


Norms and Standards respected by ANF AC



	<p><i>This specification has been prepared by ANF AC to release to third parties.</i></p>	<p>SECURITY LEVEL</p> <p>PUBLIC DOCUMENT</p>
--	---	--

This document is the property of ANF Certification Authority.

Its reproduction and dissemination is prohibited without the express authorization of ANF Certification Authority

Copyright © ANF Certification Authority

Standards and Standards ANF AC	Ref. DT_Normas y Standards.pdf	Version: 1.3
	OID: 1.3.6.1.4.1.18332.101.80.8	Page 1 of 12

BASIC INFORMATION OF THE DOCUMENT	
Guy	Control document
Document name	Norms and Standards of ANF AC
Version	1.5
Heads of the auditor document ia	A. Diaz G. Garcia
File name	DT_OID_ANFAC
Creation date	12.01.2001
Last modification	17.03.2017
State	Approved
Approval date	17.03.2017
Approved by	F. Díaz - CEO - ANF Certification Authority

Standards and Standards ANF AC	Ref. DT_Normas y Standards.pdf	Version: 1.3
	OID: 1.3.6.1.4.1.18332.101.80.8	Page 2 of 12

Index

1. Recommendations and Technical Standards	4
2. Legal Framework EU and Spain	7
3. In the Adaptation Process	9
4. Other Standards of European Reference Interest	eleven
5. Certifications of Conformity	12
5.1 PKI	12
5.2 Electronic Signature Devices and Components	12

Standards and Standards ANF AC	Ref. DT_Normas y Standards.pdf	Version: 1.3
	OID: 1.3.6.1.4.1.18332.101.80.8	Page 3 of 12

1. Recommendations and Technical Standards

- IETF RFC 1305 (Network Time Protocol (NTP v3))
- IETF RFC 2279 improved in 3629 (UTF-8, a transformation format of ISO 10646)
- IETF RFC 3161 (Time Stamp Protocol - (TSP)) updated by IETF RFC 5816.
- IETF RFC 3279. Updated by 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). It outlines the use of the most common X.520 attributes, for use in names within qualified certificates.
- 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. Updated by 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) updated by 6818. It incorporates the most common X.520 attributes, for any type of name within the certificate
- 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 updates RFC 3370 - RFC 2630
- RFC 6712 Internet X.509 Public Key Infrastructure - HTTP Transfer for the Certificate Management Protocol (CMP), updates RFC 4210 - RFC 2510
- ETSI EN 319 411-2 (supersedes 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.

Standards and Standards ANF AC	Ref. DT_Normas y Standards.pdf	Version: 1.3
	OID: 1.3.6.1.4.1.18332.101.80.8	Page 4 of 12

- ETSI TS 101 733, CADES (CMS Advanced Electronic Signatures)
- ETSI EN 319 421 (replaces TS 101 861) Time Stamping Profile
- ETSI TS 101 862 (Qualified Certificate Profile). It is defined in the standards 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 (replaces 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 (defined by the EN 319 412-2 standard)
- ETSI TS 103 171, v.2.1.1., Electronic Signatures and Infrastructures (ESI); XAdES Baseline profile. Defines the profile of XAdES signatures suitable for use within the scope of the European Services Directive, by the national authorities of the EU member states.
- ETSI TS 103 172, v.2.1.1., Electronic Signatures and Infrastructures (ESI); PAdES Baseline profile. It defines a profile of PAdES signatures (advanced signatures for PDF documents) suitable for use within the scope of the European Directive on Services, by the national authorities of the EU member states.
- ETSI TS 103 173, v.2.1.1., Electronic Signatures and Infrastructures (ESI); CADES Baseline profile. It defines a profile of CADES signatures (advanced signatures built on CMS signatures) suitable to be used within the scope of the European Directive on Services, by the national authorities of the EU member states.
- 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. Defines an ASiC container profile (Associated Signatures Container: container that encompasses in a single package a set of electronic documents and a set of XAdES or CADES electronic signatures on one, several or all documents) convenient to be used in the field of European Directive on Services, by the national authorities of the EU member states.

- 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

Standards and Standards ANF AC	Ref. DT_Normas y Standards.pdf	Version: 1.3
	OID: 1.3.6.1.4.1.18332.101.80.8	Page 5 of 12

- 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. According to this recommendation, the name contained in the Subject Name takes the form of a Distinguished Name.
- 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. For element encoding (alpha-2 code elements)
- ISO 4217. For coding values as currency.
- ISO / IEC 9594-8 / ITU-T X.509.
- ISO IEC 18014, Time-stamping services is an international standard that specifies time-stamping techniques.

ANF AC's electronic time stamping service can be adapted to the American National Standard X9.95-2005 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. It is defined in the EN 14169 standard and passes to the EN 19211 standard Secure signature creation devices "EAL 4+"... Protection profiles for secure devices from signature creation. (EN 66211)

Standards and Standards ANF AC	Ref. DT_Normas y Standards.pdf	Version: 1.3
	OID: 1.3.6.1.4.1.18332.101.80.8	Page 6 of 12

2. EU and Spain Legal Framework

REGULATION (EU) 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of July 23, 2014, on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93 / EC.

Commission Implementing Decision (EU) 2015/1505 of September 8, 2015 establishing the technical specifications and formats related to trust lists in accordance with article 22, paragraph 5, of Regulation (EU) No. 910/2014 of the European Parliament and of the Council, regarding electronic identification and trust services for electronic transactions in the internal market.

Annex of the **Commission Implementing Regulation (EU) 2015/1501 of September 8, 2015** on the interoperability framework in accordance with Article 12 (8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council, on electronic identification and trust services for electronic transactions in the internal market.

Commission Implementing Regulation (EU) 2015/1502 of September 8, 2015 on the setting of minimum technical specifications and procedures for the security levels of electronic identification means in accordance with the provisions of Article 8 (3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council, regarding to electronic identification and trust services for electronic transactions in the internal market.

Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016, concerning the protection of natural persons with regard to the processing of personal data and the free circulation of these data and by which Directive 95/46 / EC is repealed

Directive (EU) 2016/680 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data by the competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offenses or the execution of sanctions criminal law, and the free circulation of said data and repealing the Framework Decision 2008/977 / JHA of the Council.

Directive (EU) 2009/136 / EC of the European Parliament and of the Council of November 25, 2009 amending Directive 2002/22 / EC on universal service and user rights in relation to electronic communications networks and services, Directive 2002/58 / EC on the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation in the field of consumer protection.

Directive 2006/24 / EC, of the European Parliament and of the Council of March 15, 2006, on the conservation of data generated or processed in relation to the provision of public access electronic communications services or public communications networks and amending Directive 2002/58 / CE.

Directive 2004/82 / EC, of the Council of April 29, 2004, on the obligation of carriers to communicate the data of the people transported.

Directive 2002/58 / EC of the European Parliament and of the Council of July 12, 2002, regarding the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

Directive 2000/31 / EC, of the European Parliament and of the Council, of June 8, 2000, on certain legal aspects of information society services, in particular electronic commerce in the internal market (Directive on electronic commerce).

Standards and Standards ANF AC	Ref. DT_Normas y Standards.pdf	Version: 1.3
	OID: 1.3.6.1.4.1.18332.101.80.8	Page 7 of 12

BOARD DECISION of September 13, 2004 adopting the implementing rules for Regulation (EC) No 45/2001 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by Community institutions and bodies and the free circulation of these data.

Law 59/2003, of Electronic Signature of December 19, This Law regulates the electronic signature, its legal effectiveness and the provision of certification services.

Royal Legislative Decree 1/1996 Intellectual Property Law.

According to this Law, the intellectual property of a literary, artistic or scientific work corresponds to the author by the sole fact of its creation.

Law 11/2007 on Electronic Access for Citizens to Public Services

This law recognizes the right of citizens to interact with Public Administrations by electronic means. In addition, it regulates the basic aspects of the use of information technologies in administrative activity, in relations between Public Administrations, as well as in the relations of citizens with them.

Organic Law 15/1999, of December 13, Protection of Personal Data, aims to guarantee and protect, with regard to the processing of personal data, public freedoms and the fundamental rights of individuals, and especially their honor and personal privacy and family

Royal Decree 1720/2007, of December 21, which approves the Regulations for the development of Organic Law 15/1999, of December 13, on the protection of personal data

Law 25/2007, of October 18, of conservation of data related to electronic communications and to public communications networks.

Standards and Standards ANF AC	Ref. DT_Normas y Standards.pdf	Version: 1.3
	OID: 1.3.6.1.4.1.18332.101.80.8	Page 8 of 12

3. In the Adaptation Process

Technical standards that are mandatory for the AA.PP.

ANF AC respects the [standards defined by the National Interoperability Scheme](#), and which are mandatory for the AA.PP. and that develop specific aspects of interoperability between the AA.PP. and with the citizens.

More information in the ["ENI Guide for the application of the Technical Standard for Interoperability of the Standards Catalog"](#)

ANF AC is in the process of adapting:

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

Service	Usually	In scope	Profile / semantics
Creation, verification and validation of electronic signatures.	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
The creation, verification and validation of electronic stamps.	EN 319 401	EN 319 411-1 EN 319 411-2	EN 319 412-3
The creation, verification and validation of electronic time stamps.	EN 319 401	EN 319 421	EN 319 422
The creation, verification and validation of certificates for site authentication EN 319 401 Web		EN 319 411-1 EN 319 411-2	EN 319 412-4

EN standards "Secure electronic signature creation devices" SSCD

COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of April 25, 2016

EN 419 211 - Protection profiles for secure signature creation device, Parts 1 to 6 - if applicable - listed below:

- EN 419211-1: 2014 - Protection profiles for secure signature creation device - Part 1: Overview.
- EN 419211-2: 2013 - Protection profiles for secure signature creation device - Part 2: Device

Standards and Standards ANF AC	Ref. DT_Normas y Standards.pdf	Version: 1.3
	OID: 1.3.6.1.4.1.18332.101.80.8	Page 9 of 12

- with key generation (Protection profile for secure signature creation devices. Part 2: Device with key generation).
- EN 419211-3: 2013 - Protection profiles for secure signature creation device - Part 3: Device with key import.
- 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. Part 4: Extension for the device with key generation and trusted communication with certificate generation application).
- 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. Part 5: Device with key generation and trusted communication with signature creation application).
- 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. Part 6: Device with import of keys and trusted communication with signature creation application).

Standards and Standards ANF AC	Ref. DT_Normas y Standards.pdf	Version: 1.3
	OID: 1.3.6.1.4.1.18332.101.80.8	Page 10 of 12

4. Other Standards of European Reference Interest

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

It is the first European Accessibility standard for Information and Communication Technology (ICT) products and services.

Section 9 of the EN 301 549 standard refers to the accessibility requirements that apply to web content. **All A and AA level WCAG 2.0** (are included in the ISO standard: ISO / IEC 40500 (2012): "[Information technology - W3C Web Content Accessibility Guidelines \(WCAG\) 2.0](#)"). In fact, the [EN 301 549 includes on its download page](#) a ZIP file with the WCAGs 2.0 in PDF format.

Section 10 refers to accessibility requirements in documents and section 11 to software accessibility requirements, but there are others, for example those relating to hardware.

The [Annex B](#) where a table is included with all the accessibility requirements of the standard expressed in terms of functional performance (distinguishing primary and secondary relationships).

More information in the Loïc Martínez Normand edition: "[Prototype of EN 301 549 Decision tree](#)" and his presentation on how to apply them in mobile applications: [European mobile app accessibility requirements](#)

EN 319 403 (replaces TS 119 403): "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers "Standard for the certification of Electronic Trust Service Providers.

Standards and Standards ANF AC	Ref. DT_Normas y Standards.pdf	Version: 1.3
	OID: 1.3.6.1.4.1.18332.101.80.8	Page 11 of 12

5. Certifications of Conformity

5.1 PKI

- ISO 9001: 2008 Quality Management System.
- ISO 27001 (Information technology - Security techniques - Information security management systems - Requirements) . Standard for information security.
- WebTrust
- WebTrust SSL
- WebTrust EV SSL

5.2 Electronic Signature Devices and Components

The keys of the Certification Entities will be generated in cryptographic hardware that complies with the FIPS 140-2 Level 3 (or higher) standard, or Common Criteria ISO 15408 EAL 4+ (or higher).

The end users' recognized electronic signature keys, in HSM devices, will be generated and are contained in cryptographic devices that comply with FIPS 140-2 Level 3 (or higher), or Common Criteria ISO 15408 EAL 4+ (or higher).

Standards and Standards ANF AC	Ref. DT_Normas y Standards.pdf	Version: 1.3
	OID: 1.3.6.1.4.1.18332.101.80.8	Page 12 of 12