NORMS AND STANDARDS FOLLOWED BY THE PKI OF ANF AC

	This document has been prepared by ANF AC to liberated third parties.	**SECURITY LEVEL** PUBLIC DOCUMENT

BASIC INFORMATION OF THE DOCUMENT	
Type	Control Document
Name of the Document	Norms y Standards of ANF AC
Version	1.0
Responsible of the auditing of the document	E. Mata
File Name	Norms and Standards
Date of Creation	01.06.2016
Last Modification	01.09.2016
Status	Approved
Date of approval	01.06.2016
Approved by	F. Diaz - CEO - ANF AC MALTA

Index

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). Outlines the use of the most common X.520 attributes, for its application in the names inside 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 name in the certificate.

- IETF RFC 5652 Cryptographic Message Syntax (CMS)

- IETF RFC 6960 (Online Certificate Status Protocol – (OCSP))

- IETF RFC 6960 - 6277 X.509 Internet Public Key Infrastructure 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), actualiza RFC 4210 – RFC 2510

- ETSI TS 101 456 Electronic Signatures and Infrastructure (ESI) (Policy requirements for Certification Authorities issuing 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 TS 101 861 Time Stamping Profile

- ETSI TS 101 862 (Qualified Certificate Profile). It is defined in the EN 319 412-1, EN 319 412-5 standards.

- 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 TS 102 042 Electronic Signatures and Infrastructures (ESI); 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 (it is defined in the EN 319 412-2 standard).

- ETSI TS 103 171, v.2.1.1., Electronic Signatures and Infrastructures (ESI); XAdES Baseline profile. It defines a suitable XAdES signature profile to be used in the scope of the European Services Directive, by the national authorities of the Member States of the EU.

- ETSI TS 103 172, v.2.1.1., Electronic Signatures and Infrastructures (ESI); XAdES Baseline profile. It defines a suitable PAdES signature profile (advanced signatures built over CMS signatures) to be used in the scope of the European Services Directive, by the national authorities of the Member States of the EU.

- ETSI TS 103 173, v.2.1.1., Electronic Signatures and Infrastructures (ESI); CAdES Baseline profile. It defines a suitable CAdES signature profile (advanced signatures built over CMS signatures) to be used in the scope of the European Services Directive, by the national authorities of the Member States of the EU.

- 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 a suitable ASiC profile container (Associated Signatures Container: container that includes in one package a set of electronic documents and a set of XAdES or CAdES electronic signatures in one, several or all documents) to be used in the scope of the European Services Directive, by the national authorities of the Member States of the EU.

- 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.

- 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. In accordance to this recommendation the name contained in the Subject Name adopts 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 coding elements (alpha-2 code elements).

- ISO 4217 for encoding 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 X9.95-2005 standard of the 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 EN 14169 standard and passes to the EN18211 standard, secure signature creation devices “EAL4+”… Protection profiles for secure signature creation devices (EN 66211).

2 Legal Framework of EU and Malta

REGULATION (EU) No 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 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(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 of the COMMISSION IMPLEMENTING REGULATION (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to 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 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(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 on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

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 competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the

execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

DIRECTIVE 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 relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws

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 connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

COUNCIL DIRECTIVE 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data

DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2002 concerning 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 electronic commerce)

COUNCIL DECISION of 13 September 2004 adopting implementing rules concerning Regulation (EC) No 45/2001 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data

CHAPTER 426 ELECTRONIC COMMERCE ACT. AN ACT to provide in relation to electronic commerce and to provide for matters connected therewith or ancillary thereto. 10th May 2002.

CHAPTER 440 DATA PROTECTION ACT. To make provision for the protection of individuals against the violation of their privacy by the processing of personal data and for matters connected therewith or ancillary thereto. 22nd March 2002.

SUBSIDIARY LEGISLATION 440.01. PROCESSING OF PERSONAL DATA (ELECTRONIC COMMUNICATIONS SECTOR) REGULATIONS. 15th July 2003

3 In Process of Adaptation

ANF AC is currently in the process of adapting to the following standards:

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 range	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
Creation, verification and validation of electronic seals	EN 319 401	EN 319 411-1 EN 319 411-2	EN 319 412-3
Creation, verification and validation of electronic timestamps	EN 319 401	EN 319 421	EN 319 422
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

4 Other European Reference Standards of Interest.

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

This is the first Accessibility European standard for products and services of Information and Communications Technology (ICT).

Paragraph 9 of the EN 301 549 refers to the accessibility requirements that apply to web content. All A and AA level of WCAG 2.0 (they 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

Paragraph 10 refers to the accessibility requirements in documents and paragraph 11 to the accessibility requirements of the software, but there are others, such as those relating to the hardware.

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

EN 319 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers". Certifications standard for Trust Service Providers.

5 Conformity Certifications

5.1 Presentation

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

5.2 Electronic Signature Creation Devices

The keys of the Certification Entity are generated in cryptographic hardware that meets the standard FIPS 140-2 Level 3 (or higher) , or Common Criteria ISO 15408 EAL 4+ (or superior).

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