Política de Certificación de Certificados de Empleado Público

Paseo de la Castellana, 79 - 28046 - Madrid (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

Dirección: Dirección: Paseo de la Castellana, 79 - 28046 - Madrid (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

ANF Autoridad de Certificación (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.

La Infraestructura de Clave Pública (PKI) de ANF AC ha sido diseñada y es gestionada en conformidad con el marco legal del Reglamento [UE] 910/2014 del Parlamento Europeo, y con la Ley 59/2003 de Firma Electrónica de España. La PKI de ANF AC está en conformidad con las normas ETSI EN 319 411-1 (*Part 1: General Requirements*), ETSI EN 319 411-2 *(Part 2: Requirements for Trust Service Providers issuing EU Qualified Certificates)*, ETSI EN 319 411-3 *(Part 3: Policy Requirements for Certification Authorities issuing public key certificates)*, ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI), RFC 3739 (*Internet X.509 Public Key Infrastructure: Qualified Certificates Profile*).

ANF AC utiliza OID's según el estándar ITU-T Rec. X.660 y el estándar ISO/IEC 9834-1:2005 *(Procedures for the Operation of OSI Registration Authorities: General Procedures and ASN.1 Object Identifier tree top arcs).* 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 "Empleado Público" en los que el firmante es personal de la Administración Pública (en adelante AA.PP.), sea éste personal funcionario, laboral, eventual o interino, y el suscriptor titular del certificado es una AA.PP. Estos certificados pueden ser expedidos con la consideración de cualificados de acuerdo con lo establecido en el Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, y con la consideración de reconocidos según lo definido en la Ley 59/2003 de firma electrónica.

Para elaborar su contenido se ha tenido en cuenta la estructura de la IETF RFC 3647 PKIX, incluyendo aquellos apartados que resultan específicos para este tipo de certificado.

Este documento define los requisitos de procedimiento y operacionales a los que está sujeto 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, ANF AC y terceros de confianza, 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 https://www.anf.es.

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 Empleado Público**

El fin de este certificado es permitir a sus suscriptores autenticarse en sus relaciones telemáticas y ser utilizado para la generación de firmas electrónicas.

Se trata de un certificado en el que el suscritor es un representante de la Administración Pública con competencias bastantes para solicitar el certificado, y el sujeto, que está en posesión del dispositivo de creación de firma, es personal de la Administración Pública, sea éste personal funcionario, laboral, eventual o interino. El sujeto al estar en posesión del dispositivo de creación de firma, y actuando como personal de la Administración Pública, adopta las obligaciones y responsabilidades de los responsables del certificado.

En conformidad con lo establecido en el artículo 6 punto 2 de la Ley 59/2003, de 19 de diciembre, de firma electrónica (según Disposición Final 4.2 de la Ley 25/2015, de 28 de julio):

> *"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."*

Soportes disponibles:

- Token criptográfico por software.
  Token criptográfico hardware (HSM). Exclusivamente dispositivos certificados específicamente con arreglo a los requisitos aplicables de acuerdo con el artículo 30.3 del Reglamento eIDAS y, por tanto, incluidos en la lista de dispositivos cualificados mantenida por la Comisión Europea en cumplimiento de los artículos 30, 31 y 39 del Reglamento eIDAS.
  https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds

Estos certificados son emitidos con diferentes modalidades de uso:

- Autenticación.

- Firma Electrónica.
- Cifrado.

En cuanto a su consideración, tan solo el certificado de "firma electrónica" es expedido por ANF AC con la clasificación de "reconocido". El certificado, para tener esta consideración legal, incorporará la extensión de "reconocido" tal y como se especifica en este documento en conformidad con la norma ETSI EN 319 412.

Todos los Certificados emitidos bajo esta política son de conformidad con el estándar X.509 versión 3.

La validez máxima de estos certificados es de 5 años.

La comprobación de identidad se realizará de forma presencial ante una Autoridad de Registro (AR), y en base a documentación original vigente. La AR se encargará de tramitar la solicitud de acuerdo con lo establecido a tales efectos en la Declaración de Prácticas de Certificación de ANF AC. La personación del suscriptor solo se podrá obviar en aquellos supuestos que expresamente contempla y autoriza la legislación aplicable.

La comprobación de la información obtenida por una Autoridad de Registro o cualquier otra facilitada por el suscriptor, será realizada por ANF AC o por entidades colaboradoras clasificadas a efectos de este documento como Responsables de Dictámenes de Emisión (RDE), con las que ANF AC suscriba el instrumento legal pertinente.

La presente política, en cuanto a los certificados del tipo "Empleado Público", sigue las definiciones establecidas por la Dirección de Tecnologías de la Información y las Comunicaciones (DTIC) en su documento "Perfiles de certificados electrónicos" de abril de 2016.

Se definen dos niveles de aseguramiento:

a. Nivel medio/sustancial:

Este nivel corresponde a una configuración de mecanismos de seguridad apropiada para la mayoría de aplicaciones.

El riesgo previsto por este nivel es apropiado para acceder a aplicaciones clasificadas según el ENS en los niveles de Integridad y Autenticidad como de riesgo bajo o medio.

Asimismo, el riesgo previsto por este nivel corresponde a los niveles de seguridad bajo y sustancial de los sistemas de identificación electrónica del reglamento UE 910/2014. Los niveles de seguridad del reglamento eIDAS aplican únicamente a los sistemas de identificación electrónica.

Los mecanismos de seguridad mínimos aceptables incluyen los certificados X.509 en software. En los casos de certificados emitidos a personas, se corresponde con el de un "certificado cualificado", como se define en el reglamento UE 910/2014 para firma electrónica avanzada, sin dispositivo cualificado de creación de firma. El uso de dispositivos hardware de firma (dispositivo cualificado de creación de firma o HSM) también está permitido.

La validez máxima de estos certificados es de 5 años.

El riesgo previsto por este nivel corresponde al nivel 3 de garantía previsto en la Política Básica de Autenticación de IDABC *[1].

*[1] *El programa IDABC (Interoperable Delivery of Pan-European eGovernment Services to Public Administrations, Business and Citizens - prestación interoperable de servicios paneuropeos de administración electrónica al sector público, las empresas y los ciudadanos). Decisión 2004/387/CE del Parlamento Europeo y del Consejo, de 21 de abril de 2004, relativa a la prestación interoperable de servicios paneuropeos de administración electrónica al sector público, las empresas y los ciudadanos (IDABC) [Diario Oficial L 144 de 30.4.2004]*

b. Nivel alto:

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

El riesgo previsto por este nivel es apropiado para acceder a aplicaciones clasificadas según el ENS en los niveles de Integridad y Autenticidad como de riesgo alto.

Asimismo, el riesgo previsto por este nivel corresponde al nivel seguridad alto de los sistemas de identificación electrónica del reglamento UE 910/2014. Los niveles de seguridad del reglamento eIDAS aplican únicamente a los sistemas de identificación electrónica.

Los mecanismos de seguridad aceptables incluyen los certificados X.509 en hardware. En los casos de certificados emitidos a personas, se corresponde con el de un "certificado cualificado", para "firma electrónica cualificada", como se define en el reglamento UE 910/2014. Además este tipo de certificados precisa el uso de Dispositivos SSCD (HSM).

El riesgo previsto por este nivel corresponde al nivel 4 de garantía previsto en la Política Básica de Autenticación de IDABC.

La validez máxima de estos certificados es de 5 años.

1.2 Identificación

Nombre del documento	Política de Certificación de Certificados de Empleado Público
Versión	1.5
Estado de la política	APROBADO
Referencia del documento / OID	1.3.6.1.4.1.18332.4.1
Fecha de emisión	08 de noviembre de 2016
Fecha de expiración	No es aplicable
CPS 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 Empleado Publico Nivel Alto (AUTENTICACION) con algoritmo SHA-256 y longitud 2048 bits	1.3.6.1.4.1.18332.4.1.1.22
Certificado de Empleado Publico Nivel Medio con algoritmo SHA-256 y longitud 2048 bits	1.3.6.1.4.1.18332.4.1.2.22
Certificado de Empleado Publico Nivel Alto (FIRMA) con algoritmo SHA-256 y longitud 2048 bits	1.3.6.1.4.1.18332.4.1.3.22
Certificado de Empleado Publico Nivel Alto (CIFRADO) con algoritmo SHA-256 y longitud 2048 bits	1.3.6.1.4.1.18332.4.1.4.22

En el caso de "Certificado de Empleado Público Nivel Alto", la extensión CertificatePolicies (2.5.29.32) incluirá el OID:

- 2.16.724.1.3.5.7.1

En el caso de "Certificado de Empleado Público Nivel Medio", la extensión CertificatePolicies (2.5.29.32) incluirá el OID:

- 2.16.724.1.3.5.7.2

Cuando el certificado es emitido con la calificación de cualificado, en la extensión CertificatePolicies (2.5.29.32), incluirá al menos uno de los PolicyInformation siguientes:

- qcp-natural (0.4.0.194112.1.0). Certificado en token software
- qcp-natural-qscd (0.4.0.194112.1.2). Cuando el certificado cualificado de firma, está almacenado en dispositivo cualificado acorde al Reglamento (UE) 910/2014

El identificador de esta Política de Certificación solo será cambiado si se producen cambios sustanciales que afectan a su aplicabilidad.

1.3 Partes de la PKI

1.3.1 Autoridades de Certificación

Según lo definido en la DPC de ANF AC.

1.3.2 Autoridades de Registro

Según lo definido en la DPC de ANF AC.

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.

A efectos de esta política sólo el Presidente de la Junta Rectora de la PKI puede intervenir en calidad de Responsable de Dictámenes de Emisión.

1.3.4 Entidades finales

1.3.4.1 Suscriptor

Según lo definido en la DPC de ANF AC.

1.3.4.2 Sujeto

Según lo definido en la DPC de ANF AC.

1.3.4.3 Responsable del certificado

Según lo definido en la DPC de ANF AC.

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 Empleado Público del tipo Autenticación, indicado para autenticarse frente a sistemas de información y aplicaciones informáticas en general.

  El certificado incorpora extensión de uso de clave, posibilitando el acceso seguro a sistemas informáticos de información y aplicaciones informáticas en general.

- Certificado de Empleado Público del tipo Firma, especialmente indicado para realizar operaciones de firma que no requieran repudio.

- Certificado de Empleado Público del tipo Cifrado, especialmente indicado para realizar operaciones de cifrado asimétrico.

1.4.2 Límites de uso de los certificados

El sujeto solamente puede utilizar la clave privada y el certificado para los usos autorizados en esta PC, de acuerdo con el rol y el nivel de seguridad otorgado, de acuerdo con lo establecido en los campos 'KeyUsage' y 'ExtendedKeyUsage' del certificado y en conformidad con las limitaciones de uso que consten en el certificado, asumiendo la limitación de responsabilidad que consta en el OID 1.3.6.1.4.1.18332.40.1. y/o en QcLimitValue OID 0.4.0.1862.1.2.

El sujeto 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

ETSI ha elaborado normas europeas en cumplimiento del Mandato M/460 de la Comisión Europea para racionalizar los estándares en torno a la firma electrónica. La familia ETSI EN 319 412 especifica el contenido de los certificados expedidos a personas físicas.

En concreto, la parte 2 de este documento, ETSI EN **319 412-2 v2.1.1** (Part 2: *Certificate profile for certificates issued to natural persons*) define los requisitos del contenido de certificados emitidos a personas físicas. El perfil se basa en las recomendaciones IETF RFC 5280 y el estándar ITU-T X.509.

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".

Criterios de composición del campo CN (CommonName) se compone bajo los siguientes criterios:

- Incluir el **NOMBRE**, de acuerdo con lo indicado en el DNI/Pasaporte, y en mayúsculas.
- Espacio en blanco
- Incluir el **PRIMER Y SEGUNDO APELLIDO**, en mayúsculas, separados únicamente por un espacio en blanco, de acuerdo con lo indicado en el DNI/NIE. En caso de no existir el segundo apellido, se dejará en blanco (sin ningún carácter).
- Espacio en blanco
- **Guion** que separe el nombre y apellidos del número de DNI/NIE, sin espacio entre los valores ni signos de puntuación
- Espacio en blanco
- Incluir el **número de identificación fiscal**, NIF, de acuerdo con lo indicado en su DNI o NIE. Al NIF, también se le llama DNI o NIE. Sin espacio entre el número y la letra de control; la letra de control en mayúsculas.

P.ejemplo: GARCIA ABALOS JUAN ANTONIO - 00000000G

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 Guía de cumplimentación de campos específicos

De acuerdo con la RFC 5280, que usa UTF-8[*1] string, puesto que codifica grupos de caracteres internacionales incluyendo caracteres del alfabeto latino con diacríticos ("Ñ", "ñ", "Ç", "ç", "Ü", "ü ", etc.). Por ejemplo, el carácter eñe (ñ), que se representa en unicode como 0x00F1.

Para todos los literales variables:

- Todos los literales se introducen en mayúsculas, con las excepciones del nombre de dominio/subdominio y el correo electrónico que estarán en minúsculas.
- No incluir tildes en los literales alfabéticos
- No incluir más de un espacio entre cadenas alfanuméricas.
- No incluir caracteres en blanco al principio ni final de cadenas alfanuméricas.
- Se admite la inclusión de abreviaturas en base a una simplificación, siempre que no supongan dificultad en la interpretación de la información.

[*1] *Para más información ver RFC 2279 mejorada en 3629 (UTF-8, a transformation format of ISO 10646)*

Números de identificación fiscal (NIF) y personal (NIP, NRP, …)

El número de identificación fiscal, será acorde a la normativa vigente. Ejemplos:

Entidades: *incluir la letra y los números. Ej.: "S2833002"*

Personas: *incluir los números y la letra al final, sin separación de guion. Ej.: "00000000G"*

El Número de Identificación Personal (NIP) en el Registro Central de Personal está compuesto por ocho posiciones numéricas y una posición de control alfanumérica. El NIP es la clave que identifica a las personas en el Sistema de Información de Registro Central de Personal.

El NIP se construye dependiendo:

1. Del tipo de documento que aportó la persona en su primera relación con la Administración General del Estado (AGE).
2. De la fecha de incorporación en su primera relación con la AGE.

NIP		Documento presentado en la primera Relación de Servicios con la AGE		Ejemplos
Número (8 posiciones)	**Control (1 posición)**			
DNI sin letra	Blanco, 1, 2	DNI		00001234 00001234-1 00001234-2
Secuencial generado por el sistema	N	Desde 01/01/2003	Otro documento	0001234-N
Construido partiendo del documento presentado	3, 4, 5, 6, 7, 8, 9	Antes de 01/01/2003		0001234-3

3.1.3 Necesidad de que los nombres sean significativos

En todos los casos los nombres distintivos deben tener sentido.

3.1.4 Pseudónimos o anónimos

No se permiten.

3.1.5 Reglas utilizadas para interpretar varios formatos de nombres

Según lo definido en la DPC de ANF AC.

3.1.6 Unicidad de los nombres

Según lo definido en la DPC de ANF AC.

3.1.7 Resolución de conflictos relativos a nombres y marcas

Los suscriptores 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 suscriptor

Los Certificados emitidos bajo esta Política de Certificación identificarán al suscriptor a cuyo nombre se solicita la emisión del certificado, al sujeto y en su caso 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 sujeto se incorporarán en el certificado. Además, el suscriptor debe de facilitar un número de teléfono móvil y una dirección de correo electrónico de su confianza. La dirección de correo electrónico y el servicio SMS o Whatsapp asociado a su teléfono móvil, tendrán la consideración de buzones autorizados para que ANF AC pueda realizar entregar electrónicas certificadas, incluso doble autenticación en el caso de servicio de certificados de firma electrónica centralizada, o cualquier otro que se considere necesario. El usuario asume la obligación de informar a ANF AC de cualquier cambio de dirección de correo electrónico o número de teléfono móvil.

El tipo de documentación, las modalidades de tramitación, los procedimientos de autenticación y la validación se especifican 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 suscriptor 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 suscriptor 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) **Presencialmente**: el suscriptor ante podrá personarse ante una Autoridad de Registro Reconocida, en cuya presencia procederá a firmar el formulario de solicitud, que deberá estar debidamente cumplimentado.

b) **Por correo ordinario:** formulario de solicitud de certificado firmado manuscritamente por el suscriptor y legitimada su firma por Notario Público. Documentación remitida por correo ordinario.

ANF AC no genera las claves de sus usuarios. El suscriptor debe generar su par de claves y el certificado de petición en formato PKCS#10 / CSR, haciendo entrega del mismo a ANF AC junto con el Formulario de Solicitud de certificado.

4.2 Procedimiento de tramitación

4.2.1 Autenticación de identidad

4.2.1.1 Suscriptor

La solicitud de los certificados definidos en la presente Política de Certificación se encuentra limitada a Administraciones o Entidades públicas con las que se haya establecido convenio de certificación, contrato o alguna otra fórmula que instrumente la prestación del servicio por parte de ANF AC.

La identificación de la Administración o Entidad pública se realizará en el proceso de Alta de la Entidad, que será suscrito por una persona física con capacidad de representar a la Administración o Entidad.

La identificación del suscriptor se realizará mediante su personación ante la Autoridad de Registro. En ese acto acreditará su capacidad legal para representar a la AA.PP. en cuya representación se tramita la solicitud del certificado.

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 suscriptor 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 se 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 que formen parte del Espacio Económico Europeo:
      - Documento nacional de identidad (o equivalente en su país de origen), o tarjeta NIE (emitida por el Registro de Ciudadanos Miembros de la Unión), o pasaporte. La identificación física debe de ser realizada tomando como referencia uno de estos documentos que incluya fotografía 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 o tarjeta de residencia, 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).

e) El suscriptor deberá disponer de poder suficiente de representación o competencias bastantes.
f) En el caso de que el suscriptor requiera incluir otras circunstancias personales, éstas deberán comprobarse mediante los documentos oficiales que las acrediten de conformidad con su normativa específica.

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.

[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.

En el caso de intervención de Notario Público, se requerirá la legitimación de firma del suscriptor en a solicitud de expedición de un certificado (LFE 59/2003, Art. 13.1).

4.2.1.2 Sujeto / Responsable del Certificado

En el formulario de solicitud, el suscriptor deberá identificar y autorizar de forma expresa al sujeto del certificado. Esta autorización deberá ser perfeccionada con una aceptación voluntaria y expresa por parte de la persona física que asume la calificación de Sujeto del Certificado y las obligaciones y responsabilidades de los responsables del certificado.

El Sujeto deberá personarse ante la Autoridad de Registro, acreditar su identidad de la misma manera que sea realiza la identificación del Suscriptor, como se detalla en la sección anterior.

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.

En especial, comprobará la existencia y legalidad de la Administración Pública, la competencia del suscriptor para solicitar el certificado, la del sujeto y su pertenencia a la Administración Pública como empleado.

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, sujeto, responsable del certificado y terceros que confían, en especial a la DPC y a las Políticas de Certificación.

- También 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 suscriptor podrá dar por anulado el pedido y recibir las tasas que haya abonado.

El RDE puede requerir del suscriptor información o documentación complementaria y el suscriptor 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 suscriptor no es veraz, denegará la emisión del certificado, generará un incidente informando al Coordinador de Seguridad, a fin de determinar la inclusión o no del suscriptor 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 Autoridad de Certificación (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 y, 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

Según lo definido en la DPC de ANF AC.

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 suscriptor 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 horas desde su emisión.

4.4.5 Notificación de la emisión del certificado a terceros

No se efectúa notificación a terceros.

4.5 Denegación

Según lo definido en la DPC de ANF AC.

4.6 Renovación de certificados

Con carácter general, según lo definido en la DPC de ANF AC.

4.6.1 Certificados vigentes

ANF AC notifica por correo electrónico al suscriptor 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, siempre que la identificación realizada no haya superado el periodo de cinco años.

4.6.2 Personas autorizadas para solicitar la renovación

El formulario de solicitud de renovación debe ser firmado por el mismo suscriptor, ya fuera el propio suscriptor o el representante legal que tramitó la solicitud del certificado.

Las circunstancias personales del suscriptor no deben haber variado, en especial su capacidad de representación legal o competencias bastantes para solicitar el certificado.

4.6.3 Identificación y autenticación de las solicitudes de renovación rutinarias

La identificación y autenticación para la renovación del certificado se puede realizar bien 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 "cualificado", y 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 cinco años.

Para garantizar el cumplimiento del art. 13,4. b) de la Ley de firma electrónica y no superar el periodo de 5 años desde la identificación inicial, ANF AC aplica los siguientes procedimientos y medidas de seguridad técnicas:

- Los certificados de ANF AC siempre se generan utilizando un token que debe ser utilizado para poder realizar cualquier trámite de renovación.

  Este token es unívoco ante cualquier otro suministrado por ANF AC y está programado para que el usuario pueda realizar una única renovación. Este procedimiento técnico imposibilita una tramitación automática una vez hayan transcurrido 5 años desde la primera identificación.

- ANF AC sigue un sistema de registro de solicitudes, distinguiendo la fecha de solicitud -que coincide con la de identificación- y la de emisión del certificado. Este control permite una segunda renovación si no se ha alcanzado el periodo de los 5 años desde la identificación inicial.

  El sistema técnico requiere una petición expresa del usuario, la intervención directa de un operador de ANF AC el cual, a su vez, precisa validar la solicitud mediante aplicación de control de seguridad de coherencia. Si se han superado los 5 años, la propia aplicación bloquea el proceso. En caso contrario, facilita al operador el proceso hasta la renovación del certificado.

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 especificado 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, del mal uso de certificados o cualquier tipo de fraude, o

conducta impropia.

- 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 suscriptor del certificado o del responsable del mismo en la fecha de la solicitud de revocación.

- Telefónica.

    Mediante la respuesta a las preguntas realizadas desde el servicio de soporte telefónico disponible en el número 902 902 172 (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 página web http://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 suscriptor 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 definido en la DPC de ANF AC.

4.8.5 Plazo máximo de procesamiento de la solicitud de revocación

Según lo definido en la DPC de ANF AC.

4.8.6 Requisitos de comprobación de listas CRL

Los terceros que confían deben comprobar el estado de los certificados en los cuales van 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 https://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

Salvo en certificados de firma electrónica centralizada, 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 https://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

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 emitidos con la calificación de "reconocidos" (cualificados), cumplen con las normas:

- ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.

- 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 a la especificación RFC 5280.

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 al suscriptor, 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).

QCStatements

Los certificados emitidos por ANF AC siguen lo definido en la ETSI EN 319 412-5 *(Certificate Profiles-QCStatements)*:

- **QcCompliance,** se refiere a una declaración del emisor en la cual se hace constar la calificación con la que es emitido el certificado, y marco legal al que se somete. Concretamente los certificados sometidos a esta política, emitidos con la calificación de reconocidos (cualificados), reseñan:
  "Este certificado se expide con la calificación de cualificado de acuerdo con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo"

- **QcLimitValue,** 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 el importe expresado en 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,** 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,** determina que la clave privada asociada a la clave pública contenida en el certificado electrónico, está en un dispositivo cualificado de creación de firma en conformidad con el Anexo II del Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

- **QcType**, cuando el certificado se emite con el perfil (FIRMA), se reseña QcType 1

- **QcPDS**, se proporciona la URL que permite acceder a todas las políticas de la PKI en inglés. De acuerdo con ETSI 319 412-5 se utilizará protocolo https.

Subject Alternative Names

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).

7.1 Perfiles de certificados

Según lo definido en el documento perfil técnico.

7.2 Perfil de CRL

Según lo definido en la DPC de ANF AC. y documentación perfil técnico.

7.3 Perfil de OCSP

Según lo definido en la DPC de ANF AC. y documentación perfil técnico.

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.