

## Política de Certificación

### Certificados de Sello Electrónico

---



### **Nivel de Seguridad**

Documento 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 – 2022 CC-BY- ND (Creative commons licenses)**

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

Teléfono: 932 661 614 (Llamadas desde España) Internacional (+34) 933 935 946

Web: [www.anf.es](http://www.anf.es)

# ÍNDICE

<b>1. Introducción .....</b>	<b>6</b>
1.1. Descripción de los certificados.....	6
1.2. Nombre del documento e identificación .....	7
1.3. Partes de la PKI.....	8
1.3.1. Sujeto.....	8
1.4. Uso de los certificados .....	9
1.4.1. Usos permitidos.....	9
1.4.2. Límites de uso de los certificados.....	9
1.4.3. Usos prohibidos .....	9
1.5. Datos de contacto de la Entidad de Certificación .....	9
1.6. Definiciones y Acrónimos.....	9
<b>2. Repositorios y Publicación de la Información .....</b>	<b>10</b>
2.1. Repositorios .....	10
2.2. Publicación de la información .....	10
2.3. Frecuencia de actualizaciones.....	10
2.4. Controles de acceso a los repositorios.....	10
2.5. Certificados PSD2 .....	10
<b>3. Identificación y Autenticación .....</b>	<b>11</b>
3.1. Registro de nombres .....	11
3.1.1. Tipos de nombres .....	11
3.1.2. Necesidad de que los nombres sean significativos .....	11
3.1.3. Pseudónimos o anónimos .....	11
3.1.4. Reglas utilizadas para interpretar varios formatos de nombres .....	11
3.1.5. Unicidad de los nombres .....	11
3.1.6. Resolución de conflictos relativos a nombres y marcas.....	11
3.2. Validación inicial de la identidad.....	12
3.2.1. Prueba de posesión de clave privada .....	12
3.2.2. Autenticación de la identidad.....	12
3.3. Renovación de la clave.....	12

3.4.	Solicitud de Revocación .....	12
<b>4.</b>	<b>Requisitos Operacionales .....</b>	<b>13</b>
4.1.	Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad. ....	13
4.1.1	Operación y gestión de la Infraestructura de Clave Pública.....	13
4.1.2	Interoperabilidad.....	13
4.2.	Solicitud del certificado.....	13
4.3.	Procedimiento de tramitación .....	14
4.3.1.	Autenticación de identidad .....	14
4.3.2.	Aprobación o rechazo de las solicitudes de certificados.....	16
4.3.3.	Tiempo para procesar la emisión de certificados.....	18
4.4.	Emisión del certificado.....	18
4.4.1.	Acciones de la Entidad de Certificación durante el proceso de emisión.....	18
4.4.2.	Notificación al suscriptor .....	18
4.5.	Aceptación del certificado .....	18
4.5.1.	Aceptación .....	18
4.5.2.	Devolución .....	18
4.5.3.	Seguimiento.....	19
4.5.4.	Publicación del certificado.....	19
4.5.5.	Notificación de la emisión del certificado por la AC a terceros.....	19
4.6.	Denegación.....	<b>¡Error! Marcador no definido.</b>
4.7.	Renovación de certificados .....	19
4.7.1.	Certificados vigentes .....	19
4.7.2.	Personas autorizadas para solicitar la renovación .....	19
4.7.3.	Identificación y autenticación de las solicitudes de renovación rutinarias.....	19
4.7.4.	Renovación de certificados que han superado los 5 años desde la identificación inicial. <b>¡Error!</b>	
	<b>Marcador no definido.</b>	
4.7.5.	Aprobación o rechazo de las solicitudes de renovación .....	20
4.7.6.	Notificación de la renovación del certificado .....	20
4.7.7.	Aceptación de la renovación del certificado .....	20
4.7.8.	Publicación del certificado renovado .....	21
4.7.9.	Notificación a otras entidades.....	21

4.7.10.	Identificación y autenticación de las solicitudes de renovación de clave después de una revocación -Clave no comprometida- .....	21
4.8.	Modificación del certificado.....	21
4.9.	Revocación y suspensión de certificados.....	21
4.9.1.	Causas de revocación .....	¡Error! Marcador no definido.
4.9.2.	Identificación y autenticación de solicitudes de revocación .....	¡Error! Marcador no definido.
4.9.3.	Procedimiento para la solicitud de revocación .....	¡Error! Marcador no definido.
4.9.4.	Periodo de gracia de la solicitud de revocación .....	¡Error! Marcador no definido.
4.9.5.	Plazo máximo de procesamiento de la solicitud de revocación..	¡Error! Marcador no definido.
4.9.6.	Requisitos de comprobación de listas CRL .....	¡Error! Marcador no definido.
4.9.7.	Frecuencia de emisión de listas CRL .....	¡Error! Marcador no definido.
4.9.8.	Disponibilidad de comprobación on-line de la revocación .....	¡Error! Marcador no definido.
4.9.9.	Requisitos de la comprobación on-line de la revocación .....	¡Error! Marcador no definido.
4.9.10.	Suspensión del certificado.....	¡Error! Marcador no definido.
4.9.11.	Identificación y autenticación de solicitudes de suspensión.....	¡Error! Marcador no definido.
4.10.	Depósito y recuperación de claves .....	22
<b>5.</b>	<b>Controles de Seguridad Física, Instalaciones, Gestión y Operacionales.....</b>	<b>23</b>
5.1.	Controles de seguridad física .....	23
5.2.	Controles de procedimiento .....	23
5.3.	Controles de personal .....	23
<b>6.</b>	<b>Controles de Seguridad Técnica .....</b>	<b>24</b>
<b>7.</b>	<b>Perfiles de Certificados, Listas CRL y OCSP.....</b>	<b>25</b>
7.1.	Perfiles de certificados.....	25
7.2.	Perfil de CRL .....	25
7.3.	Perfil de OCSP.....	25
<b>8.</b>	<b>Auditoría de Conformidad .....</b>	<b>26</b>
<b>9.</b>	<b>Disposiciones Generales.....</b>	<b>27</b>

## 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 (en adelante Reglamento eIDAS, y con la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. 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.

El presente documento es la Política de Certificación (PC) correspondiente a los certificados emitidos por ANF AC del tipo **Certificados cualificados de sello electrónico**, de acuerdo con lo establecido en el Anexo III del Reglamento eIDAS, y lo definido en la Ley 6/2020. Detalla y complementa lo especificado en la Declaración de Prácticas de Certificación de ANF AC y su adenda, define los requisitos de procedimiento y operacionales a los que está sujeto el uso de estos certificados, y 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 roles, 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.

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.

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://anf.es/repositorio-legal>

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 con el Anexo III del 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 emite los siguientes tipos de certificados cualificados de sello electrónico:

- **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 Público (LRJ). Se adapta a los perfiles y las definiciones establecidas por la Subdirección General de Información, Documentación y Publicaciones del Ministerio de Hacienda y Administraciones Públicas en su documento “*Perfiles de certificados electrónicos*” (apartado 10: *Certificado de sello electrónico*) para los niveles de aseguramiento<sup>1</sup> **alto** (apartado 9.2) y **medio/sustancial** (apartado 9.3).
- **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.

La validez máxima de los certificados cualificados para sello electrónico emitidos por ANF AC es de 5 años.

Estos certificados pueden ser emitidos en los siguientes soportes:

- **Software criptográfico**, incluyendo el servicio de distribución de claves.
- **Dispositivo cualificado de creación de sello (QSCD<sup>2</sup>)**. El par de claves ha sido generado en el dispositivo QSCD que las almacena.
- **Servicio Centralizado de certificados de sello electrónico**. Los datos de creación de **sello** han sido generados en un dispositivo 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.

## 1.2. Nombre del documento e identificación

<b>Nombre del documento</b>	Política de Certificación de Certificados de Sello electrónico		
<b>Versión</b>	1.9		
<b>Estado de la política</b>	APROBADO		
<b>OID</b>	1.3.6.1.4.1.18332.25.1.1		
<b>Fecha de aprobación</b>	01/03/2022	<b>Fecha de publicación</b>	01/03/2022

<sup>1</sup> Ver apartado 2.1 Niveles de aseguramiento del documento “Perfiles de certificados electrónicos”.

<sup>2</sup> 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 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>

La versión de esta Política de Certificación sólo será cambiada si se producen cambios sustanciales que afectan a su aplicabilidad.

Versión	Cambios	Aprobación	Publicación
1.9.	Revisión y aclaraciones.	01/03/2022	01/03/2022
1.8.	Revisión y aclaraciones.	19/02/2021	19/02/2021
1.7.	Revisión e inclusión certificados de Sello para PSD2.	30/01/2019	30/01/2019
1.6.	Revisión.	30/03/2017	30/03/2017
1.5.	Revisión y adaptación a eIDAS.	19/10/2016	19/10/2016
1.4.	Revisión.	03/04/2015	03/04/2015
1.3.	Revisión.	03/05/2014	03/05/2014
1.2.	Ampliación certificados de sello disponibles	08/07/2014	08/07/2014
1.1.	Inclusión Certificado de Sello Electrónico Nivel Alto	01/06/2012	01/06/2012
1.0.	Creación del documento	06/02/2011	06/02/2011

### 1.3. Partes de la PKI

Según lo definido en la DPC de ANF AC.

#### 1.3.1. Sujeto

Según lo definido en la DPC de ANF AC.

##### 1.3.1.1. 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.

##### 1.3.1.2. 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.

##### 1.3.1.3. 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.

## 1.4. Uso de los certificados

### 1.4.1. Usos permitidos

Estos certificados deberán utilizarse en conformidad con la Ley 6/2020. El uso de las claves y el certificado por parte del suscriptor, presupone la aceptación de las condiciones de uso establecidas en la DPC de ANF AC y su adenda.

- **Sellado de documentos.** Key usage tendrá el bit “ContentComitment”.
- 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”).

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

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

### 1.4.3. Usos prohibidos

Según lo definido en la DPC de ANF AC.

## 1.5. Datos de contacto de la Entidad de Certificación

Según lo definido en la DPC de ANF AC.

## 1.6. Definiciones y Acrónimos

Según lo definido en la DPC de ANF AC.

## 2. Repositorios y Publicación de la Información

### 2.1. Repositorios

Según lo definido en la DPC de ANF AC.

### 2.2. Publicación de la información

Según lo definido en la DPC de ANF AC.

### 2.3. Frecuencia de actualizaciones

Según lo definido en la DPC de ANF AC.

### 2.4. Controles de acceso a los repositorios

Según lo definido en la DPC de ANF AC.

### 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”:

#### 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.

#### 3.1.2. Necesidad de que los nombres sean significativos

En todos los casos los nombres distintivos deben tener sentido.

#### 3.1.3. Pseudónimos o anónimos

No se permiten.

#### 3.1.4. Reglas utilizadas para interpretar varios formatos de nombres

Según lo definido en la DPC de ANF AC.

#### 3.1.5. Unicidad de los nombres

Según lo definido en la DPC de ANF AC.

#### 3.1.6. Resolución de conflictos relativos a nombres y marcas

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 un Operador de una Oficina de Verificación Presencial (OVP) adscrita a una Autoridad de Registro (AR), identificando al solicitante mediante documento de identidad aceptado por la legislación nacional, siendo documento original y en estado vigente. En su presencia procederá a firmar el formulario de solicitud que deberá estar debidamente cumplimentado.

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

- b) **Por correo ordinario:** Si los formularios correspondientes han sido debidamente cumplimentados, y la firma del suscriptor ha sido legitimada en presencia notarial, adjuntando copias compulsadas de los documentos de identidad, autorización y representación legal.

- c) **Telemáticamente:** 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 cualificado de firma electrónica vigente o identificándose y aceptando los documentos mediante uno de los medios de identificación a distancia que estén legalmente aprobados, en conformidad con el Art.7. 2) de la Ley 6/2020.

### 4.3. Procedimiento de tramitación

#### 4.3.1. Autenticación de identidad

El suscriptor debe de facilitar un número de teléfono móvil y una dirección de correo electrónico de su confianza. A estos buzones ANF AC envía 2 códigos de verificación para poder confirmar la solicitud. 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 entregas 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.

##### 4.3.1.1. Suscriptor

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

- DNI o pasaporte (*Ciudadanos españoles*)
- Documento de Identidad/Pasaporte/tarjeta NIE (emitida por el Registro de Ciudadanos Miembros de la Unión), y Certificado emitido por el Registro de Ciudadanos Miembros de la Unión. (*Ciudadanos extranjeros, miembros de la UE o Espacio Económico Europeo*)
- Pasaporte o tarjeta de residencia permanente. (*Ciudadanos extranjeros no miembros de la UE*)
- Dirección física y otros datos que permitan contactar con él. En especial, buzones de contacto personales de su confianza como número de teléfono móvil y dirección de correo electrónico. Si el OVP, 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 OVP, ARR o el RDE conocen de forma personal al suscriptor podrán emitir y firmar una Declaración de Identidad<sup>3</sup>.
- El Representante deberá disponer de poder suficiente de representación.

---

<sup>3</sup> **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.

Los documentos empleados para verificar la identidad (DNI, NIE, Pasaporte, tarjeta de residencia) deberán incluir una fotografía que permita cotejar la identidad de la persona compareciente. En caso de escasa nitidez, o duda en su reconocimiento del, se podrá solicitar otro documento oficial que incorpore fotografía de mayor calidad (p.ej., licencia de conducir).

#### 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. 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:

<b>Según forma jurídica</b>	
<b>Sociedades mercantiles y demás personas jurídicas cuya inscripción sea obligatoria en el Registro Mercantil</b>	Copia auténtica la escritura de constitución inscrita en el Registro Mercantil, o certificación extendida por el Registro Mercantil. Para acreditar la representación: <ul style="list-style-type: none"> <li>○ 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,</li> <li>○ en caso de Apoderados, copia auténtica de la escritura de poder.</li> </ul>
<b>Asociaciones, Fundaciones y Cooperativas</b>	Original o copia auténtica de un certificado del registro público donde consten inscritas, relativo a su constitución.
<b>Sociedades civiles y demás personas jurídicas</b>	Original o copia auténtica del documento que acredite su constitución de manera fehaciente.
<b>Administraciones Públicas y entidades pertenecientes al sector público</b>	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.
<b>Fondos de inversión, fondos de capital-riesgo, fondos de regulación del mercado de títulos hipotecarios, fondos de titulación hipotecaria, fondos de titulación de activos, fondos de garantía de inversiones y fondos de pensiones</b>	Certificado de inscripción en el registro correspondiente del Ministerio de Economía y Hacienda o de la Comisión Nacional del Mercado de Valores, deberá constar en el certificado la identificación de la entidad gestora del fondo
<b>Uniones Temporales de Empresas</b>	Que se hayan acogido al régimen fiscal especial, y si estuvieran inscritas en el Registro especial de Uniones Temporales de Empresas del Ministerio de Economía y Hacienda, adscrito a la Agencia Estatal de Administración Tributaria, aportarán certificado de dicha inscripción. En el caso de no

	estar inscritas, documento suscrito por una mayoría de miembros o socios, en el que certifican la vigencia de la entidad
<b>Otras</b>	Cuando la entidad no corresponda a ninguna de las tipologías anteriormente reseñadas y, por lo tanto, no deba de estar inscrita en ninguno de esos registros, se presentarán junto con la solicitud los documentos que posea al respecto el suscriptor, siendo el Responsable de Dictámenes de Emisión el que determine la suficiencia o insuficiencia de los mismos

#### 4.3.2. Tramitación en el despacho de OVP o ARR

Cuando la tramitación se realice de forma presencial ante un Operador de una Oficina de Verificación Presencial (OVP) adscrita a una Autoridad de Registro (AR), se requerirá acreditación del acto presencial con el fin de imposibilitar el repudio del trámite realizado, para ello se obtendrán una o varias evidencias que quedarán asociadas al formulario de solicitud, P.ej. firma manuscrita, firma grafométrica, fotografía, video, voz, huellas dactilares, o lectura del chip ensamblado en el documento de identidad oficial.

#### 4.3.3. Tramitación por legitimación de firma por notario público o compulsas por operador ARR u OVP

En el caso de intervención de Notario Público, se requerirá la legitimación de firma del suscriptor en la solicitud de expedición de un certificado (LRDASEC 6/2020, Art. 7.1). Se realizará el siguiente procedimiento:

- a) ANF AC pone a disposición del suscriptor políticas de certificación, precios y el formulario de solicitud y el contrato de prestación de servicios de certificación, así como los medios técnicos para que realice la tramitación de solicitud: cumplimentar formulario de solicitud y facilitar documentos acreditativos de identidad y filiación personal.  
Los documentos requeridos para la acreditación serán los mismos que los requeridos en la tramitación ante ARR y OVP.
- b) El suscriptor, en su caso, estampa su firma manuscrita o firma grafo-métrica (biométrica) en los documentos correspondientes al trámite de solicitud del certificado.
- c) Cumplido este trámite, ANF AC pone a disposición del suscriptor los medios técnicos necesarios para llevar a cabo la generación de su par de claves, selección de PIN (datos de activación de firma), y generación del certificado de petición (CSR bajo estándar PKCS#10).
- d) La firma del formulario de solicitud y el contrato de prestación de servicios, será legitimada por conocimiento de firma por notario público o compulsada por un operador OVP o ARR.”

#### 4.3.4. Aprobación o rechazo de las solicitudes de certificados

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 (en adelante RDE), con las que ANF AC suscriba el instrumento legal pertinente.

El RDE 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. El 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.
- Y supervisará que se cumplen todos los requisitos impuestos por la legislación aplicable en materia de protección de datos, a efectos del RGPD, la LOPDPGDD y según lo previsto en el artículo 8 de la Ley 6/2020.

El RDE puede requerir del suscriptor información o documentación complementaria y el suscriptor dispondrá de 30 días para hacer entrega de la misma. Transcurrido este plazo sin que se haya cumplimentado este requerimiento, la solicitud será rechazada automáticamente. 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, rechazará la solicitud del certificado.

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 comprobación de la información y documentación recibida, se podrán utilizar los siguientes medios:
  - Consulta a los registros públicos oficiales en los que deba estar inscrita la entidad a efectos de comprobar existencia, vigencia de cargos y otros aspectos legales, como actividad y fecha de constitución.
  - Boletines Oficiales de ámbito nacional o regional de los organismos públicos a los que pertenecen organismos y empresas públicas.
- Se verifica automáticamente que ninguna de las personas físicas o jurídicas asociadas a la solicitud consta en la lista negra de personas y entidades.
- 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.

#### **4.3.5. Tiempo para procesar la emisión de certificados**

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.

#### **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.

La emisión de un certificado implica la aprobación final y completa de una solicitud por parte del Responsable de Dictámenes de Emisión. La emisión del 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.

##### **4.4.1. Acciones de la Entidad de Certificación durante el proceso de emisión**

Según lo definido en la DPC de ANF AC.

##### **4.4.2. Notificación al suscriptor**

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

#### **4.5. 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. Rechazo**

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 firmando 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.

#### **4.7.4. 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 de certificados**

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

En los certificados PSD2, si la Autoridad Nacional Competente (ANC), 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 ANC, 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](mailto:info@anf.es)

La ANC, como propietaria de la información específica de PSD2, puede solicitar la revocación de los certificados PSD2 siguiendo el procedimiento definido en la DPC. 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 ANC, 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 la DPC.

#### 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](mailto: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

Según lo definido en la DPC de ANF AC.

## 7. Perfiles de Certificados, Listas CRL y OCSP

### 7.1. Perfiles de certificados

Según lo definido en el documento perfil técnico.

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

Tipo	Soporte	OID
Certificado de Sello electrónico	Software criptográfico	1.3.6.1.4.1.18332.25.1.1.1
	QSCD	1.3.6.1.4.1.18332.25.1.1.4
	Servicio Centralizado	1.3.6.1.4.1.18332.25.1.1.9
Certificado de Sello electrónico AAPP	Nivel medio	Software criptográfico 1.3.6.1.4.1.18332.25.1.1.3
	Nivel alto	QSCD (Nivel alto) 1.3.6.1.4.1.18332.25.1.1.2
		Servicio Centralizado 1.3.6.1.4.1.18332.25.1.1.11
Certificado de Sello electrónico PSD2	Software criptográfico	1.3.6.1.4.1.18332.25.1.1.5
	QSCD	1.3.6.1.4.1.18332.25.1.1.6
	Servicio Centralizado	1.3.6.1.4.1.18332.25.1.1.7

### 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 documento perfil técnico

## 8. Auditoría de Conformidad

Según lo definido en la DPC de ANF AC.

## 9. Disposiciones Generales

Según lo definido en la DPC de ANF AC.