Norms and Standards respected by ANF AC

AUTORIDAD DE CERTIFICACIÓN ANF-AC CERTIFICATION AUTHORITY	*This specification has been prepared by ANF AC to release third parties.*	**SECURITY LEVEL** PUBLIC DOCUMENT

BASIC INFORMATION OF THE DOCUMENT	
Type	Control document
Name of the document	Norms and Standards ANF AC
Version	1.5
Responsible for the audit of the document	A. Díaz G. García
File name	DT_OID_ANFAC
Creation date	12.01.2001
Last modification	17.03.2017
Status	Approved
Approval date	17.03.2017
Approved by	F. Díaz - CEO - ANF Autoridad de Certificación

Index

1 Recommendations and Techincal Standards

- 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. Defines the profile of convenient XAdES signatures to be used 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. Defines a profile of PAdES signatures (advanced signatures for PDF documents) suitable for use within the scope of the European Services Directive, 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. Defines a profile of CAdES signatures (advanced signatures built on CMS signatures) suitable for use within the scope of the European Services Directive, 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 includes in a single package a set of electronic documents and a set of electronic signatures XAdES or CAdES on one, several or all documents) suitable for use in the field of European Services Directive, 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

- 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 coding (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.

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

2 Legal Framework EU and Spain

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

Annex to Commission Implementing Regulation (EU) 2015/1501 of 8 September 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 , relating to electronic identification and trust services for electronic transactions in the internal market.

Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on the setting of specifications and minimum technical procedures for the security levels of electronic identification means in accordance with the provisions of Article 8, paragraph 3, 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.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data and laying repeals Directive 95/46 / EC

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 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 criminal sanctions, and the free circulation of said data and repealing Council Framework Decision 2008/977 / JHA.

Directive (EU) 2009/136 / EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22 / EC on universal service and users' rights in relation to networks and electronic communications 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 protection of electronic communications the consumers.

Directive 2006/24 / EC, of the European Parliament and of the Council of 15 March 2006, on the retention of data generated or processed in relation to the provision of electronic communications services of public access or of public communication networks and by the that Directive 2002/58 / EC is amended.

Directive 2004/82 / CE, of the Council of April 29, 2004, on the obligation of carriers to communicate the data of the persons transported

Directive 2002/58 / EC of the European Parliament and of the Council of 12 July 2002 on 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 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce in the internal market (Directive on trade electronic).

COUNCIL DECISION of 13 September 2004 laying down detailed rules for the implementation of 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 the institutions and community bodies and the free circulation of these data

3 In Process of Adaptation

Technical standards that are mandatory to be met by the Public Administrations.

ANF AC respects the norms defined by the National Interoperability Scheme, and that are mandatory by the Public Administrations and that they develop concrete aspects of the interoperability between the Public Administrations and with citizens.

More information in the "ENI Guide for the Application of the Technical Standard of Interoperability of the Catalog of Standards"

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	EN general	EN of 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 the authentication of websites	EN 319 401	EN 319 411-1 EN 319 411-2	EN 319 412-4

Norms EN "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 — where appropriate — 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 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.

— 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.

— 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.

4 Other Standards of Interest of European Reference

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

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

Section 9 of standard EN 301 549 refers to the accessibility requirements that apply to web content. All of level A and AA of the 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, EN 301 549 includes in its download page a ZIP file with WCAG 2.0 in PDF format.

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

Annex B which includes a table with all the accessibility requirements of the standard expressed in terms of functional performance (distinguishing primary and secondary relations

More information in the edition of Loïc Martínez Normand: "Prototype of EN 301 549 Decision tree" and its presentation on how to apply them in mobile applications: European requirements for accessibility of mobile applications

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.

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