Procedimiento de

Firma electrónica Cualificada a distancia

Paseo de la Castellana, 79 – 28046 - Madrid (España)
Teléfono: 902 902 172 (llamadas desde España)
Internacional (+34) 933 935 946
Fax: (+34) 933 031 611 · Web: www.anf.es

Nivel de Seguridad

Público

CONTROL DEL DOCUMENTO:

Versión	Fecha modificación / creación	Autor / modificado por
1.0	2017/03/15	*F. Díaz*

Versión	Propuesto por	Aprobado por	Fecha modificación	Fecha Aprobación	Autor

---

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 de conformidad con el marco legal del Reglamento [UE] 910/2014 del Parlamento Europeo [eIDAS], y con la Ley 59/2003 de Firma Electrónica de España. La PKI de ANF AC es conforme 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*).

El Reglamento eIDAS permite la firma electrónica cualificada a distancia (servidor de firma). El servicio de firma electrónica cualificada a distancia ha sido diseñado respetando las normas ETSI / CEN publicadas para tales firmas: prEN 419 241-1: General System requirements; prEN 419 241-2: Protection Profile for QSCD for Server Signing; prEN 419 221-5: Cryptographic module.

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-)*.

ANF Autoridad de Certificación ofrece servicios de firma electrónica cualificada a distancia. El presente documento determina los procedimientos de gestión y administrativos específicos que son utilizados para la prestación del servicio, así mismo se detallan los sistemas y productos que garantizan que el entorno de creación de firmas electrónicas es fiable y que el firmante tiene, con un alto nivel de confianza, el control exclusivo del uso de sus datos de creación de firma electrónica.

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, los perfiles de certificados para firma centralizada quedan detallados en las Políticas de Certificación a las que se somete su emisión. 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.

2 Certificados para firma electrónica centralizada

La solicitud, tramitación, emisión y perfil de los certificados para firma electrónica centralizada quedan detallados en las Políticas de Certificación a las que se somete su emisión.

Como norma general cabe determinar que:

- Los certificados para firma electrónica centralizada, exclusivamente se generan en dispositivos seguros de creación de firma certificados 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
  Concretamente ANF AC utiliza en la actualidad dispositivos
  Código = NC 4433E-500
  Modelo = NShield Solo 500 + F3
  Fabricante = Thales e-Security, Inc.
  Dentro de la extensión QcStatement, queda activado *QcSSCD*, el cual 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.
- Los certificados para firma electrónica centralizada, exclusivamente se emiten con la calificación de "cualificado".
  Dentro de la extensión QcStatement, queda activado *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"

2.1 Datos de creación de firma y Datos de activación de firma

Tal y como queda detallado en la DPC, y en la respetiva Política de Certificación a la que se somete la emisión de los certificados para firma electrónica centralizada, el solicitante del certificado sigue el mismo procedimiento que en cualquier otro tipo de certificado:

- Recibe un Acta de Identificación de la Autoridad de Registro, la cual está firmada por el AR y cifrada con doble clave simétrica solo son conocidas por el solicitante.
- Para la generación del par de claves asimétricas, pública y privada, el solicitante utiliza el dispositivo HSM indicado anteriormente.
- Para la generación del certificado de petición, el solicitante utiliza el mismo dispositivo HSM y el acta de identificación recibida de la Autoridad de Registro.

El procedimiento seguido por el solicitante:

1. Conexión mediante comunicación cifrada SSL, a la Web corporativa de ANF AC.
2. El solicitante selecciona el Acta de Identificación y descarga el documento cifrado.
3. El servidor de confianza de ANF AC, dispone de una copia cifrada de esa acta, la cual fue remitida por la Autoridad de Registro. El servidor obtiene el hash del acta cifrada almacenada y obtiene el hash del acta cifrada que ha transmitido el solicitante. Se comparan ambos hash para asegurar que son idénticos.
4. En caso de conformidad de hash, el servidor de confianza de ANF AC, requiere al solicitante que introduzca las dos claves simétricas de descifrado de acta.
5. El servidor de confianza de ANF AC descifra el acta, y realiza una verificación de la firma electrónica del Operador AR que la autentico.
6. En caso de conformidad de firma del AR, el servidor de confianza de ANF AC requiere al solicitante que indique:
    a. Datos de activación de firma que desea utilizar (PIN). El sistema incluye una biblioteca de claves no autorizadas (*inseguras*), requiere utilizar una clave de al menos 8 dígitos alfanuméricos, al menos un carácter tiene que ser mayúsculas.
    b. Si desea activar el proceso de Doble Factor de Autenticación (2FA), en caso de conformidad:
        i. No desea activar 2FA
        ii. Si desea recibir token por SMS *(clave de sesión)*
        iii. Si desea recibir token por eMail *(clave de sesión)*
        iv. Si desea recibir token por Notificaciones Push *(clave de sesión)*

    Clave de sesión=clave distinta para cada solicitud, se genera *aleatoriamente*.

7. Una vez introducidos los valores indicados en el punto 6, el dispositivo HSM (SSCD) instalado en el servidor de confianza de ANF AC, procede a:
    a. generar el par de claves asimétricas (*datos de generación de firma-pública y privada*-), y
    b. elaborar el certificado de petición (CSR), según estándar PKCS#10.
8. El PIN seleccionado por el solicitante no es almacenado por ANF AC, tan solo se emplea en el momento que es requerido por el Dispositivo Seguro de Creación de Firma.
9. Los datos de generación de firma solo son accesibles empleando el Dispositivo Seguro de Creación de Firma que los custodia.
10. El interesado recibe un email y un sms conforme se ha activado el Acta de Identificación y se ha tramitado la solicitud de emisión de un certificado de firma a distancia. En estos comunicados se indica identificador de certificado

Este procedimiento garantiza un alto nivel de confianza por parte del suscriptor del certificado y garantiza un control exclusivo de los datos de creación de firma:

- Se ha empleado una comunicación electrónica segura para la transmisión de: *Acta de Identificación, claves de descifrado y los datos de creación de firma*.
- Solo el interesado conoce los datos de creación de firma, ANF AC no almacena estos datos ni tiene la oportunidad de hacerlo, por lo tanto, solo el firmante puede emplearlos.
- Los datos de generación de firma son generados por el propio dispositivo seguro de creación de firma, por lo tanto, esos datos están custodiados de forma segura.
- Como en cualquier otro tipo de certificado, se remite al suscriptor un comunicado a la cuenta de email y al móvil que calificó como personales y seguros en el momento de la autenticación ante la Autoridad de Registro. En este correo además de informar del identificador de certificado se facilitan datos de contacto del Servicio de Asistencia Legal de ANF AC.

El procedimiento seguido es básicamente el mismo que en cualquier otro tipo de certificado, por lo tanto, el nivel de seguridad logrado es equiparable al de cualquier otros certificados almacenados en dispositivo HSM físico en posesión del firmante.

Otras especificaciones técnicas en documento "Viafirma –fortress"

2.2 Emisión del certificado electrónico y descarga

El procedimiento para certificados de firma a distancia es el mismo que para el resto de certificados, e igualmente se remite información al suscriptor cuando el certificado es emitido.

Según lo definido en la DPC y Políticas de Certificación a la que se somete la emisión del certificado.

3 Servidor de firma a distancia y estándares

El servidor de firma a distancia de ANF AC ha sido desarrollado respetando los estándares ETSI / CEN publicados para tales firmas:

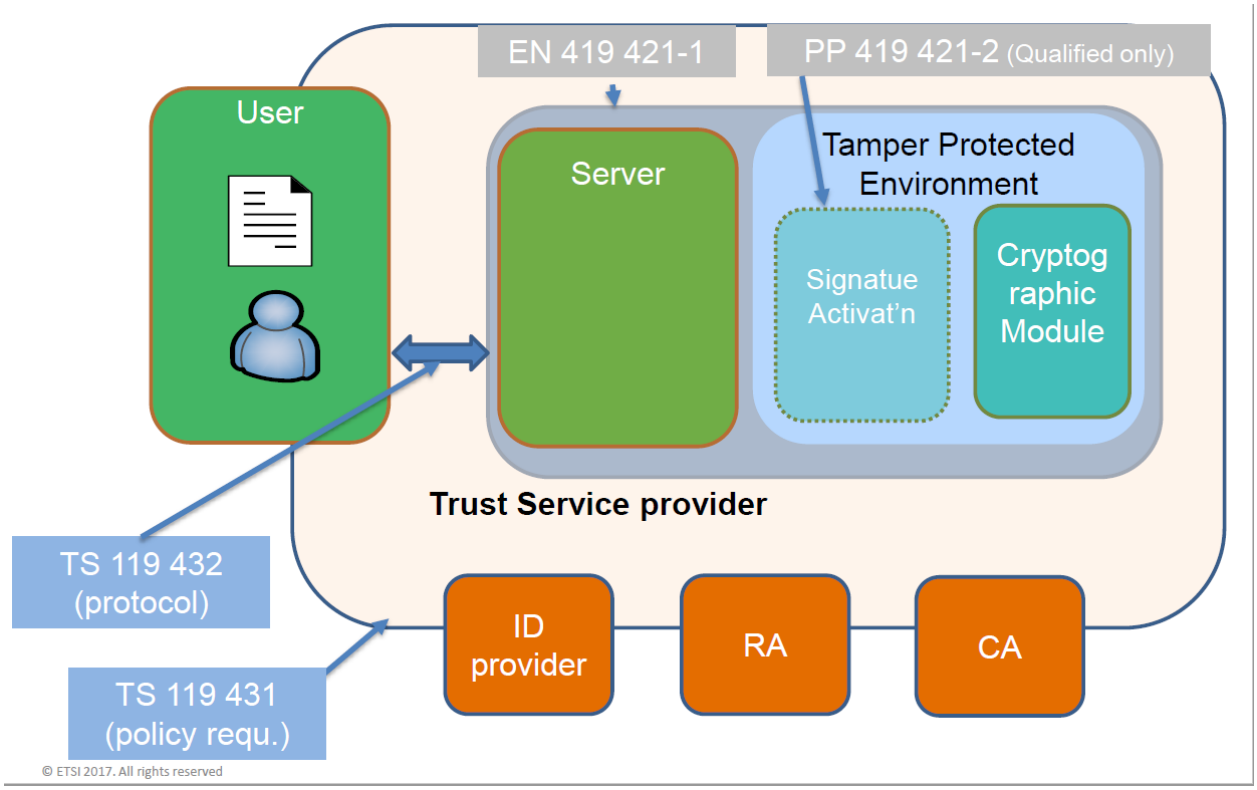
- prEN 419 241-1: General System requirements.
- prEN 419 241-2: Protection Profile for QSCD for Server Signing.
- prEN 419 221-5: Cryptographic module. PP para módulos criptográficos TSP, en particular su

Parte 5 PP para módulos criptográficos para TSP

- TS 119 431-1: Policy and security requirements for TSP service components operating a remote QSCD / SCD
- TS 119 431-2: Policy and security requirements for TSP service components supporting AdES digital signature creation
- TS 119 432: Protocols for remote digital signature creation

Diagrama funcional del servicio de firma a distancia

Alcance de los estándares de firma remota.



4 Procedimiento de firma a distancia

4.1 Selección del archivo a firmar

El firmante accede al servicio Web de ANF AC empleando un canal de comunicación segura SSL.

El firmante dispone de las siguientes opciones:

- Transmitir un documento electrónico a los servidores de confianza.
- Transmitir el hash de un documento electrónico a los servidores de confianza.

4.2 Selección del certificado

El firmante accede al servicio Web de ANF AC empleando un canal de comunicación segura SSL.
Introduce el identificador de certificado (*Pto. 2.1 10)*) para seleccionar el certificado que desea utilizar.

4.3 Control de autenticación 2FA

El servicio de firma a distancia determina la modalidad de uso establecida por el firmante (*Pto. 2.1 6)*):

1. Sin 2FA
2. Envío de clave de sesión por eMail.
3. Envío de clave de sesión por SMS.
4. Envío de clave de sesión por Notificación Push.

Si el firmante tiene activado 2FA, recibirá la clave de sesión por el medio requerido. El firmante deberá introducir la clave para poder continuar con el proceso de firma.

Otras especificaciones técnicas en documento "Viafirma –fortress"

Mediante este procedimiento, el firmante tiene la opción de complementar la seguridad del sistema de firma a distancia con 2FA:

- Lo que conozco, datos de activación de firma (PIN)
- Lo que poseo, email, móvil, o servicio web PC.

4.4 Activación del proceso de firma

Superado el proceso 3.2, el servicio de firma a distancia, empleando canal de comunicación seguro SSL, permite continuar con el proceso de firma. Concretamente:

- Muestra al firmante el archivo que ha solicitado firmar, y le permite poder visualizar contenido.
- Le requiere que introduzca su PIN (Datos de activación de firma) para activar el proceso de firma.

El servicio de firma a distancia, empleando el Dispositivo Seguro de Creación de Firma (HSM) y el PIN del firmante, procede a firmar el archivo requerido.

Una vez firmado el archivo, el firmante puede proceder a su descarga.

5 Controles de seguridad física, instalaciones, gestión y operacionales

Según lo definido en la Política de Certificación a la que se somete la emisión del certificado.

5.1 Controles de seguridad física

Según lo definido en la DPC de ANF AC.

5.2 Controles de procedimiento

Según lo definido en la DPC de ANF AC.

5.3 Controles de personal

Según lo definido en la DPC de ANF AC.

6 Controles de seguridad técnica

6.1 Generación e instalación del par de claves

Según lo definido en la DPC de ANF AC.

6.2 Protección de la clave privada

Según lo definido en la DPC de ANF AC.

6.3 Otros aspectos de gestión del par de claves

Según lo definido en la DPC de ANF AC.

6.4 Datos de activación

Según lo definido en la DPC de ANF AC.

6.5 Controles de seguridad informática

Según lo definido en la DPC de ANF AC.

6.6 Controles técnicos del ciclo de vida

Según lo definido en la DPC de ANF AC.

6.7 Controles de seguridad de la red

Según lo definido en la DPC de ANF AC.

6.8 Sellado de tiempo

Según lo definido en la DPC de ANF TSA CA.

6.9 Controles de seguridad de los módulos criptográficos

Según lo definido en la DPC de ANF AC.