identificación Personal Representante legal Titulo acreditativo del Representante legal Si la capacidad es mancomunada	

1.3.6.1.4.1.18332.10.7.	Dirección correo electrónico	
7. Issuer Alternate Names . dNSName . rfc822Name	Igual a la extensión subjectAltName del certificado de la CA emisora URL dominio organización Correo electrónico de contacto de la Entidad de Certificación emisora	**NO**
8. Basic Constraints Entidad final	CA: FALSE	**SI**
9. CRLDistributionPoints	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=https://www.anf.es/anf/certificacion/certificados-electonicos/gestion/200.1.33.html [2]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=https://crl.anf.es/AC/ANFServerCA.crl	**NO**
10. Auth. Information Access authorityInfoAccess	http://ocsp.anf.es:8094	**NO**
11. QcStatements QcCompliance *OID 0.4.0.1862.1.1* QcLimitValue *OID 0.4.0.1862.1.2* QcRetentionPeriod *OID 0.4.0.1862.1.3* **QCForLegalPerson**	Certificado reconocido Importe límite de responsabilidad asumido por el emisor 15 años Certificado emitido a persona jurídica	**NO**

12. Subject	Street = Calle y número (opcional) postalCode = Código Postal (opcional) serialNumber = Cédula Identificación Fiscal titular GivenName = Nombre del Responsable del Certificado (como constan en el DNI) SurName = Nombre del Responsable del Certificado (como constan en el DNI) T, Title = Nombre del Responsable del Certificado EmailAddress (EA) = Dirección correo electrónico organización	**NO**
13. businessCategory	[OID.2.5.4.15] Valores posibles: -"PrivateOrganization" para Organización privada -"GovernmentEntity" para Entidad pública -"Business Entity" para Empresa -"Non-comercial Entity" para Entidad no comercial	**NO**
14. jurisdictionOfIncorporationLocalityName	[OID: 1.3.6.1.4.1.311.60.2.1.1] Localidad en la que está registrada la empresa (Opcional)	**NO**
15. jurisdictionOfIncorporationStateOrProvinceName	[OID: 1.3.6.1.4.1.311.60.2.1.2] Provincia en la que está registrada la empresa	**NO**
16. jurisdictionOfIncorporationCountryName	[OID: 1.3.6.1.4.1.311.60.2.1.3] País en el que está registrada la empresa	**NO**
17. dNSName	Dominios DNS adicionales (Opcional)	**NO**

*[1] Non Repudiation (Content Commitment)

7.1.6. Certificado de Sede Electrónica con EV (SHA-256)

Perfil del Certificado de Sede Electrónica con EV		
Campos de X509v1		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
1. Versión	V3	
2. Serial Number	Número secuencial único.	
3. Signature Algorithm	SHA256WithRSAEncryption	
4. Issuer (emisor)	Igual al campo subject del certificado de la CA emisora	
5. Validez notBefore notAfter	2 años Válido desde Válido hasta	
6. Subject	CN = Dominio DNS OU = Sede Electrónica O = Entidad suscriptora L = Localidad ST = Provincia C = País (Código de país de dos dígitos según ISO 3166-1).	
7. Subject Public Key Info OID 1.3.14.3.2.26	Algoritmo: RSA Encryption Longitud clave: 2048 mínimo	

Campos de X509v3		
1. Subject Key Identifier	Derivada de utilizar la función de hash sobre la clave pública del sujeto	**NO**
2. Authority Key Identifier	Derivada de utilizar la función de hash sobre la clave pública de la CA emisora	**NO**
3. KeyUsage	Digital Signature = 1	**SI**
	Non Repudiation *[1] = 0	
	Key Encipherment = 1	
	Data Encipherment = 0	
	Key Agreement = 1	
	Key Certificate Signature = 0	
	CRL Signature = 0	
4. extKeyUsage	Autenticación TLS webServer	**SI**
5. Certificate Policies Policy Identifier Policy Qualifier ID Policy CPS Location userNotice	1.3.6.1.4.1.18332.55.4.1 1.3.6.1.4.1.18332.55.1.1 https://www.anf.es/AC/documentos/ Certificado reconocido de Sede Electrónica, nivel alto. ANF Autoridad de Certificación es un emisor de certificados electrónicos reconocidos, conforme a lo establecido en la Ley 29/2003 de firma electrónica de España. Consulte las condiciones de uso en CPS	**NO**
6. Subject Alternate Names	Dirección email según RFC 822 dnsName = Nombre de Dominio DNS	**NO**

Directory Name *Tipo de certificado* **OID: 2.16.724.1.3.5.1.1.1** *Nombre entidad suscriptora* **OID: 2.16.724.1.3.5.1.1.2** *NIF entidad suscriptora* **OID: 2.16.724.1.3.5.1.1.3** *Nombre descriptivo sede* **OID: 2.16.724.1.3.5.1.1.4** *Denominación dominio* **OID: 2.16.724.1.3.5.1.1.5**	***Identidad Administrativa*** Sede Electrónica Propietaria del certificado NIF Célula FIscal Breve descripción de la Sede indicando un nombre Dominio al que pertenece la Sede	
1.3.6.1.4.1.18332.29.1. 1.3.6.1.4.1.18332.29.2. 1.3.6.1.4.1.18332.29.3. 1.3.6.1.4.1.18332.29.4. 1.3.6.1.4.1.18332.29.5. 1.3.6.1.4.1.18332.29.7.	Nombre del responsable del certificado Primer Apellido del Responsable del Certificado Segundo Apellido del Responsable del Certificado Cédula de Identificación Personal Responsable Correo electrónico del Responsable del Certificado Departamento al que está adscripto Responsable	
1.3.6.1.4.1.18332.10.1. 1.3.6.1.4.1.18332.10.2. 1.3.6.1.4.1.18332.10.3. 1.3.6.1.4.1.18332.10.4. 1.3.6.1.4.1.18332.10.5.	Nombre del Representante legal Primer del Representante legal Segundo Apellido del Representante legal Cédula de Identificación Personal Representante legal Titulo acreditativo del Representante legal	

1.3.6.1.4.1.18332.10.6. 1.3.6.1.4.1.18332.10.7.	Si la capacidad es mancomunada Dirección correo electrónico	
7. Issuer Alternate Names . dNSName . rfc822Name	Igual a la extensión subjectAltName del certificado de la CA emisora URL dominio organización Correo electrónico de contacto de la Entidad de Certificación emisora	**NO**
8. Basic Constraints Entidad final	CA: FALSE	**SI**
9. CRLDistributionPoints	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=https://www.anf.es/anf/certificacion/certificados-electonicos/gestion/200.1.33.html [2]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=https://crl.anf.es/AC/ANFServerCA.crl	**NO**
10. Auth. Information Access authorityInfoAccess	http://ocsp.anf.es:8094	**NO**
11. QcStatements QcRetentionPeriod *OID 0.4.0.1862.1.3* QcCompliance *OID 0.4.0.1862.1.1* QcSSCD *OID 0.4.0.1862.1.4*	 15 años Certificado reconocido Dispositivo Hardware Criptográfico/HSM	**NO**

QcLimitValue *OID 0.4.0.1862.1.2* **QCForLegalPerson**	Importe límite de responsabilidad asumido por el emisor Certificado emitido a persona jurídica	
12. Subject	Street = Calle y número (opcional) postalCode = Código Postal (opcional) serialNumber = Cédula Identificación Fiscal organización GivenName = Nombre del Responsable del Certificado (como constan en el DNI) SurName = Apellidos del Responsable del Certificado (como constan en el DNI) T, Title = Cargo del Responsable del Certificado EmailAddress (EA) = Dirección correo electrónico organización	**NO**
13. businessCategory	[OID.2.5.4.15] Valores posibles: - "PrivateOrganization" para Organización privada -"GovernmentEntity" para Entidad pública -"Business Entity" para Empresa - "Non-comercial Entity" para Entidad no comercial	**NO**
14. jurisdictionOfIncorporationLocalityName	[OID: 1.3.6.1.4.1.311.60.2.1.1] Localidad en la que está registrada la empresa (Opcional)	**NO**
15. jurisdictionOfIncorporationStateOrProvinceName	[OID: 1.3.6.1.4.1.311.60.2.1.2] Provincia en la que está registrada la empresa	**NO**
16. jurisdictionOfIncorporationCountryName	[OID: 1.3.6.1.4.1.311.60.2.1.3] País en el que está registrada la empresa	**NO**

17. dNSName	Dominios DNS adicionales (Opcional)	**NO**

*[1] Non Repudiation (Content Commitment)

7.1.7. Identificadores de objeto (OID) de los algoritmos

Identificador de Objeto (OID) de los algoritmos Criptográficos:

·SHA1withRSAEncryption (1.2.840.113549.1.1.5)

·SHA256withRSAEncryption (1.2.840.113549.1.1.11)

Identificador de Objeto (OID) de Clave Pública:

·rsaEncryption (1.2.840.113549.1.1.1)

7.1.8. Formatos de nombres

Los certificados emitidos por ANF AC contienen el distinguished name X.500 del emisor y el subscriptor del certificado en los campos issuer name y subject name respectivamente.

El campo cn del subject name se cumplimenta obligatoriamente en mayúsculas, prescindiendo de acentos y sustituyendo la letra "Ñ" por la "N" y la letra "Ç" por la "C". Esta característica se da únicamente en el atributo CommonName.

7.1.9. Restricciones de los nombres

Los nombres contenidos en los certificados están restringidos a distinguished names X.500, únicos y no ambiguos.

Los atributos CN (Common Name) y serialNumber del DN serán los que distingan a los DN entre sí.

7.1.10. Identificador de objeto (OID) de la Política de Certificación

El identificador de objeto definido por ANF AC para identificar la presente política es el siguiente: 1.3.6.1.4.1.18332.55.1.1.

7.1.11. Uso de la extensión "Policy Constraints"

Según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

7.1.12. Sintaxis y semántica de los calificadores de política

No estipulado

7.1.13. Tratamiento semántico para la extensión critica "Certificate Policy"

La extensión "Certificate Policy" identifica la política que define las prácticas que ANF AC asocia explícitamente con el certificado. Adicionalmente la extensión puede contener un calificador de la política.

7.1.14. Guía de cumplimentación de campos de los certificados

Salvo lo reseñado en el anterior aparado 7.1.6 sobre el campo CN del Subject name, se sigue lo recomendado por la RFC 5280, utilizando UTF-8 string, complementado por la RFC 2279 mejorada en RFC 3629 (UTF-8, a transformation format of ISO 10646). En base a ello se codifica grupos de caracteres internacionales incluyendo caracteres del alfabeto latino con diacríticos ("Ñ", "ñ", "Ç", "ç", "Ü", "ü ", etc.) Por ejemplo, el carácter eñe (ñ), que se representa en unicode como 0x00F1.

Además y con el fin de establecer un marco común en todos los certificados emitidos en el ámbito de la PKI de ANF AC, se tratará de mantener las siguientes recomendaciones en la emisión de certificados:

- Todos los literales se introducen en mayúsculas, con las excepciones del nombre de dominio/subdominio y el correo electrónico que estarán en minúsculas.
- Se codificarán los nombres tal y como aparece en la documentación acreditativa.
- Respecto a los apellidos de personas físicas, Incluir obligatoriamente el PRIMER Y SEGUNDO APELLIDO, separados únicamente por un espacio en blanco, de acuerdo con lo indicado en el DNI/NIE. En caso de no existir el segundo apellido, se dejará en blanco (sin ningún carácter).
- Incluir obligatoriamente el número de DNI/NIE, junto con la letra de control, de acuerdo con lo indicado en el DNI/NIE.
- Se puede incluir opcionalmente el literal "DNI" antes del número de DNI/NIE
- Incluir obligatoriamente el SÍMBOLO / que separe el nombre y apellidos del número de DNI o dirección de correo electrónico, en el caso incluirlos en el mismo campo.
- No incluir tildes en los literales alfabéticos
- No incluir más de un espacio entre cadenas alfanuméricas.
- No incluir caracteres en blanco al principio ni final de cadenas alfanuméricas.
- Se admite la inclusión de abreviaturas en base a una simplificación, siempre que no supongan dificultad en la interpretación de la información.
- Se podrán eliminar los acentos, para garantizar la mayor compatibilidad técnica posible.
- El user notice no tendrá más de 200 caracteres.

7.2. Perfil de CRL

El perfil de las CRL's se corresponde con el propuesto en las políticas de certificación correspondientes, y con el estándar X.509 versión 3 de la RFC 3280

"Internet X.509 Public Key Infrastructure Certificate and CRL Profile". Las CRL's son firmadas por la autoridad de certificación que ha emitido los certificados.

7.2.1. Número de versión

El formato de las CRLs utilizadas en la presente política es el especificado en la versión 2 (X509 v2).

7.2.2. CRL y extensiones

La presente Política de Certificación soporta y utiliza CRLs conformes al estándar X.509.

7.2.2.1. CRL de la autoridad raíz

Campo	VALORES
Versión	*V2 (versión del estándar X509)*
Número de serie CRL	*Código único con respecto a esa determinada jerarquía del emisor*
Algoritmo de firma	Sha1WithRSAEncryption
Emisor (Issuer)	E=info@anf.es CN= ANF Server CA L= Barcelona (see current address at https://www.anf.es/address/) O= ANF Autoridad de Certificación SERIALNUMBER = G63287510 C=ES
Fecha efectiva de emisión	(fecha de emisión de la CRL, tiempo UTC)
Fecha de próxima actualización	Fecha efectiva de emisión + días
Identificador de la clave	Id. de clave=be 3b f6 b4 31 b7 73 24 48 39 c5 57 13

de autoridad	94 75 aa 9f 81 3f 2c
Punto de distribución:	https://crl.anf.es/AC/ANFServerCA.crl
Sólo contiene Certificados de usuario	NO
Sólo contiene Certificados de la entidad emisora	NO
Lista de revocación de certificados (CRL) indirecta	NO
Entradas de la CRL	Nº de serie del certificado Fecha de revocación Código de razón

7.2.2.2. CRL de la autoridad de certificación intermedia

Campo	**VALORES**
Versión	*V2 (versión del estándar X509)*
Número de serie CRL	*Código único con respecto a esa determinada jerarquía del emisor*
Algoritmo de firma	Sha1WithRSAEncryption
Emisor (Issuer)	E=info@anf.es CN= ANF Clase SubCA1 L= Barcelona (see current address at https://www.anf.es/address/) O= ANF Autoridad de Certificación SERIALNUMBER = G63287510 C=ES
Fecha efectiva de emisión	(fecha de emisión de la CRL, tiempo UTC)
Fecha de próxima actualización	Fecha efectiva de emisión + 1 día
Identificador de la clave de autoridad	Id. de clave=
Punto de distribución:	https://crl.anf.es/AC/ANFServerCA.crl

Sólo contiene Certificados de usuario	NO
Sólo contiene Certificados de la entidad emisora	NO
Lista de revocación de certificados (CRL) indirecta	NO
Entradas de la CRL	Nº de serie del certificado Fecha de revocación Código de razón

8. Auditoría de conformidad

ANF AC realiza periódicamente una auditoría de cumplimiento para determinar que está operando conforme a los requisitos de seguridad y de operación especificados en la presente política de certificación.

8.1. Frecuencia de los controles de conformidad para cada entidad

ANF AC somete su PKI a anualmente a un proceso de auditoría, además de las auditorías bajo demanda que pueda llevar a cabo bajo su propio criterio, a causa de una sospecha de incumplimiento de alguna medida de seguridad o por un compromiso de claves.

8.2. Identificación/cualificación del auditor

ANF AC dispone de un departamento de auditoría interno, el cual se encargar de llevar a cabo la auditoría de cumplimiento.

8.3. Relación entre el auditor y la entidad auditada

Las auditorías de cumplimiento ejecutadas por terceros, son llevadas a cabo por una entidad independiente a ANF AC.

8.4. Listado de elementos objeto de auditoria

Los elementos objeto de auditoría serán los siguientes:

- Procesos de certificación de clave pública.
- Sistemas de información.

- Protección del centro de proceso

- Cumple de todos los requerimientos establecidos en esta Política y en su DPC.

- Documentación del servicio.

8.5. Acciones a emprender como resultado de una falta de conformidad

Una vez recibido el informe de la auditoría de cumplimiento llevada a cabo, ANF AC analiza con la entidad que ha ejecutado la auditoría, las posibles deficiencias encontradas, diseñando un plan correctivo que solvente dichas deficiencias, y estableciendo su ejecución.

Una vez que las deficiencias sean subsanadas, se realiza una nueva auditoría para confirmar su implantación y la efectividad de las soluciones tomadas.

9. Requisitos comerciales y legales

9.1. Confidencialidad

9.1.1. Tipo de información que debe protegerse

La siguiente información será considerada como sensible, y por tanto se adoptan las medidas de protección necesarias en cuanto a acceso y tratamiento:

- Solicitudes de certificados, aprobadas o denegadas, así como toda otra información personal obtenida para la expedición y mantenimiento de certificados, excepto las informaciones indicadas en la sección siguiente.

- Las claves privadas generadas y/o almacenadas por ANF AC.

- Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.

- Registros de auditoría interna y externa, creados y/o mantenidos por el ANF AC y sus auditores.

- Planes de continuidad de negocio y de emergencia.

- Política y planes de seguridad.

- Documentación de operaciones y restantes planes de operación, como archivo, monitorización y otros análogos.

- La identidad cierta de los suscriptores de certificados emitidos bajo seudónimo.

- Toda otra información identificada como "Sensible".

9.1.2. Información no sensible

La siguiente información será considera no sensible:

- Los certificados emitidos o en trámite de emisión.

- La vinculación del titular a un certificado.

- El nombre y los apellidos del titular del certificado, así como cualquier otra circunstancia o dato personal del titular, en el supuesto de que sea significativa en función de la finalidad del certificado.

- La dirección de correo electrónico del titular del certificado o la dirección de correo electrónico que corresponda.

- Los usos y límites económicos reseñados en el certificado.

- El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.

- El número de serie del certificado.

- Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.

- Las listas de revocación de certificados (CRLs), así como las restantes informaciones de estado de revocación.

- La información contenida en los repositorios de certificados.

- Toda otra información que no esté indicada en la sección anterior de esta política.

9.1.3. Divulgación de información de suspensión y revocación

Según lo reseñado en los puntos anteriores.

9.1.4. Divulgación legal de información

ANF AC atenderá los requerimientos de información clasificada como sensible, atendiendo la legislación vigente.

En concreto, los registros que avalan la fiabilidad de los datos contenidos en el certificado serán divulgados en caso de ser requerido para ofrecer evidencia de la correcta emisión y gestión del ciclo de vida del certificado en caso de un procedimiento judicial, incluso sin consentimiento del suscriptor del certificado.

Se indicarán estas circunstancias en la política de intimidad prevista en la sección 9.2 de esta política.

9.1.5. Divulgación de información por petición de su titular

ANF AC incluirá, en la política de intimidad prevista en la sección 9.2 de esta política, prescripciones para permitir la divulgación de la información del suscriptor y, en su caso, del responsable del certificado, directamente a los mismos o a terceros.

9.1.6. Otras circunstancias de divulgación de información

No estipulado

9.2. Protección de datos personales

Para la prestación del servicio, ANF AC precisa recabar y almacenar ciertas informaciones, que incluyen datos personales. Tales informaciones son recabadas directamente de los afectados, con su consentimiento explícito o en los casos en los que la ley permita se recaba la información sin consentimiento del afectado.

Se recabarán los datos exclusivamente necesarios para la expedición y el mantenimiento del certificado.

ANF AC cuenta con una política de intimidad, de acuerdo con la Ley Orgánica 15/99, de 13 de diciembre, de Protección de Datos de Carácter Personal, y documenta en su Declaración de Prácticas de Certificación los aspectos y procedimientos de seguridad correspondientes al documento de seguridad previsto en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Dicha Declaración de Prácticas de Certificación tiene la consideración de documento de seguridad.

ANF AC no divulga ni cede datos personales, excepto en los casos previstos en las secciones 9.1.2 a 9.1.6 de esta política, y en la sección 5.8, en caso de terminación de su actividad.

La información confidencial de acuerdo con la LOPD será protegida de su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado, de acuerdo con las prescripciones establecidas en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

9.3. Derechos de propiedad intellectual

9.3.1. Propiedad de los certificados e información de revocación

La emisión y entrega de los certificados emitidos por ANF AC, no presupone renuncia alguna sobre los derechos de propiedad intelectual que sobre los ellos ostenta.

ANF AC salvo autorización expresa, prohíbe el almacenamiento de los datos de sus certificados en repositorios ajenos a la PKI de ANF AC, y especialmente cuando tenga como fin la prestación de servicios de información sobre el estado de vigencia o revocación.

Los certificados y la información de estado, solo pueden ser utilizados para los fines de uso especificados en este documento.

9.3.2. Propiedad de la política de certificación y Declaración de Prácticas de Certificación

ANF AC es propietaria de todos los documentos que publica en el ámbito de su PKI.

9.3.3. Propiedad de la información relativa a nombres

El suscriptor conserva cualquier derecho, de existir éste, relativo a la marca, producto o nombre comercial contenido en el certificado.

El suscriptor es el propietario del nombre distinguido del certificado, formado por las informaciones especificadas en la sección 3.1 de esta política.

9.3.4. Propiedad de claves

Los pares de claves serán propiedad de los suscriptores de los certificados.

Cuando una clave se encuentre fraccionada en partes, todas las partes de la clave son propiedad del propietario de la clave.

9.4. Obligaciones y responsabilidad civil

9.4.1. Modelo de obligaciones de ANF AC

De acuerdo con lo establecido en la legislación vigente, ANF AC es la única entidad responsable del cumplimiento de los procedimientos descritos en esta política, incluso cuando una parte de las operaciones sea subcontratada externamente.

9.4.2. Garantías ofrecidas a suscriptores y terceros que confían en los certificados

ANF AC asume las obligaciones establecidas en la legislación vigente y las reseñadas en su Declaración de Practicas de Certificación. Ademas garantiza:

Suscriptor:

- Que no hay errores de hecho, conocidos por ANF AC, en las informaciones contenidas en los certificados.

- Que no hay errores de hecho en las informaciones contenidas en los certificados, debidos a falta de diligencia en la gestión de la solicitud de certificado o en la creación del mismo.

- Que los certificados cumplen con todos los requisitos materiales establecidos de la Declaración de Prácticas de Certificación.

- Que los servicios de revocación y el empleo del Repositorio cumplen con todos los requisitos materiales establecidos en la Declaración de Prácticas de Certificación.

Tercero que confía en el certificado:

- Que la información contenida o incorporada por referencia en el certificado es correcta, excepto cuando se indique lo contrario.

- En caso de certificados publicados en el Repositorio, que el certificado ha sido emitido al suscriptor identificado en el mismo y que el certificado ha sido aceptado, de acuerdo con la sección 4.4 de la presente política de certificación.

- Que en la aprobación de la solicitud de certificado y en la emisión del certificado, se han cumplido todos los requisitos materiales establecidos en la Declaración de Prácticas de Certificación.

- La rapidez y seguridad en la prestación de los servicios, en especial de los servicios de revocación y de Repositorio.

En los certificados de firma electrónica, ANF AC garantiza al suscriptor y al tercero que confía en el certificado:

- Que el certificado contiene las informaciones que debe contener un certificado reconocido, de acuerdo con el artículo 11 de la Ley 59/2003, de 19 de diciembre.

- ANF AC asume el límite económico de responsabilidad indicado en sus certificados, y en caso de no constar la extensión correspondiente "QcLimitValue *OID 0.4.0.1862.1.2"*, se deberá interpretar que el certificado es emitido sin responsabilidad económica asumida por ANF AC.

9.4.3. Rechazo de otras garantías

ANF AC rechaza asumir cualquier otra garantía que no sean legalmente exigible, y aquellas ya contempladas en la punto 9.4.2.

9.4.4. Limitación de responsabilidades

ANF AC limita su responsabilidad a la emisión y gestión de certificados y, suministro de dispositivos criptográficos (de firma y verificación de firma, así como de cifrado o descifrado).

Los Certificados técnicos de Servidor Seguro SSL y de Sede Electrónica no son certificados digitales reconocidos según la Ley 59/2003 de 19 de diciembre de firma electrónica de España.

ANF AC podrá incluir otras limitaciones de uso en los certificados, tal y como se detalla en la Declaración de Practicas de Certificación y en este documento.

9.4.5. Exención de responsabilidades

9.4.5.1. Exención de responsabilidades con el suscriptor

El suscriptor, con la aceptación del certificado, exime de toda responsabilidad a ANF AC, y en especial, se compromete a mantener indemne a ANF AC de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación

letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Falsedad o manifestación errónea realizada por el usuario del certificado.

- Error del usuario del certificado al facilitar los datos de la solicitud, si en la acción u omisión medió dolo o negligencia con respecto a ANF AC, la entidad de registro o cualquier persona que confía en el certificado.

- Negligencia en la protección de la clave privada, en el empleo de un sistema fiable o en el mantenimiento de las precauciones necesarias para evitar el compromiso, la pérdida, la divulgación, la modificación o el uso no autorizado de dicha clave.

- Empleo por el suscriptor de un nombre (incluyendo nombres comunes, dirección de correo electrónico y nombres de domino), u otras informaciones en el certificado, que infrinja derechos de propiedad intelectual o industrial de terceros.

- Uso indebido de la clave privada del certificado, para operaciones que no están autorizadas en el mismo.

- El incumplimiento en el pago de las tasas de emisión, renovación, pago del dispositivo de firma, firmas electrónicas…etc. o cualquier otro que el suscriptor haya contratado.

9.4.5.2. Exención de responsabilidades con tercero que confía en el certificado

El tercero que confía en el certificado se compromete a mantener indemne a ANF AC de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Incumplimiento de las obligaciones del tercero que confía en el certificado.

- Confianza temeraria en un certificado, a tenor de las circunstancias.

- Falta de comprobación del estado de un certificado, para determinar que no se encuentra suspendido o revocado.

- Comprobación del certificado utilizando dispositivos no homologados por ANF AC.

- No utilizar el servicio de retimbrado de firmas, cuando alguno de los componentes criptográficos entre en situación de riesgo en conformidad con la publicación que al efecto ANF AC realiza en www.anf.es

9.4.6. Caso fortuito y fuerza mayor

En caso de incidente fortuito y en caso de fuerza mayor, ANF AC no asumirá responsabilidad por las denegaciones de servicio que se puedan producir durante el tiempo que tarde en reactivar sus servicios.

9.4.7. Ley applicable

La ley aplicable en la prestación de los servicios de certificación, es la ley española.

9.5. Tarifas

9.5.1. Tarifas de emisión de certificado o renovación

Los precios correspondientes a los productos y servicios prestados por ANF AC, son públicos y de libre acceso en la sección Tasas de www.anf.es.

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

El acceso a las listas de revocación CRLs, es libre y gratuita.

9.5.3. Política de reintegros

No se prevén reintegros de las cantidades entregadas para el pago de este tipo de certificados.

9.6. Capacidad financiera

9.6.1. Indemnización a los terceros que confían en los certificados emitidos por ANF AC.

Tal y como se especifica en la Declaración de Prácticas de Certificación (CPS) de ANF AC, se dispone de garantía de cobertura suficiente de responsabilidad civil a través de póliza de seguros de RC emitida por la Lloyd's, por importe de TRES MILLONES DE EUROS (3.000.000 €), que cubre el riesgo de la responsabilidad por los daños y perjuicios que pudiera ocasionar el uso de los certificados expedidos por esta Autoridad de Certificación, cumpliendo así con la obligación establecida en el artículo 20.2 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

ANEXO I. CONTRATO DE PRESTACIÓN DE SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA

CONTRATACIÓN DE PRESTACIÓN DE SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA SERVIDOR SEGURO SSL, SERVIDOR SEGURO SSL CON VALIDACIÓN EXTENDIDA (EV), SEDE ELECTRÓNICA y SEDE ELECTRÓNICA CON EV.

El presente Acuerdo tiene como objeto dejar constancia por escrito, de la voluntad de las partes para establecer un marco de colaboración entre ANF AUTORIDAD DE CERTIFICACIÓN, en su calidad de Prestador de servicios de certificación electrónica y , como Usuario Final y en calidad de **SUSCRIPTOR** de los servicios.

PARTES

DE UNA PARTE, D Florencio Díaz Vilches, mayor de edad, con N.I.F. 37.271.387W, con domicilio a efectos del presente contrato en Gran Vía de les Corts Catalanes, 996, Plantas 3ª y 4ª de Barcelona.

DE OTRA PARTE, D. ..... mayor de edad, con N.I.F....., con domicilio a efectos de este contrato en la Calle ....., ... de .....

INTERVIENEN

D. Florencio Díaz Vilches en nombre y representación, en su calidad de Presidente, de **ANF Autoridad de Certificación**, entidad sin ánimo de lucro constituida al amparo de la Ley Orgánica 1/2002 del 22 de marzo e inscrita en el Ministerio del Interior con el número nacional 11.465, CIF G-63287510 y con domicilio social en Barcelona, Gran Vía de les Corts Catalanes, 996, Plantas 3ª y 4ª, en adelante ANF AC.

D. ..... en nombre y representación, en su calidad de .....,de

....., CIF ....., y domiciliado en la Calle....., ..., en adelante, el SUSCRIPTOR.

Y reconociéndose mutuamente la capacidad legal necesaria para la eficacia del presente contrato, libremente y de forma voluntaria,

MANIFIESTAN

I. Que **ANF AC**, es una entidad prestadora de servicios de certificación electrónica, que emite varias clases de certificados electrónicos con la cualificación de reconocidos.

II. Que en conformidad a lo dispuesto en la normativa española, ha realizado la comunicación prevista en el artículo 30.2 de la Ley 59/2003 de firma electrónica, apareciendo publicado en el web del Ministerio de industria, Comercio y Turismo habilitado al efecto.

III. Que la actividad de **ANF AC**, como prestadora de servicios de certificación electrónica, se encuentra regulada por la Ley 59/2003 de Firma Electrónica, de 19 de diciembre, y en el ámbito de su infraestructura de clave pública, conforme a lo estipulado en su Declaración de Prácticas de Certificación (en adelante, DPC) y las respectivas políticas de certificación (PC) del tipo de certificado solicitado.

IV. Que el **SUSCRIPTOR** conoce los servicios de certificación electrónica ofrecidos por **ANF AC**, y desea hacer uso de los mismos.

V. Que el **SUSCRIPTOR** conoce y acepta las tarifas asociadas a estos servicios de certificación electrónica, las cuales están permanentemente publicadas y actualizadas en https://www.anf.es .

VI. Que el **SUSCRIPTOR** conoce lo establecido en *la Política de Certificación asociada a este certificado, la Declaración de Practicas de Certificación*

de ANF AC, la CPS de ANF AC como Autoridad de Sellos de Tiempo, y Politicas de Certificación vinculadas a la TSA, documentos que se encuentran publicados y disponibles en el web www.anf.es y a través de solicitud enviada al correo electrónico soporte@anf.es .

Por tanto, las partes acuerdan la instrumentación del presente Contrato con sujeción a las siguientes

CONDICIONES

1.- OBJETO

El objeto del presente documento es regular la contratación de los servicios de certificación electrónica de **ANF AC**.

2.- REGULACIÓN

Las relaciones surgidas entre **ANF AC** y el **SUSCRIPTOR**, dentro del marco dado por el Sistema de Certificación desarrollado por **ANF AC**, se regirán por el presente Contrato, por la Declaración de Prácticas de Certificación (DPC), la Política específica del certificado contratado (PC), y conforme a la legislación vigente.

Tanto la DPC y las PC's son documentos públicos y están permanente disponibles en la URL http://www.anf.es

3.- OBLIGACIONES DEL SUSCRIPTOR

3.1. Facilitar información veraz y actualizada en la tramitación de sus solicitudes de certificados.

3.2. No permitir la intervención de terceros en el proceso de generación de los datos de creación de firma.

3.3. Custodiar de forma adecuada los instrumentos de Firma Electrónica, y especial mantener confidencialidad en cuanto a los datos de activación de firma.

3.4. Adecuar el uso del certificado electrónico a los usos permitidos de acuerdo con lo establecido en la Política de Certificación a la que están asociados.

3.5. Informar inmediatamente a **ANF AC**, sobre cualquier sospecha de riesgo del certificado, y no utilizarlo una vez notificada.

3.6. Informar inmediatamente a **ANF AC**, sobre cualquier variación de los datos aportados en la solicitud del certificado.

3.7. Abonar las tasas correspondientes a los servicios solicitados.

3.8. Declara conocer y acepta la equiparación legal de la firma electrónica a la firma manuscrita.

3.9. Acepta que todas las comunicaciones electrónicas autenticadas empleando la firma digital generada con las claves de activación de firma, tienen el mismo efecto legal, validez y fuerza vinculante que una comunicación escrita debidamente autenticada.

3.10. Acepta que los documentos electrónicos obtenidos tras el proceso de digitalización llevado a cabo mediante la aplicación AR Manager de gestión de solicitudes de certificados electrónicos, se corresponden a la imagen fiel de los respectivos documentos originales.

3.11. En caso de revocación del certificado, se obliga a cesar en su uso.

3.12. El **SUSCRIPTOR** garantiza que las denominaciones, nombres o dominios reseñados en el formulario de solicitud en este contrato de prestación de servicios, no infringe derechos de terceros.

3.12. Utilizar el certificado respetando las restricciones que le vienen impuestas según la Política de Certificación y Política de Firma Electrónica.

Y en general todas las especificadas en la DPC de con especial relevancia las reseñadas en el apartado 9.5.7 Responsabilidades de los Suscriptores y de los Responsables de los certificados.

3.13. A las obligaciones generales anteriormente expresadas se añadirán otras relativas a los requerimientos de la tipología del certificado:

- En los certificados técnicos SSL y de Sede Electrónica, con o sin EV, el **SUSCRIPTOR** deberá designar un responsable técnico, como interlocutor de ANF AC.

- En los certificados técnicos SSL y de Sede electrónica, ANF AC podrá requerir al **SUSCRIPTOR** información o documentación adicional relativa a la comprobación de DNS y cuentas de correo.

- La negativa por parte del **SUSCRIPTOR** a facilitar esa información o documentación complementaria, mencionada en el párrafo anterior, conllevará por parte de **ANF AC** la imposibilidad de prestar el servicio de certificación contratado, sin que ello suponga la renuncia a las tasas previstas, que deberán ser abonadas sin dilación por el Suscriptor.

- Cualquier otro requerimiento o condición expresado en la Política de Certificación de certificados de Servidor seguro SSL, de Servidor Seguro SSL con validación extendida, de Sede Electrónica y de Sede Electrónica con validación extendida.

4.- DENEGACIÓN

4.1. El Suscriptor declara que ha informado al Operado AR de todas aquellas solicitudes de certificados que han dado como resultado denegación del servicio. Así como las causas que han motivado tal denegación.

4.2. Un sistema PKI se desarrolla en un marco de confianza mutua y en una relación de buena fe. El Suscriptor declara que no tiene o ha tenido conflicto de intereses con **ANF AC** o miembros de su Junta Rectora.

4.3. Se prohíbe la solicitud de certificados o servicios de certificación a personas o entidades que tengan una relación directa, o dependencia indirecta, con entidades que son competencia de **ANF AC**. En caso de llevar a cabo una tramitación con falsedad manifiesta, el **SUSCRIPTOR** indemnizará con CINCUENTA MIL EUROS (50.000 €) en concepto de penalización.

5.- PRESTACIÓN DE SERVICIOS, OBLIGACIONES-RESPONSABILIDADES DE LA CA

5.1. **ANF AC** presta los servicios de certificación de acuerdo con lo previsto en la DPC, en la Política de certificación específica y en la Ley 59/2003 de Firma Electrónica.

5.2. Responderá por negligencia o falta de la debida diligencia según los términos del presente contrato, excepto en los supuestos de limitación de responsabilidad establecidos en la DPC de **ANF AC** y en sus Políticas.

Mediante la aceptación del certificado el Suscriptor se obliga a mantener indemne y, en su caso, a indemnizar a ANF AC de cualquier acto u omisión que provoque daños, pérdidas, deudas, gastos, procesales o de cualquier tipo, incluyendo los honorarios profesionales, en los que ANF pueda incurrir, que sean causadas por la utilización o publicación de los certificados y que provengan de cualquiera de las causas previstas en la DPC o en las Políticas aplicables al certificado solicitado.

5.3. **ANF AC** no podrá modificar un certificado que ya ha sido emitido.

5.4. **ANF AC**, de acuerdo con las funciones que tiene atribuidas en virtud de este contrato, garantizará en todo momento la seguridad lógica y física de los procesos de certificación que deba realizar.

5.5. **ANF AC** garantiza que a solicitud del **SUSCRIPTOR** procederá a la revocación del certificado electrónico.

5.6. **ANF AC** se compromete a no almacenar ni copiar los datos de creación de firma de los usuarios a los que hayan prestado sus servicios.

5.7. ANF AC conservará registrada toda la información y documentación relativa a los certificados emitidos y las declaraciones de prácticas de certificación vigentes en cada momento, durante un plazo de 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo.

5.8. **ANF AC,** de conformidad con el artículo 18, c) de la Ley 5972003 de Firma Electrónica, garantiza la publicación de listas de certificados revocados, las cuales son libremente accesibles a través de la URL www.anf.es

Los periodos de actualización de las listas de certificados revocados están especificados en la DPC y Política de Certificación a la que se somete cada tipo de certificado, además se especifica en el campo de la CRL la fecha máxima de próxima actualización.

6.- CONDICIONES DEL SERVICIO

6.1. Para la prestación de los servicios de certificación electrónica, **ANF AC** tiene publicadas normas de funcionamiento y de seguridad, como la DPC. Así mismo, las relaciones con terceras personas y entidades están formalizadas mediante el correspondiente acuerdo contractual escrito.

6.2. **ANF AC** ha informado al **SUSCRIPTOR** de este documento por escrito y facilitando acceso electrónico a la información acerca de los siguientes extremos:

1.º Las obligaciones del firmante, la forma en que han de custodiarse los datos de creación de firma, el procedimiento que ha de seguirse para comunicar la pérdida o posible utilización indebida de dichos datos y determinados dispositivos de creación y de verificación de firma electrónica que sean compatibles con los datos de firma y con el certificado expedido.

2.º Los mecanismos para garantizar la fiabilidad de la firma electrónica de un documento a lo largo del tiempo.

3.º El método utilizado por el prestador para comprobar la identidad del firmante u otros datos que figuren en el certificado.

4.º Las condiciones precisas de utilización del certificado, sus posibles límites de uso y la forma en que el prestador garantiza su responsabilidad patrimonial.

5.º Las certificaciones obtenidas por el prestador de servicios de certificación y los procedimientos aplicables para la resolución extrajudicial de los conflictos que pudieran surgir por el ejercicio de la actividad de certificación.

6.º El resto de informaciones contenidas en la declaración de prácticas de certificación .

7º Igualmente, ANF AC se compromete a facilitar a requerimiento de los terceros afectados por los certificados la información citada en los puntos anteriores.

6.3. La vigencia del certificado será por un periodo de 2 años, contados a partir del momento de su emisión.

6.4. La revocación de un certificado tiene efectos irreversibles, produciendo su cancelación definitiva.

6.5. **ANF AC** no almacena, ni tiene oportunidad de hacerlo, datos de creación de firma, datos de activación, ni tan siquiera contraseña de activación del Acta de Identificación. En consecuencia, no es

posible recuperar ninguno de estos valores en caso de pérdida.

7.- HONORARIOS

Las tasas correspondientes a los servicios prestados por esta entidad de certificación, están publicadas en la URL www.anf.es

8.- PROTECCIÓN DE DATOS

ANF AC en el tratamiento de los datos personales que precisa para el desarrollo de su actividad como prestador de servicios de certificación se sujeta a las disposiciones de la Ley orgánica 15/1999 de protección de datos de carácter personal, a sus disposiciones de desarrollo y a la Ley 59/2003 de firma electrónica.

El **SUSCRIPTOR** conoce que la información de datos de carácter personal facilitada a ANF AC será incorporada a un fichero automatizado cuyo responsable es ANF AC.

El **SUSCRIPTOR** consiente, especialmente, en la captación y guarda de su imagen fotográfica y huellas dactilares, en los casos que sea preciso para la prestación del servicio de certificación solicitado.

El suscriptor debe defender, indemnizar y eximir de responsabilidad a ANF AC de cualquier pérdida o daño que sea resultado de una infracción imputable al Suscriptor en materia de protección de datos de carácter personal.

ANF AC no podrá modificar un certificado que ya haya sido emitido con la finalidad de rectificar o cancelar datos de carácter personal contenidos en el mismo, puesto que para ello es necesaria la revocación del certificado.

Asimismo, los datos rectificados o cancelados, relativos a los certificados revocados serán mantenidos por ANF AC durante un periodo de 15 años, con arreglo a lo previsto en el artículo 20,1,f) de la Ley 59/2003 de firma electrónica.

9.- LEGISLACIÓN Y JURISDICCIÓN

8.1. El presente Contrato se regirá por la legislación española, con arreglo a la cual deberá ser interpretado su contenido.

8.2. *ANF AC, con arreglo a lo previsto en su DPC, se acoge a la resolución extrajudicial de conflictos que pudieran surgir entre las partes, a tal efecto* se somete voluntariamente para la solución de cualquier cuestión litigiosa que pudiera surgir por el ejercicio de su actividad, al arbitraje institucional del Tribunal Arbitral del Consejo Empresarial de la Distribución (TACED), al que se le encarga la designa del Árbitro – que será único – y la administración del arbitraje – que será de equidad – con arreglo a su Reglamento, obligándose desde ahora, al cumplimiento de la decisión arbitral.

Surgido el conflicto, la otra parte (SUSCRIPTOR) deberá adherirse expresamente al arbitraje institucional mencionado en el párrafo anterior.

Caso de no aceptarse por el SUSCRIPTOR, llegado el caso, el procedimiento arbitral, desde este momento, las parte someten sus

discrepancias al conocimiento y resolución de los Juzgados y Tribunales de la ciudad de Barcelona.

Ambas partes en prueba de conformidad con todos y cada uno de los extremos consignados en el presente contrato, lo firman, por duplicado y a un solo efecto, en,

Barcelona a de de 201

ANEXO II. FORMULARIO DE RENOVACIÓN

Certificados **Reconocidos**

CARTA DE SOLICITUD DE RENOVACIÓN

INSTRUCCIONES: *Para la renovación de su Certificado Electrónico, simplemente debe de firmar este modelo de carta. Es imprescindible que para la generación de la firma utilice el certificado que desea renovar.*

A/A del Responsable Dictámenes de Emisión

ANF AUTORIDAD DE CERTIFICACIÓN

Estimado Sr.:

Dado que no han transcurrido más de 5 años desde que realicé el proceso de identificación ante una de sus Autoridades de Registro, y estando próxima la fecha de caducidad de mi certificado electrónico, deseo comunicarles mi deseo de que procedan a su renovación.

Les agradeceré que su Departamento de Administración me informe, mediante correo electrónico, de las opciones disponibles para abonar las tasas de renovación.

Mediante la firma de este documento, expreso mi formal solicitud de renovación del certificado electrónico, el cual he empleado para llevar a cabo esta autenticación. Así mismo declaro que no se han producido cambios en los datos incorporados en dicho certificado.

Reciban un cordial saludo,

IMPORTANTE: *De acuerdo con lo establecido en el Apartado 3.3.1* "Identificación y autenticación de las solicitudes de renovación rutinarias." *de la Política de Certificación a la que se somete este certificado, tan solo se podrán realizar este tipo de renovaciones si no ha transcurrido un período de tiempo superior a cinco años desde que se realizó la identificación ante una AR.*

ANEXO III. FORMULARIO DE REVOCACIÓN

Formulario de REVOCACIÓN Referencia solicitud

Detalles conocidos del certificado: *Ref. /Solicitud*

Número de serie del certificado:

Tipo de certificado:

Datos del suscriptor del certificado*:*

Nombre del titular:

DNI (persona física) ó CIF (persona jurídica):

Datos de la persona que requiere la revocación:

Nombre: DNI:

Apellido 1º: Apellido2º:

Tfno.: Email:

Actúa en nombre propio*:* *SI / NO (tache lo que no proceda)*

Actúa en representación del suscriptor*:* *SI / NO (tache lo que no proceda)*

Poder Notarial: .....

.....

Otra representación*:*

Información al respecto: .....

.....

Motivo de la revocación (marque la casilla, o especifique otras causas)

- ☐ Solicitud voluntaria del titular.
- ☐ Solicitud voluntaria del representante.
- ☐ Pérdida del soporte de almacenamiento.
- ☐ Daños en el soporte de almacenamiento.
- ☐ Fallecimiento del suscriptor, incapacidad sobrevenida, total o parcial.
- ☐ Fallecimiento del representante, incapacidad sobrevenida, total o parcial.
- ☐ Finalización de la representación.
- ☐ Cese de operaciones
- ☐ Clave comprometida
- ☐ Información obsoleta.
- ☐ Emisión defectuosa de un certificado debido a que:
  - ☐ 1 No se ha cumplido un requisito material para la emisión del certificado.
  - ☐ 2 La creencia razonable de que un dato fundamental relativo al certificado es, o puede ser falso.
  - ☐ 3 Existencia de un error de entrada de datos u otro error de proceso
- ☐ El mal uso deliberado de claves y certificados, o la falta de observancia o contravención de los requerimientos operacionales contenidos en la DPC o la presente PC.
- ☐ Certificado sustituido.
- ☐ El longitud de claves pierde se revela como insegura.
- ☐ Los algoritmos criptográficos empleados se revelan como inseguros.
- ☐ Alguno de los certificados superiores de la Ruta de Certificación (CA Raíz-CA subordinada) pierde su vigencia.

- ☐ Otros:

El solicitante DECLARA:

Que ha sido informado de que con carácter previo a la revocación del certificado, ANF Autoridad de Certificación (en adelante, ANF AC) deberá realizar las comprobaciones correspondientes en cuanto a la identidad del solicitante, y su capacidad para tramitar esta solicitud de revocación.

Que conoce lo establecido en la Declaración de Prácticas de Certificación y Política de Certificación a la que se asocia el certificado de ANF AC y que los efectos de revocación son irreversibles.

Que tiene capacidad legal para tramitar esta solicitud de revocación, y que en caso contrario asume los daños y perjuicios que conlleve este trámite, tanto desde el punto de vista de los gastos administrativos que ha ocasionado a ANF AC, como por los perjuicios que genere en el Suscriptor del certificado.

Que los efectos de revocación serán efectivos a partir del momento en que se produce la publicación en los repositorios de ANF AC.

En , a de de 201

Firma del solicitante