ANF AUTORIDAD DE CERTIFICACIÓN

2021

DECLARACIÓN DIVULGATIVA DE PRODUCTO

PDS (*PRODUCT DISCLOSURE STATEMENT*)

SERVICIO CUALIFICADO DE SELLADO DE TIEMPO ELECTRÓNICO-TIMESTAMPING CON TECNOLOGÍA BLOCKCHAIN-

© ANF Autoridad de Certificación
Paseo de la Castellana,79 -28046- Madrid (España)
Teléfono: 932 661 614 (Llamadas desde España)
Internacional +34 933 935 946
Web: www.anf.es

ETSI EN 319401 ETSI EN 319421 ETSI EN 319411 ETSI EN 319402 ISO 27001 ISO 9001 ISO 17024 ISO 26000

ANF AUTORIDAD DE CERTIFICACIÓN

Nivel de Seguridad

Documento Público

Aviso Importante

Este documento es propiedad de ANF Autoridad de Certificación
Está prohibida su reproducción y difusión sin autorización expresa de ANF Autoridad de Certificación

Dirección: **Paseo de la Castellana, 79 - 28046 - Madrid** (España)
Teléfono: **932 661 614** (llamadas desde España)
Internacional **(+34) 933 935 946**
www.anf.es

Información de contacto del Prestador Cualificado de Servicios de Confianza

Servicios de Confianza Cualificados

ANF Autoridad de Certificación (ANF AC), NIF G63287510, es la Autoridad de Certificación que, en calidad de Prestador Cualificado de Servicios de Confianza, emite certificados cualificados bajo eIDAS.

Dirección corporativa

Paseo de la Castellana,79

28046- Madrid (España)

Administración – Servicios jurídicos – Ingeniería

Gran de les Vía Corts Catalanes, 996

08018 – Barcelona (España)

Sede electrónica:

https://www.anf.es

Sede electrónica:

info@anf.es

ANF AC pone a disposición pública formularios de contacto a través de la sede electrónica de ANF AC

- Asuntos general en **https://www.anf.es/contacto/**
- Prensa en **https://www.anf.es/contacto/#prensa**

Sellos de tiempo electrónico, certificado TSU y procedimientos de validación

Las "Unidades de Sellado de Tiempo" disponen de Certificados TSU para crear Sellos Cualificados de Tiempo Electrónico (QTST).

Los sellos de tiempo electrónico (TST – TimeStamp Token), son cualificados en cumplimiento con los requisitos del Art. 42 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 (eIDAS).

Puede comprobarse su inclusión en la lista de confianza de prestadores de servicios de confianza (TSL – Trusted Service List) de España, a través del enlace,

https://sede.serviciosmin.gob.es/Prestadores/TSL/TSL.pdf

La validación del estado de vigencia de los certificados TSU, se puede comprobar a través del servicio de información y consulta en línea que provee ANF AC, empleando protocolo OCSP *(conforme a RFC 6960)*, disponible en la ubicación del respondedor OCSP en el propio certificado.

Límites de uso de los certificados TSU

El certificado de CAi de la TSA es "ANF High Assurance EV CA1" cual el cual se firma y se emiten los certificados TSU. **El certificado de CAi está sometido a la DPC de ANF AC OID 1.3.6.1.4.1.18332.1.9.1.1,** los certificados TSU están sometidos a la Política de Sellado de Tiempo (TimeStamping) **OID 1.3.6.1.4.1.18332.15.1.** La clave pública que permite la validación de los certificados TSU y de los sellos cualificados de tiempo electrónico se encuentra publicada en la TSL de España.

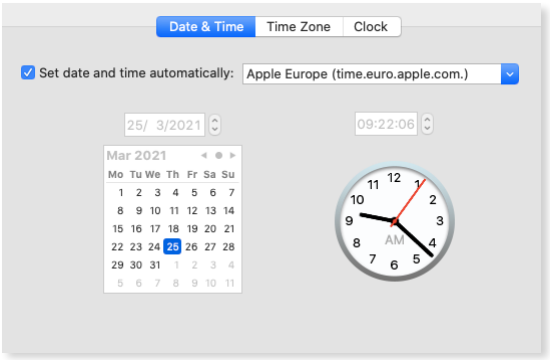
Los certificados TSU incluyen, **siguiendo las recomendaciones de las normas ETSI EN 319 421 y ETSI EN 319 422,** la extensión privateKeyUsage, que limita el uso de la **Clave privada** estableciendo una fecha de cese de uso de la clave, que es anterior a la caducidad de la clave pública, de manera que **se asegure un tiempo suficiente para la renovación de los TST emitidos por una TSU antes de la caducidad de su certificado.**

Los certificados electrónicos de TSU incluyen la extensión "id-kp-timestamping" que indica que este certificado se utilizará con el fin exclusivo de expedir sellos de tiempo electrónico.

El certificado TSU no puede ser renovado y no podrá ser utilizado cuando expire su periodo de validez. Cuando sea solicitada su revocación o se cumpla alguna de las otras causas de extinción de su vigencia establecidas en la **Declaración de Prácticas TSA y Política de Sellado de tiempo (TimeStamping) OID 1.3.6.1.4.1.18332.15.1 y en la DPC ANF AC OID 1.3.6.1.4.1.18332.1.9.1.1**

ANF AC registra y custodia aquellos eventos significativos necesarios para verificar la actividad de esta Autoridad de Sellos de Tiempo durante un periodo que nunca será inferior a 15 años.

Obligaciones del suscriptor y terceros que confían



En las secciones 5.2 y 5.3 de la Declaración de Prácticas TSA y Política de Sellado de Tiempo (Timestamping) OID 1.3.6.1.4.1.18332.15.1 quedan definidas las obligaciones de todas las partes que actúan en relación con el uso de los sellos cualificados de tiempo electrónico expedidos por la TSA de ANF AC.

En especial, el suscriptor y los terceros que confían antes de depositar su confianza en los sellos de tiempo electrónico, tienen la obligación de verificar la validez del certificado TSU y del Sello de Tiempo, debiendo emplear para ello un sistema de v**alidación cualificado de firma y sellos electrónicos** que disponga de **verificación de TST que cumpla lo indicado en la sección 6.7.5 (Validación del Sello de Tiempo) de la referida política y practicas OID 1.3.6.1.4.1.18332.15.1**

Obligaciones de la TSA, sus responsabilidades y exoneración

En la sección 5 Declaración de Prácticas TSA y Política de Sellado de Tiempo (Timestamping) OID 1.3.6.1.4.1.18332.15.1 quedan definidas las obligaciones, responsabilidades y exoneración de responsabilidad de la TSA.

> **La Autoridad de Sellado de Tiempo de ANF AC , para afrontar el riesgo de la responsabilidad por los daños y perjuicios que pueda ocasionar el servicio de sello de tiempo, ha suscrito el correspondiente seguro de responsabilidad civil de CINCO MILLONES DE EUROS (5.000.000. €).**

Número Póliza:
HD IP6 2056529

Aseguradora
HISCOX, S.A,

Se aplican las "Limitaciones de servicio" establecidas en la sección 4.2.3 de la política y prácticas TSA.

Limitaciones de servicio

En la sección 4.2.3 Declaración de Prácticas TSA y Política de Sellado de Tiempo (Timestamping) quedan definidas las "Limitaciones del servicio".

En especial,

- **ANF AC se responsabiliza de la variación de la referencia temporal,** en relación al tiempo proporcionado por servicio del **Real Instituto y Observatorio de la Armada,** incluida en el sello cualificado de tiempo electrónico en el momento de la solicitud, pero en ningún caso de la veracidad ni contenido de los datos electrónicos remitidos por los suscriptores del servicio, que son el objeto del Sello de tiempo electrónico emitido.

- **ANF AC no responderá ante los suscriptores o terceros que confían, cuyo comportamiento en la utilización del servicio cualificado de sellado de tiempo electrónico haya sido negligente,** debiendo considerarse a estos efectos y en todo caso como negligencia la falta de observancia de lo dispuesto en la presente **Declaración de Prácticas y Política de Sellado de Tiempo**, en el Contrato de Servicio, en los Términos y Condiciones, y en especial, en lo dispuesto en los apartados referidos a las obligaciones y a la responsabilidad de los suscriptores y de las partes que confían.

- **ANF AC no garantiza los algoritmos criptográficos ni se responderá de los daños causados por ataques exitosos externos a los algoritmos criptográficos usados,** en especial, si guardó la diligencia debida de acuerdo al estado actual de la técnica, el presente documento y su adenda, y lo establecido en el Reglamento eIDAS y Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

- **No responderá por ningún software que no haya proporcionado directamente por ANF AC.**

- En defecto de regulación específica que se acepte expresamente en el contrato de prestación de servicios, el suscriptor del servicio y los terceros que confían limitarán la responsabilidad de ANF AC a un máximo de CINCO MIL EUROS (5.000€). **Esta cuantía queda fijada como máximo exigible en concepto de daños y perjuicios que ANF AC debiera satisfacer por imperativo judicial.**

Política de privacidad

El servicio de sellado de tiempo electrónico no realiza tratamiento de datos personales, por tanto, no esta afectado por el Reglamento (UE) 679/2016 General de Protección de Datos (RGPD), ni por la Ley Orgánica 3/2018 de Protección de Datos y Garantía de Derechos Digitales (LOPDyGDD)

ANF AC garantiza que no recoge datos personales ni tiene oportunidad de hacerlo. Los sellos de tiempo son solicitados sin incluir la identidad del solicitante *(sea persona física o jurídica*) ni del tercero de confianza. Del sello de tiempo no se puede obtener información del contenido del documento al que se asocia, por tanto, los sellos de tiempo son anónimos.

Política de devolución

No se aplica al servicio de sellado de tiempo electrónico.

Ley aplicable, consultas y quejas

El servicio de sellado de tiempo electrónico de ANF AC, se realiza en conformidad con,

- **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 (eIDAS).
- **Ley 6/2020, de 11 de noviembre,** reguladora de determinados aspectos de los servicios electrónicos de confianza.

ANF AC, pone a disposición de los suscriptores y terceros que confían servicio en línea para,

- **Reportar problema con tu certificado en,** https://micertificado.anf.es/
- **Reportar incumplimiento o uso indebido en,** https://anf.es/sat-incumplimiento-uso-indebido/
- **Abrir una incidencia en,** https://www.anf.es/ac/abrir-incidencia

Además ofrece atención al público por los siguientes canales:

- **Presencial, dirección administrativa**, legal y técnica, concertando entrevista previa días laborables de **9 h a 14 h y de 15 h. a 18 h**.
- Telefónicamente, **+34 932 661 614**
- **eMAIL,**
  - Administración: **administracion@anf.es**
  - Técnico: **soporte@anf.es**
  - Comercial: **info@anf.es**
  - Legal: **mcmateo@anf.es**
  - Protección datos : **delegadoprotecciondatos@anf.es**

Normas y estándares aplicables

El servicio de sellado de tiempo electrónico de ANF AC, se realiza en conformidad con normas de reconocimiento internacional, a modo meramente enunciativo cabe destacar:

- **ETSI EN 319 421:** "Policy and Security Requirements for Trust Service Providers issuing Time-Stamps."
- **ETSI EN 319 422:** "Time-stamping protocol and time-stamp token profiles."
- **ETSI EN 319 401:** "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers"
- **ETSI TS 119 312:** "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites"
- **IETF RFC 3628:** "Policy Requirements for Time-Stamping Authorities (TSAs)"
- **IETF RFC 3161:** "Internet X.509 Public Key Infrastructure Time-stamp Protocol"

Resolución de disputas

PROCEDIMIENTO EXTRAJUDICIAL

ANF AC se esforzará en resolver de forma amistosa los conflictos que surjan con terceras partes por el ejercicio de su actividad, sólo recurriendo al procedimiento previsto en apartado siguiente, cuando el acuerdo entre las partes resulte inalcanzable.

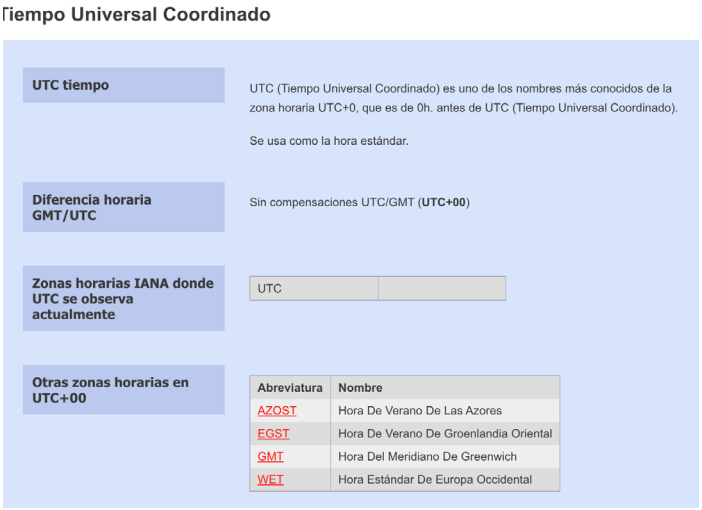
PROCEDIMIENTO JUDICIAL

ANF AC se somete voluntariamente, para la solución de cualquier cuestión litigiosa que pudiera surgir por el ejercicio de su actividad, al arbitraje institucional del Tribunal Arbitral del Consejo Empresarial de la Distribución (TACED) https://www.taced.es, al que se le encarga la designa del Árbitro – que será único – y la administración del arbitraje – que será de equidad – con arreglo a su Reglamento, obligándose desde ahora, al cumplimiento de la decisión arbitral.

Si por alguna causa no fuera posible dirimir la controversia mediante el procedimiento arbitral reseñado en el punto anterior, las Partes, renuncian a cualquier otro fuero que pudiera corresponderles y se someten para la resolución de cualquier conflicto que pudiera surgir entre las mismas, a los Tribunales de la ciudad de Barcelona, con renuncia a su fuero propio si fuera distinto.

Fuente segura de tiempo

ANF AC garantiza que el reloj de los servidores TSU, está sincronizado con la hora UTC dentro de la exactitud declarada de más de (1) segundo, utilizando fuente segura de tiempo (ROA) y protocolo de sincronización Network Time Protocol (NTP).



Tiempo Universal Coordinado

UTC tiempo	UTC (Tiempo Universal Coordinado) es uno de los nombres más conocidos de la zona horaria UTC+0, que es de 0h. antes de UTC (Tiempo Universal Coordinado). Se usa como la hora estándar.
Diferencia horaria GMT/UTC	Sin compensaciones UTC/GMT (**UTC+00**)
Zonas horarias IANA donde UTC se observa actualmente	UTC
Otras zonas horarias en UTC+00	

Abreviatura	Nombre
AZOST	Hora De Verano De Las Azores
EGST	Hora De Verano De Groenlandia Oriental
GMT	Hora Del Meridiano De Greenwich
WET	Hora Estándar De Europa Occidental

1

EL SERVICIO DE SELLADO DE TIEMPO SE ENCUENTRA EN ESPAÑA.

Se sincroniza con una señal de tiempo a través del ROA (Real Observatorio de la Armada), laboratorio reconocido por el organismo público internacional Bureau International des Poids et Mesures (BIPM).

2

EL TIEMPO ROA,

esta declarado a efectos legales como Patrón Nacional de dicha unidad, así como del mantenimiento y difusión oficial de la escala “Tiempo Universal Coordinado” (UTC (ROA)), considerado a todos los efectos como la base de la hora legal en todo el territorio nacional (R.D. 23 octubre 1992, núm. 1308/1992).

3

EL SERVICIO DE SELLADO DE TIEMPO

utiliza protocolo NTP para realizar la sincronización de los servidores TSU con la fuente segura de tiempo (ROA). Con esa configuración, se alcanza una precisión de +/- de 100 ms o superior con respecto al UTC.

Encadenamiento hash (BlockChain)

El servicio de sellado de tiempo electrónico de ANF AC, ha sido diseñado y desarrollado con el principio de máxima seguridad, por el cual, ni la propia TSA pueda crear falsos sellos de tiempo.

Para lograr este objetivo se siguen y respetan los principios de Stuart Haber and W. Scott Stornetta, los cuales propusieron por primera vez (How to time-stamp, 1991) un producto de cadena de protección de cifrado en bloque (base del modelo tecnológico de Blockchain), único procedimiento que garantiza la seguridad de una TSA y, además, permite demostrarlo.

Cada Unidad de Sellado de Tiempo de ANF AC, gestiona un servicio de encadenamiento de hash relativo a todos los TST emitidos. El encadenamiento se basa en una cadena de bloques en la cual:

- El hash entrante corresponde al inmediatamente anterior cronológico de hash saliente.
- El has actual corresponde al hash del documento asociado al sello de tiempo.
- El hash saliente es el resultado de procesar el conjunto de la información del sello de tiempo.

Mediante este procedimiento se imposibilita cualquier intento de modificación. No la propia TSA podría realizar un sello de tiempo fuera del tiempo real, puesto que provocaría que la secuencia cronológica de la cadena de bloques quedará rota.

Este procedimiento es además el único que permite demostrar las emisiones de una TSA. Además, **ANF AC realiza deposito notarial de las actas de resumen general de los hash entrante-actual-saliente asociados a los TST emitidos.** ANF AC TSA podrá pedir al tercero que confía cubrir los costos de comprobación de existencia de hash, en caso de solicitud de evidencia.

Auditorías y acreditaciones oficiales de ANF AC

ANF AC, como Prestador Cualificado de Servicios de Confianza, ha logrado acreditación oficial de su Infraestructura de Clave Pública (PKI) en los siguientes servicios:

- Emisión de certificados cualificados de **firma electrónica.**
- Emisión de certificados cualificados de **empleado público.**
- Emisión de certificados cualificados **centralizados.**
- Emisión de certificados cualificados **PSD2.**
- Emisión de certificados cualificados de **sello electrónico.**
- Emisión de certificados cualificados de **sello electrónico PSD2.**
- Emisión de certificados cualificados de **sello electrónico y sello AAPP.**
- Emisión de certificados cualificados de **servidor seguro SSL.**
- Emisión de certificados cualificados de **servidor seguro SSL Sede Electrónica.**
- Servicio de firma electrónica **cualificada a distancia.**
- Servicio cualificado de **sellos de tiempo electrónico.**
- Servicio cualificado de **entrega electrónica.**
- Servicio cualificado de **preservación a largo plazo.**
- Servicio cualificado de **validación de firmas y sellos electrónicos cualificados.**

Además, ANF AC, dispone de otras acreditaciones y homologaciones de servicios avanzados TI:

- Homologación Mozilla, Microsoft, Apple, Google para la **emisión de certificados electrónicos SSL**:
  - **DV**
  - **OV**
  - **EV**
- **Entidad de Certificación (EC)** conforme al Esquema de la Agencia de Protección de Datos para Delegados de Protección de Datos.
- **Servicios de Digitalización Certificada (LegalSnapScan)** acreditado por la Agencia Española de Administración Tributaria.

Además de las auditorías ETSI (servicios eIDAS), ANF AC ha logrado auditorías de conformidad contra los estándares:

- **ISO 27001:2013** Sistema de Gestión de Seguridad de la Información
- **ISO 9001** Calidad de servicio CA
- **ISO 17024** Certificación de Personas
- **ISO 14001** Sistema de Gestión Medioambiental

Módulos Hardware Criptográfico (HSM) empleado para la prestación del servicio de sellado de tiempo,

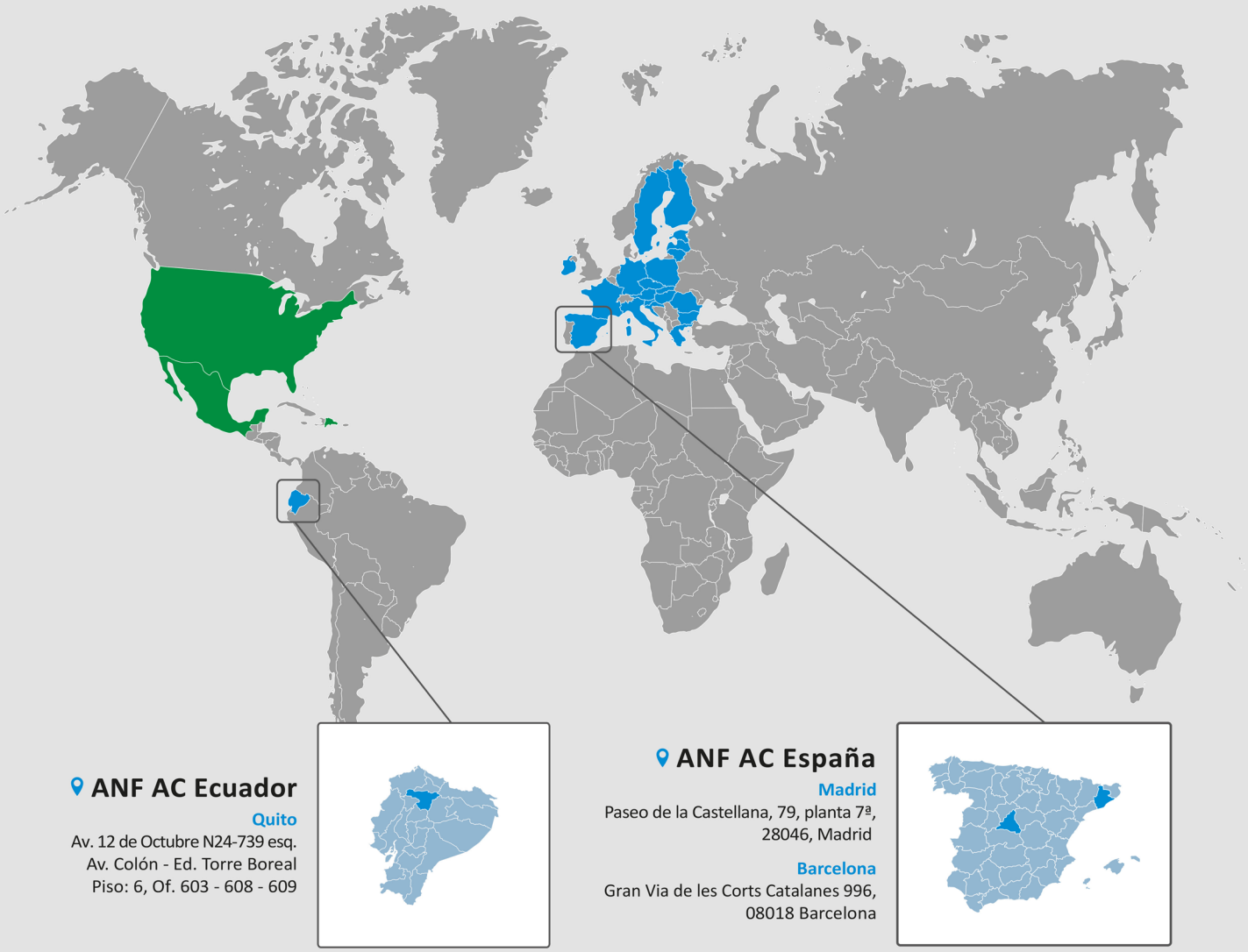
- Las claves privadas de CA, CAi, TSU, y certificados centralizados de usuario final, se generan y custodian en un dispositivo criptográfico seguro (HSM) certificado como dispositivos cualificados de firma electrónica (QSCD). Cumplen los requerimientos que se detallan en FIPS PUB 140-2 nivel 3 o superior, o con un nivel EAL 4+ o superior de acuerdo con ISO/IEC 15408.
- Las SmartCard QSCD suministradas a usuarios finales, se encuentran certificadas y cumplen los requerimientos que se detallan en FIPS PUB 140-2 nivel 3 o superior, o con un nivel EAL 4+ o superior de acuerdo con ISO/IEC 15408.

En la utilización de sellos de tiempo para procedimientos de nivel bajo, medio o alto del Esquema Nacional de Seguridad (ENS), se seguirán las indicaciones de la Guía de Seguridad de las TIC -CCN-STIC-807-

Certificaciones de conformidad publicadas en,

https://www.anf.es/auditorias-de-conformidad/

Ámbito geográfico de interoperabilidad legal



ANF AC Ecuador

Quito
Av. 12 de Octubre N24-739 esq.
Av. Colón - Ed. Torre Boreal
Piso: 6, Of. 603 - 608 - 609

ANF AC España

Madrid
Paseo de la Castellana, 79, planta 7ª,
28046, Madrid

Barcelona
Gran Via de les Corts Catalanes 996,
08018 Barcelona

ANF AC acreditación gubernamental.

Acuerdo de reconocimiento mutuo internacional.

Datos de Contacto

ANF AC España

Teléfono: 93 266 16 14
Dpto. Cíal: info@anf.es
Dpto. SAT: soporte@anf.es

ANF AC Ecuador

Teléfono: +593 02 3826877
Dpto. Cíal: ecuador@anf.ac
Dpto. SAT: soporte.ec@anf.ac