Bugzilla ID:
Bugzilla Summary:

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 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 O = ANF Autoridad de Certificación
Certificate Summary	This root has six internal ly-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	2009-12-01
Valid To	2021-12-01
Certificate Version	3
Certificate Signature Algorithm	SHA1RSA
Signing key parameters	Modulus length: 2048 bits
Test Website URL (SSL) Example Certificate (non-SSL)	Pending Pending
CRL URL	https://www.anf.es/AC/ANFServerCA.crl (Next update in 7 days) ANF Autoridad de Certificación CPS, section 4.9.6 Frequency of issue of CRLs:

	ANF AC shall publish a new CRL at maximum interval of one week.
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 EV
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 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	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=1449

	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=1451 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 3.2.4: ANF AC shall check the documentation by consulting the "Whois" database, and shall verify that the domain is registered consulting valid records. A copy of the whois query will be attached to the validation act.
Organization Verification Procedures	CP SSL Certificates, section 3.2.3: The request must be made in person by the legal representative of the organization that requests the issuance of the the certificate, before a Registration Authority authorized by ANF AC. Original identity documentation must be showed, including at least: - ID Card or passport for nationals. In the case of legal persons: - Tax Identification. The Registration Authority obtains, through its electronic signature, a certified digital copy of all the original documents that the applicant has submitted for identification. All parties (registration authority, applicant and legal representative) sign in manuscript form the Contract for the Provision of Electronic Certification Services. ANF AC shall verify through official records that the organization is legally established and in full operation, checking the validity of the power of attorney used by the person requesting the certificate.
Email Address Verification Procedures	

Code Signing Subscriber Verification Procedures	
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.
Network Security	CPS , section 6.7: Access to internal ANF AC networks is limited to authorized personnel. In particular: • Controls are implemented to protect the internal network from external domains accessible by third parties. Firewalls are configured so as to prevent access and protocols that are not required for service operations. • Sensitive data is encrypted when exchanged over unsecured networks (including such data as subscriber registration). It is ensured that local network components are located in secure environments, and their settings periodically audited.

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.