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	Private Corporation
Primark Market / Customer Base	Enterprises or government agencies and employees of these entities.
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	Internet Explorer
CA Contact Information	CA Email Alias: info@anf.es CA Phone Number: 00 34 93 393 06 94 Title / Department: ANF Autoridad de Certificación

Technical information about each root certificate

Certificate Name	ANF Server CA
Certificate Issuer Field	CN = ANF Server CA Object Identifier (2 5 4 5) = G63287510 OU = ANF Clase 1 CA O = ANF Autoridad de Certificación L = Barcelona (see current address at https://www.anf.es/address/) ST = Barcelona C = ES
Certificate Summary	This root has six internally-operated subordinate CAs which sign end-entity certificates for individuals and organizations.
Root Cert URL	http://www.anf.es/es/certificates_download/ANF_Server_CA.cer
SHA1 Fingerprint	CE:A9:89:0D:85:D8:07:53:A6:26:28:6C:DA:D7:8C:B5:66:D7:0C:F2
Valid From	2009-11-30
Valid To	2021-11-30
Certificate Version	3
Certificate Signature Algorithm	PKCS #1 SHA-1 With RSA Encryption

Signing key parameters	2048
Test Website URL (SSL)	For testing purposes, please provide a URL to a website whose SSL cert chains up to this root. Note that this can be a test site.
CRL URL	https://www.anf.es/AC/ANFServerCA.crl (Next update in 7 days) CPS, section 4.9.7: ANF AC will publish new CRLs at intervals no greater than 7 days
OCSP URL (Required now)	http://www.anf.es/AC/RC/ocsp
Requested Trust Bits	Websites (SSL/TLS)
SSL Validation Type	DV, OV
EV Policy OID(s)	Not requesting EV enablement at this time.
Non-sequential serial numbers and entropy in cert	end-entity certificates contain at least 20 bits of unpredictable random data

CA Hierarchy information for each root certificate

CA Hierarchy	This root has the following internally-operated sub-CAs: - ANF EC 1: Issues end entity certificates for Ecuador. - ANF Cripto SubCA1: This CA no longer issues certificates (CRL signing only). - ANF Clase SubCA1: Issues end entity certificates. - ANF High Assurance EV CA1: This CA no longer issues certificates (CRL signing only). - ANF SSL Sede CA1: Issues SSL certificates. - ANF TSA CA: Issues TSU certificates.
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	Document Repository (English): http://www.anf.es/en/ CPS (English): https://www.anf.es/es/pdf/DPC_ANF_AC_EN.pdf SSL CP (English): https://www.anf.es/es/pdf/PC_SSL_Sede_EV_EN.pdf Document Repository (Spanish): http://www.anf.es/es/politicas/psc-acreditado/documentos-publicados CPS (Spanish): http://www.anf.es/es/pdf/DPC_ANF_AC.pdf SSL CP (Spanish): http://www.anf.es/es/pdf/PC_SSL_Sede_EV.pdf
Audits	Audit Type: WebTrust CA Auditor: DNB, http://www.dnbcons.com Audit Report: https://cert.webtrust.org/SealFile?seal=1449&file=pdf (2013.01.31) Please note that the next audit must include a BR Audit. https://wiki.mozilla.org/CA:CertificatePolicyV2.1#Audit_Criteria

Baseline Requirements (SSL)	Please see the Baseline Requirements (https://www.cabforum.org/documents.html), section 8.3. I see the info about the EV guidelines, but not the Baseline Requirements.
Organization Verification Procedures	SSL CP, section 4.1 Applicants must complete the Application Form of the certificate by taking responsibility for the accuracy of the information listed, and submit it to ANF AC using any of the following means: a) Electronically: the https://www.anf.es website includes an application form that should be filled and **electronically signed with a qualified certificate**, according to Electronic Signature Law 59/2003. The certificate used must have been issued by a Registration Authority recognized by ANF AC. b) In person: the applicant may appear before a Recognized Registration Authority, and shall duly complete and sign the application form. c) By mail: the applicant may submit the application form to the offices of ANF AC certificate, **having duly completed and authenticated his signature before a Collaborating Registration Authority.** SSL CP, section 4.2.1: Performing identification and authentication functions.
SSL Verification Procedures	SSL CP, section 4.2.2: The Issuance Reports Manager (IRM) assumes the final response assumes the ultimate responsibility to verify the information contained in the Application Form, and to assess the adequacy of the documents provided and of the application, in accordance with the provisions of this Certification Policy. SSL CP, 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. Is the IRM always an employee of ANF? Where is it documented who an IRM can be for issuance of SSL certs?
Email Address Verification Procedures	Not applicable. Not requesting the email trust bit.
Code Signing Subscriber Verification Procedures	Not applicable. Not requesting the code signing trust bit.
Multi-factor Authentication	CPS , section 6.2.2: The use of the private key of the CA requires the approval of at least two operators authorized by the Governing Board of the PKI. Actually, this item is about the person approving/issuing SSL certificates. The purpose is in case the IRM's computer gets compromised; the perpetrator will not be able to issue SSL certs. Baseline Requirements (https://www.cabforum.org/documents.html), section 16.5: "The CA SHALL enforce multi-factor authentication for all accounts capable of directly causing certificate issuance."
Network Security	CPS, section 6: Technical security controls CPS, section 6.7: Network security controls

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

Publicly Available CP and CPS	Yes. See above.
CA Hierarchy	Yes. See above.
Audit Criteria	Yes. See above.
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	Yes. See above.
Verifying Email Address Control	Not applicable. Not requesting email trust bit.
Verifying Identity of Code Signing Certificate Subscriber	Not applicable. Not requesting code signing trust bit.
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	SSL CP section 4.10: ANF AC has as a good practice to NOT issue certificates that can be used as wildcard domains.
Email Address Prefixes for DV Certs	SSL CP section 4.10: 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.
Delegation of Domain / Email validation to third parties	SSL CP section 4.10: ANF AC directly validates the identification of e-mail address in the whois, avoiding the delegation to third identification.
Issuing end entity certificates directly from roots	Root does not sing end-entity certs for customers. See hierarchy above.
Allowing external entities to operate subordinate CAs	SSL CP section 4.10: Subordinate CA certificates issued by ANF AC, are managed directly and exclusively by ANF AC, who in no case allows its operation by external entities.
Distributing generated private keys in PKCS#12 files	SSL CP section 4.1: ANF AC does not generate the keys of its users. The applicant must generate his/her own key pair and certificate request in PKCS#10 /CSR format, using in this process a device approved by ANF AC, together with the application form.
Certificates referencing hostnames or private IP addresses	SSL CP section 4.10: ANF AC only issues SSL certificates to public domains that can be resolved on the Internet, avoiding the issue of certificates to private IP can use the certificates for an organization or

	home network and domains that can not be resolved by DNS.
Issuing SSL Certificates for Internal Domains	SSL CP section 4.10: ANF AC only issues SSL certificates to public domains that can be resolved on the Internet, avoiding the issue of certificates to private IP can use the certificates for an organization or home network and domains that can not be resolved by DNS.
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	ANF in Issuer CN and O.
Lack of Communication With End Users	CPS, Section 1.5.1: ANF Autoridad de Certificación contact details are included.