Política de Certificación de Certificados de Aplicación, Firma de Código y Cifrado

Registro Nacional de Asociaciones. Número 171.443. CIF G-63287510

© ANF Autoridad de Certificación

Gran Vía de les Corts Catalanes 996. 08018 Barcelona (España)
Teléfono: 902 902 172 (Llamadas desde España)
Internacional +34 933 935 946
Fax: +34 933 031 611 · Web: www.anf.es

Nivel de Seguridad

Documento Público

Aviso Importante

Este documento es propiedad de ANF Autoridad de Certificación

Está prohibida su reproducción y difusión sin autorización expresade ANF Autoridad de Certificación

Copyright © ANF Autoridad de Certificación 2014

Dirección: Gran Via de les Corts Catalanes 996. 08018 Barcelona (España)

Teléfono: 902 902 172 (Llamadas desde España) Internacional +34 933 935 946

Fax: +34 933 031 611. Web: www.anf.es

Índice

1 Introducción 7

1.1 Descripción de los certificados 8

1.2 Identificación 8

1.3 Comunidad de usuarios 9

1.3.1 Autoridades de Certificación 9

1.3.2 Autoridades de Registro 9

1.3.2.1 Autoridad de Registro Reconocida 9

1.3.2.2 Autoridad de Registro Colaboradora 9

1.3.3 Responsable de Dictámenes de Emisión 10

1.3.4 Entidades finales 10

1.3.4.1 Suscriptor del certificado 10

1.3.4.2 Solicitante del certificado 10

1.3.4.3 Responsable del certificado 10

1.3.4.4 Terceros que confían 10

1.4 Uso de los certificados 10

1.4.1 Usos permitidos 10

1.4.2 Límites de uso de los certificados 11

1.4.3 Usos prohibidos 11

1.5 Datos de contacto de la Entidad de Certificación 11

1.6 Definiciones y Acrónimos 11

2 Repositorios y publicación de la información 12

2.1 Repositorios 12

2.2 Publicación de la información 12

2.3 Frecuencia de actualizaciones 12

2.4 Controles de acceso a los repositorios 12

3 Identificación y Autenticación 13

3.1 Registro de nombres 13

3.1.1 Tipos de nombres 13

3.1.2 Necesidad de que los nombres sean significativos 13

3.1.3 Pseudónimos o anónimos 13

3.1.4 Reglas utilizadas para interpretar varios formatos de nombres 13

3.1.5 Unicidad de los nombres 13

3.1.6 Resolución de conflictos relativos a nombres y marcas 13

3.2 Validación inicial de la identidad 14

3.2.1 Prueba de posesión de clave privada 14

3.2.2 Autenticación de la identidad del solicitante 14

3.3 Renovación de la clave 14

3.4 Solicitud de Revocación 14

4 Requisitos Operacionales 15
4.1 Solicitud del Certificado 15
4.2 Procedimiento de tramitación 15
4.2.1 Autenticación de identidad 15
4.2.1.1 Solicitante 15
4.2.1.2 Responsable del certificado 16
4.2.1.3 Suscriptor 17
4.2.1.3.1 Personas jurídicas 17
4.2.1.3.2 Personas físicas 17
4.2.2 Aprobación o rechazo de las solicitudes de certificados 18
4.2.3 Tiempo para procesar la emisión de certificados 19
4.3 Emisión del certificado 19
4.3.1 Acciones de la Entidad de Certificación durante el proceso de emisión 19
4.3.2 Notificación al suscriptor 19
4.4 Aceptación del certificado 19
4.4.1 Aceptación 19
4.4.2 Devolución 20
4.4.3 Seguimiento 20
4.4.4 Publicación del certificado 20
4.4.5 Notificación de la emisión del certificado a terceros 20
4.5 Denegación 20
4.6 Renovación de certificados 20
4.6.1 Certificados vigentes 20
4.6.2 Personas autorizadas para solicitar la renovación 21
4.6.3 Identificación y autenticación de las solicitudes de renovación rutinarias 21
4.6.4 Aprobación o rechazo de las solicitudes de renovación 21
4.6.5 Notificación de la renovación del certificado 21
4.6.6 Aceptación de la renovación del certificado 21
4.6.7 Publicación del certificado renovado 21
4.6.8 Notificación a otras entidades 21
4.6.9 Identificación y autenticación de las solicitudes de renovación de clave después de una revocación -Clave no comprometida- 22
4.7 Modificación del certificado 22
4.8 Revocación y suspensión de certificados 22
4.8.1 Causas de revocación 22
4.8.2 Identificación y autenticación de solicitudes de revocación 22
4.8.3 Procedimiento para la solicitud de revocación 23
4.8.4 Periodo de gracia de la solicitud de revocación 24
4.8.5 Plazo máximo de procesamiento de la solicitud de revocación 24
4.8.6 Requisitos de comprobación de listas CRL 24
4.8.7 Frecuencia de emisión de CRL 24

4.8.8 Disponibilidad de comprobación on-line de la revocación 24
4.8.9 Requisitos de la comprobación on-line de la revocación 24
4.8.10 Suspensión del certificado 24
4.8.11 Identificación y autenticación de solicitudes de suspensión 25
4.9 Depósito y recuperaciónde claves 25

5 Controles de seguridad física, instalaciones, gestión y operacionales 26
5.1 Controles de seguridad física 26
5.2 Controles de procedimiento 26
5.3 Controles de personal 26

6 Controles de seguridad técnica 27
6.1 Generación e instalación del par de claves 27
6.2 Protección de la clave privada 27
6.3 Otros aspectos de gestión del par de claves 27
6.4 Datos de activación 27
6.5 Controles de seguridad informática 27
6.6 Controles técnicos del ciclo de vida 27
6.7 Controles de seguridad de la red 27
6.8 Sellado de tiempo 27
6.9 Controles de seguridad de los módulos criptográficos 27

7 Perfiles de certificados, listas CRL y OCSP 28
7.1 Perfiles de certificados 28
7.1.1 Campos y extensiones comunes 29
7.1.2 Campos específicos según algoritmo de firma 35
7.1.3 Campos específicos según longitud de clave 36
7.1.4 Campos específicos según tipo de certificado 36
7.1.4.1 Certificado de Aplicación 36
7.1.4.2 Certificado de Firma de Código 37
7.1.4.3 Certificado de Cifrado 38
7.2 Perfil de CRL 38
7.3 Perfil de OCSP 38

8 Auditoría de conformidad 39
8.1 Frecuencia de los controles de conformidad para cada entidad 39
8.2 Identificación del personal encargado de la auditoría 39
8.3 Relación entre el auditor y la entidad auditada 39
8.4 Listado de elementos objeto de auditoría 39
8.5 Acciones a emprender como resultado de una falta de conformidad 39
8.6 Tratamiento de los informes de auditoría 39

9 Disposiciones generales 40
9.1 Tarifas 40

9.2 Responsabilidad financiera 40
9.3 Confidencialidad de la información 40
9.4 Privacidad de la información personal 40
9.5 Derechos de Propiedad Intelectual 40
9.6 Obligaciones y garantías 40
9.7 Exclusión de garantías 40
9.8 Limitaciones de responsabilidad 40
9.9 Interpretación y ejecución 40
9.10 Administración de la PC 40

Anexo I Formulario de Solicitud de Certificado Electrónico 41

Anexo II Contrato de Prestación de Servicios de Certificación Electrónica 47

Anexo III Acta de Autorización y Aceptación de Responsabilidad en la utilización del Certificado 52

Anexo IV Carta de Solicitud de Renovación de Certificado 53

Anexo V Formulario de Solicitud de Revocación del Certificado 54

Anexo VI Acta de Recepción y Aceptación del Certificado 56

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-).

El presente documento es la Política de Certificación (PC) correspondiente a los certificados emitidos por ANF AC del tipo “Aplicación, Firma de Código y Cifrado”. Esta documentación define los requisitos de procedimiento y operacionales a los que se sujeta el uso de estos certificados, y define las directrices que ANF AC utiliza para su emisión, gestión, revocación, renovación y cualquier otro proceso que afecte al ciclo de vida. Se describen los papeles, responsabilidades y relaciones entre el usuario final y ANF AC, así como las reglas de solicitud, renovación y revocación que se deben atender.

Este documento es sólo uno de los diversos documentos que rigen la PKI de ANF AC, detalla y complementa lo definido en la Declaración de Prácticas de Certificación y su adenda, ANF AC tutela y supervisa que esta PC sea compatible y esté en coherencia con el resto de documentos que ha elaborado. Toda la documentación está a libre disposición de usuarios y terceros que confían en el sitio web https://www.anf.es.

La Infraestructura de Claves Públicas (PKI) de ANF AC, ha sido diseñada y es gestionada en conformidad con la norma técnica ETSI TS 101 456 (Política de requisitos para las Autoridades de Certificación que emiten certificados reconocidos). Las especificaciones técnicas (TS) que se definen en esta norma TS 101 456 marcan los requisitos básicos en lo que se refiere a la gestión y prácticas de certificación de entidades certificadoras que emiten certificados reconocidos, dentro del marco legal de la Directiva 1999/93/EC del Parlamento europeo incorporada al régimen jurídico español en la ley de firma electrónica 59/2003. Asimismo, la PKI está en conformidad con la norma ETSI TS 102 042 v.2.1.1 (Policy Requirements for certification authorities issuing public key certificates).

De conformidad con el marco IETF RFC 3647 PKIX, esta PC se divide en nueve secciones que cubren los controles de seguridad, las prácticas y procedimientos para la certificación o servicios de estampado de tiempo en la PKI de ANF AC. Para preservar el esquema especificado por el documento RFC 3647, se han respetado los títulos de cada sección. Cuando no son de aplicación a esta PKI, se reseña "no aplicable". En el caso de que estén definidos en otro documento publicado por ANF AC, se reseña “Según lo definido en –*nombre del documento*-”.

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.

1.1 Descripción de los certificados

ANF AC, en el marco de su Servicio de Certificación Electrónica, emite certificados de identidad del tipo:

- **Certificado de Aplicación**

Se trata de un certificado empleado por una aplicación informática para asegurar la autenticidad e integridad de su información.

La validez de estos certificados es de 2 años.

- **Certificado de Firma de Código**

Se trata de un certificado empleado para la firma de código ejecutable, con el objetivo de garantizar la identidad del autor y la integridad del contenido (código) de una aplicación de software.

La validez de estos certificados es de 2 años.

- **Certificado de Cifrado**

Se trata de un certificado empleado para la realización de procesos de cifrado asimétrico.

La validez de estos certificados es de 2 años.

1.2 Identificación

Nombre del documento	Política de Certificación de Certificados de Aplicación, Firma de Código y Cifrado
Versión	1.5
Estado de la política	APROBADO
Referencia del documento / OID	1.3.6.1.4.1.18332.34.1.1
Fecha de emisión	17 de junio de 2014
Fecha de expiración	No es aplicable
DPC relacionada	Declaración de Prácticas de Certificación (DPC) de ANF AC
Localización	https://www.anf.es/documentos/

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

Certificado	OID
Certificado de Aplicación Con algoritmo SHA-1 y longitud 1024 bits	1.3.6.1.4.1.18332.34.1.1.1.11
Certificado de Aplicación Con algoritmo SHA-1 y longitud 2048 bits	1.3.6.1.4.1.18332.34.1.1.1.12

Certificado de Aplicación Con algoritmo SHA-256 y longitud 2048 bits	1.3.6.1.4.1.18332.34.1.1.1.22
Certificado de Firma de Código Con algoritmo SHA-1 y longitud 1024 bits	1.3.6.1.4.1.18332.34.1.1.2.11
Certificado de Firma de Código Con algoritmo SHA-1 y longitud 2048 bits	1.3.6.1.4.1.18332.34.1.1.2.12
Certificado de Firma de Código Con algoritmo SHA-256 y longitud 2048 bits	1.3.6.1.4.1.18332.34.1.1.2.22
Certificado de Cifrado Con algoritmo SHA-1 y longitud 1024 bits	1.3.6.1.4.1.18332.34.1.1.3.11
Certificado de Cifrado Con algoritmo SHA-1 y longitud 2048 bits	1.3.6.1.4.1.18332.34.1.1.3.12
Certificado de Cifrado Con algoritmo SHA-256 y longitud 2048 bits	1.3.6.1.4.1.18332.34.1.1.3.22

1.3 Comunidad de usuarios

1.3.1 Autoridades de Certificación

Según lo definido en la Declaración de Prácticas de Certificación (DPC) de ANF AC. Son las entidades que emiten los certificados electrónicos que vinculan una clave pública con la identidad del suscriptor. Actúan como tercera parte de confianza, entre el Suscriptor y el Tercero que confía.

1.3.2 Autoridades de Registro

Son las entidades que realizan los procedimientos de inscripción de los solicitantes de certificados de entidad final. Llevan a cabo la identificación y autenticación de las personas físicas que intervienen en la solicitud, y tienen la capacidad de iniciar o colaborar en los trámites de revocación o renovación de certificados.

Estas entidades pueden pertenecer a la propia organización de la entidad de certificación, y pueden ser colaboradores externos, en cuyo caso ANF AC define dos tipos:

1.3.2.1 Autoridad de Registro Reconocida

Según lo definido en la DPC de ANF AC.

1.3.2.2 Autoridad de Registro Colaboradora

Según lo definido en la DPC de ANF AC.

1.3.3 Responsable de Dictámenes de Emisión

Según lo definido en la DPC de ANF AC.

1.3.4 Entidades finales

1.3.4.1 Suscriptor del certificado

Es la persona, física o jurídica, titular del certificado.

1.3.4.2 Solicitante del certificado

El certificado debe ser solicitado por una persona física, mayor de edad, con plena capacidad de obrar y, en caso de actuar en nombre de tercero, con capacidad legal suficiente para asumir la representación del suscriptor.

1.3.4.3 Responsable del certificado

El responsable del certificado deberá de contar con una autorización expresa por parte del solicitante, y su identidad será incluida en el certificado.

El responsable del certificado tiene que ser una persona física mayor de edad, con plena capacidad de obrar y debe hacer constar su consentimiento para asumir esta responsabilidad.

El responsable del certificado está en posesión del dispositivo de creación de firma, es responsable de su uso y custodia. Su identidad será incluida en el certificado en calidad de representante legal y de acuerdo con el Artículo 6 de la Ley 59/2003:

> "*el firmante es la persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa.*"

1.3.4.4 Terceros que confían

Según lo definido en la DPC de ANF AC.

1.4 Uso de los certificados

1.4.1 Usos permitidos

De forma general según lo establecido en la Declaración de Prácticas de Certificación de ANF AC, y de forma específica:

- Certificado de Aplicación: se utilizará exclusivamente para firmar aplicaciones, o partes de ellas, para garantizar su autenticación e integridad.

- Certificado de Firma de Código: se utilizará para garantizar la identidad del autor y la integridad del contenido de una aplicación software.

- Certificado de Cifrado: se utilizará para realizar operaciones de cifrado de datos.

1.4.2 Límites de uso de los certificados

De forma general, según lo establecido en la Declaración de Prácticas de Certificación de ANF AC.

De forma específica, cabe reseñar que este certificado será utilizado por los suscriptores en las relaciones que mantengan con terceros que confían, de acuerdo con los usos autorizados en los campos 'Key Usage' y 'Extended Key Usage' del certificado y en conformidad con las limitaciones de uso que consten en el certificado y, además, asumiendo la limitación de responsabilidad que consta en el OID 1.3.6.1.4.1.18332.41.1 y/o en QcLimitValueOID 0.4.0.1862.1.2.

El suscriptor sólo podrá utilizar el par de claves y el certificado tras aceptar las condiciones de uso establecidas en la DPC.

1.4.3 Usos prohibidos

Según lo definido en la DPC de ANF AC.

1.5 Datos de contacto de la Entidad de Certificación

Según lo definido en la DPC de ANF AC.

1.6 Definiciones y Acrónimos

Según lo definido en la DPC de ANF AC.

2 Repositorios y publicación de la información

2.1 Repositorios

Según lo definido en la DPC de ANF AC.

2.2 Publicación de la información

Según lo definido en la DPC de ANF AC.

2.3 Frecuencia de actualizaciones

Según lo definido en la DPC de ANF AC.

2.4 Controles de acceso a los repositorios

Según lo definido en la DPC de ANF AC.

3 Identificación y Autenticación

3.1 Registro de nombres

3.1.1 Tipos de nombres

En conformidad con el Artículo 11.2 letra e) de la Ley 59/2003, de 19 de diciembre de 2003, los atributos contenidos en el campo Subject permiten la identificación del firmante.

Todos los certificados contienen un nombre distintivo (DN) del titular del certificado, definido de acuerdo con lo previsto en la Recomendación ITUT X.501 y contenido en el campo Subject, incluyendo un componente CommonName.

El atributo CN (CommonName) del DN tiene que hacer referencia al nombre del suscriptor o al departamento al que está adscrito y al cargo que ostenta.

El atributo O (Organization) debe hacer referencia al nombre de la entidad privada o pública con la que el suscriptor tiene una vinculación profesional, y esta vinculación debe quedar acreditada documentalmente ante la Autoridad de Registro y ser verificada por el RDE.

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 Necesidad de que los nombres sean significativos

Los nombres distintivos deben tener sentido, salvo en el caso de certificados emitidos bajo seudónimos.

3.1.3 Pseudónimos o anónimos

En el caso de certificados emitidos con seudónimo, el atributo CN especificará el concepto “Seudónimo”.

3.1.4 Reglas utilizadas para interpretar varios formatos de nombres

Según lo definido en la DPC de ANF AC.

3.1.5 Unicidad de los nombres

Según lo definido en la DPC de ANF AC.

3.1.6 Resolución de conflictos relativos a nombres y marcas

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

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

3.2 Validación inicial de la identidad

3.2.1 Prueba de posesión de clave privada

Según lo definido en la DPC de ANF AC.

3.2.2 Autenticación de la identidad del solicitante

Los Certificados emitidos bajo esta Política de Certificación identificarán al suscriptor que solicita la emisión del certificado, al solicitante del certificado y, en caso de ser persona distinta del solicitante, al responsable del certificado.

El Responsable de Dictámenes de Emisión utilizará los medios oportunos para asegurarse de la veracidad de la información contenida en el certificado. Entre estos medios se cuentan bases registrales externas y la posibilidad de requerir información o documentación complementaria al suscriptor.

Los identificativos fiscales del suscriptor y del solicitante se incorporarán en el certificado.

El tipo de documentación, las modalidades de tramitación, los procedimientos de autenticación y la validación quedan especificados en las siguientes secciones.

3.3 Renovación de la clave

En el supuesto de renovación de la clave, ANF AC informará previamente al suscriptor sobre los cambios que se hayan producido en los términos y condiciones respecto a la emisión anterior.

Se podrá emitir un nuevo certificado manteniendo la anterior clave pública, siempre que siga considerándose criptográficamente segura.

3.4 Solicitud de Revocación

Todas las solicitudes de revocación deben estar autenticadas. ANF AC comprobará la capacidad del solicitante para tramitar este requerimiento.

4 Requisitos Operacionales

4.1 Solicitud del Certificado

ANF AC sólo admite solicitud de emisión de certificado tramitada por una persona física mayor de edad, con capacidad plena de obrar y con representación legal suficiente.

El solicitante deberá cumplimentar el Formulario de Solicitud del certificado, asumiendo la responsabilidad de la veracidad de la información reseñada, y tramitarlo ante ANF AC utilizando alguno de los siguientes medios:

a) Por vía telemática. En el sitio web https://www.anf.es, los interesados disponen del formulario de solicitud, que deberá ser cumplimentado y firmado electrónicamente mediante un certificado reconocido, de acuerdo con lo establecido en la Ley 59/2003, de 19 de diciembre, de firma electrónica. El certificado utilizado debe haber sido emitido por una Autoridad de Certificación admitida por ANF AC.

b) Presencialmente: el solicitante podrá personarse ante una Autoridad de Registro Reconocida, en cuya presencia procederá a firmar el formulario de solicitud que deberá estar debidamente cumplimentado.

c) Por correo ordinario: el solicitante podrá remitir a las oficinas de ANF AC el formulario de solicitud del certificado, debidamente cumplimentado y habiendo autenticado su firma ante una Autoridad de Registro Colaboradora.

ANF AC no genera las claves de sus usuarios. El solicitante debe generar su par de claves y el certificado de petición en formato PKCS#10, utilizando en este proceso un dispositivo homologado por ANF AC.

En el caso del certificado de aplicación, el solicitante habrá generado previamente un par de claves en el propio servidor entregando a ANF AC la clave pública junto con el formulario de solicitud.

4.2 Procedimiento de tramitación

4.2.1 Autenticación de identidad

4.2.1.1 Solicitante

Cuando la tramitación se realice de forma presencial ante una Autoridad de Registro Reconocida, deberá acreditar su identidad y presentar, en vigor, original o copia auténtica de la siguiente documentación:

a) Dirección física y otros datos que permitan contactar con él. Si la ARR o el RDE lo consideran necesario, pueden solicitar documentos adicionales para cotejar la fiabilidad de la información, como por ejemplo facturas recientes de servicios públicos o extractos de cuenta bancaria. Si la ARR o el RDE conocen de forma personal al solicitante, deberán emitir y firmar una Declaración de Identidad*[1].

b) La ARR, como acreditación del acto presencial y con el fin de imposibilitar el repudio del trámite realizado, podrá obtener un conjunto de evidencias biométricas: fotografía y/o huellas dactilares.

c) Cédula de identificación o pasaporte en caso de ciudadanos nacionales, cuya fotografía permita cotejar la identidad de la persona compareciente, en caso de escasa nitidez podrá solicitar otro documento oficial que incorpore fotografía (p.ej., licencia de conducir).

d) En caso de ciudadanos extranjeros, se requerirá:

I. A miembros de la Unión Europea o de Estados parte del Espacio Económico Europeo:

- Documento nacional de identidad (o equivalente en su país de origen) o pasaporte que incluya fotografía que permita cotejar la identidad de la persona compareciente. En caso de escasa nitidez, se podrá solicitar otro documento oficial que incorpore fotografía (p.ej., licencia de conducir).

- Certificado emitido por el Registro de Ciudadanos Miembros de la Unión.

II. A ciudadanos extracomunitarios:

- Pasaporte, tarjeta de residencia y permiso de trabajo, que incluya fotografía que permita cotejar la identidad de la persona compareciente. En caso de escasa nitidez podrá solicitar otro documento oficial que incorpore fotografía, (p. ej., licencia de conducir).

e) En caso de que el solicitante intervenga en representación de tercero, se requerirá poder suficiente de representación.

La documentación acreditativa de poder suficiente que posee el representante legal del suscriptor puede tener tal consideración:

- Administradores. Original o copia auténtica de las escrituras o del Certificado del Registro correspondiente relativo a su nombramiento y vigencia del cargo.

- Se considera que tienen poder bastante los representantes voluntarios cuando tengan otorgado un poder específico, claramente determinado y enunciado expresamente para solicitar certificado electrónico, en nombre y representación de la persona jurídica.

Podrá prescindirse de la personación ante la Autoridad de Registro en alguno de los siguientes supuestos:

1. Si los formularios correspondientes han sido debidamente cumplimentados y la firma del suscriptor ha sido legitimada en presencia notarial, adjuntado copias compulsadas de los documentos de identidad, autorización y representación legal.

2. Tramitación vía telemática. En el sitio web https://www.anf.es los interesados disponen del formulario de solicitud, que deberá ser cumplimentado y firmado electrónicamente mediante un certificado reconocido de acuerdo con lo establecido en la Ley 59/2003, de 19 de diciembre, de firma electrónica. El certificado utilizado debe haber sido emitido por una CA admitida por ANF AC.

4.2.1.2 Responsable del certificado

Se seguirá el mismo procedimiento que el especificado en el anterior apartado “4.2.1.1 Solicitante”, con la particularidad de que, en este supuesto, el poder de representación requerido al solicitante será sustituido por la firma del Acta de Autorización y Aceptación de Responsabilidad incluida en este documento. El acta deberá ser firmada por el Solicitante y por el Responsable del Certificado.

4.2.1.3 Suscriptor

4.2.1.3.1 Personas jurídicas

Se requiere:

- Dirección física y otros datos que permitan contactar con la entidad. Si la ARR o el RDE lo consideran necesario, pueden solicitar documentos adicionales para cotejar la fiabilidad de la información como, por ejemplo, facturas recientes de servicios públicos o extractos de cuenta bancaria. Si el ARR o el RDE conocen de forma personal al suscriptor, deberán emitir y firmar una Declaración de Identidad[*1].

- Cedula de identificación fiscal (CIF) de la entidad.

- Según forma jurídica:

    - Sociedades mercantiles y demás personas jurídicas cuya inscripción sea obligatoria en el Registro Mercantil, acreditarán la válida constitución mediante la aportación de original o copia auténtica del Registro Mercantil relativo a los datos de constitución y cargos vigentes de administración de la entidad.

    - 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.

    - Sociedades civiles y demás personas jurídicas, aportarán original o copia auténtica del documento público que acredite su constitución de manera fehaciente.

    - 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.

        - Entidades creadas por norma, aportarán referencia a la norma de creación.

***1 Declaración de Identidad**

Consiste en una declaración formal jurada, en la que el declarante manifiesta que conoce de forma personal y directa a una determinada persona física o a una persona jurídica. Además, hace constar, hasta donde alcance su conocimiento directo, que ha verificado los datos de filiación reseñados en el Formulario de Solicitud: dirección, teléfono y correo electrónico, y que son ciertos. La Declaración de Identidad incorpora la identidad del declarante, su cédula de identidad, la información que ha sido validada, la fecha y hora de la verificación, la firma del declarante y los apercibimientos legales correspondientes en caso de incurrir en perjurio.

4.2.1.3.2 Personas físicas

Se seguirá el mismo procedimiento que el especificado en el apartado anterior “4.2.1.1 Solicitante del certificado”.

4.2.2 Aprobación o rechazo de las solicitudes de certificados

El Responsable de Dictámenes de Emisión (RDE) asume la responsabilidad última de verificar la información contenida en el Formulario de Solicitud, valorar la suficiencia de los documentos aportados y la adecuación de la solicitud de acuerdo con lo establecido en esta Política de Certificación.

Además, determinará:

- Que el suscriptor ha tenido acceso a la información que establece los términos y condiciones relativos al uso del certificado, así como a las tasas de emisión del mismo.

- Que el suscriptor ha tenido acceso y tiene permanente acceso a toda la documentación relativa a las obligaciones y responsabilidades de la CA, del suscriptor, del solicitante, del responsable del certificado y de terceros que confían, en especial a la DPC y Políticas de Certificación.

Y supervisará que se cumplen todos los requisitos impuestos por la legislación aplicable en materia de protección de datos, siguiendo lo establecido en el documento de seguridad incluido en la DPC, a efectos de la LOPD según lo previsto en el artículo 19.3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

El proceso de emisión del certificado no se iniciará en tanto en cuanto el Responsable de Dictámenes de Emisión no haya emitido el correspondiente informe de conformidad. El plazo máximo establecido para la emisión del informe será de 15 días. Transcurrido ese plazo sin emisión del preceptivo informe, el solicitante podrá dar por anulado el pedido y recibir las tasas que haya abonado.

El RDE puede requerir del solicitante información o documentación complementaria y el solicitante dispondrá de 15 días para hacer entrega de la misma. Transcurrido este plazo sin que se haya cumplimentado este requerimiento, el RDE emitirá informe denegando la emisión. En caso de atender el requerimiento, el RDE dispondrá de 7 días para emitir informe definitivo.

En caso de que el RDE compruebe que la información facilitada por el solicitante no es veraz, denegará la emisión del certificado y generará un incidente informando al Coordinador de Seguridad, a fin de determinar la inclusión o no del solicitante en la lista negra de personas y entidades 1.3.6.1.4.1.18332.56.2.1.

El procedimiento de validación, según tipo de certificado, es:

- El RDE comprobará la documentación aportada por el solicitante y por la Autoridad de Registro.

- En el proceso de validación intervendrán dando soporte el Departamento Jurídico y el Departamento Técnico que revisará y validará técnicamente el certificado de petición PKCS#10.

- En el proceso de comprobación de la información y documentación recibida, se podrán utilizar los siguientes medios:

    - Consulta a los registros públicos oficiales en los que deba estar inscrita la entidad a efectos de comprobar existencia, vigencia de cargos y otros aspectos legales, como actividad y fecha de constitución.

    - Boletines Oficiales de ámbito nacional o regional de los organismos públicos a los que pertenecen organismos y empresas públicas.

- Se comprobará que el suscriptor no está sometido a procedimiento concursal, ni que sus antecedentes comerciales hagan sospechar actividades fraudulentas, mediante consulta a

Registros debidamente autorizados al efecto.

- Se verifica que ninguna de las personas físicas asociadas a la solicitud consta en la lista negra de personas y entidades 1.3.6.1.4.1.18332.56.2.1.

4.2.3 Tiempo para procesar la emisión de certificados

La emisión de un certificado implica la aprobación final y completa de una solicitud por parte del Responsable de Dictámenes de Emisión. La emisión de certificado debe realizarse en un plazo máximo de 48 horas una vez emitido el informe del RDE, según lo definido en la DPC de ANF AC.

4.3 Emisión del certificado

Según lo definido en la DPC de ANF AC.

ANF AC evitará generar certificados que caduquen con posterioridad a los certificados de la CA que los emitió.

4.3.1 Acciones de la Entidad de Certificación durante el proceso de emisión

Según lo definido en la DPC de ANF AC.

Una vez emitido el certificado electrónico, la entrega del certificado siempre se realiza de forma telemática. Se debe emplear el mismo dispositivo criptográfico que el suscriptor o su representante legal utilizó para la generación del par de claves criptográficas y el certificado de petición PKCS#10.

El dispositivo criptográfico establece conexión segura con los servidores de confianza de ANF AC. El sistema realiza de forma automática las correspondientes comprobaciones de seguridad. En caso de confirmación, el certificado es descargado e instalado automáticamente.

4.3.2 Notificación al suscriptor

ANF AC, mediante correo electrónico, notifica al suscriptor la emisión y publicación del certificado.

4.4 Aceptación del certificado

4.4.1 Aceptación

A partir de la entrega del certificado, el suscriptor dispondrá de un periodo de siete días naturales para comprobar el certificado, determinar si es adecuado y si los datos se corresponden con la información requerida. El suscriptor dispone de un plazo de 15 días para firmar el Acta de Recepción y Aceptación del certificado recibido.

Mediante la firma del Acta de Recepción y Aceptación, el suscriptor confirma la recepción del certificado; su aceptación a la emisión realizada; la correcta funcionalidad del producto; su capacidad de utilizarlo al firmar la propia acta con este certificado; su sometimiento a la DPC y a las Políticas de ANF AC; su compromiso de utilizarlo de acuerdo con las limitaciones de uso y dentro de la finalidad para el que ha

sido emitido; su responsabilidad en mantener la confidencialidad de la clave privada; y el compromiso de cesar en su uso después de la pérdida de vigencia, bien por caducidad o por revocación.

4.4.2 Devolución

El suscriptor dispone de un periodo de 7 días desde la entrega del certificado para comprobar el correcto funcionamiento del mismo.

En caso de defectos de funcionamiento por causas técnicas o por errores en los datos contenidos en el certificado, el solicitante o el responsable del certificado puede mandar un email firmado electrónicamente a ANF AC, informando del motivo de la devolución. ANF AC verificará las causas de devolución, revocará el certificado emitido y procederá a emitir un nuevo certificado en un plazo máximo de 72 horas.

4.4.3 Seguimiento

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, este puede ser revocado.

4.4.4 Publicación del certificado

El certificado es publicado en los repositorios de ANF AC en un plazo máximo de 24 h. desde que se ha producido su emisión.

4.4.5 Notificación de la emisión del certificado a terceros

No se efectúa notificación a terceros.

4.5 Denegación

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

4.6 Renovación de certificados

Con carácter general, según lo establecido en la Declaración de Prácticas de Certificación de ANF AC.

4.6.1 Certificados vigentes

ANF AC notifica por correo electrónico al suscriptor y al solicitante la caducidad del certificado, remitiendo el formulario de solicitud, con el objetivo de proceder a su renovación. Estas notificaciones se envían con 90, 30 y 15 días de antelación a la fecha de caducidad del certificado.

Sólo los certificados en estado de vigencia pueden ser renovados.

4.6.2 Personas autorizadas para solicitar la renovación

El formulario de solicitud de renovación debe ser firmado por el mismo representante legal que tramitó la solicitud del certificado. Las circunstancias personales del solicitante no deben haber variado, en especial su capacidad de representación legal.

4.6.3 Identificación y autenticación de las solicitudes de renovación rutinarias

La identificación y autenticación para la renovación del certificado se puede realizar presencialmente, utilizando alguno de los medios descritos en esta sección, o bien tramitando la solicitud de renovación telemáticamente cumplimentando el formulario correspondiente y firmándolo electrónicamente con un certificado vigente emitido con la calificación de "reconocido", en el que figure como titular el suscriptor del certificado del que se solicita renovación.

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

4.6.4 Aprobación o rechazo de las solicitudes de renovación

Se seguirá el mismo procedimiento que el realizado en el proceso de emisión especificado en este documento.

4.6.5 Notificación de la renovación del certificado

Se seguirá el mismo procedimiento que el realizado en el proceso de emisión especificado en este documento.

4.6.6 Aceptación de la renovación del certificado

Se seguirá el mismo procedimiento que el realizado en el proceso de emisión especificado en este documento.

4.6.7 Publicación del certificado renovado

Se seguirá el mismo procedimiento que el realizado en el proceso de emisión especificado en este documento.

4.6.8 Notificación a otras entidades

Según lo indicado en el apartado "4.4.5 Notificación de la emisión del certificado a terceros".

4.6.9 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.

4.7 Modificación del certificado

No es aplicable.

4.8 Revocación y suspensión de certificados

Con carácter general según lo establecido en la Declaración de Prácticas de Certificación de ANF AC.

4.8.1 Causas de revocación

Además de lo previsto en la Declaración de Prácticas de Certificación, ANF AC:

- Facilitará instrucciones y dará soporte jurídico para la presentación de denuncias o sospechas de compromiso de la clave privada, de mal uso de certificados o de cualquier tipo de fraude o conducta impropia.

- ANF AC investigará las incidencias de las que tenga conocimiento dentro de las veinticuatro horas siguientes a su recepción. El Responsable de Seguridad, en base a las indagaciones y comprobaciones realizadas, emitirá informe al Responsable de Dictámenes de Emisión, el cual determinará en su caso la correspondiente revocación mediante Acta fundamentada, en la cual constará:

    - La naturaleza de la incidencia.

    - Informaciones recibidas.

    - Normas legales y regulación sobre la que se fundamente la orden de revocación.

4.8.2 Identificación y autenticación de solicitudes de revocación

Podrán solicitar la revocación de un certificado:

- El suscriptor del certificado.

- El representante legal del suscriptor.

- Un representante debidamente autorizado.

- ANF AC.

- La Autoridad de Registro Reconocida que intervino en la tramitación de la solicitud de emisión del certificado.

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 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 los números:
  902 902 172 (Llamadas desde España)
  Internacional +34 933 935 946.

- De forma presencial: personándose el suscriptor o el representante legal del titular del certificado en alguna de las oficinas de ANF AC publicadas en la dirección web www.anf.es/sedes.html; acreditando su identidad mediante documentación original y firmando de forma manuscrita el formulario correspondiente.

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

4.8.3 Procedimiento para la solicitud de revocación

El solicitante de la Revocación debe cumplimentar el Formulario de Solicitud de Revocación y tramitarlo ante ANF AC por cualquiera de los medios que están previstos en este documento.

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.

Una vez autenticada la petición, ANF AC podrá revocar directamente el certificado e informar al suscriptor y, en su caso, al responsable del certificado sobre el cambio de estado del certificado.

4.8.4 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 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.

4.8.5 Plazo máximo de procesamiento de la solicitud de revocación

La solicitud de revocación será procesada en el mínimo plazo posible, siempre siguiendo el procedimiento de verificación y autenticación de la solicitud presentada, cuya responsabilidad recae en el Responsable de Dictámenes de Emisión.

4.8.6 Requisitos de comprobación de listas CRL

Los terceros que confían deben comprobar el estado de los certificados en los cuales va a confiar. Para ello pueden comprobar la última CRL emitida dentro del periodo de vigencia del certificado de interés.

4.8.7 Frecuencia de emisión de CRL

Según lo definido en la DPC de ANF AC.

4.8.8 Disponibilidad de comprobación on-line de la revocación

ANF AC pone a disposición de los terceros que confían un servicio on-line de comprobación de revocaciones, el cual está disponible las 24 horas del día los 7 días de la semana.

4.8.9 Requisitos de la comprobación on-line de la revocación

Los terceros que confían pueden comprobar de forma on-line la revocación de un certificado a través del sitio web www.anf.es.

El sistema de consulta de certificados de ANF AC requiere el conocimiento previo de algunos parámetros del certificado de interés. Este procedimiento impide la obtención masiva de datos.

Este servicio cumple los requerimientos establecidos en materia de Protección de Datos de Carácter Personal y únicamente suministra copia de estos certificados a terceros debidamente autorizados.

El acceso a este sistema de consulta de certificados es libre y gratuito.

4.8.10 Suspensión del certificado

No es aplicable.

4.8.11 Identificación y autenticación de solicitudes de suspensión

No está permitida la suspensión del certificado.

4.9 Depósito y recuperación de claves

ANF AC no almacena, ni tiene la posibilidad de almacenar, la clave privada de los suscriptores y, por lo tanto, no presta servicio de recuperación de claves.

5 Controles de seguridad física, instalaciones, gestión y operacionales

ANF AC mantiene los siguientes criterios con relación a la información disponible para auditorías y análisis de incidentes que pueda haber con los certificados.

a) Control y detección de incidentes

Cualquier interesado puede comunicar sus quejas o sugerencias a través de los siguientes medios:

- Por teléfono: 902 902 172 (Llamadas desde España) Internacional +34 933 935 946.
- Por correo electrónico: info@anf.es
- Cumplimentando el formulario electrónico disponible en el sitio web www.anf.es.
- Mediante personación en una de las oficinas de las Autoridades de Registro Reconocidas.
- Mediante personación en las oficinas de ANF AC.

El protocolo de auditoría interna anual requiere específicamente la realización de una revisión de la operativa de emisión de los certificados con una muestra mínima del 3% de los certificados emitidos.

b) Registro de Incidentes

ANF AC dispone de un Registro de Incidentes en el que se inscribe toda incidencia que se haya producido con los certificados emitidos y las evidencias obtenidas. Estos incidentes se registran, analizan y solucionan según los procedimientos del Sistema de Gestión de la seguridad de la Información de ANF AC.

El Coordinador de Seguridad determina la gravedad del incidente y nombra un responsable y, en caso de incidentes de seguridad relevantes, informa a la Junta Rectora de la PKI.

5.1 Controles de seguridad física

Según lo definido en la DPC de ANF AC.

5.2 Controles de procedimiento

Según lo definido en la DPC de ANF AC.

5.3 Controles de personal

Según lo definido en la DPC de ANF AC.

6 Controles de seguridad técnica

6.1 Generación e instalación del par de claves

Según lo definido en la DPC de ANF AC.

6.2 Protección de la clave privada

Según lo definido en la DPC de ANF AC.

6.3 Otros aspectos de gestión del par de claves

Según lo definido en la DPC de ANF AC.

6.4 Datos de activación

Según lo definido en la DPC de ANF AC.

6.5 Controles de seguridad informática

Según lo definido en la DPC de ANF AC.

6.6 Controles técnicos del ciclo de vida

Según lo definido en la DPC de ANF AC.

6.7 Controles de seguridad de la red

Según lo definido en la DPC de ANF AC.

6.8 Sellado de tiempo

Según lo definido en la DPC de ANF TSA CA.

6.9 Controles de seguridad de los módulos criptográficos

Según lo definido en la DPC de ANF AC.

7 Perfiles de certificados, listas CRL y OCSP

7.1 Perfiles de certificados

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

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.

El periodo de validez del certificado está reseñado en Tiempo Coordinado Universal y codificado conforme la especificación RFC 3280.

La clave pública del sujeto está codificada de acuerdo con la especificación RFC 5280, así como la generación y codificación de la firma.

Dentro de los certificados, además de los campos comunes ya estandarizados, se incluyen un conjunto de campos "propietarios" que aportan información relativa del suscriptor, o del representante legal, o del responsable del certificado, o de todos ellos; además, pueden incluir limitaciones de uso, de responsabilidad asumida por la Entidad de Certificación u otra información de interés.

Campos propietarios

Se han asignado identificadores unívocos a nivel internacional. Concretamente:

- Los campos referenciados con el identificador de objeto (OID) 1.3.6.1.4.1.18332.x.x son extensiones propietarias de ANF AC. La relación completa de códigos OID y la información asociada a los mismos puede ser consultada en la Sección "Campos Propietarios ANF AC" de la Declaración de Prácticas de Certificación de ANF AC.
- Los campos con el ISO/IANA del MPR 2.16.724.1.3.5.x.x son extensiones propietarias requeridas e identificadas en el Esquema de Identificación y Firma Electrónica v.1.7.6 publicado por el Consejo Superior de Administración Electrónica.
- Los campos con el OID 1.3.6.1.4.1.18838.1.1 son extensiones propietarias de la Agencia Estatal de Administración Tributaria (AEAT).

En cuanto a los campos propietarios de ANF AC, todos ellos están referenciados en la Declaración de Prácticas de Certificación de ANF AC, con descripción detallada de la información que pueden contener.

Certificados reconocidos

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. Además, el valor "Certificado Reconocido" se incluye en la extensión propietaria del OID 1.3.6.1.4.1.18332.40.1.

La lista de "QCStatements" es:

- QcCompliance (OID 0.4.0.1862.1.1) establece la calificación con la que se ha realizado la emisión «Certificado reconocido».

- QcLimitValue (OID 0.4.0.1862.1.2) informa del límite monetario que asume la CA como responsabilidad en la pérdida de transacciones a ella imputables. Este OID contiene la secuencia de valores: moneda (codificado conforme a la ISO 4217), cantidad y exponente. P.ej., EUROS 100x10 elevado a 1, lo que presupone límite monetario de 1000 EUROS.

  Además, con el fin de facilitar la consulta de esta información, el límite de responsabilidad se incluye en la extensión propietaria del OID 1.3.6.1.4.1.18332.41.1, que reseña de forma absoluta directamente. P.ej. 1000 euros. En caso de duda o discrepancia siempre se debe dar preferencia a la lectura del valor reseñado en el OID 1.3.6.1.4.1.18332.41.1

- QcEuRetentionPeriod (OID 0.4.0.1862.1.3) 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.

- QcSSCD (OID 0.4.0.1862.1.4) informa de si el certificado y las claves están contenidas en un dispositivo token criptográfico (en conformidad con la descripción realizada en la DPC de ANF AC).

SubjectAlternativeNames

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.

- 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 los nombres son verificados por la entidad emisora cuando son incluidos en el certificado.

7.1.1 Campos y extensiones comunes

Jerarquía ANF Global Root CA

I. Campos comunes

X.509v1 Field			
CAMPO	**CONTENIDO**	**CRÍTICO**	**OBLIGATORIO**
Versión	V3		**SI**

SerialNumber *[1]	Establecido automáticamente por la Entidad de Certificación. Se utilizará para identificar de manera unívoca el certificado		**SI**
SignatureValue	Firma codificada como cadena de bits		**SI**
Issuer (Emisor)			
CommonName (CN)	Nombre Común de la CA emisora del certificado		**SI**
SerialNumber	CIF del Prestador de Servicios de Certificación		**SI**
OrganizationalUnit (OU)	Unidad organizativa dentro del Prestador de Servicios de Certificación responsable de la emisión del certificado		**SI**
Organization (O)	Nombre oficial del Prestador de Servicios de Certificación		**SI**
Country (C)	País del Prestador de Servicios de Certificación		**SI**
Locality (L)	Localidad/dirección del Prestador de Servicios de Certificación		
State (ST)	Provincia donde se encuentra el Prestador de Servicios de Certificación		
EmailAddress (E)	Correo electrónico del Prestador de Servicios de Certificación		
Validity (Validez)			**SI**
notBefore	Fecha de inicio de validez		
notAfter	Fecha de fin de validez		
Subject (Sujeto)			**SI*[2]**
Organization (O) (String UTF8) Size 128 [RFC 5280]	Denominación o razón social del suscriptor. En caso de tratarse de persona física, el suscriptor podrá incluir un nombre comercial o marca registrada de la que tenga debida autorización de uso		**SI**
GivenName	Nombre del suscriptor. En el caso de persona jurídica, nombre del solicitante (como consta en la cédula de identidad)		
SurName	Apellidos del suscriptor. En el caso de persona jurídica, nombre del solicitante (como consta en la cédula de identidad)		

1.3.6.1.4.1.18838.1.1	NIF del solicitante		
SerialNumber	NIF del suscriptor. En el caso de persona jurídica, CIF del suscriptor		**SI**
Country (C)	País (Código de país de dos dígitos según ISO 3166-1)		**SI** *[3]
Locality (L)	Localidad/dirección del suscriptor		
State (ST)	Provincia del suscriptor		
Email (E)	Correo electrónico del suscriptor		

II. Extensiones comunes

X.509v3 Extensions			
CAMPO	**CONTENIDO**	**CRÍTICO**	**OBLIGATORIO**
AuthorityKeyIdentifier			**SI**
KeyIdentifier	Identificador de la clave pública del emisor. Conforme con RFC2459 & PKCS#1.		
AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier		
AuthorityCertSerialNumber	Número de serie del certificado de CA		
IssuerAlternativeName			
rfc822Name (String) Size 255 [RFC 5280]	Correo electrónico de contacto de la Entidad de Certificación emisora del certificado		
dNSName	DNS de la Entidad de Certificación emisora del certificado		
SubjectKeyIdentifier			**SI**
KeyIdentifier	Identificador derivado de utilizar la función de hash sobre la clave pública del sujeto Conforme con RFC2459 & PKCS#1		
CertificatePolicies			**SI**
PolicyIdentifier	Según lo indicado en el apartado 1.2 Identificación		
PolicyQualifierID			
PolicyCPSLocation	https://www.anf.es/documentos/		

userNotice (longitud nosuperior a 200 caracteres)	Se expresa una declaración realizada por la CA emisora, en la que se hace referencia a determinadas normas legales.		
SubjectAlternativeNames			
rfc822Name (String) Size [RFC 5280] 255	Dirección de correo electrónico de contacto indicada por el suscriptor		
dNSName	DNS indicada por el suscriptor		
SubjectDirectoryAttributes*[4]			
Title (T) (2.5.4.12)	Título/ cargo / rol del representante legal		
Description (2.5.4.13)	Información de interés del suscriptor		
TelephoneNumber (2.5.4.20)	Teléfono del suscriptor		
Facsimile (2.5.4.23)	Fax del suscriptor		
StreetAddress (2.5.4.9)	Dirección del suscriptor		
PostalAddress (2.5.4.16)	Dirección postal del suscriptor		
PostalCode (2.5.4.17)	Código postal del suscriptor		
CommonName (2.5.4.3)	Nombre completo del titular del certificado, de acuerdo con el documento de identidad y en mayúsculas		
Name (2.5.4.41)	Nombre de pila del representante legal		
SurName (2.5.4.4)	Apellidos del representante legal		
SerialNumber(2.5.4.5)	DNI / NIE*[5] del representante legal		
knowldgeinformation (2.5.4.2)	Protocolo y notario del poder de representación legal		
Extensiones propietarias			
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	NIF del responsable del certificado		
1.3.6.1.4.1.18332.29.5	Dirección de correo electrónico del responsable del certificado		

1.3.6.1.4.1.18332.29.6	Cargo/título/rol del responsable del certificado		
1.3.6.1.4.1.18332.29.7	Departamento al que está adscrito el responsable del certificado		
1.3.6.1.4.1.18332.29.8	Tipo de cédula de identidad presentada por el responsable del certificado		
1.3.6.1.4.1.18332.29.9	Nacionalidad del responsable del certificado		
1.3.6.1.4.1.18332.29.10	Dirección donde reside el responsable del certificado		
1.3.6.1.4.1.18332.29.11	Población donde reside el responsable del certificado		
1.3.6.1.4.1.18332.29.12	Provincia donde reside el responsable del certificado		
1.3.6.1.4.1.18332.29.13	Código postal donde reside el responsable del certificado		
1.3.6.1.4.1.18332.29.14	País donde reside el responsable del certificado		
1.3.6.1.4.1.18332.29.15	Teléfono fijo del responsable del certificado		
1.3.6.1.4.1.18332.29.16	Teléfono móvil del responsable del certificado		
1.3.6.1.4.1.18332.29.17	Dirección de correo electrónico del responsable del certificado		
1.3.6.1.4.1.18332.29.18	Fax del responsable del certificado		
BasicConstraints			
Entidad final CA : FALSE	Tipo de asunto=Entidad final Restricción de longitud de ruta=Ninguna	**SI**	**SI**
CRLDistributionPoints *[6]			
DistributionPoint[1]	Punto de distribución de la Web donde reside la CRL número 1		**SI**
DistributionPoint[2]	Punto de distribución de la Web donde reside la CRL número 2		
DistributionPoint[3]	Punto de distribución de la Web donde reside la CRL número 3		
AuthorityInformationAccess			**SI**
AccessMethod	Id-ad-ocsp con OID: 1.3.6.1.5.5.7.48.1		

AccessLocation	Dirección web para realizar consultas On-line Certificate Status Protocol		
caIssuers	URL de descarga del certificado emisor		
QcStatements OID 0.4.0.1862.1			
QcRetentionPeriod*[7] *OID 0.4.0.1862.1.3*	15 años Periodo de conservación de la información de uso del certificado		
QcCompliance *OID 0.4.0.1862.1.1*	Especifica si el certificado es emitido con la calificación de reconocido		
QcLimitValue *OID 0.4.0.1862.1.2*	Importe límite de responsabilidad asumido por el emisor expresado en EUROS		
QcSSCD *OID 0.4.0.1862.1.4*	Uso del dispositivo HSM para almacenar el certificado y firmar		
Campos condicionados por el uso del certificado			
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		
JurisdictionOfIncorporationLocalityName	[OID: 1.3.6.1.4.1.311.60.2.1.1] Localidad en la que está registrada la empresa (Opcional)		
JurisdictionOfIncorporationStateOrProvinceName	[OID: 1.3.6.1.4.1.311.60.2.1.2] Provincia en la que está registrada la empresa		
JurisdictionOfIncorporationCountryName	[OID: 1.3.6.1.4.1.311.60.2.1.3] País en el que está registrada la empresa		
Algoritmo de identificación	SHA1		**SI**
Huella digital	Huella digital del certificado		**SI**

***1** Según RFC5280. Número entero positivo, no mayor de 20 octetos (1- 2^{159}).

***2** Según RFC5280. El campo Subject debe de ser cumplimentado con carácter obligatorio.

***3** Según la ETSI-QC se debe reflejar obligatoriamente el campo Country (Ver RFC3739 / ETSI 101862).

***4** Según RFC5280. Atributos de Directorio del Sujeto (OID 2.5.29.9).

*[5] Número de Identificación de Extranjeros (NIE). En España, un código compuesto por una "X", "Y" o "Z", 8 dígitos y una letra, que sirve para la identificación de los no nacionales. Si el NIE tiene 7 dígitos, se suele añadir un 0 después de la X.

De acuerdo con el artículo 101 del Reglamento de Extranjería español, aprobado por Real Decreto 2393/2004, de 30 de diciembre, los extranjeros que, por sus intereses económicos, profesionales o sociales, se relacionen con España, serán dotados, a efectos de identificación, de un número personal, único y exclusivo, de carácter secuencial. El número personal será el identificador del extranjero, que deberá figurar en todos los documentos que se le expidan o tramiten, así como las diligencias que se estampen en su tarjeta de identidad o pasaporte.

*[6] Web donde resida la CRL (punto de distribución HTTPS o LDAP con servidor autenticado).

*[7] Según la norma ETSI TS 101 862 v1.3.3, describe el periodo de conservación de toda la información relevante para el uso de un certificado tras la caducidad de este.

7.1.2 Campos específicos según algoritmo de firma

X.509 v1 Field			
CAMPO	**CONTENIDO**	**CRÍTICO**	**OBLIGATORIO**
SignatureAlgorithm	Identificador del tipo de algoritmo de firma		**SI**
SignatureHashAlgorithm	Identificador del tipo de algoritmo de hash		**SI**

Pueden ser emitidos con algoritmo de firma:

- SHA-1WithRSAEncryption
- SHA-256WithRSAEncryption

En el supuesto de:

- "SHA-1WithRSAEncryption" el valor del campo SignatureHashAlgorithm es SHA1

En el caso de:

- "SHA-256WithRSAEncryption" el valor del campo SignatureHashAlgorithm es SHA256

La emisión de certificados con algoritmo de firma SHA256WithRSAEncryption requiere que la CA emisora utilice un certificado de igual o superior nivel.

7.1.3 Campos específicos según longitud de clave

X.509 v1 Field			
CAMPO	**CONTENIDO**	**CRÍTICO**	**OBLIGATORIO**
SubjectPublicKeyInfo	Clave pública del sujeto, codificado conforme con RFC2459 & PKCS#1		**SI**

Pueden ser emitidos con algoritmo y longitud de clave:

- RSA (1024 bits)
- RSA (2048 bits)

Los certificados emitidos con algoritmo de firma SHA-256WithRSAEncryption utilizarán longitud de clave mínima de 2048 bits.

7.1.4 Campos específicos según tipo de certificado

7.1.4.1 Certificado de Aplicación

X.509 v1 Field			
CAMPO	**CONTENIDO**	**CRÍTICO**	**OBLIGATORIO**
Subject (Sujeto)			**SI**
OrganizationalUnit (OU)	Certificado de Aplicación		**SI**
CommonName (CN)	Nombre de la Aplicación		**SI**

X.509v3 Extensions			
CAMPO	**CONTENIDO**	**CRÍTICO**	**OBLIGATORIO**
Uso de la clave			**SI**
KeyUsage -digitalSignature, nonRepudiation-	Digital Signature = 1	**SI**	
	Non Repudiation*[1] = 0		
	Key Encipherment = 0		
	Data Encipherment = 0		
	Key Agreement = 0		
	Key CertificateSignature = 0		

	CRL Signature = 0		
extKeyUsage (Uso extendido del certificado)	Autenticación del cliente (1.3.6.1.5.5.7.3.2)		
	Protección de e-mail (1.3.6.1.5.5.7.3.4)		

*[1] Non Repudiation (Content Commitment)

7.1.4.2 Certificado de Firma de Código

X.509v1 Field			
CAMPO	**CONTENIDO**	**CRÍTICO**	**OBLIGATORIO**
Subject (Sujeto)			**SI**
OrganizationalUnit (OU)	Certificado de Firma de Código		**SI**
CommonName (CN)	Nombre de la entidad o departamento, en mayúsculas		**SI**

X.509v3 Extensions			
CAMPO	**CONTENIDO**	**CRÍTICO**	**OBLIGATORIO**
Uso de la clave			**SI**
KeyUsage -digitalSignature, nonRepudiation-	Digital Signature = 0	**SI**	
	Non Repudiation*[1] = 1		
	Key Encipherment = 0		
	Data Encipherment = 0		
	Key Agreement = 0		
	Key CertificateSignature = 0		
	CRL Signature = 0		
extKeyUsage (Uso extendido del certificado)	codeSigning (1.3.6.1.5.5.7.3.3)		

*[1] Non Repudiation (Content Commitment)

7.1.4.3 Certificado de Cifrado

X.509v1 Field			
CAMPO	**CONTENIDO**	**CRÍTICO**	**OBLIGATORIO**
Subject (Sujeto)			**SI**
OrganizationalUnit (OU)	Certificado de Cifrado		**SI**
CommonName (CN)	Nombre del suscriptor, de acuerdo con el documento de identidad y en mayúsculas		**SI**

X.509v3 Extensions			
CAMPO	**CONTENIDO**	**CRÍTICO**	**OBLIGATORIO**
Uso de la clave			**SI**
KeyUsage	Digital Signature = 0	**SI**	
	Non Repudiation*1 = 0		
	Key Encipherment = 1		
	Data Encipherment = 1		
	Key Agreement = 0		
	Key CertificateSignature = 0		
	CRL Signature = 0		
extKeyUsage (Uso extendido del certificado)	Protección de e-mail (1.3.6.1.5.5.7.3.4)		
	anyExtendedKeyUsage (2.5.29.37.0)		

*1 Non Repudiation (Content Commitment)

7.2 Perfil de CRL

Según lo definido en la DPC de ANF AC.

7.3 Perfil de OCSP

Según lo definido en la DPC de ANF AC.

8 Auditoría de conformidad

8.1 Frecuencia de los controles de conformidad para cada entidad

Según lo definido en la DPC de ANF AC.

8.2 Identificación del personal encargado de la auditoría

Según lo definido en la DPC de ANF AC.

8.3 Relación entre el auditor y la entidad auditada

Según lo definido en la DPC de ANF AC.

8.4 Listado de elementos objeto de auditoría

Según lo definido en la DPC de ANF AC.

8.5 Acciones a emprender como resultado de una falta de conformidad

Según lo definido en la DPC de ANF AC.

8.6 Tratamiento de los informes de auditoría

Según lo definido en la DPC de ANF AC.

9 Disposiciones generales

9.1 Tarifas

Según lo definido en la DPC de ANF AC.

9.2 Responsabilidad financiera

Según lo definido en la DPC de ANF AC.

9.3 Confidencialidad de la información

Según lo definido en la DPC de ANF AC.

9.4 Privacidad de la información personal

Según lo definido en la DPC de ANF AC.

9.5 Derechos de Propiedad Intelectual

Según lo definido en la DPC de ANF AC.

9.6 Obligaciones y garantías

Según lo definido en la DPC de ANF AC.

9.7 Exclusión de garantías

Según lo definido en la DPC de ANF AC.

9.8 Limitaciones de responsabilidad

Según lo definido en la DPC de ANF AC.

9.9 Interpretación y ejecución

Según lo definido en la DPC de ANF AC.

9.10 Administración de la PC

Según lo definido en la DPC de ANF AC.

Anexo I
Formulario de Solicitud de Certificado Electrónico

Formulario de Solicitud de Certificado Electrónico

I. Tipo de Certificado

Por favor, especifique en primer lugar el tipo de certificado que desea solicitar.

Tipo de Certificado	
Certificado de Aplicación	☐
Certificado de Firma de Código	☐
Certificado de Cifrado	☐

II. Suscriptor del Certificado

Por favor, rellene los campos de persona física o jurídica, según corresponda.

Persona jurídica
Denominación:
CIF:
Forma jurídica:

Persona física
Nombre:
Primer apellido:
Segundo apellido:
Nacionalidad:
Tipo de cédula de identidad (DNI/NIE/Pasaporte):
Número de cédula de identidad *Incluir letra.

Datos de contacto	
Dirección:	
Población:	Provincia:
País:	Código postal:
Teléfono:	Fax:
E-mail:	Sitio web:

Datos profesionales
Nombre del Departamento:
Nombre de la Aplicación:

Tipo de entidad	
Organización privada	☐
Entidad pública	☐
Empresa	☐
Entidad no comercial	☐

III. Solicitante del Certificado

En caso de que la solicitud sea tramitada por una tercera persona en representación del suscriptor, se debe disponer de Poder Notarial de representación legal.

Datos personales
Nombre:
Primer apellido:
Segundo apellido:
Nacionalidad:
Tipo de cédula de identidad (DNI/NIE/Pasaporte):
Número de cédula de identidad *Incluir letra:

Datos de contacto	
Dirección:	
Población:	Provincia:
País:	Código postal:
Teléfono fijo:	Teléfono móvil:
E-mail:	Fax:

Datos de representación
Título de representación (Administrador, apoderado…):
Notario que protocoliza los poderes (u otro otorgante):
Número de protocolo / identificador:
Fecha:

IV. Responsable del Certificado

Datos personales
Nombre:
Primer apellido:
Segundo apellido:
Nacionalidad:
Tipo de cédula de identidad (DNI/NIE/Pasaporte):
Número de cédula de identidad *Incluir letra:

Datos de contacto	
Dirección:	
Población:	Provincia:
País:	Código postal:
Teléfono:	Fax:
E-mail:	

Datos de representación
Título de representación (Director técnico, webmaster…):
Departamento al que pertenece:

V. Datos Opcionales

Nombre comercial o marca registrada			
Nombre comercial	☐	Marca registrada	☐
Especifique el nombre o marca:			

Nota: Solo podrá incluir el nombre o marca si es su legítimo propietario o si cuenta con autorización expresa. En cualquier caso, deberá adjuntar documento acreditativo.

Atributos informativos a incorporar en el certificado

Nota: Aporte documentación en la que quede acreditada la información reseñada. Recuerde que ANF AC se reserva el derecho de incluir solo aquella información sobre la cual pueda comprobar su veracidad.

VI. El Solicitante/Suscriptor HACE CONSTAR:

Que ANF AC ha puesto a disposición del suscriptor, de forma previa a la entrega del certificado:

- El dispositivo criptográfico de firma, verificación de firma, cifrado o descifrado, de alguno de los tipos especificados en la Política de Certificación específica, en función de donde se creen y residan el par de claves.
- 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.

Que ha sido informado de que toda la información que seguidamente se detalla se encuentra disponible en la web http://www.anf.es. Concretamente:

- Modelo de Formulario de Solicitud de Certificados.
- Modelo de Contrato de Prestación de Servicios de Certificación.
- Ley 59/2003 de Firma Electrónica.
- Ley Orgánica de Protección de Datos.

- Reglamento de Protección de Datos.
- Declaración de Prácticas de Certificación de ANF AC.
- Declaración de Prácticas de Certificación de ANF TSA CA.
- Política de Certificación a la que está sometido el certificado solicitado.
- Política de Firma Electrónica asociada al certificado y dispositivo de firma.
- Tasas de emisión y servicios de certificación.

VII. El Solicitante/Suscriptor DECLARA:

1. Que realiza la solicitud del certificado por libre voluntad y sin que medie coacción alguna.
2. Que el solicitante / suscriptor no ha sido inhabilitado judicialmente.
3. En caso de que el solicitante actúe en representación de tercero, que el suscriptor se encuentra en posesión de sus facultades mentales, tiene capacidad intelectual suficiente para conocer el alcance del certificado de firma electrónica y realiza este trámite siguiendo sus instrucciones.
4. Que NO ha sido rechazada la tramitación de certificado por ningún otro Prestador de Servicios de Certificación Electrónica.

Que ha sido instruido adecuadamente con carácter previo a la solicitud sobre las siguientes cuestiones:

1. Sus obligaciones sobre:
   a) La generación de los datos de creación de firma sin mediación de terceros y su conocimiento exclusivo de la contraseña de activación.
   b) La forma en que han de custodiarse los datos de creación de firma y la contraseña de activación.
   c) El procedimiento que ha de seguir para comunicar la pérdida o posible utilización indebida de dichos datos y la obligación de proceder a la revocación del certificado.
   d) La forma en que han de utilizarse los dispositivos de certificación que le han sido entregados.
2. Sobre los mecanismos para garantizar la fiabilidad de la firma electrónica de un documento a lo largo del tiempo.
3. Sobre el método utilizado por el prestador para comprobar la identidad del firmante y otros datos que figuren en el certificado.
4. Sobre las condiciones precisas de utilización del certificado, sus posibles límites de uso y la forma en que el prestador garantiza su responsabilidad patrimonial.
5. Sobre las certificaciones obtenidas por ANF AC y los procedimientos aplicables para la resolución extrajudicial de los conflictos que pudieran surgir por el ejercicio de su actividad.
6. El titular del certificado reconoce haber sido informado de que los datos facilitados, incluidos sus datos biométricos obtenidos en el proceso de identificación, serán cargados en ficheros automatizados, resultando aplicable la legislación vigente en materia de protección de datos de carácter personal. Autoriza expresamente a ANF AC, responsable de los ficheros, a su almacenamiento informático y a que los pueda ceder a terceros en el ámbito de la infraestructura de clave pública, para la prestación de los servicios de certificación electrónica.
7. El suscriptor autoriza a la publicación de su certificado
8. La dirección y datos de contacto de ANF AC están permanentemente actualizados en https://www.anf.es/address/.

VIII. El Solicitante/Suscriptor ACEPTA sin salvedad alguna:

1. La Política de Certificación asociada a este certificado, la Declaración de Practicas de Certificación de ANF AC, la DPC de ANF AC como Autoridad de Sellos de Tiempo, y las Políticas de Certificación vinculadas a la TSA, las acepta plenamente y sin formular salvedad alguna.

2. Los usos permitidos, restringidos y prohibidos del certificado solicitado que se detallan en la Política de Certificación asociada a este certificado, así como las limitaciones de uso.
3. Que ANF AC limita su responsabilidad a la emisión y gestión de certificados y al suministro de dispositivos criptográficos (de firma y verificación de firma, así como de cifrado o descifrado).
4. Que ANF AC dispone de una garantía de cobertura suficiente de responsabilidad civil a través de póliza de seguros de RC emitida por Lloyd's, por importe de CINCO MILLONES DE EUROS (5.000.000 €), 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.
5. El límite de uso del certificado electrónico y de los servicios de certificación de ANF AC es de 1.000 euros. La utilización del certificado electrónico o de servicios de certificación de ANF AC, que exceda de ese límite, será bajo la exclusiva responsabilidad del solicitante/suscriptor.
6. La responsabilidad que asume al utilizar su certificado, equiparándolo a la firma manuscrita.
7. Que, en caso de considerarse perjudicado por los servicios de certificación recibidos, ha sido instruido en cuanto a los mecanismos de reclamación y solicitud de indemnización por los daños y perjuicios que haya podido sufrir.
8. Que todos los datos reseñados en este documento son verdaderos y asume la obligación de notificar a ANF AC cualquier variación que los mismos puedan sufrir a lo largo del tiempo.
9. Que los datos facilitados serán cargados en ficheros automatizados; que ha sido instruido sobre los derechos de acceso, rectificación, cancelación, y oposición que le otorga la normativa de seguridad de ANF AC; que el almacenamiento es informático y que ANF AC los puede ceder a terceros en el ámbito de su infraestructura de clave pública.

El Operador de la Autoridad de Registro que tramita esta solicitud declara haber comprobado de forma minuciosa la identidad de todos los intervinientes en la solicitud, asegura que los documentos acreditativos que le han sido mostrados son, a su leal saber y entender, originales y que las copias digitalizadas adjuntadas al formulario electrónico han sido cotejadas, y se asevera su plena coincidencia con los originales.

Los comparecientes solicitan de ANF Autoridad de Certificación la emisión de un Certificado Electrónico de Aplicación / Código / Cifrado:

En a de de

Firma del Solicitante / Suscriptor

Firma del Responsable del Certificado

Firma de la Autoridad de Registro

Anexo II
Contrato de Prestación de Servicios de Certificación Electrónica

Contratación de Prestación de Servicios de Certificación Electrónica

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/SOLICITANTE** 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 Via 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 Via 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/SOLICITANTE**.

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/SOLICITANTE** conoce los servicios de certificación electrónica ofrecidos por **ANF AC**, y desea hacer uso de los mismos.

V. Que el **SUSCRIPTOR/SOLICITANTE** 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/SOLICITANTE** 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 Políticas de Certificación vinculadas a la TSA**,** documentos que se encuentran publicados y disponibles en el sitio 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**, consistentes en la emisión de un certificado electrónico, de conformidad a la solicitud realizada por el **SUSCRIPTOR/SOLICITANTE,** que quedará unida por anexo al presente contrato.

2. REGULACIÓN

Las relaciones surgidas entre **ANF AC** y el **SUSCRIPTOR/SOLICITANTE**, 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 son documentos públicos y están permanente disponibles en la URL https://www.anf.es.

3. OBLIGACIONES DEL SUSCRIPTOR/SOLICITANTE

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, en especial, 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 electrónica 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/SOLICITANTE** 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.

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

3.14. El **SUSCRIPTOR/SOLICITANTE** solicita en este acto que se active el servicio de estampación de Sellos Digitales de Tiempo.

3.15. El **SUSCRIPTOR/SOLICITANTE** se compromete a facilitar cuanta información y documentación complementaria le sea requerida por **ANF AC** relacionada con la solicitud de certificado tramitada, asumiendo que la negativa a facilitar esa información o documentación complementaria 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.

3.16. Cualquier otro requerimiento o condición expresada en la Política de Certificación de Certificados de Aplicación, Código y Cifrado.

4. DENEGACIÓN

4.1. El Suscriptor/Solicitante declara que ha informado al Operador 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/Solicitante 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/SOLICITANTE** 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/SOLICITANTE** 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/SOLICITANTE** 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/SOLICITANTE** 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 y 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.

7. º 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/SOLICITANTE** 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/SOLICITANTE** consiente, especialmente, en la captación y guarda de su imagen fotográfica y huellas dactilares, en los casos que sean precisos para la prestación del servicio de certificación solicitado.

El **SUSCRIPTOR/SOLICITANTE** consiente, igualmente, en la publicación de la parte pública de sus certificados electrónicos.

El **SUSCRIPTOR/SOLICITANTE** debe defender, indemnizar y eximir de responsabilidad a ANF AC de cualquier pérdida o daño que sea resultado de una infracción imputable al Suscriptor/Solicitante 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

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

9.2. **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/SOLICITANTE**) deberá adherirse expresamente al arbitraje institucional mencionado en el párrafo anterior.

Caso de no aceptarse por el **SUSCRIPTOR/SOLICITANTE**, 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 III
Acta de Autorización y Aceptación de Responsabilidad en la utilización del Certificado

Acta de Autorización y Aceptación de Responsabilidad

Presentes el solicitante del certificado, D./Dª ……, con DNI ……..., en su calidad de legal representante del Suscriptor del certificado, ……, con CIF …….. y el/la Responsable del Certificado, D./Dª ……, con DNI …….

DECLARAN Y ACUERDAN

- Que el Solicitante hace entrega, en este acto, del dispositivo de firma electrónica que contiene los componentes de firma electrónica al Responsable del certificado, autorizándole para su uso, siguiendo las instrucciones dadas por el Solicitante/Suscriptor y con las limitaciones contenidas en el propio certificado o expresadas por el Solicitante/Suscriptor en documento aparte.
- Que el Responsable del Certificado acepta el dispositivo de firma electrónica entregado por el Solicitante, hará uso del mismo en representación del Suscriptor, en las condiciones y con los límites expresados en el punto anterior.
- Que el Responsable del Certificado se compromete a hacer un uso adecuado y responsable del certificado electrónico, respetando las limitaciones de uso contenidas en el mismo y la finalidad de emisión, así como las instrucciones del suscriptor del certificado.
- Que el Responsable del Certificado se compromete a custodiar la clave privada del certificado y el dispositivo electrónico que lo contiene con la diligencia debida. Manteniendo con absoluta privacidad y confidencialidad los datos de activación de firma (PIN).
- Que el Responsable del Certificado se compromete a cesar en el uso del mismo al primer requerimiento del suscriptor, comunicación que deberá guardar la forma escrita y que podrá realizarse por cualquier medio que acredite la recepción por parte del interesado, incluso mediante correo electrónico o SMS.
- Que, asimismo, el Responsable del Certificado se compromete a cesar en el uso del certificado cuando este haya perdido su vigencia, ya sea por caducidad o por revocación.
- Que, igualmente, de forma unilateral, el Responsable podrá desistir del compromiso como Responsable del Certificado, devolviéndolo al suscriptor, junto con la información y documentación relevante y comprometiéndose a no copiar ni desvelar esa información.

Y en prueba de conformidad suscriben la presente acta, en ……..., a ……. de ……..de 201..

EL SOLICITANTE DEL CERTIFICADO

EL RESPONSABLE DEL CERTIFICADO

Anexo IV
Carta de Solicitud de Renovación de Certificado

Carta de Solicitud de Renovación

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

A/A del/la Responsable de Dictámenes de Emisión

ANF AUTORIDAD DE CERTIFICACIÓN

Estimado Sr./ Sra.:

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 que se proceda a su renovación por la Autoridad de Certificación a la que me dirijo.

Muestro mi conformidad a que el coste de las tasas de renovación, establecido en su web www.anf.es, más los impuestos correspondiente, se carguen en la cuenta bancaria, de la que soy titular, número .....

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.

Reciba un cordial saludo,

Importante: De acuerdo con lo establecido en el Artículo 13, apartado 4, letras a y b de la Ley 59/2003, de 19 de diciembre, de firma electrónica, 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 Autoridad de Registro.

Anexo V
Formulario de Solicitud de Revocación del Certificado

Formulario de Solicitud de Revocación

Referencia de Solicitud:

Detalles conocidos del certificado	
Número de serie del certificado:	
Tipo de certificado:	

Datos del suscriptor del certificado	
Nombre del titular:	
DNI (persona física) o CIF (persona jurídica):	

Datos del solicitante de la revocación:	
Nombre:	
Primer apellido:	
Segundo apellido:	
Tipo de cédula de identidad (DNI/NIE/Pasaporte):	
Número de cédula de identidad *Incluir letra:	
Teléfono:	E-mail:

Actúa en nombre propio: SI ☐ NO ☐

Actúa en representación del suscriptor: SI ☐ NO ☐

Poder Notarial:

Otra representación *Añadir información al respecto:

Motivo de la solicitud de revocación:	
☐	Solicitud voluntaria del titular
☐	Pérdida del soporte de almacenamiento
☐	Fallecimiento del suscriptor, incapacidad sobrevenida, total o parcial
☐	Finalización de la representación
☐	Clave comprometida
☐	Información obsoleta
Emisión defectuosa de un certificado debido a:	
☐	1. Incumplimiento de un requisito material para la emisión del certificado
☐	2. 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
☐	Mal uso deliberado de claves y certificados, o falta de observancia o contravención de los requerimientos operacionales contenidos en la DPC o la presente PC.
☐	Certificado sustituido
☐	Longitud de claves insegura
☐	Algoritmos inseguros
☐	Pérdida de vigencia de alguno de los certificados superiores de la Ruta de Certificación
☐	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 por 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

Anexo VI
Acta de Recepción y Aceptación del Certificado

Acta de Recepción y Aceptación

El signatario, cuyos datos se corresponden a los consignados en el certificado electrónico empleado para firmar la presente acta de aceptación y recepción del certificado,

DECLARA

- Su conformidad con la emisión del certificado realizada por ANF Autoridad de Certificación (ANF AC), y aceptación en la recepción del mismo.
- Que, con carácter previo a la emisión del certificado, la entidad emisora puso a su disposición la documentación e información siguiente:
    - Declaración de Prácticas de Certificación (DPC).
    - Política de Certificación (PC) asociada al certificado emitido.
    - Tarifas aplicables.
    - Formulario de solicitud, renovación y revocación de certificados.
    - Procedimiento para solicitar la revocación de certificados.
    - Procedimiento para solicitar la renovación de certificados.
    - Forma de contacto con la entidad emisora:
        - Telefónica: 902 902 172 (Llamadas desde España)
          Internacional +34 933 935 946
        - Web: https://www.anf.es
        - Correo electrónico: info@anf.es
        - Presencial: Barcelona, Gran Via de les Corts Catalanes, 996, 4º. C.P: 08018.
- Que, con carácter previo a la emisión del certificado, la entidad emisora puso a su disposición el dispositivo de generación de claves, elaboración de certificado de petición (PKCS#10), dispositivo de firma electrónica y verificación de firma. Mediante estos instrumentos y sin intervención de terceros, seleccionó privadamente y libremente los datos de activación de firma (PIN) y generó las claves de firma y el certificado de petición.
- Que ha procedido a descargar el certificado en el mismo dispositivo electrónico que contiene las claves criptográficas asociadas al mismo.
- Que conoce, comprende y acepta la Declaración de Prácticas de Certificación de ANF AC, Política de Firma, Política de Certificación y demás documentos asociados al presente certificado electrónico.
- Que se compromete a hacer un uso adecuado y responsable del certificado, respetando las limitaciones de uso contenidas en el mismo y finalidad de emisión.
- Que asume la limitación de responsabilidad de la entidad emisora reflejada en el certificado electrónico.
- Se compromete a custodiar la clave privada del certificado y el dispositivo electrónico que lo contiene con la diligencia debida, manteniendo con absoluta privacidad y confidencialidad los datos de activación de firma (PIN).
- Que ha comprobado toda la información contenida en el certificado, declarando ser veraz y conforme.
- Que asume sus obligaciones como suscriptor o, en su caso, como representante legal del suscriptor y se compromete a comunicar de forma inmediata a la entidad emisora cualquier variación de la información contenida en el certificado, cesando inmediatamente en su uso

cuando la seguridad haya quedado comprometida o albergue sospechas al respecto, solicitando la revocación del certificado.

- Que se compromete, asimismo, a cesar en el uso del certificado cuando éste haya perdido su vigencia, ya sea por caducidad o por revocación.
- Que conoce y acepta que desde la recepción del certificado dispone de 15 días para verificar su correcta funcionalidad, y que transcurrido dicho plazo se considerará que tanto el certificado como el dispositivo electrónico en el que se aloja cumplen los requisitos técnicos y funcionales exigibles, sin que padezcan deficiencia alguna.
- Que ratifica los documentos previamente suscritos y asociados al formulario de solicitud y al contrato de emisión de certificado.
- Que ratifica la autorización de publicación de la parte pública de los certificados que recibe y acepta en este acto.

Y, en prueba de conformidad, suscribe la presente acta, en la fecha que acredita el sello de tiempo.