Política de Validación

	Esta especificación ha sido preparada por ANF AC para liberar a terceras partes.	**NIVEL DE SEGURIDAD** DOCUMENTO PÚBLICO

Gran Via de les Corts Catalanes 996. Barcelona - España - CP 08018 - Tel 902 902 172 / Fax 933 031 611

ÍNDICE

1. Introducción

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

Este documento tiene como objetivo describir el funcionamiento de los Servicios de Validación de certificados electrónicos de ANF AC y establecer las condiciones de uso, obligaciones y responsabilidades de las distintas entidades involucradas.

Esta Política de Validación de Certificados está subordinada a lo establecido en la Declaración de Prácticas de Certificación de ANF Autoridad de Certificación.

Una Autoridad de Validación es un Prestador de Servicios de Certificación que proporciona certeza sobre la validez de los certificados digitales y sobre los documentos firmados electrónicamente en un momento dado.

ANF AC es una Autoridad de Validación (VA o Validation Authority) que actúa como tercera parte de confianza validando certificados electrónicos.

1.1. Presentación

El Servicio de Validación de Certificados es uno de los elementos esenciales que, junto con el servicio de “Sellado de Tiempo Electrónico”, permiten dotar de larga vigencia a las firmas electrónicas. Mediante Respondedores OCSP, se garantiza la vigencia del certificado electrónico en el momento exacto en que la firma de un documento se produjo, la validación se extiende a toda la ruta de certificación.

De esta manera la Validación de Certificados se convierte en un servicio de alto valor añadido, fundamental en transacciones electrónicas que requieran contar con una evidencia legal a largo plazo.

1.2. Identificación

1.2.1. Nombre del Documento

Este documento se denomina Política de Validación de ANF AC.

1.2.4. Especificaciones

Nombre del documento	Política de Validación
Versión	2.0
Estado de la DPC	APROBADO
Referencia del documento / OID	1.3.6.1.4.1.18332.56.1.1
Fecha de emisión	1 de junio de 2016
Fecha de expiración	No es aplicable
Localización última versión en vigor	https://www.anf.es/AC/documentos/

1.3. Comunidad y Aplicabilidad

1.3.1. Entidades y personas que intervienen

- **Autoridad de Validación**.
- **Suscriptores**.

- **Terceros que confían**.

1.3.1.a Autoridad de Validación

Una Autoridad de Validación es un Prestador Cualificado de Servicios Electrónicos de Confianza que en conformidad con el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, y la Ley 59/2003, de firma electrónica, proporciona certeza sobre la validez de los certificados electrónicos.

ANF AC como Autoridad de Validación, ofrece diversos sistemas informáticos para determinar el estado de vigencia de los certificados electrónicos, todos ellos descritos en el apartado correspondiente de este documento.

1.3.1.b Suscriptores

Son las personas físicas o jurídicas titulares de los certificados electrónicos que, previamente a aceptarlo, verifican los datos contenidos en él, y utilizan para su recepción los dispositivos homologados por ANF AC.

1.3.1.c Terceros que confían

Son las personas físicas o jurídicas receptoras del certificado electrónico que, previamente a confiar en él, validan su estado de vigencia y verifican su autenticidad e integridad

1.4. Uso de los servicios de validación

1.4.1. Usos permitidos

Los servicios de validación de ANF AC solo pueden utilizarse para atender necesidades de validación en calidad de suscriptor o terceros que confían.

1.4.2. Usos prohibidos

Queda expresamente prohibido utilizar los servicios de validación de ANF AC para prestar servicios de validación a terceros. Esta prohibición se extiende especialmente a procesos en los que una plataforma multivalidación de una tercera entidad ajena al transaccional, es decir que no cumple los requisitos de ser considerado suscriptor o tercero que confía, opera como mero intermediario en la formulación de la consulta.

Se establece como penalización por el uso no autorizado de estos servicios, el costo de 1 euro por consulta realizada a cualquiera de los servicios de validación de ANF AC, ya sea a los servidores OCSP Responder, o por cualquier otro servicio de validación, presente o futuro, que ANF AC ponga en explotación. Se fija 10.000 euros el mínimo de penalización.

La utilización de los servicios de validación, presupone un conocimiento explicito de este documento, y por lo tanto, una aceptación de la penalización que será aplicable.

1.5. Definiciones y Acrónimos

1.5.1. Definiciones

Las definiciones pueden ser consultadas en la DPC localizada en:

https://www.anf.es/AC/documentos/

1.5.2. Acrónimos

Los acrónimos pueden ser consultados en la DPC localizada en:

https://www.anf.es/AC/documentos/

2. Descripción de los servicios de Validación.

Los Servicios de Validación de ANF AC permiten conocer el estado de vigencia de los certificados electrónicos, además se dispone de la aplicación informática que permite determinar la integridad y autenticidad de los certificados electrónicos emitidos por ANF AC.

ANF AC ofrece diferentes servicios de validación:

- **Servicio OCSP**.

  Se trata de una infraestructura distribuida de Respondedores OCSP que realizan consultas en tiempo real y directamente sobre los repositorios de la entidad emisora. Las respuestas OCSP están firmadas electrónicamente y respectan la norma IETF RFC 6960, X.509, Internet Public Key Infrastructure Online Certificate Status Protocol –OCSP.

  Los campos opcionales según la especificación RFC6960:

Campo	Definición
CertID.hashAlgorithm	Identificador del algoritmo hash
CertID. issuerNameHash	Hash del DN del emisor (OCTET STRING)
CertID.serialNumber	Número de serie del certificado que se desea validar
CertID. issuerKeyHash	Hash de la clave pública del emisor (OCTET STRING)
nonce	Opcional
certReq	Todas las respuestas contienen la cadena de certificación de ANF AC hasta la raíz. Su presencia y valor es ignorada.

Se detalla a continuación un ejemplo de consulta con OpenSSL:

OpenSSL ocsp -CAfile <certificado_ca>
-issuer <certificado_ia> -cert <certificado_a_consultar>
-url <url_de_verificación>

El campo <url_de_verificación > deberá ser el indicado en el campo "Authority Information Access" del certificado.

Ejemplo para realizar consultas tipo GET con open SSL:

Se genera el request:
openssl ocsp
-noverify
-no_nonce
-respout ocsp.resp
-reqout ocsp.req
-issuer AssuredID64.cer
-cert rev64.cer
-url"http://ocsp.anf.es/spain/AV"
-header "HOST" "ocsp.anf.es"
-text
Se convierte a B64
openssl enc
-in ocsp.req
-out ocsp.req.b64 -a

Aclaración: Se ha detectado que OpenSSL puede emitir las siguientes respuestas de error:

1/ Si la CA raíz ha firmado directamente el certificado de entidad final, OpenSSL devuelve:

Response Verify Failure
Verify error: self signed certificate in certificate chain

2/ Si la respuesta del OCSP responder es de un tipo CRL, OpenSSL devuelve:

Response Verify
Failure signer certificate not found

3/ Los servidores OCSP Responder de ANF AC soportan consultas GET y POST.

En la web corporativa de ANF AC se ofrece información técnica para realizar consultas OCSP, y certificados empleados por los respondedores OCSP.

www.anf.es

El proceso de validación comprende el certificado sometido a consulta y toda la cadena de la Jerarquia de Certificación hasta primer nivel (excluido CA Raíz).
Son públicas y accesibles en las URLs especificadas en el campo "CRLDistributionPoints" en el servidor OCSP de ANF AC.

- **Servicio LDAP**

El Protocolo de Acceso Ligero a Directorios LDAP (por sus siglas en inglés, Lightweight Directory Access Protocol), ofrece un método estandarizado para el almacenamiento de certificados y listas CRL de certificados revocados.

La versión actual, LDAP v.3., se detalla en el documento RFC 4510 de la Internet Engineering Task Force (IETF).

Son públicas y accesibles en las URLs especificadas en el campo "CRLDistributionPoints" en el servidor LDAP de ANF AC.

- **Servicio CRL - ARL**

Las Listas de Revocación de Certificados (CRL), recogen los números de serie de aquellos certificados electrónicos de entidad final que han sido revocados antes de que expire su plazo de vigencia. Para cada certificado se especifica fecha, hora y causa de revocación.

Las Listas de Revocación de Autoridades de Certificación (ARL) recogen los números de serie de aquellos certificados de Autoridades de Certificación Intermedias que han sido revocados antes de que expire su plazo de vigencia. Para cada certificado se especifica fecha, hora y causa de revocación.

Son públicas y accesibles en las URLs especificadas en el campo "CRLDistributionPoints" del servidor Web de ANF AC.

Los certificados de Autoridades de Certificación Raíz que hayan sido revocados antes de que expire su plazo de vigencia, son publicados en la página corporativa de ANF AC:

www.anf.es

Durante la prestación de servicios de certificación de ANF AC, a fecha de publicación de esta Política de Validación, **ningún certificado de CA Raíz ha sido revocado**.

- **Dispositivo de Verificación de Certificados**

Se trata de una aplicación desarrollada por ANF AC, gratuita y de libre distribución, Está disponible en modalidad de usuario final, y en modalidad API para desarrolladores. Este dispositivo permite:

  - Comprobar la vigencia del certificado.
  - Verificar la integridad y autenticidad del certificado.

- **Servicio de Búsqueda de Certificados**

Disponible en la Web de ANF AC

www.anf.es

es posible hacer búsquedas que permiten determinar el estado de vigencia de los certificados emitidos, e incluso obtener una copia del mismo.

3. Procedimiento de Validación.

Para validar un certificado electrónico emitido por ANF AC es necesario seguir los procedimientos descritos en el estándar ***RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".***

Siguiendo el estándar RFC 5280 podremos validar técnicamente cualquier certificado electrónico, aunque para ello necesitaremos:

- Disponer del certificado raíz de la CA emisora. Publicados en la web corporativa de ANF AC

  www.anf.es

- Tener una copia del certificado electrónico de interés, el número de serie, o nombre del suscriptor.

3.1. Autenticidad y vigencia del certificado raíz

La autenticidad y la vigencia del certificado raíz, es una cuestión critica en la validación de los certificados. ANF AC garantiza la autenticidad y vigencia de los certificados raíz obtenidos mediante alguno de los siguientes métodos:

- Descargados de la Web de ANF AC mediante protocolo SSL:

  https://www.anf.es

- Integrados en dispositivos criptográficos de ANF AC cuya procedencia es de confianza. Son fuentes de confianza:

  - La Web de ANF AC mediante protocolo SSL:

    https://www.anf.es

  - Los dispositivos homologados por ANF AC,publicados en:

    https://www.anf.es

Todos los dispositivos criptográficos de ANF AC mantienen un control de versionado, y actualización en línea.

4. Servicios de Validación

4.1. Listas de Certificados Revocados (CRL) (ARL)

La generación de Listas de Certificados Revocados está definida en el documento "Declaración de Prácticas de Certificación de ANF AC".

Cada CA de la Jerarquía de Certificación de ANF AC emite su propia CRL:

- Las CAs Raíz emiten una Lista de CA's intermedias revocadas (ARL), como mínimo dentro del plazo establecido en la propia ARL, o extraordinariamente, cuando se produzca la revocación de un certificado de autoridad.
- Los certificados electrónicos de entidad final que han sido revocados previa a su fecha de caducidad, son incluidos en la Lista de Certificados Revocados (CRL), como mínimo dentro del periodo establecido en la propia CRL, o cada vez que se revoque un certificado.

En el caso extraordinario de revocación de un certificado de CA Raíz, la revocación queda publicada en la web corporativa de ANF AC

www.anf.es

Se recuerda que ANF AC no contempla a suspensión temporal de certificados.

4.2. Webservice de AEAT

La Agencia Estatal de Administración Tributaria (A.E.A.T.) exige a los Prestadores de Servicios de Certificados que pongan a su disposición un servicio de validación de certificados que cumpla con las especificaciones definidas por la propia AEAT en https://aeat.es/ycaestec.html

Este servicio SOAP es de uso exclusivo de AEAT.

4.3. Servicio de consulta de estado de certificados Web

La consulta se realiza mediante localización selectiva de certificados mediante formulario publicado en la Web www.anf.es

Como resultado se obtiene el estado de vigencia actual (válido, o revocado), del certificado que coincide con el criterio de búsqueda. En caso de que su estado sea revocado, se especifica la fecha de perdida de vigencia. Se recuerda que ANF AC no contempla a suspensión temporal de certificados.

4.4. Consulta OCSP

Las respuestas sobre la validación de un certificado están firmadas por ANF AC, lo que permite obtener una evidencia electrónica sobre la respuesta generada. Según norma RFC 6960 Online Certificate Status Protocol – OCSP".

4.4.1. Petición de Validación

El formato básico de envío de las solicitudes sigue el siguiente esquema:

Content type ***: application/ocsp-request***

Method ***: POST***

Content-length ***: required***

Contiene la respuesta OCSP en ASN.1 (RFC2459), codificada en DER (X.690)

Los campos opcionales según la especificación RFC6960:

Campo	Definición
CertID.hashAlgorithm	El algoritmo de hash empleado.
CertID. issuerNameHash	Hash del DN del emisor (OCTET STRING)
CertID.serialNumber	Número de serie del certificado que se desea validar
CertID. issuerKeyHash	Hash de la clave pública del emisor (OCTET STRING)
nonce	Opcional
certReq	Todas las respuestas contienen la cadena de certificación de ANF AC, salvo la CA raíz, cuya presencia y valor es ignorada (debe de ser verificada por consulta en web corporativa.

4.4.2. Respuesta a la petición de validación

4.4.2.1. Respuestas definitivas

Todos los mensajes de respuesta definitiva son firmados electrónicamente. El certificado utilizado para firmar la respuesta, es un certificado especialmente emitido para el OCSP responder que firma la validación, y ha sido emitido por ANF AC.

Los indicadores definidos para la respuesta definitiva son:

- Bueno.
- Revocado*[1]
- Desconocido

*[1] De acuerdo con la RFC 6960 Pto. 2.2 la definición de revocado incluye certificados revocados y certificados no emitidos.

4.4.2.2. Casos de excepción

En caso de errores, la respuesta de OCSP puede devolver un mensaje de error. Estos mensajes no están firmados. Los errores pueden ser de los siguientes tipos:

Causa	Definición
MalformedRequest (1)	Error causado porque la solicitud recibida no se ajusta a la sintaxis de OCSP
InternalError (2)	Indica que el OCSP responder ha llegado a un estado interno de inconsistencia
TryLater (3)	El OCSP responder temporalmente es incapaz de responder
SigRequired (5)	El OCSP responder requiere que el cliente firme la solicitud.
Unauthorized (6)	Se devuelve en caso de que el cliente es no está autorizado a hacer esta consulta a este servidor

(4) conforme a la RFC 6960 no se utiliza

Los campos opcionales según la especificación RFC6960:

Campo	Definición
certReq	Todas las respuestas contienen la cadena de certificación de ANF AC hasta la raíz. Su presencia y valor es ignorada.
Nonce *[1]	Opcional. Si la petición lo contiene, está presente y con el mismo valor.

*[1] Nonce: criptográficamente una petición y una respuesta para prevenir los ataques de repetición.

5. Obligaciones y responsabilidades

5.1. Autoridad de Validación

5.1.1. Obligaciones

ANF Autoridad de Certificación como Autoridad de Validación (VA) se obliga a:

- Mantener y publicar esta Política de Validación de Certificados en coherencia con su Declaración de Prácticas de Certificación y restantes políticas asociadas.
- Respetar lo establecido en la Declaración de Prácticas de Certificación y en esta Política de Validación de Certificados.
- Generar respuestas de validación conforme a esta Política y a los estándares en esta materia.
- Generar respuestas de validación según la información enviada por el cliente y libres de errores de entrada de datos.
- Custodiar las respuestas generadas protegiéndolas ante pérdida, destrucción o falsificación.
- Actualizar de manera inmediata las CRLs de ANF AC cada vez que se revoque o suspenda un certificado
- Mantener un servicio público de acceso a las CRLs con alta disponibilidad 24x7

ANF AC, en su actividad de prestación de servicios de certificación, responderá por el incumplimiento de lo establecido en esta Política de Validación de Certificados y,

allí donde sea aplicable, por lo que dispone la Ley 59/2003, de 19 de diciembre, de firma electrónica o su normativa de desarrollo.

6. Requerimientos operacionales

6.1. Obtención de información fiable

ANF AC tan solo responde a peticiones formuladas sobre certificados que han sido emitidos por alguna de sus jerarquías de certificación.

La Autoridad de Validación tiene acceso directo al propio repositorio de la CA emisora, y es fuente autorizada para decidir sobre la validez de un determinado certificado.

6.2. Certificado para la prestación de los servicios de validación

La generación de los certificados necesarios para la prestación de los servicios como Autoridad de Validación, esta regulada por la Declaración de Prácticas de Certificación y Políticas específicas.