Normas y Estándares respetados por ANF AC

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

INFORMACIÓN BÁSICA DEL DOCUMENTO	
Tipo	Documento de control
Nombre del documento	Normas y Estándares de ANF AC
Versión	1.5
Responsables de la auditoria del documento	A. Díaz G. García
Nombre del fichero	DT_OID_ANFAC
Fecha de creación	12.01.2001
Última modificación	17.03.2017
Estado	Aprobado
Fecha aprobación	17.03.2017
Aprobado por	F. Díaz - CEO - ANF Autoridad de Certificación

Índice

1. Recomendaciones y Estándares Técnicos

- IETF RFC 1305 (Network Time Protocol (NTP v3))
- IETF RFC 2279 mejorada en 3629 (UTF-8, a transformation format of ISO 10646)
- IETF RFC 3161 (Time Stamp Protocol – (TSP)) actualizada por IETF RFC 5816.
- IETF RFC 3279. Actualizada por RFC 4055, RFC 4491, RFC 5480, RFC 5758 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile.
- IETF RFC 3339 (Date and Time on the Internet: Timestamps)
- IETF RFC 3447 Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1
- IETF RFC 3628 (Policy Requirements for Time-Stamping Authorities (TSAs))
- IETF RFC 3647 (Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling)
- IETF RFC 3739 (Internet X.509 Public Key Infrastructure: Qualified Certificates Profile).Perfila el empleo de los atributos X.520 más habituales, para su uso en los nombres dentro de certificados cualificados.
- IETF RFC 3850 (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework)
- IETF RFC 4055. Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Actualizada por RFC 5756 Updates for RSAES-OAEP and RSASSA-PSS Algorithm Parameters
- IETF RFC 4158. Internet X.509 Public Key Infrastructure: Certification Path Building
- IETF RFC 4510 Lightweight Directory Access Protocol (LDAP):Technical Specification Road Map
- IETF RFC 4511 Lightweight Directory Access Protocol (LDAP): The Protocol
- IETF RFC 4949 (Internet Security Glossary, Version 2": cross-certification)
- IETF RFC 5280 (Internet X.509 Public Key Infrastructure Certificate and CRL Profile) actualizada por 6818. Incorpora los atributos X.520 más habituales, para cualquier tipo de nombre dentro del certificado
- IETF RFC 5652 Cryptographic Message Syntax (CMS)
- IETC RFC 6960 - 6277 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP
- IETF RFC 6960 (Online Certificate Status Protocol – (OCSP))
- IETF RFC 7382. (Template for a Certification Practice Statement (CPS))
- IETF RFC 7905 (The Transport Layer Security (TLS) Protocol Version 1.2), - 6176 – 5246
- RFC 5754 Using SHA2 Algorithms with Cryptographic Message Syntax actualiza RFC 3370 – RFC 2630
- RFC 6712 Internet X.509 Public Key Infrastructure -- HTTP Transfer for the Certificate Management Protocol (CMP), actualiza RFC 4210 – RFC 2510
- ETSI EN 319 411-2 (reemplaza a TS 101 456) Part 2: Requirements for trust service providers issuing EU qualified certificates.
- ETSI TS 101 533, Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management.

- ETSI TS 101 733, CAdES (CMS Advanced Electronic Signatures)
- ETSI EN 319 421 (reemplaza TS 101 861) Time Stamping Profile
- ETSI TS 101 862 (Qualified Certificate Profile). Queda definida en las normas EN 319 412-1, EN 319 412-5)
- ETSI TS 101 903, XAdES (XML Advanced Electronic Signatures)
- ETSI TS 102 023, Electronic Signatures and Infrastructures (ESI), Policy requirements for time-stamping authorities
- ETSI TS 102 038, TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies
- ETSI EN 319 411-3 (reemplaza a TS 102 042). Part 3: Policy Requirements for Certification Authorities issuing public key certificates
- ETSI TS 102 778, PAdES (PDF Advanced Electronic Signatures).
- ETSI TS 102 853 Electronic Signatures and Infrastructures (ESI); Signature verification procedures and policies
- ETSI TS 102 860 Certificate Profile for Certificates Issued to Natural Persons (queda definida por la norma EN 319 412-2)
- ETSI TS 103 171, v.2.1.1., Electronic Signatures and Infrastructures (ESI); XAdES Baseline profile. Define el perfil de firmas XAdES convenientes para ser utilizadas en el ámbito de la Directiva Europea de Servicios, por las autoridades nacionales de los estados miembros de la UE.
- ETSI TS 103 172, v.2.1.1., Electronic Signatures and Infrastructures (ESI); PAdES Baseline profile. Define un perfil de firmas PAdES (firmas avanzadas para documentos PDF) convenientes para ser utilizadas en el ámbito de la Directiva Europea de Servicios, por las autoridades nacionales de los estados miembros de la UE.
- ETSI TS 103 173, v.2.1.1., Electronic Signatures and Infrastructures (ESI); CAdES Baseline profile. Define un perfil de firmas CAdES (firmas avanzadas construidas sobre firmas CMS) convenientes para ser utilizadas en el ámbito de la Directiva Europea de Servicios, por las autoridades nacionales de los estados miembros de la UE.
- ETSI TS 103 174 Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile
- ETSI TS 103 174, v.2.1.1., Electronic Signatures and Infrastructures (ESI); ASiC Baseline profile. Define un perfil de contenedor ASiC (Associated Signatures Container: contenedor que engloba en un solo paquete un conjunto de documentos electrónicos y un conjunto de firmas electrónicas XAdES o CAdES sobre uno, varios o todos los documentos) convenientes para ser utilizadas en el ámbito de la Directiva Europea de Servicios, por las autoridades nacionales de los estados miembros de la UE.
- ETSI TS 119 124-(5 pts), v.2.1.1., Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability;
- ETSI TS 119 134-(5 pts), v.2.1.1., Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability;
- ETSI TS 119 144-(5 pts), v.2.1.1., Electronic Signatures and Infrastructures (ESI); PAdES digital signatures - Testing Conformance and Interoperability;
- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); - Cryptographic Suites
- prEN 419 241-1: General System requirements
- prEN 419 241-2: Protection Profile for QSCD for Server Signing

- prEN 419 221-5: Cryptographic module
- 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
- ITU X.520 - ISO/IEC 9594-6 Information technology -- Open Systems Interconnection -- The Directory -- Part 6: Selected attribute types
- ITU X.1254 Entity authentication assurance framework
- ITU-T Rec. X.501. De acuerdo con esta recomendación el nombre contenido en el Subject Name adopta la forma de un Nombre Distinguido
- ITU-T Rec. X.660
- ITU-T Rec. X.660 - ISO/IEC 9834-1:2005 (Procedures for the Operation of OSI Registration Authorities: General Procedures and ASN.1 Object Identifier tree top arcs)
- ISO 3166-1. Para codificación de elementos (alpha-2 code elements)
- ISO 4217. Para codificación de valores como moneda.
- ISO/IEC 9594-8/ITU-T X.509.
- ISO IEC 18014, Time-stamping services is an international standard that specifies time-stamping techniques.

El servicio de sellado electrónico de tiempo de ANF AC puede ser adaptado al estándar X9.95-2005 de American National Standard.

- ISO / IEC 29115: 2013 Information technology -- Security techniques -- Entity authentication assurance framework
- ISO 32000-1:2008, v.1.7., PDF (Portable Document Format).
- CA/Browser Forum. Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates.
- CA/Browser Forum. Guidelines For The Issuance And Management of Extended Validation Certificates.
- CWA 14169. Queda definida en la norma EN 14169 y pasa a la norma EN 19211 Dispositivos seguros de creación de firma "EAL 4+"... Perfiles de protección para los dispositivos seguros de creación de firma. (EN 66211)

2. Marco Legal UE y España

REGLAMENTO (UE) 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.

Decisión de Ejecución (UE) 2015/1505 de la Comisión de 8 de septiembre de 2015 por la que se establecen las especificaciones técnicas y los formatos relacionados con las listas de confianza de conformidad con el artículo 22, apartado 5, del Reglamento (UE) no 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

Anexo del **Reglamento de Ejecución (UE) 2015/1501 de la Comisión de 8 de septiembre de 2015** sobre el marco de interoperabilidad de conformidad con el artículo 12, apartado 8, del Reglamento (UE) no 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

Reglamento de Ejecución (UE) 2015/1502 de la Comisión de 8 de septiembre de 2015 sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) no 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE

Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

Directiva (UE)2009/136/CE del Parlamento Europeo y del Consejo de 25 de noviembre de 2009 por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) no 2006/2004 sobre la cooperación en materia de protección de los consumidores.

Directiva 2006/24/CE, del Parlamento Europeo y del Consejo de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

Directiva 2004/82/CE, del Consejo de 29 de abril de 2004, sobre la obligación de los transportistas de comunicar los datos de las personas transportadas.

Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre privacidad y las comunicaciones electrónicas).

Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).

DECISIÓN DEL CONSEJO de 13 de septiembre de 2004 por la que se adoptan las normas de desarrollo del Reglamento (CE) no 45/2001 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.

Ley 59/2003, de Firma Electrónica de 19 de diciembre, Esta Ley regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación.

Real Decreto Legislativo 1/1996 Ley de Propiedad Intelectual.
Según esta Ley, la propiedad intelectual de una obra literaria, artística o científica corresponde al autor por el solo hecho de su creación.

Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos
Esta ley reconoce el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos. Además, regula los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa, en las relaciones entre las Administraciones Públicas, así como en las relaciones de los ciudadanos con las mismas.

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, tiene el objeto de garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal

Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

3. En Proceso de Adaptación

Normas técnicas que son de obligado cumplimiento por las AA.PP.

ANF AC respeta las normas definidas por el Esquema Nacional de Interoperabilidad, y que son de obligado cumplimiento por las AA.PP. y que desarrollan aspectos concretos de la interoperabilidad entre las AA.PP. y con los ciudadanos.

Más información en la "Guía de ENI de aplicación de la Norma Técnica de Interoperabilidad de Catálogo de estándares"

ANF AC está en proceso de adaptación de:

ETSI EN 319 412 Certificates Profiles
- Part 1: Overview and common data structures
- Part 2: Certificate profile for certificates issued to natural persons
- Part 3: Certificate profile for certificates issued to legal persons
- Part 4: Certificate profile for web site certificates issued to organizations
- Part 5: QCStatements

ETSI EN 319 411: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates.
- Part 1: General requirements
- Part 2: Part 2: Requirements for trust service providers issuing EU qualified certificates

Servicio	EN general	EN de alcance	Perfil/semántica
Creación, verificación y validación de firmas electrónicas.	EN 319 401	EN 319 411-1 EN 319 411-2	EN 319 412-1 EN 319 412-2 EN 319 412-3 EN 319 412-4 EN 319 412-5
La creación, verificación y validación de sellos electrónicos.	EN 319 401	EN 319 411-1 EN 319 411-2	EN 319 412-3
La creación, verificación y validación de sellos de tiempo electrónicos.	EN 319 401	EN 319 421	EN 319 422
La creación, verificación y validación de certificados para la autenticación de sitios Web	EN 319 401	EN 319 411-1 EN 319 411-2	EN 319 412-4

Normas EN "Dispositivos seguros de creación de firma electrónica" SSCD
DECISIÓN DE EJECUCIÓN (UE) 2016/650 DE LA COMISIÓN de 25 de abril de 2016

EN 419 211 — Protection profiles for secure signature creation device (Perfiles de protección para los dispositivos seguros de creación de firma), Partes 1 a 6 —en su caso— enumeradas a continuación:

— EN 419211-1:2014 — Protection profiles for secure signature creation device — Part 1: Overview (Perfiles de protección para los dispositivos seguros de creación de firma. Parte 1: Generalidades).
— EN 419211-2:2013 — Protection profiles for secure signature creation device — Part 2: Device

with key generation (Perfil de protección para los dispositivos seguros de creación de firma. Parte 2: Dispositivo con generación de claves).

— EN 419211-3:2013 — Protection profiles for secure signature creation device — Part 3: Device with key import (Perfil de protección para los dispositivos seguros de creación de firma. Parte 3: Dispositivo con importación de claves).

— EN 419211-4:2013 — Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application (Perfil de protección para los dispositivos seguros de creación de firma. Parte 4: Extensión para el dispositivo con generación de claves y comunicación confiada con aplicación de generación de certificado).

— EN 419211-5:2013 — Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted channel to signature creation application (Perfil de protección para los dispositivos seguros de creación de firma. Parte 5: Dispositivo con generación de claves y comunicación confiada con aplicación de creación de firma).

— EN 419211-6:2014 — Protection profiles for secure signature creation device — Part 6: Extension for device with key import and trusted channel to signature creation application (Perfil de protección para los dispositivos seguros de creación de firma. Parte 6: Dispositivo con importación de claves y comunicación confiada con aplicación de creación de firma).

4. Otras Normas de Interés de Referencia Europea

EN 301 549: Accessibility requirements suitable for public procurement of ICT products and services in Europe.

Se trata de la primera norma europea de Accesibilidad para productos y servicios de Tecnologías de la Información y Comunicación (TIC).

El apartado 9 de la norma EN 301 549 hace referencia a los requisitos de accesibilidad que se aplican al contenido web. **Todos los de nivel A y AA de las WCAG 2.0** (están incluidos en la norma ISO: ISO/IEC 40500 (2012): "Information technology - W3C Web Content Accessibility Guidelines (WCAG) 2.0"). De hecho, la EN 301 549 incluye en su página de descarga un archivo ZIP con las WCAG 2.0 en formato PDF.

El apartado 10 hace referencia a los requisitos de accesibilidad en documentos y el apartado 11 a los requisitos de accesibilidad del software, pero hay otros, por ejemplo los referentes al hardware.

El Anexo B donde se incluye una tabla con todos los requisitos de accesibilidad de la norma expresados en términos de rendimiento funcional (distinguiendo relaciones primarias y secundarias).

Más información en la edición de Loïc Martínez Normand: "Prototype of EN 301 549 Decision tree" y su presentación sobre cómo aplicarlos en aplicaciones móviles: Requisitos europeos de accesibilidad de aplicaciones móviles

EN 319 403 (reemplaza a TS 119 403): "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers" Norma para la certificación de Prestadores de Servicios de Confianza Electrónica.

5. Certificaciones de Conformidad

5.1 PKI

• ISO 9001:2008 Sistema de Gestión de la Calidad.
• ISO 27001 (Information technology - Security techniques - Information security management systems – Requirements) . Estándar para la seguridad de la información.
• WebTrust
• WebTrust SSL
• WebTrust EV SSL

5.2 Dispositivos de Firma Electrónica y Componentes

Las claves de las Entidades de Certificación se generarán en hardware criptográfico que cumple el estándar FIPS 140-2 Nivel 3 (o superior), o Common Criteria ISO 15408 EAL 4+ (o superior).

.

Las claves de firma electrónica reconocida de los usuarios finales, en dispositivos HSM, se generarán y están contenidas en dispositivos criptográficos que cumplen el estándar FIPS 140-2 Nivel 3 (o superior), o Common Criteria ISO 15408 EAL 4+ (o superior).