Bugzilla ID: 555156
Bugzilla Summary: Add ANF root certificate

CAs wishing to have their certificates included in Mozilla products must

1) Comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/)
2) Supply all of the information listed in http://wiki.mozilla.org/CA:Information_checklist.
    a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
    b. Review the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic_Practices

General information about the CA's associated organization

CA Company Name	ANF Autoridad de Certificación
Website URL	http://www.anf.es
Organizational type	Enterprises or government agencies and employees of these entities.
Primark Market / Customer Base	Private Corporation
Impact to Mozilla Users	ANF Autoridad de Certificación is currently approved by the public administration to issue qualified certificates in the European Union and Ecuador, Panamá and Rumania, so Mozilla users in these areas will improve their user experience when relating with government or with other citizens using Mozilla applications.
Inclusion in other major browsers	Yes, Internet Explorer.
CA Contact Information	CA Email Alias: info@anf.es CA Phone Number: 00 34 93 393 59 46 Title / Department: ANF Autoridad de Certificación

Technical information about each root certificate

Certificate Name	ANF Global Root CA
Certificate Issuer Field	CN = ANF Global Root CA O = ANF Autoridad de Certificacion
Certificate Summary	This root has four internal fully-operated subordinate CAs which sign end-entity certificates for individuals and organizations.
Root Cert URL	http://www.anf.es/es/certificates_download/ANF_Global_Root_CA_SHA256.cer
SHA1 Fingerprint	26:CA:FF:09:A7:AF:BA:E9:68:10:CF:FF:82:1A:94:32:6D:28:45:AA
Valid From	2013-06-10
Valid To	2033-06-05
Certificate Version	3
Certificate Signature Algorithm	SHA256RSA
Signing key parameters	Modulus length: 4096 bits
Test Website URL (SSL)	https://kerberosns.com/cloud
CRL URL	For intermediate CAs: https://www.anf.es/crl/ANF_Global_Root_CA_arl.crl (Next update in 30 days)

	For end-entity certs: https://crl.anf.es/crl/ANF_High_Assurance_EV_CA1_SHA256.crl (Next update in 7 days) https://crl.anf.es/crl/ANF_High_Assurance_AP_CA1_SHA256.crl (Next update in 7 days) https://crl.anf.es/crl/ANF_Global_CA1_SHA256.crl (Next update in 7 days) https://crl.anf.es/crl/ANF_Assured_ID_CA1_SHA256.crl (Next update in 7 days) ANF Autoridad de Certificación CPS, section 4.9.6 Frequency of publication of certificate revocation lists (CRLs and ARLs) ANF AC publishes a weekly CRL.
OCSP URL (Required now)	https://ocsp.anf.es/spain/AV The time elapsing from the revocation of an end entity or CA certificate until OCSP responders are updated to reflect that revocation is immediately
Requested Trust Bits	Websites (SSL/TLS)
SSL Validation Type	DV, OV, EV
EV Policy OID(s)	1.3.6.1.4.1.18332.55.1.1.2.12 1.3.6.1.4.1.18332.55.1.1.2.22 1.3.6.1.4.1.18332.55.1.1.5.12 1.3.6.1.4.1.18332.55.1.1.5.22 1.3.6.1.4.1.18332.55.1.1.6.12 1.3.6.1.4.1.18332.55.1.1.6.22
Non-sequential serial numbers and entropy in cert	Yes.

CA Hierarchy information for each root certificate

CA Hierarchy	This root has the following internally-operated sub-CAs: • **ANF High Assurance EV CA1:** Issues technical certificates for authentication services SSL, SSL EV, Encryption and Code Signing. • **ANF High Assurance AP CA1:** Issues end-entity certificates for Public Administrations. • **ANF Global CA1:** Issues certificates for the management and administration of the PKI of ANF AC. • **ANF Assured ID CA1:** Issues end-entity in accordance with the provisions of Electronic Signature Law 59/2003.
Externally Operated SubCAs	ANF Autoridad de Certficación does not have externally operated sub-CAs, and does not plan to have them in the future.
Cross-Signing	ANF Autoridad de Certificación does not have cross-signing certificates with other CA.
Technical Constraints on Third-party Issuers	ANF Autoridad de Certificación does not have third-party issuers.

Verification Policies and Practices

Policy Documentation	Documents are in Spanish. CPS and some CPs has been translated into English. English Document repository (EN): http://www.anf.es/en/ CPS: https://anf.es/es/pdf/DPC_ANF_AC_EN.pdf CP SSL Certificates: https://anf.es/es/pdf/PC_SSL_Sede_EV_EN.pdf CP Physical Person Certificates: https://anf.es/es/pdf/PC_Clase2_PF_EN.pdf CP Legal Person Certificates: https://anf.es/es/pdf/PC_Clase2_PJ_Entidad_sin_PJ_EN.pdf Spanish Document repository (ES): http://www.anf.es/es/politicas/psc-acreditado/documentos-publicados CPS: http://anf.es/es/pdf/DPC_ANF_AC.pdf All CP Documents listed by certificate usage: http://www.anf.es/es/politicas/psc-acreditado/politicas-certificacion.html
Audits	Audit Type: WebTrust CA Auditor: DNB Auditor Website: http://www.dnbcons.com URL to Audit Report and Management's Assertions: https://cert.webtrust.org/ViewSeal?id=1625 Audit Type: WebTrust CA Extended Validation Auditor: DNB Auditor Website: http://www.dnbcons.com URL to Audit Report and Management's Assertions: https://cert.webtrust.org/ViewSeal?id=1626 Audit Type: ISO 9001 Auditor: SPG Auditor Website: http://www.certificadoiso9001.com URL to Audit Report and Management's Assertions: http://www.anf.es/es/pdf/ISO-9001.pdf Audit Type: ISO 27001 Auditor: SPG Auditor Website: http://www.certificadoiso9001.com URL to Audit Report and Management's Assertions: http://www.anf.es/es/pdf/ISO-27001.pdf
Baseline Requirements (SSL)	CP SSL Certificates, section 1 Introduction. This document indicates the policies ANF AC employs to meet the requirements of the "Guidelines for the Issuance and Management of Extended Validation Certificates" published by the CA/Browser Forum. ANF AC always conforms to the latest version of the EV SSL Certificate Guidelines published by the CA/Browser Forum and, in case of incompatibility, the Guidelines override this document. The Timestamping processes employeed conform to standards IETF RFC 3161, ANSI X9.95, ETSI 102 023, and ETSI 101 861.
SSL Verification Procedures	CP SSL Certificates, section 4.2.2.1:

	The IRM shall check the documentation by consulting the whois database, verifying that the domain is registered, by consulting valid registrars. A copy of the whois query is attached to the validation act.
Email Address Verification Procedures	Not applicable.
Code Signing Subscriber Verification Procedures	Not applicable.
Multi-factor Authentication	CPS , section 6.2.2: In order to use the CA private keys, it is necessary the approval of at least two operators authorized by the PKI Governing Board.
Network Security	CPS , section 6.7: Access to different ANF AC networks is limited to authorized persons. Specifically: • Checks are implemented to protect the internal network of external domains accessible by third parties. Firewalls are configured to prevent access and protocols which are not necessary to normal operations. • Sensitive data are encrypted when transferred through non-secure networks (including subscriber registration information). • It is guaranteed that local network components are located in secure environments as well as period auditing of all configurations.

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)

Publicly Available CP and CPS	Our practices don't differ from this recommended practice.
CA Hierarchy	Our practices don't differ from this recommended practice.
Audit Criteria	Our practices don't differ from this recommended practice.
Document Handling of IDNs in CP/CPS	Our practices don't differ from this recommended practice.
Revocation of Compromised Certificates	Our practices don't differ from this recommended practice.
Verifying Domain Name Ownership	Our practices don't differ from this recommended practice.
Verifying Email Address Control	Not include Requested Trust Bits Email (S/MIME)
Verifying Identity of Code Signing Certificate Subscriber	Not include Requested Trust Bits Code (Code Signing)
DNS names go in SAN	Our practices don't differ from this recommended practice.
Domain owned by a Natural Person	Our practices don't differ from this recommended practice.
OCSP	Our practices don't differ from this recommended practice.

Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)

Long-lived DV certificates	The ANF certificates for end entitiy has a máximum duration of two years (24 months).
Wildcard DV SSL certificates	Issuance of wildcard certificates is not allowed. SSL CP section 4.10.
Email Address Prefixes for DV Certs	ANF AC limits the set of email verification addresses to the following:

	• admin @ domain • administrador @ domain • webmaster @ domain • hostmaster @ domain • postmaster @ domain as well as any address appearing in the technical or administrative contact field of the "Whois" domain, regardless of the domains of the addresses. *SSL CP section 4.10.*
Delegation of Domain / Email validation to third parties	E-mail addresses inscribed in "Whois" are directly validated, avoiding the delegation of identification tasks to others. SSL CP section 4.10
Issuing end entity certificates directly from roots	SSL certificates are directly issued from an intermediate authority, so the private root key is not compromised. SSL CP section 4.10.
Allowing external entities to operate subordinate CAs	Certificates for intemediate CAs are directly and exclusively managed by ANF Autoridad de Certificación, which in no case assigns this task to external entities. SSL CP section 4.10.
Distributing generated private keys in PKCS#12 files	The user generates its own private keys. SSL CP section 4.10.
Certificates referencing hostnames or private IP addresses	SSL certificates are only issued to domains that can be resolved and are public, avoiding the issuance of certificates t private IPs that may use the certificates for an organization or local network and to domains that cannot be resolved by DNS. SSL CP section 4.10.
Issuing SSL Certificates for Internal Domains	SSL certificates are only issued to domains that can be resolved and are public, avoiding the issuance of certificates t private IPs that may use the certificates for an organization or local network and to domains that cannot be resolved by DNS. SSL CP section 4.10.
OCSP Responses signed by a certificate under a different root	Responder certificates are issued with the same certificate that issued the certificate being queried.
CRL with critical CIDP Extension	No "partitioned" CRLs are issued.
Generic names for CAs	In CAs, the CN attribute clearly defines the belonging of a CA to ANF Autoridad de Certificación. Besides, the OU attribute defines if a CA is an intermediate authority.
Lack of Communication With End Users	CPS, Section 1.5.1

	ANF Autoridad de Certificación contact details are included.