Bugzilla ID: 555156
Bugzilla Summary: Add ANF root certificate

CAs wishing to have their certificates included in Mozilla products must comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/) and must supply the information necessary to determine whether or not the policy's requirements have been satisfied, as per http://wiki.mozilla.org/CA:Information_checklist.

CA's are also encouraged to review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices.

General Information	Data
CA Name	ANF Autoridad de Certificación
Website URL	http://www.anf.es
Organizational type.	Is this CA operated by a private or public corporation, government agency, academic institution or consortium, NGO ?
Primary market / customer base	Which types of customers does this CA serve? Are there particular vertical market segments in which it operates?
Impact to Mozilla Users	ANF Autoridad de Certificación is currently approved by the public administration to issue qualified certificates in the European Union and it is the process of being approved in other countries (Ecuador and Panama), so Mozilla users in these areas will improve their user experience when relating with government or with other citizens using Mozilla applications.
CA Contact Information	CA Email Alias: info@anf.es CA Phone Number: 00 34 932 661 614 Title / Department: ANF Autoridad de Certificación

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	Data
Certificate Name	ANF Server CA
Cert summary / comments	
The root CA certificate URL	https://bugzilla.mozilla.org/attachment.cgi?id=436519 When I manually import the root certificate into Firefox and Thunderbird, then look at the details, it shows a recursive list of "ANF Server CA" root certificates signing themselves. I've never seen this before, so I have no idea what would cause this behavior. Please test if your version of the root does this. Maybe it's a problem with the way I created the .cer file.
SHA-1 fingerprint	12:61:25:C5:7D:B7:7B:9D:A8:47:D9:0D:6C:3E:9F:8A:D0:F7:C0:1E
Valid from	2009-11-30
Valid to	2021-11-30
Cert Version	3
Modulus length	2048

Test Website	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://crl.anf.es/AC/ANFServerCA.crl When I try to manually import this CRL into Firefox, I get crl.anf.ex.443 uses an invalid security certificate (Error code: sec_error_untrusted_issuer) I should not have to import any other root (besides this root) to import the CRL. What is the nextUpdate set to in the CRLs for end-entity certificates?
OCSP Responder URL	http://www.anf.es/AC/RC/ocsp
CA Hierarchy	Please provide a list or description of subordinate CAs chaining to this root. Please indicate which are operated by the CA organization and which are operated by external third parties. Please indicate the types of certs that each sub-CA signs.
Sub-CAs Operated by 3rd parties	Does this root have any subordinate CAs that are operated by external third parties?
Cross-Signing	List any other root CAs that have issued cross-signing certificates for this root CA
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type DV, OV, and/or EV	Do you perform identity/organization verification for all SSL certificates? Is it ever the case for SSL certs that the ownership of the domain name is verified, but the identity/organization of the subscriber is not verified?
EV policy OID(s)	Not requesting EV enablement
CP/CPS	Certification Practice Statement pointer in root: https://www.anf.es/AC/documentos/ I have imported this root, but I still cannot access the https://www.anf.es website. ANF Certificate Practice Statements: http://www1.anf.es/anf/certificacion/certificados-electonicos/anf-ac/200.1.6.html Declaration of Practices (DPC) for this root (ANF Server CA): http://www.anf.es/anf/ssl/pdf/DPC_ANF_Server_CA_1.3.6.1.4.1.18332.1.9_v_1.0.pdf DPC is the Certification Practice Statement. Certification Policies are provided in addition to the DPC. SSL Certificates: http://www1.anf.es/anf/ssl/pdf/CPSSL.pdf Encryption Certificates: http://www1.anf.es/anf/ssl/pdf/CPEncryption.pdf Registration Authority Certificates: http://www1.anf.es/anf/ssl/pdf/CPANFAR.pdf OCSP Certificates: http://www1.anf.es/anf/ssl/pdf/CPOCSP.pdf CRL Certificates: http://www1.anf.es/anf/ssl/pdf/CPANFCRL.pdf

	Root Certs and Sub-CAs issued by ANF: http://www1.anf.es/anf/certificacion/certificados-electonicos/anf-ac/200.1.5.html I don't see this root listed on the page.
AUDIT	Please see sections 8, 9, and 10 of http://www.mozilla.org/projects/security/certs/policy/ We need a publishable statement or letter from an auditor (who meets the policy requirements) that states that they have reviewed the practices as outlined in the CP/CPS for these roots, and that the CA does indeed follow these practices and meets the requirements of one of: • ETSI TS 101 456 • ETSI TS 102 042 • WebTrust Principles and Criteria for Certification Authorities
Organization Identity Verification	Please provide translations into English of the sections of the CP/CPS documents pertaining to Verification of Identity and Organization. Please also list the documents and section or page numbers where the original text can be found.
Domain Name Ownership / Control	section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: • for a certificate to be used for SSL-enabled servers, the CA takes reasonable measures to verify that the entity submitting the certificate signing request has registered the domain(s) referenced in the certificate *or* has been authorized by the domain registrant to act on the registrant's behalf; Please provide translations into English of the sections of the CP/CPS documents that describe the procedures for verifying that the domain referenced in an SSL cert is owned/controlled by the subscriber. Please also list the corresponding document(s) and section or page numbers containing the original text. Please provide the specific document(s) and section or page numbers where the procedures are described for verifying that the domain referenced in an SSL cert is owned/controlled by the subscriber. All documents supplied as evidence should be publicly available and must be addressed in any audit. Any substantial omissions submitted afterwards may need to be confirmed by auditor, at Mozilla's discretion.
Email Address Ownership / Control	section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: • for a certificate to be used for digitally signing and/or encrypting email messages, the CA takes reasonable measures to verify that the entity submitting the request controls the email account associated with the email address referenced in the certificate *or* has been authorized by the email account holder to act on the account holder's behalf; Please provide translations into English of the sections of the CP/CPS documents that describe the procedures for verifying that the email account associated with the email address in the cert is owned/controlled by the subscriber. Please also list the corresponding document(s) and section or page numbers containing the original

	text. Please provide the specific document(s) and section or page numbers where the procedures are described for verifying that the email account associated with the email address in the cert is owned/controlled by the subscriber. All documents supplied as evidence should be publicly available and must be addressed in any audit. Any substantial omissions submitted afterwards may need to be confirmed by auditor, at Mozilla's discretion.
Identity of Code Signing Subscriber	section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: • for certificates to be used for digitally signing code objects, the CA takes reasonable measures to verify that the entity submitting the certificate signing request is the same entity referenced in the certificate *or* has been authorized by the entity referenced in the certificate to act on that entity's behalf; Please provide translations into English of the sections of the CP/CPS documents that describe the identity verification procedures for code signing certs. Please also list the corresponding document(s) and section or page numbers containing the original text. Please provide the specific document(s) and section or page numbers where the procedures for code signing certs are described.
Potentially Problematic Practices	Please review the list of Potentially Problematic Practices (http://wiki.mozilla.org/CA:Problematic_Practices). Identify the ones that are and are not applicable. For the ones that are applicable, please provide further information and translations into English of the CP/CPS where relevant. • Long-lived DV certificates o • Wildcard DV SSL certificates o • Delegation of Domain / Email validation to third parties o • Issuing end entity certificates directly from roots o • Allowing external entities to operate unconstrained subordinate CAs o • Distributing generated private keys in PKCS#12 files o • Certificates referencing hostnames or private IP addresses o

	• Issuing SSL Certificates for Internal Domains
	  o
	• OCSP Responses signed by a certificate under a different root
	  o
	• CRL with critical CIDP Extension
	  o
	• Generic names for CAs
	  o