Política de Certificación

Certificados de Sello Electrónico

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

© ANF Autoridad de Certificación
Paseo de la Castellana, 79 – 28046 - Madrid (España)
Teléfono: 902 902 172 (llamadas desde España)
Teléfono: (+34) 933 935 946 (llamadas Internacional)
Web: www.anf.es

Nivel de Seguridad

Público

Aviso Importante

Este documento es propiedad de ANF Autoridad de Certificación

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

2000 – 2020 Copyright © ANF Autoridad de Certificación

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

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

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 319 401 *(General Policy Requirements for Trust Service Providers)*, 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 319 412 *(Electronic Signatures and Infrastructures (ESI): Certificate Profiles)* y RFC 3739 *(Internet X.509 Public Key Infrastructure: Qualified Certificates Profile)*. Los certificados del tipo PSD2 están en conformidad con la ETSI TS 119 495, cumplen las normas técnicas de regulación del Reglamento Delegado (UE) 2018/389 de la Comisión, por el que se complementa la Directiva (UE) 2015/2366, y el Real Decreto-ley 19/2018 de España, respetando las directrices establecidas por la Autoridad Nacional Competente de servicios de pago.

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 "Sello Electrónico", "Sello Electrónico AA.PP." y, "Sello Electrónico PSD2". 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 cualificados según lo definido en la legislación vigente.

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 sello electrónico. 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

Estos certificados, de conformidad al Reglamento UE 910/2014 (eIDAS), sirven como prueba de que un documento electrónico ha sido expedido por una persona jurídica, aportando certeza sobre el origen y la integridad del documento.

ANF AC, en el marco de su servicio de certificados cualificados de sello electrónico, emite los siguientes tipos:

- **Certificado Cualificado de Sello Electrónico**
  Son certificados con el perfil básico.

- **Certificado Cualificado de Sello Electrónico AA.PP.**

  Son certificados electrónicos en servicios públicos de acuerdo con el artículo 37 del Reglamento (UE) 910/2014, derivados del Real Decreto 1671/2009 y conforme a las disposiciones de la Ley 39/2015 de 1 de Octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, la Ley 40/2015 de 1 de Octubre, de Régimen Jurídico del Sector Publico (LRJ).

- **Certificado Cualificado de Sello Electrónico PSD2**

  Son certificados cualificados de sello electrónico PSD2, de acuerdo con la Directiva (UE) 2015/2366, y el Real Decreto-ley 19/2018 de España, están en conformidad con la ETSI TS 119 495, y respeta las directrices establecidas por la Autoridad Nacional Competente de servicios de pago.

Estos certificados pueden ser emitidos en los siguientes soportes:

- Token de software criptográfico, incluyendo el servicio de distribución de claves.

- QSCD *(Qualified Seal Creation Device)*: Token criptográfico, exclusivamente dispositivos certificados específicamente con arreglo a los requisitos aplicables de acuerdo con el artículo 39 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

- Servicio Centralizado de certificados cualificados de sello electrónico.
  Los datos de creación de **sello** han sido generados en un token criptográfico QSCD y, de acuerdo con los requisitos del art. 8 y del art. 24 (b y c), el entorno de uso es gestionado por ANF AC en nombre del creador de sello, y se encuentran bajo el control exclusivo de su titular.

La presente política, en cuanto a los certificados cualificados del tipo "Sello Electrónico AAPP", 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 token criptográfico de software. El uso de dispositivos QSCD, o el servicio centralizado 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 soporte QSCD, y el servicio centralizado también está permitido.

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 Nombre del documento e identificación

Nombre del documento	Política de Certificación de Certificados de Sello electrónico		
Versión	1.7		
Estado de la política	APROBADO		
OID	1.3.6.1.4.1.18332.25.1.1		
Fecha de aprobación	30/01/2019	**Fecha de publicación**	30/01/2019

Versión	Cambios	Aprobación	Publicación
1.0.	Creación del documento	06/02/2011	06/02/2011
1.1.	Inclusión Certificado de Sello Electrónico Nivel Alto	01/06/2012	01/06/2012
1.2.	Ampliación certificados de sello disponibles	08/07/2014	08/07/2014
1.3.	Revisión.	03/05/2014	03/05/2014
1.4.	Revisión.	03/04/2015	03/04/2015
1.5.	Revisión y adaptación a eIDAS.	19/10/2016	19/10/2016
1.6.	Revisión.	30/03/2017	30/03/2017
1.7.	Revisión e inclusión certificados de Sello para PSD2.	30/01/2019	30/01/2019

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

	Soporte	Especificación técnica	OID
Certificado de Sello Electrónico	Token de software criptográfico	Algoritmo SHA-256 y longitud 2048 bits.	1.3.6.1.4.1.18332.25.1.1.1
	QSCD	Algoritmo SHA-256 y longitud 2048 bits.	1.3.6.1.4.1.18332.25.1.1.4
	Servicio Centralizado	Algoritmo SHA-256 y longitud 2048 bits.	1.3.6.1.4.1.18332.25.1.1.9
	Software con gestión distribuida de claves	Algoritmo SHA-256 y longitud 2048 bits.	1.3.6.1.4.1.18332.25.1.1.10
Certificado de Sello Electrónico AAPP	En token software criptográfico	Nivel Alto Nivel Medio Algoritmo SHA-256 y longitud 2048 bits.	1.3.6.1.4.1.18332.25.1.1.3
	QSCD	Nivel Alto Nivel Medio Algoritmo SHA-256 y longitud 2048 bits.	1.3.6.1.4.1.18332.25.1.1.2
	Servicio Centralizado	Algoritmo SHA-256 y longitud 2048 bits.	1.3.6.1.4.1.18332.25.1.1.11
	Software con gestión distribuida de claves	Algoritmo SHA-256 y longitud 2048 bits.	1.3.6.1.4.1.18332.25.1.1.12
Certificado de Sello Electrónico PSD2	En token software criptográfico	Algoritmo SHA-256 y longitud 2048 bits.	1.3.6.1.4.1.18332.25.1.1.5
	QSCD	Algoritmo SHA-256 y longitud 2048 bits.	1.3.6.1.4.1.18332.25.1.1.6
	Servicio Centralizado	Algoritmo SHA-256 y longitud 2048 bits.	1.3.6.1.4.1.18332.25.1.1.7
	Software con gestión distribuida de claves	Algoritmo SHA-256 y longitud 2048 bits.	1.3.6.1.4.1.18332.25.1.1.8

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

En el caso de "Certificado de Sello Electrónico AA.PP. Nivel Alto", la extensión CertificatePolicies (2.5.29.32) incluirá el OID:

- 2.16.724.1.3.5.6.1

En el caso de "Certificado de Sello Electrónico AA.PP. Nivel Medio", la extensión CertificatePolicies (2.5.29.32) incluirá el OID:

- 2.16.724.1.3.5.6.2

Además, al ser emitidos con la calificación de cualificado, se incluye la extensión CertificatePolicies (2.5.29.32), que contiene al menos uno de los PolicyInformation siguientes:

- qcp-legal (0.4.0.194112.1.1). Certificado en token software
- qcp-legal-qscd (0.4.0.194112.1.3). Cuando el certificado cualificado de sello, está almacenado en dispositivo cualificado acorde al Reglamento UE 910/2014

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.

1.3.4 Entidades finales

1.3.4.1 Sujeto

Según lo definido en la DPC de ANF AC.

1.3.4.1.1 Certificado de Sello Electrónico

Se trata de una persona jurídica, que suscribe los términos y condiciones de uso de un certificado, y cuya identidad queda vinculada a los Datos de Verificación de sello (Clave Pública) del certificado emitido por ANF AC. Por lo tanto, la identidad del suscriptor del certificado queda vinculada a lo sellado electrónicamente por el creador de sello, utilizando los Datos de Creación de Sello (Clave Privada) asociados al certificado emitido por ANF AC.

1.3.4.1.2 Certificado de Sello Electrónico AA.PP.

Se trata de una Administración Pública, órgano o entidad de derecho público, que suscribe los términos y condiciones de uso de un certificado, cuya identidad y, en su caso, sede electrónica, quedan vinculadas a los Datos de verificación de sello (Clave Pública) del certificado emitido por ANF AC. Por lo tanto, la identidad del suscriptor del certificado queda vinculada a lo sellado electrónicamente por el Firmante, utilizando los Datos de Creación de Sello (Clave Privada) asociados al certificado emitido por ANF AC.

1.3.4.1.3 Certificado de Sello Electrónico PSD2.

Se trata de un Proveedor de Servicios de Pago (PSP), que suscribe los términos y condiciones de uso del certificado de acuerdo con los requerimientos establecidos en el Reglamento Delegado (UE) 2018/389 de la Comisión, por el que se complementa la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo en lo relativo a las normas técnicas de regulación para la autenticación reforzada de clientes y unos estándares de comunicación abiertos comunes y seguros. La identidad del suscriptor queda vinculada a los datos de verificación de Sello (Clave Pública) del certificado emitido por ANF AC.

1.3.4.2 Suscriptor del certificado

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 acuerdo con el uso de claves:

- Sellado de documentos. Key usage tendrá el bit "ContentComitment".
- Sellado de código. Keyusage tendrá el bit "digitalSignature" combinado con el extendedkeyusage "codeSigning".
- Autenticación de activo de la persona jurídica. Actuando como certificado de componente por ejemplo para autenticación en servidores de aplicaciones) (keyusage tendrá el bit "digitalSignature" combinado con el keyEncipherment (o KeyAgreement) y con extendedkeyusage ("serverAuth", "clientAuth").

Este certificado nunca debe de utilizarse en exclusiva para cifrado, ni como certificado de autenticación de servidor web.

1.4.2 Límites de uso de los certificados

El suscriptor sólo puede utilizar la clave privada y el certificado para los usos autorizados en esta PC y restringido a la aplicación o departamento que consta en el certificado.

Su utilización y aceptación debe estar 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 QcLimitValueOID 0.4.0.1862.1.2. Del mismo modo, el titular solo podrá utilizar el par de claves y el certificado tras aceptar las condiciones de uso establecidas en la DPC.

El suscriptor solo 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.

2.5 Certificados PSD2

La Autoridad Nacional Competente, puede solicitar información sobre los certificados que contienen un número de autorización de un Prestador de Servicios de Pago (PSP) asignado por esa institución. ANF AC informará sobre los certificados emitidos de acuerdo con lo establecido en cada repositorio.

3 Identificación y Autenticación

3.1 Registro de nombres

3.1.1 Tipos de nombres

El atributo CN (CommonName) ha de hacer referencia a la denominación de la aplicación o del departamento que hace uso del mismo. En el caso de Certificados de Sello Electrónico, por motivos de compatibilidad, es posible la inclusión en el CommonName del Subject de ciertos atributos que pudieran ser necesarios para el tratamiento, como es el caso del nombre de la entidad suscriptora o responsable del sello, y su NIF.

En los certificados de Sello Electrónico, la razón social está incluida en el atributo "organizationName" y el NIF en el atributo "organizationIdentifier":

> *"Additional attributes other than those listed above may be present. In particular, when a natural person subject is associated with an organization, the subject attributes **may** also identify such organization using attributes such as **organizationName** and **organizationIdentifier**. Certificates may include one or more semantics identifiers as specified in ETSI EN 319 412-1 [i.4], clause 5 which defines the semantics for the organizationIdentifier attribute"*

Atributos	Contenido	Ejemplo
organizationName	Razón Social, tal como figura en los registros oficiales.	Nombre empresa. S.L.
organizationIdentifier	NIF, tal como figura en los registros oficiales. Codificado Según la Norma Europea ETSI EN 319 412-1	VATES-B0085974Z

En el caso de certificados con atributo de PSD2, la el número de autorización está incluido en el atributo "organizationIdentifier", tal y como indica la ETSI TS 119 495:

Campo	Contenido	Ejemplo	tamaño *
Literal	PSD	PSD	3
Código País	Código de país acorde con ISO 3166	ES	2

Literal	Guion (0x2D (ASCII), U+002D (UTF-8))	-	
Identificador de la ANC	Identificador de la Autoridad Nacional Competente en Mayúsculas, sin espacios	BDE	2-8
Literal	Guion (0x2D (ASCII), U+002D (UTF-8))	-	
Identificador PSP	Número de autorización del Prestador de Servicios de Pago	3DFD21	El tamaño es establecido por la Autoridad Nacional Competente

Cualquier separador en el identificador ANC será eliminado *(ETSI 119495 Clausula 5.2.1)*

Ejemplo = "PSDES-BDE-3DFD21"
Certificado emitido a un PSP con número de autorización 3DFD21 emitido por la Autoridad Nacional Competente española Banco de España.

3.1.2 Guía de cumplimentación de campos de certificados

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)*

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)*

DNI/NIE

El término NIF abarca tanto a DNI como a NIE.

Caso de optar por la etiqueta DNI o NIE, en lugar de NIF, se usará aquella que corresponda.

Se admiten las siguientes codificaciones:

1.- Semántica propuesta por la norma ETSI EN 319 412-1. Formada por:

- Tres caracteres para indicar el tipo de documento de acuerdo con la codificación siguiente:

- "PAS" para la identificación basada en el número de pasaporte.
- "IDC" para la identificación basada en el número de tarjeta nacional de identidad (DNI/NIE).
- "PNO" para la identificación basada en () número personal nacional (número de registro nacional cívica).
- "TAX" para la identificación en base a un número de identificación fiscal personal expedido por una autoridad fiscal nacional. Este valor está en desuso. El valor "Número de identificación" se debe utilizar en su lugar. Número de identificación fiscal "TIN", según la Comisión Europea - Impuestos y Unión Aduanera, según especificación publicada en: (Https://ec.europa.eu/taxation_customs/tin/tinByCountry.html).

- Dos caracteres para identificar el país. Codificado de acuerdo a “ISO 3166-1- alpha-2 code elements”.

- Número de identidad con letra de identificación fiscal.

Ejemplo: IDCES-00000000G.

2.- Semántica básica. Formada por:

El número y letra conforme consta en el documento de identidad.
Ejemplo: ID00000000G.

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

ANF AC no asume compromiso alguno sobre el uso de marcas comerciales en la emisión de los Certificados expedidos bajo la presente Política de Certificación. ANF AC no está obligada a verificar la titularidad o registro de marcas registradas y demás signos distintivos.

Los suscriptores de certificados no incluirán nombres en las solicitudes que puedan suponer infracción.

No se permite el uso de signos distintivos cuyo derecho de uso no sea propiedad del suscriptor o esté debidamente autorizado.
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

Los Certificados emitidos bajo esta Política de Certificación identifican al sujeto a cuyo nombre se solicita la emisión del certificado y al suscriptor 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 encuentran bases registrales externas y la posibilidad de requerir información o documentación complementaria al suscriptor.

Los identificativos fiscales del sujeto y del suscriptor 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 sello 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.

En conformidad con el Art. 13.3 de la Ley 59/2003 de Firma Electrónica, cuando el certificado reconocido (cualificado) contenga otras circunstancias personales o atributos del suscriptor, como su condición de titular de un cargo público, su pertenencia a un colegio profesional o su titulación, éstas deberán comprobarse mediante los documentos oficiales que las acrediten, de conformidad con su normativa específica.
El tipo de documentación, modalidades de tramitación, procedimientos de autenticación y validación quedan especificados en este documento.

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 Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad.

4.1.1 Operación y gestión de la Infraestructura de Clave Pública

Las operaciones y procedimientos realizados para la puesta en práctica de esta Política de Certificación se realizan siguiendo los controles requeridos por los estándares reconocidos para tal efecto, describiéndose estas actuaciones en los apartados "Controles de Seguridad Física, Instalaciones, Gestión y Operacionales" y "Controles de Seguridad Técnica" de la Declaración de Prácticas de Certificación de ANF AC.

La Declaración de Prácticas de Certificación de ANF AC, da respuesta a diferentes apartados de la norma ETSI EN 319 411-2.

4.1.2 Interoperabilidad

Los certificados correspondientes a esta Política de Certificación son expedidos por ANF AC conforme a la Resolución de 29 de noviembre de 2012, de la Secretaría de Estado de Administraciones Públicas, por la que se publica el Acuerdo de aprobación de la Política de Firma Electrónica y de Certificados de la Administración General del Estado y se anuncia su publicación en la sede correspondiente, y concretamente el perfil de este tipo de certificados es conforme al perfil aprobado por el Consejo Superior de Administración Electrónica, en reunión de la Comisión Permanente de 30 de mayo de 2012 y publicado en el anexo II de la citada Resolución.

4.2 Solicitud del certificado

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

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 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.

4.3 Procedimiento de tramitación

4.3.1 Autenticación de identidad

4.3.1.1 Suscriptor

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 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 permanente, 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 Representante deberá disponer de poder suficiente de representación.
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 (cualificado) 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).

4.3.1.2 Responsable del certificado

Se seguirá el mismo procedimiento que el especificado en el anterior apartado "4.3.1.1 Suscriptor", con la particularidad de que, en este supuesto, el poder de representación requerido al suscriptor será sustituido

por la firma del Acta de Autorización y Aceptación de Responsabilidad incluida en este documento. El acta deberá ser firmada por el Representante Legal y por el Responsable del Certificado.

4.3.1.3 Sujeto

El suscriptor que tramita la solicitud de certificado, deberá presentar original o copia auténtica de la siguiente documentación vigente:

1.- 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 la copia auténtica la escritura de constitución inscrita en el Registro Mercantil, o certificación extendida por el Registro Mercantil.
  Para acreditar la representación:
  - en caso de Administradores o Consejo de Administración, copia auténtica de la escritura de nombramiento inscrita en el Registro Mercantil o certificación del nombramiento extendida por el Registro Mercantil,
  - en caso de Apoderados, copia auténtica de la escritura de poder.
- 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 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.

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

- 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 y 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 con OID 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 suscriptor 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.

    - En el certificado de sello electrónico PSD2, ANF AC verificará, utilizando información auténtica de la Autoridad Nacional Competente los atributos específicos de PSD2,
        - número de autorización,
        - roles, y
        - nombre de la Autoridad Nacional Competente facilitados por el sujeto,

      Si la Autoridad Nacional Competente proporciona normas para la validación de estos atributos, ANF AC aplicará esas normas.

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

- Se verifica que ninguna de las personas físicas o jurídicas asociadas a la solicitud consta en la lista negra gestionada con el identificados OID 1.3.6.1.4.1.18332.56.2.1.

4.3.3 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.

4.4 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.

4.4.1 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 se 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, de forma automática, realiza las correspondientes comprobaciones de seguridad. En caso de confirmación, el certificado es descargado e instalado automáticamente.

4.4.2 Notificación al suscriptor

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

4.5 Aceptación del certificado

4.5.1 Aceptación

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

4.5.2 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.

4.5.3 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.

4.5.4 Publicación del certificado

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

4.5.5 Notificación de la emisión del certificado por la AC a terceros

No se efectúa notificación a terceros.

4.6 Denegación

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

4.7 Renovación de certificados

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

4.7.1 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.

4.7.2 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.

4.7.3 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.

- Antes de la renovación de los certificados PSD2, ANF AC repetirá la verificación de los atributos específicos de PSD2 incluidos en el certificado. Si la Autoridad Nacional Competente proporciona normas para la validación de estos atributos, ANF AC aplicará esas normas.

4.7.3.1 Renovación de certificados que han superado los 5 años desde la identificación inicial.

Se requiere la formalización de la solicitud mediante firma manuscrita del suscriptor, trámite realizado con presencia física del interesado y utilizando documentación original suficiente. Los trámites podrán ser realizados ante:

- **Autoridad de Registro Reconocida** que, según la definición de la DPC de ANF AC, son las personas físicas o jurídicas a las que ANF AC ha dotado de la tecnología necesaria para realizar las funciones de entidad de registro, habiendo formalizado el correspondiente contrato de asunción de responsabilidades y convenio de colaboración.

- **Autoridad de Registro Colaboradora** que, según la definición de la DPC de ANF AC, son personas que, de acuerdo con la legislación vigente, tienen atribuciones de fedatario público.

- **Entidad de Confianza** que, según la definición de la DPC de ANF AC, son entidades que, a criterio de ANF AC, tienen la capacidad necesaria para determinar la identidad, capacidad y libertad de acción de los suscriptores.

4.7.4 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.

4.7.5 Notificación de la renovación del certificado

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

4.7.6 Aceptación de la renovación del certificado

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

4.7.7 Publicación del certificado renovado

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

4.7.8 Notificación a otras entidades

No se contempla.

4.7.9 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.

4.8 Modificación del certificado

No es aplicable.

4.9 Revocación y suspensión de certificados

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

4.9.1 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 Coordinador 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.

- En los certificados PSD2, si la Autoridad Nacional Competente, como propietaria de la información específica de PSD2, notifica a ANF AC que ha cambiado información relevante, ANF AC investigará esta notificación independientemente de su contenido y formato. ANF AC determinará si los cambios afectan a la validez del certificado, en cuyo caso revocará el/los certificado/s afectado/s. ANF AC llevará a cabo esta verificación y valoración en un plazo máximo de 72 horas, salvo causa justificada.

Las Autoridades Nacionales Competentes, para notificar los cambios en la información reglamentaria PSD2 relevante del Prestador de Servicios de Pago (PSP), pueden remitir correo electrónico a,

info@anf.es

4.9.2 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 dirección web https://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.

4.9.3 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 de 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.

En el caso de los certificados PSD2, la Autoridad Nacional Competente, como propietaria de la información específica de PSD2, puede solicitar la revocación del certificado siguiendo el procedimiento definido en este documento. Este procedimiento permite a la Autoridad Nacional Competente especificar la razón de la revocación.

ANF AC procesará dichas solicitudes y validará su autenticidad. Si no se proporciona una razón o la razón no está en el área de responsabilidad de la Autoridad Nacional Competente, ANF AC podrá decidir no tomar medidas. Basándose en una solicitud auténtica, ANF AC revocará el certificado si se cumple alguna de las siguientes condiciones:

- Se ha revocado la autorización del PSP,
- el número de autorización de la PSP ha cambiado,
- el nombre o identificador Autoridad Nacional Competente ha cambiado,
- se ha revocado cualquier rol de PSP incluido en el certificado,
- la revocación es obligatoria por ley.
- Cualquier otra causa de revocación establecida en esta Política de Certificación.

4.9.4 Periodo de gracia de la solicitud de revocación

Según lo definido en la DPC de ANF AC.

4.9.5 Plazo máximo de procesamiento de la solicitud de revocación

Según lo definido en la DPC de ANF AC.

4.9.6 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 consultar la última CRL emitida dentro del periodo de vigencia del certificado de interés.

4.9.7 Frecuencia de emisión de listas CRL

Según lo definido en la DPC de ANF AC.

4.9.8 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.

4.9.9 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.

4.9.10 Suspensión del certificado

No es aplicable.

4.9.11 Identificación y autenticación de solicitudes de suspensión

No está permitida la suspensión del certificado.

4.10 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 en 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 la Política de Autoridad de Sellado de Tiempo y Declaración de Practicas

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 "cualificados" cumplen con las normas:

- ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI) Certificate Profiles, Part 5: QCStatements
- ETSI TS 119 495 *(certificados PSD2)*
- 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 del sello.

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 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 sello en conformidad con el artículo 39 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 2

- **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.

Los certificados emitidos por ANF AC del tipo PSD2 además de los anteriormente reseñados, se incluye PSD2QcType, conforme lo establecido en la ETSI TS 119 495 clausula 5.1:

a) La función del Prestador de Servicios de Pago (PSP), que puede ser una o más de las siguientes:

i. servicio de cuentas (PSP_AS);
ii. iniciación de pago (PSP_PI);
iii. información de la cuenta (PSP_AI);
iv. emisión de instrumentos de pago basados en tarjeta (PSP_IC).

b) Nombre de la Autoridad Nacional Competente donde el PSP está registrado. Esta información se proporciona en dos formas: *la cadena de nombre completo (NCAName) en inglés y un identificador único abreviado (NCAId).*

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).

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 documento perfil técnico

7.3 Perfil de OCSP

Según lo definido en la DPC de ANF AC. y do5cumento 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.