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

Paseo de la Castellana, 79 - 28046 - Madrid (España)
Teléfono: 902 902 172 (Llamadas desde España)
Internacional (+34) 933935 946
Fax: (+34) 933 031 611 · Web: www.anf.es

Nivel de Seguridad

Público

Aviso Importante

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

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

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

Índice

1 Introducción

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

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

ANF AC utiliza OID's según el estándar ITU-T Rec. X.660 y el estándar ISO/IEC 9834-1:2005 *(Procedures for the Operation of OSI Registration Authorities: General Procedures and ASN.1 Object Identifier tree top arcs).* ANF AC tiene asignado el código privado de empresa *(SMI Network Management Private Enterprise Codes)* 18332 por la organización internacional IANA -Internet Assigned Numbers Authority-, bajo la rama iso.org.dod.internet.private.enterprise *(1.3.6.1.4.1 -IANA –Registered Private Enterprise-)*.

El presente documento es la Política de Certificación (PC) correspondiente a los certificados emitidos por ANF AC del tipo "Servidor Seguro SSL", "Servidor Seguro SSL con Validación Extendida (EV)" "Sede Electrónica nivel medio y nivel alto" y, "Sede Electrónica con Validación Extendida (EV) nivel medio y nivel alto". Estos certificados pueden ser expedidos con la consideración de cualificados de acuerdo con lo establecido en el Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, y con la consideración de reconocidos según lo definido en la Ley 59/2003 de firma electrónica.

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

Este documento define los requisitos de procedimiento y operacionales a los que está sujeto el uso de estos certificados, y define las directrices que ANF AC utiliza para su emisión, gestión, revocación, renovación y cualquier otro proceso que afecte al ciclo de vida. Se describen los papeles, responsabilidades y relaciones entre el usuario final, ANF AC y terceros de confianza, así como las reglas de solicitud, renovación y revocación que se deben atender.

El marco legal y normativo en la que se basa la emisión de estos certificados es:

- CA/Browser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates
- CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates
- ETSI EN 319 411-1 (Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements)
- ETSI EN 319 411-2 (Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates)
- ETSI EN 319 412-4 (Certificate profile for web site certificates) Perfil de certificado de sede electrónica definido por el Ministerio de Hacienda y Administraciones Públicas
- 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. En adelante eIDAS.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica de España.

En el ámbito del proyecto de Google Certificate Transparency (CT), los certificados emitidos con la calificación EV (Extended Validation) serán publicados en diferentes operadores de CT Log, para cumplir con la política definida por Google.

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

Esta Política de Certificación asume que el lector conoce los conceptos de PKI, certificado y firma electrónica; en caso contrario se recomienda al lector que se forme en el conocimiento de los anteriores conceptos antes de continuar con la lectura del presente documento.

1.1 Descripción de los certificados

ANF AC, en el marco de su servicio de certificación electrónica, emite certificados técnicos del tipo:

- **Servidor Seguro SSL**

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

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

- La encriptación de las comunicaciones entre el usuario y el sitio web, facilitando el intercambio de las claves de cifrado necesarias para el cifrado de la información a través de Internet.
  La validez máxima de estos certificados es de 5 años.

Este tipo de certificados puede ser emitido en las siguientes modalidades:

- **DV y DV Wildcard**

  Este certificado, con la consideración de no cualificado según eIDAS, será utilizado para la identificación de la titularidad del dominio que alberga el sitio web, proporcionando una garantía razonable al usuario de un navegador de Internet. El DV Wildcard contiene un "comodín" en el nombre de host (ej.: *.frater.com). Se emiten según ETSI EN 319 411-1.
  La validez de estos certificados puede ser de hasta 3 años.

- **OV y OV Wildcard**

  Este certificado, con la consideración de no cualificado según eIDAS, será utilizado para la identificación de la titularidad del dominio y acreditación de la organización, proporcionando una garantía razonable al usuario de un navegador de Internet de que el sitio web al que accede es titularidad de la organización identificada en el certificado. El OV Wildcard contiene un "comodín" en el nombre de host (ej.: *.frater.com). Se emiten según la política OVCP de ETSI EN 319 411-1. La validez de estos certificados puede ser de hasta 3 años.

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

Este certificado, con la consideración de no cualificado según eIDAS, será utilizado para la identificación de la titularidad del dominio y acreditación de la organización, proporcionando una garantía robusta al usuario de un navegador de Internet de que el sitio web al que accede es titularidad de la organización identificada en el certificado. Se emiten según la política EV de ETSI EN 319 411-1. La validez de estos certificados puede ser hasta 2 años.

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

El objetivo de los Certificados SSL EV es su utilización en protocolos TLS / SSL con la finalidad de garantizar la validez de la constitución de la organización identificada en el certificado, evitando casos de *phishing* u otros casos de fraude de identidad en línea. Además, este tipo de certificados precisa el uso de Dispositivos SSCD (HSM).

ANF AC cumple lo indicado en las guías del CA/Browser Forum publicadas en su sitio web https://www.cabforum.org, incluyendo la aceptación de los programas de auditoría especificados en las mismas.

- **Sede electrónica**

En el ámbito de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, ANF AC emite certificados del tipo sede electrónica. Se emiten según la política de ETSI EN 319 411-2 y el perfil de certificado de sede definido por el Ministerio de Hacienda y Administraciones Públicas. Se trata de un certificado con la consideración de cualificado según eIDAS en el que se identifica a la Administración Pública, órgano o entidad administrativa titular de la sede.

La validez de estos certificados es de 2 años.

El fin de este certificado es establecer comunicaciones de datos vía TLS/SSL en servicios y aplicaciones informáticas.

- **Sede electrónica con Validación Extendida (EV)**

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

Además, ANF AC cumple lo indicado en las guías del CA/Browser Forum publicadas en su sitio web https://www.cabforum.org, incluyendo la aceptación de los programas de auditoría especificados en las mismas.

La validez de estos certificados es de 2 años.

1.2 Identificación

Nombre del documento	Política de Certificación de certificados de Servidor Seguro SSL, Servidor Seguro SSL con Validación Extendida (EV), Sede Electrónica y Sede Electrónico con Validación Extendida (EV)
Versión	2.2
Estado de la política	APROBADO
Referencia del documento / OID	1.3.6.1.4.1.18332.55.1.1
Fecha de emisión	04 de noviembre de 2016
Fecha de expiración	No es aplicable
DPC relacionada	Declaración de Prácticas de Certificación (DPC) de ANF AC
Localización	https://www.anf.es/documentos

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

Certificado	OID
Servidor Seguro SSL DV Con algoritmo SHA-256 y longitud 2048 bits	1.3.6.1.4.1.18332.55.1.1.1.22
Servidor Seguro SSL OV Con algoritmo SHA-256 y longitud 2048 bits	1.3.6.1.4.1.18332.55.1.1.7.22
Servidor Seguro SSL EV Con algoritmo SHA-256 y longitud 2048 bits	1.3.6.1.4.1.18332.55.1.1.2.22
Sede Electronica Nivel Medio Con algoritmo SHA-256 y longitud 2048 bits	1.3.6.1.4.1.18332.55.1.1.3.22
Sede Electronica EV Nivel Medio Con algoritmo SHA-256 y longitud 2048 bits	1.3.6.1.4.1.18332.55.1.1.5.22
Sede Electronica Nivel Alto Con algoritmo SHA-256 y longitud 2048 bits	1.3.6.1.4.1.18332.55.1.1.4.22

Sede Electronica EV Nivel Alto Con algoritmo SHA-256 y longitud 2048 bits	1.3.6.1.4.1.18332.55.1.1.6.22

Cuando el certificado es del tipo "Servidor Seguro SSL", en la extensión CertificatePolicies (2.5.29.32), incluirá al menos uno de los PolicyInformation siguientes:

- Si se realiza exclusivamente validación de dominio (Compliant with Baseline Requirements – No entity identity asserted) [CA/B FORUM - SSL DV]:
    - 2.23.140.1.2.1

- Si el suscriptor es una persona jurídica, organización o institución (Compliant with Baseline Requirements – Organization identity asserted) [CA/B FORUM - SSL OV]:
    - 2.23.140.1.2.2

- Si el suscriptor es una persona física (Compliant with Baseline Requirements – Individual identity asserted):
    - 2.23.140.1.2.3

En el caso de certificados de "Sede Electrónica Nivel Alto Nivel Alto", la extensión CertificatePolicies (2.5.29.32) incluirá el OID:

- 2.16.724.1.3.5.5.1

En el caso de "Sede Electrónica Nivel Medio", la extensión CertificatePolicies (2.5.29.32) incluirá el OID:

- 2.16.724.1.3.5.5.2

Todos los certificados cumplen con la norma ETSI TS 102 042 y ETSI 101 456 requisitos, en relación con las políticas de los certificados identificados:

0.4.0.2042.1.1	Advanced Certificate Policy (Individual or Professional) [1]
0.4.0.2042.1.2	Advanced Certificate Policy (Individual or Professional) issued on cryptographic device [2]
0.4.0.2042.1.7	TLS/SSL Certificate Policy with Organization validation [3]
0.4.0.2042.1.6	TLS/SSL Certificate Policy with Domain validation [4]
0.4.0.1456.1.1	Qualified Certificate Policy [5]

[1] *Política de Certificación Normalizada (NCP) conforme con el estándar ETSI TS 102 042*
[2] *Política de Certificación Normalizada Extendida (NCP+) conforme con el estándar ETSI TS 102 042*
[3] *Política de validación de certificados Organización (OVCP) conforme con el estándar ETSI TS 102 042*
[4] *Política de validación de certificados de dominio (DVCP) conforme con el estándar ETSI 102 042*
[5] *Referida a QCP+SSCD (Qualified Certificate Policy + Secure Signature Creation Device) conforme con el estándar ETSI TS 101 456*

En el caso de incluir la extensión "Extended Validation", la extensión CertificatePolicies (2.5.29.32) incluirá el OID de SSL EV [ETSI TS 102 042 - EVCP]:

- 0.4.0.2042.1.4

Además, conforme a [CA/B FORUM - SSL EV] incluirá el OID de SSL EV

- 2.23.140.1.1

Y, cuando el certificado es emitido con la calificación de cualificado de sitio web según eIDAS, cumple con los requerimientos de la política QCPW de ETSI EN 319 411-2, y el anexo IV de eIDAS. En la extensión CertificatePolicies (2.5.29.32), incluirá al menos uno de los PolicyInformation siguientes:

- qcp-web (0.4.0.194112.1.4)

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

1.3 Tipo de soporte

Estos certificados pueden ser emitidos en dos tipos de soporte:

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

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

Se definen dos niveles de aseguramiento

a. Nivel medio:

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

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

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

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

La validez máxima de estos certificados es de 5 años, salvo en certificados emitidos con Extended Validation, cuyo periodo máximo de validez 27 meses.

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

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

b. Nivel alto:

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

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

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

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

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

La validez máxima de estos certificados es de 5 años, salvo en certificados emitidos con Extended Validation, cuyo periodo máximo de validez 27 meses.

1.4 Partes de la PKI

1.4.1 Autoridades de Certificación

Según lo definido en la DPC de ANF AC.

1.4.2 Autoridades de Registro

Según lo definido en la DPC de ANF AC.

1.4.2.1 Autoridad de Registro Reconocida

Según lo definido en la DPC de ANF AC.

1.4.2.2 Autoridad de Registro Colaboradora

Según lo definido en la DPC de ANF AC.

1.4.3 Responsable de Dictámenes de Emisión

Según lo definido en la DPC de ANF AC.

1.4.4 Entidades finales

1.4.4.1 Suscriptor del certificado

Según lo definido en la DPC de ANF AC.

1.4.4.2 Sujeto

Según lo definido en la DPC de ANF AC.

1.4.4.3 Responsable del certificado

Según lo definido en la DPC de ANF AC.

1.4.4.4 Terceros que confían

Según lo definido en la DPC de ANF AC.

1.5 Ámbito de aplicación

1.5.1 Usos permitidos

El Certificado emitido bajo esta Política puede ser utilizado con los siguientes propósitos:

- Identificación del DNS. El Certificado emitido bajo la presente Política permite identificar y vincular una determinada DNS –Domain Name System- (en español: sistema de nombre de Dominio) a la entidad titular de ese dominio, que es el suscriptor del certificado.
- La encriptación de las comunicaciones entre el usuario y el sitio web, facilitando el intercambio de las claves de cifrado necesarias para el cifrado de la información a través de Internet.

1.5.2 Límites de uso de los certificados

Según lo definido en la DPC de ANF AC.

1.5.3 Usos prohibidos

No se permite un uso distinto al establecido en esta Política y en la Declaración de Prácticas de Certificación de ANF AC.

1.6 Datos de contacto de la Entidad de Certificación

Según lo definido en la DPC de ANF AC.

1.7 Definiciones y Acrónimos

Según lo definido en la DPC de ANF AC.

2 Repositorios y Publicación de la información

2.1 Repositorios

Según lo definido en la DPC de ANF AC.

2.2 Publicación de la información

Según lo definido en la DPC de ANF AC.

2.3 Frecuencia de actualizaciones

Según lo definido en la DPC de ANF AC.

2.4 Controles de acceso a los repositorios

Según lo definido en la DPC de ANF AC.

3 Identificación y Autenticación

3.1 Registro de nombres

3.1.1 Tipos de nombres

Todos los certificados requieren un nombre distintivo (DN o Distinguished Name) conforme al estándar X.500.

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

3.1.2 Necesidad de que los nombres sean significativos

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

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

3.1.3 Pseudónimos o anónimos

No se permiten.

3.1.3.1 Reglas utilizadas para interpretar varios formatos de nombres

Se atenderá en todo caso a lo marcado por el estándar X.500 de referencia en la norma ISO/IEC 9594.

3.1.4 Unicidad de los nombres

El certificado se emitirá con el nombre completo al que responda el servicio que se va a dotar con características SSL. Este nombre debe ser único en la red. No se aceptarán nombres parciales.

3.1.5 Resolución de conflictos relativos a nombres y marcas

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

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

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

3.2 Validación inicial de la identidad

3.2.1 Prueba de posesión de clave privada

Según lo definido en la DPC de ANF AC.

3.2.2 Autenticación de la identidad del suscriptor, del responsable del certificado y del sujeto

Los Certificados emitidos bajo esta Política de Certificación identificaran al sujeto a cuyo nombre ha sido registrado un dominio DNS. También identificaran al suscriptor del certificado y en su caso, al responsable del certificado (caso de haber sido nombrado por el suscriptor).

ANF AC comprueba, por si misma o por medio de sus Autoridades de Registros, la solicitud, la identidad y cualesquiera otras circunstancias de los suscriptores y sujetos de los certificados. El instrumento legal existente entre las partes incluirá la exigencia de cumplimiento de lo indicado en los requisitos de ETSI y CABForum.

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

El identificativo fiscal del suscriptor, del sujeto y del responsable del certificado se incorporará en el certificado. Además, el suscriptor debe de facilitar un número de teléfono móvil y una dirección de correo electrónico de su confianza. La dirección de correo electrónico y el servicio SMS o WhatsApp asociado a su teléfono móvil, tendrán la consideración de buzones autorizados para que ANF AC pueda realizar entregar electrónicas certificadas, incluso doble autenticación en el caso de servicio de certificados de firma electrónica centralizada, o cualquier otro que se considere necesario. El usuario asume la obligación de informar a ANF AC de cualquier cambio de dirección de correo electrónico o número de teléfono móvil.

Tipo de documentación, modalidades de tramitación, procedimientos de autenticación y validación quedan especificados en las siguientes secciones.

3.3 Renovación de la clave

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

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

3.4 Solicitud de Revocación

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

4 Requisitos Operacionales

4.1 Solicitud del Certificado

La solicitud del certificado debe ser realizada por una persona física, mayor de edad, que actúa en nombre y representación propios o como representante legal de un tercero.

El suscriptor deberá cumplimentar el Formulario de Solicitud del certificado, que podrá ser autenticado mediante:

- Firma manuscrita
- Firma electrónica reconocida

En el formulario constará que el suscriptor asume la responsabilidad de la veracidad de la información reseñada. Podrá 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.

4.2 Procedimiento de tramitación

4.2.1 Autenticación de identidad

4.2.1.1 Suscriptor

Excepto en el caso de certificados de Servidor Seguro SSL DV, el suscriptor del certificado deberá acreditar su identidad y vigencia de la entidad sujeto:

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 y 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 parte del Espacio Económico Europeo:

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

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

II. A ciudadanos extracomunitarios:

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

En caso de actuar en nombre y representación de un tercero deberá aportar:

- Poder suficiente de representación.

  Se considerará que tienen poder suficiente, además de los administradores y representantes legales, los representantes voluntarios cuando acrediten poder suficiente para la realización de actos de administración o celebración de contratos en nombre de la entidad.

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 representante legal del suscriptor (o del propio suscriptor en caso de tratarse de persona física) y la del responsable del certificado han sido legitimadas en presencia notarial, adjuntado copias compulsadas de los documentos de identidad, autorización y representación legal. En el caso de entidades de derecho público, la figura notarial podrá ser sustituida por la presencia de un funcionario con atribuciones de fedatario público, según normativa legal al efecto.

2. Tramitación vía telemática.

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

4.2.1.2 Sujeto

4.2.1.2.1 Personas jurídicas

Excepto en el caso de certificados de Servidor Seguro SSL DV, se requiere:

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

Según forma jurídica:

- Las sociedades mercantiles y demás personas jurídicas cuya inscripción sea obligatoria en el Registro Mercantil acreditarán la válida constitución mediante la aportación de:

    - Para solicitudes de certificados SSL OV, nota simple del Registro Mercantil relativa a los datos de constitución y cargos vigentes de administración de la entidad.

    - Para solicitudes de certificados SSL EV, original o copia auténtica del Registro Mercantil relativo a los datos de constitución y cargos vigentes de administración de la entidad.

- Las asociaciones, fundaciones y cooperativas acreditarán la válida constitución mediante la aportación de original o copia auténtica de un certificado del registro público donde consten inscritas, relativo a su constitución.

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

- Las Administraciones Públicas y entidades pertenecientes al sector público:

    - Entidades cuya inscripción sea obligatoria en un Registro acreditarán la válida constitución mediante la aportación de original o copia auténtica de un certificado relativo a los datos de constitución y personalidad jurídica de las mismas.

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

4.2.1.2.2 Personas físicas

En el caso de personas físicas se seguirá el mismo procedimiento que el reseñado en el apartado anterior.

En conformidad con las normas de CAB FORUM no se expedirán certificados EV con Validación Extendida a personas físicas.

4.2.1.3 Responsable del certificado

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

El Responsable del certificado deberá personarse ante la Autoridad de Registro, 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, ej., facturas recientes de servicios públicos y extractos de cuenta bancaria. Si el ARR o el RDE conoce 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, podrá solicitar otro documento oficial que incorpore fotografía, p.ej., licencia de conducir.

d) En caso de ciudadanos extranjeros, se requerirá:

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

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

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

II. A ciudadanos extracomunitarios:

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

***1 Declaración de Identidad**

Consiste en una declaración formal jurada, en la que el declarante manifiesta que conoce de forma personal y directa a una determinada persona física o a una persona jurídica. Además, hace constar, hasta donde alcance su conocimiento directo, que ha verificado los datos de filiación reseñados en el Formulario de Solicitud: dirección, teléfono y correo electrónico, y que son ciertos.

La Declaración de Identidad incorpora la identidad del declarante, su cédula de identidad, la información que ha sido validada, la fecha y hora de la verificación, la firma del declarante y los apercibimientos legales correspondientes en caso de incurrir en perjurio.

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

4.2.2 Aprobación o rechazo de las solicitudes de certificados

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

En especial, comprobará la existencia del suscriptor, del suscriptor, la existencia del dominio y la pertenencia de este al suscriptor. En función del tipo de certificado:

Tipo certificado	Procedimiento
DV OV EV Sede Electrónica	➢ El titular (registrant) deberá coincidir con la organización sujeto. En caso contrario, el suscriptor deberá acreditar el derecho de uso por parte del sujeto. Comprobación de que el suscriptor tiene el derecho de uso del dominio o subdominio: • Dominios .es: www.nic.es • Dominios .eu: www.eurid.eu • Dominio .eus: whois.nic.eus • Resto dominios: whois.icann.org ➢ Comprobación del CAA en caso de que estén registrados y en cualquier caso siguiendo las directrices de la RFC 6844. En el caso de certificados SSL DV y SSL OV se permitirán los wildcard en subdominios o nombres de host, pero no en dominios de nivel superior (TLD) o en el nombre de dominio. La entidad suscriptora deberá poder demostrar su legítimo control del dominio completo, en caso contrario se rechazará la solicitud. Por ejemplo, no se pueden emitir *.co.uk, *.local o ejemplo.*, pero si *.ejemplo.com a la empresa Ejemplo S.A.
DV OV EV Sede Electrónica	➢ Verificación de la identidad y vigencia de la entidad sujeto ➢ Comprobación de la competencia del suscriptor para usar el nombre de la entidad ➢ Comprobación por email de que el suscriptor tiene conocimiento de la tramitación del certificado. ➢ Verificación de la dirección postal en: • Agencias de Protección de Datos. • Páginas de operadores telefónicos. • Registro Mercantil En el caso de discrepancia entre la documentación aportada y la comprobada, el RDE verificará que la dirección que consta en la Solicitud corresponde a una ubicación en la que la Organización sujeto opera de manera estable. ➢ Verificación del país en: • AGPD • Páginas amarillas • Registro Mercantil ➢ Comprobación de lista de denegados en bases de datos interna de ANF AC ➢ Comprobación de peticiones de alto riesgo en McAfee TrustedSource
Sede Electrónica EV	➢ Comprobación de pertenencia del número de teléfono fijo (no móvil) a la entidad sujeto en: • Páginas de operadores telefónicos, Agencias de Protección de Datos. • Mediante llamada directa ➢ Comprobación de la existencia operativa. Las entidades privadas deberán acreditar que realizan movimientos bancarios con una institución financiera regulada. ANF AC realiza una comprobación dual, interviniendo el Área Técnica y la Asesoría Jurídica. Además, en los mismos casos todas las validaciones son revisadas por el Responsable del Área Técnica

Además, determinará:

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

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

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

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

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

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

El procedimiento de validación que seguirá, según el tipo de certificado, es el siguiente:

4.2.2.1 Certificados SSL

El RDE comprobará la documentación aportada por el suscriptor y la Autoridad de Registro. Verificará, en conformidad con las normas de CAB Forum, que el sujeto no es una persona física.

Además, debido a que, en determinados países, como puede ser Estados Unidos, las personas jurídicas registran la denominación social en el estado donde son constituidas, pero no en el resto de estados, esto puede conllevar a que se emitan dos certificados SSL a sociedades legítimamente constituidas en diferentes estados. Es por ello que, para la emisión de certificados a personas jurídicas constituidas en estos países, se incluirán además de la denominación social de la organización, el estado en el que fue

constituida. En aquellos casos de nombres de organizaciones de especial relevancia y conocimiento público, ANF AC solo emitirá certificados con la denominación social de la persona jurídica, a la matriz de especial reconocimiento público. Asimismo, un suscriptor puede requerir que el nombre de su empresa quede bloqueado para los 50 estados de EE.UU. o, incluso para todo el ámbito internacional, en cuyo caso se aplicarán tasas especiales.

4.2.2.2 Certificados Sede

Comprobará la norma de creación de la Sede y el titular de la misma.

4.2.2.3 Certificados SSL EV y Sede EV

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

En el proceso de validación intervendrá, dando soporte, el Departamento Jurídico y el Departamento Técnico que revisará y validará técnicamente el certificado de petición PKCS#10 / CRS.

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.

- Con respecto a dominios y direcciones de Internet, ANF AC consultará únicamente en registradores asignados por ICANN/IANA los nombres de dominio y direcciones asociadas al certificado. En esta consulta se verificará:

    - Que el titular (*registrant*) coincide con el sujeto.
    - Personas y datos de contacto asociadas a ese registro de dominio.

- Se contactará con una de las personas de contacto que figure en el protocolo *Whois* para verificar conformidad de la solicitud de emisión de certificado asociada a ese dominio.

- Comprobación de los datos de contacto del suscriptor, sujeto y responsable del certificado:
    - Teléfono:

        - Suscriptor: deberá ser un teléfono fijo (no móvil). Se comprobará mediante consulta a las páginas amarillas, AEPD (Agencia Española de Protección de Datos) y llamada personal.

        - Sujeto y responsable del certificado: mediante llamada personal.

    - Dirección Postal, que se comprobará mediante alguno de los siguientes medios: Páginas Amarillas, AEPD, Informa.

- E-mail: se comprobará mediante envío de un correo electrónico solicitando confirmación de recepción.

- Se comprobará que el suscriptor no está incluido en la lista de personas no autorizadas (documento OID 1.3.6.1.4.1.18332.56.3.1) o que no está operando desde un lugar donde la política de la CA impida la emisión de certificados (documento OID 1.3.6.1.4.1.18332.56.2.1).

- Se verificará que el dominio no consta entre aquellos listados como de riesgo, en Anti Phishing Workgroup http://www.antiphishing.org/ o similares.

- Se verificará que ninguna de las personas físicas asociadas a la solicitud consta como delincuente en los registros públicos.

ANF AC actualiza periódicamente su base de datos con todas las personas que aparecen en búsqueda y captura, y vincula esta lista negra al control de peticiones de certificados.

Asimismo, para dominios asociados a nombres que pueden crear en terceros que confían por:

- Confusión de identidad o actividad.

  No se autorizará emisión de certificado cuando el nombre del dominio pueda crear confusión respecto a la verdadera actividad del suscriptor (p. ej.www.bancoprogreso.com, cuando la actividad del suscriptor no se corresponde al de una entidad financiera).

- Marcas especialmente relevantes.

  En caso de dominio asociado a marca especialmente relevante, se comprobará el Registro de Patentes y Marcas. Cuando el nombre del dominio este asociado a una marca de especial relevancia y conocimiento público se verificará si el propietario de la marca corresponde al suscriptor. En caso negativo, el RDE solicitará aclaración al suscriptor si tiene algún tipo de autorización acreditativa.

  No se autorizará emisión de certificado cuando el nombre esté asociado a una marca relevante de la que no es propietario el suscriptor del dominio, ni tiene autorización del propietario de la marca, dado que puede causar confusión a terceros que confían (p.ej., www.chanel.zn, www.cocacola.eu, etc.).

En los casos en los que no se pueda realizar la validación en las fuentes definidas anteriormente, se justificará en el acta de comprobación emitida por el RDE y se indicará el origen alternativo utilizado.

4.2.3 Tiempo para procesar la emisión de certificados

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

4.3 Emisión del Certificado

Según lo definido en la DPC de ANF AC.

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

Según lo definido en la DPC de ANF AC.

ANF AC entregará el certificado, por correo electrónico firmado, al Responsable Técnico que conste en el Formulario de Solicitud de Emisión.

4.3.2 Notificación al suscriptor

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

4.4 Aceptación del certificado

4.4.1 Aceptación

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

Mediante la firma del Acta de Recepción y Aceptación, el suscriptor confirma la recepción del certificado; su aceptación a la emisión realizada; la correcta funcionalidad del producto; su capacidad de utilizarlo al firmar la propia acta con este certificado; ratifica su sometimiento a la DPC y a las Políticas de ANF AC y a utilizarlo de acuerdo con las limitaciones de uso y dentro de la finalidad para el que ha sido emitido; su responsabilidad en mantener la confidencialidad de la clave privada; y el compromiso de cesar en su uso después de la pérdida de vigencia, bien por caducidad o bien por revocación.

4.4.2 Devolución del certificado

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 e-mail firmado electrónicamente a ANF AC, informando del motivo de la devolución. ANF AC verificará las causas de devolución, revocará el certificado emitido y procederá a emitir un nuevo certificado en un plazo máximo de 72 horas.

4.4.3 Seguimiento

ANF AC no es responsable de la monitorización, investigación o confirmación de la exactitud de la información contenida en el certificado con posterioridad a su emisión. En el caso de recibir información sobre la inexactitud o la no aplicabilidad actual de la información contenida en el certificado, este puede ser revocado.

4.4.4 Publicación del certificado

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

4.4.5 Notificación de la emisión del certificado a terceros

No se efectúa notificación a terceros.

4.5 Denegación

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

4.6 Renovación de certificados

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

4.6.1 Certificados vigentes

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

Sólo los certificados en estado de vigencia pueden ser renovados siempre que la identificación realizada no haya superado el periodo de cinco años.

4.6.2 Personas autorizadas para solicitar la renovación

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

4.6.3 Identificación y autenticación de las solicitudes de renovación rutinarias

El proceso para remisión/renovación es el mismo que para nueva emisión. La documentación que debe aportar el suscriptor y los pasos de validación, emisión y entrega de certificados son los mismos que para la emisión de un certificado nuevo.

Se contemplan dos modalidades de renovación:

4.6.3.1 Renovación de certificados con cambio de clave

Según lo definido en la DPC de ANF AC.

4.6.3.2 Renovación de certificados sin cambio de clave

Según lo definido en la DPC de ANF AC.

4.6.4 Aprobación o rechazo de las solicitudes de renovación

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

4.6.5 Notificación de la renovación del certificado

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

4.6.6 Aceptación de la renovación del certificado

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

4.6.7 Publicación del certificado renovado

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

4.6.8 Notificación de la renovación del certificado

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

4.6.9 Identificación y autenticación de las solicitudes de renovación de clave después de una revocación (clave no comprometida)

No se autoriza la renovación de certificados caducados ni revocados.

4.7 Modificación del certificado

No es aplicable.

4.8 Revocación y suspensión de certificados

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

4.8.1 Causas de revocación

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

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

  Las instrucciones están publicadas y permanentemente actualizadas en:
  https://www.anf.es/es/show/section/instrucciones_generales

  Puede interponer directamente su sospecha o denuncia en:
  https://www.anf.es/es/show/section/comunicar_sospecha-denuncia

  Cualquier persona que precise instrucciones técnicas o soporte jurídico en esta materia, puede realizar gratuitamente sus consultas mediante alguno de los siguientes procedimientos:

  - Mediante llamada telefónica en horario de oficina:
    902 902 172 (llamadas desde España) (lunes a viernes de 9 h. a 18 h.)
    +34 933 935 946 (Internacional)

  - Procedimiento online. El interesado puede acceder a la consulta en línea en:
    https://www.anf.es/

  - Enviando un correo electrónico a: soporte@anf.es

- ANF AC investigará las incidencias de las que tenga conocimiento dentro de las veinticuatro horas siguientes a su recepción. El Responsable de Seguridad, en base a las indagaciones y

comprobaciones realizadas, emitirá informe al Responsable de Dictámenes de Emisión, el cual determinará, en su caso, la correspondiente revocación mediante Acta fundamentada, en la cual constará:

- Naturaleza de la incidencia.
- Informaciones recibidas.
- Normas legales y regulación sobre la que se fundamente la orden de revocación.

Cualquier persona interesada puede abrir una incidencia mediante alguno de los siguientes procedimientos:

- Mediante llamada telefónica en horario de oficina:
  902 902 172 (llamadas desde España) (lunes a viernes de 9 h. a 18 h.)
  +34 933 935 946 (Internacional)

- Procedimiento online. El interesado debe abrir una incidencia en el servicio web:
  https://www.anf.es/es/show/section/abrir_una_incidencia

4.8.2 Identificación y autenticación de solicitudes de revocación

Podrán solicitar la revocación de un certificado:

- El suscriptor del certificado.
- El responsable del certificado.
- La Autoridad de Registro Reconocida.

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) o (+34) 933 935 946 (Internacional)

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

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

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

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

4.8.3 Procedimiento para la solicitud de revocación

El 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. En caso de realizarse la revocación mediante un correo electrónico, deberá ser enviado a la dirección info@anf.es.
La solicitud de revocación deberá contener, como mínimo, la siguiente información:

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

La solicitud de revocación será procesada a su recepción.

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

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

4.8.4 Periodo de gracia de la solicitud de revocación

Según lo definido en la DPC de ANF AC.

4.8.5 Plazo máximo de procesamiento de la solicitud de revocación

Según lo definido en la DPC de ANF AC.

4.8.6 Requisitos de comprobación de listas CRL

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

4.8.7 Frecuencia de emisión de CRL

Según lo definido en la DPC de ANF AC.

4.8.8 Disponibilidad de comprobación on-line de la revocación

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

4.8.9 Requisitos de la comprobación on-line de la revocación

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

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

Este servicio cumple los requerimientos establecidos en materia de Protección de Datos de Carácter Personal y únicamente suministra copia de estos certificados a terceros debidamente autorizados.
El acceso a este sistema de consulta de certificados es libre y gratuito.

4.8.10 Suspensión del certificado

No es aplicable.

4.8.11 Identificación y autenticación de solicitudes de suspensión

No está permitida la suspensión del certificado.

4.9 Depósito y recuperación de claves

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

4.10 Buenas prácticas

a) Claves privadas generadas en archivos PKCS#12

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

b) Dominios validados

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

c) Larga vida de certificados validados

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

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

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

d) Dominios comodines

Algunas entidades emisoras de certificados de dominio validados emiten certificados que pueden

funcionar como certificados de comodines, por ejemplo, un certificado para *. example.com donde el CA verifica sólo la propiedad y el control del dominio example.com.

Esto posibilita que un suscriptor pueda establecer un sitio web malicioso con protección SSL, cuyo objetivo es imitar sitios legítimos como, por ejemplo, paypal.example.com, y todo ello sin el conocimiento de la CA. ANF AC tiene como buena práctica NO emitir certificados que puedan ser utilizados como dominios comodines.

e) Prefijos de Dirección de correo electrónico de Certificados de Dominio Validado

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

- admin @ dominio
- administrador @ dominio
- webmaster @ dominio
- hostmaster @ dominio
- postmaster @ dominio

Así como cualquier dirección que aparece en el campo de contacto técnico o administrativo de registro del dominio *whois*, independientemente de los dominios de las direcciones.

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

f) Delegación de validación de correos a terceros

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

g) Expedición directamente de la entidad final desde la raíz

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

h) Permitir a entidades externas operar con CA subordinadas

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

i) Certificados a nombre de HOST o direcciones IP privadas

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

j) Tamaños mínimos de clave

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

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

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

b) Registro de Incidentes:

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

El Coordinador de Seguridad determina la gravedad del incidente y nombra un responsable y, en caso de incidentes de seguridad relevantes, informa a la Junta Rectora de la PKI. En casos de fraude o *phishing*, reporta la información en el sitio web del Anti-PhishingWorkingGroup,

http://www.antiphishing.org/report-phishing/

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 y Listas de Certificados Revocados

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

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

- ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI) Certificate Profiles, Part 5: QCStatements
- RFC 3739 Internet X.509 Public Key Infrastructure: Qualified Certificates Profile.

El periodo de validez del certificado está reseñado en Tiempo Coordinado Universal, y codificado conforme a la especificación RFC 5280.

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

Dentro de los certificados, además de los campos comunes ya estandarizados, se incluyen un conjunto de campos "propietarios" que aportan información relativa al suscriptor, u otra información de interés.

Campos propietarios

Se han asignado identificadores unívocos a nivel internacional. Concretamente:

- Los campos referenciados con el identificador de objeto (OID) 1.3.6.1.4.1.18332.x.x, son extensiones propietarias de ANF AC. La relación completa de códigos OID y la información asociada a los mismos puede ser consultada en la Sección "Campos Propietarios ANF AC" de la Declaración de Prácticas de Certificación de ANF AC.

- Los campos con el ISO/IANA del MPR 2.16.724.1.3.5.x.x, son extensiones propietarias requeridas e identificadas en el Esquema de Identificación y Firma Electrónica v.1.7.6 publicado por el Consejo Superior de Administración Electrónica.

- Los campos con el OID 1.3.6.1.4.1.18838.1.1, son extensiones propietarias de la Agencia Estatal de Administración Tributaria (AEAT).

QCStatements

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

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

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

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

- **QcEuRetentionPeriod,** determina el periodo de conservación de toda la información relevante para el uso de un certificado, tras la caducidad de este. En el caso de ANF AC, es de 15 años.

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

- **QcType**, cuando el certificado se emite con el perfil (FIRMA), se reseña QcType 2

- **QcPDS**, se proporciona la URL en inglés que permite acceder a todas las políticas de la PKI de ANF AC *(PDS Policy Disclosure Statements)*

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 documento 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.