Print this page

Mozilla - CA Program

Case Information

Case Number	00000001	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	ANF Autoridad de Certificación	**Request Status**	Ready for Public Discussion

Additional Case Information

Subject	Include ANF root certificate	**Case Reason**	New Owner/Root inclusion requested

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=555156

General information about CA's associated organization

CA Email Alias 1	info@anf.es		
CA Email Alias 2	serviciotecnico@anf.es		
Company Website	http://www.anf.es	**Verified?**	Verified
Organizational Type	Private Corporation	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	European Union	**Verified?**	Verified
Primary Market / Customer Base	Enterprises or government agencies and employees of these entities.	**Verified?**	Verified
Impact to Mozilla Users	ANF Autoridad de Certificación (ANF AC) is a private Certification Authority, recognized and accredited by the Spanish Government as a Certificate Services Provider (CSP). ANF AC has accredited more than 1000 Registry Authorities throughout Spain to issue qualified user identity certificates. ANF CA also issues certificates for SSL with and without Extended Validation.	**Verified?**	Verified

Response to Mozilla's list of Recommended Practices

Recommended Practices	https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's list of Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Recommended Practices		**Verified?**	Verified

Response to Mozilla's list of Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org /CA:Problematic_Practices#Potentially_problematic_CA_practices	**Problematic Practices Statement**	I have reviewed Mozilla's list of Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Problematic Practices	* The ANF certificates for end entitiy has a máximum duration of two years (24 months). * SSL CP section 4.10: ANF AC has as a good practice to NOT issue certificates that can be used as wildcard domains. * 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. * SSL CP section 4.10: ANF AC directly validates the identification of e-mail address in the whois, avoiding the delegation to third identification. * 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. * 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. * 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.	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Certificate Name	ANF Global Root CA	**Root Case No**	R00000000
Request Status	Ready for Public Discussion	**Case Number**	00000001

Additional Root Case Information

Subject	Include ANF Global Root CA root cert

Technical Information about Root Certificate

O From Issuer Field	ANF Autoridad de Certificacion	**Verified?**	Verified
OU From Issuer Field	ANF Clase 1 CA	**Verified?**	Verified
Certificate Summary	This root has eight internally-operated subordinate CAs which sign end-entity certificates for individuals and organizations.	**Verified?**	Verified
Root Certificate Download URL	http://www.anf.es/es/certificates_download/ANF_Global_Root_CA_SHA256.cer	**Verified?**	Verified

Valid From	2013 Jun 10	**Verified?**	Verified
Valid To	2033 Jun 05	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-256	**Verified?**	Verified
Signing Key Parameters	4096	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://ssl.anf.es/	**Verified?**	Verified
CRL URL(s)	https://www.anf.es/crl/ANF_Global_Root_CA_arl.crl https://www.anf.es/crl/ANF_High_Assurance_EV_CA1_SHA256.crl NextUpdate for End-entity CRLs: 7 days	**Verified?**	Verified
OCSP URL(s)	http://ocsp.anf.es/spain/AV	**Verified?**	Verified
Revocation Tested	http://certificate.revocationcheck.com/ssl.anf.es	**Verified?**	Verified
Trust Bits	Websites	**Verified?**	Verified
SSL Validation Type	DV; OV; EV	**Verified?**	Verified
EV Policy OID(s)	1.3.6.1.4.1.18332.55.1.1.2.22	**Verified?**	Verified
EV Tested	// CN=ANF Global Root CA,serialNumber=G63287510,E=info@anf.es,OU=ANF Clase 1 CA,O=ANF Autoridad de Certificacion,L=Barcelona (see current address at http://www.anf.es/es/address-direccion.html),ST=Barcelona,C=ES "1.3.6.1.4.1.18332.55.1.1.2.22", "ANF EV OID", SEC_OID_UNKNOWN, { 0xE3, 0x26, 0x8F, 0x61, 0x06, 0xBA, 0x8B, 0x66, 0x5A, 0x1A, 0x96, 0x2D, 0xDE, 0xA1, 0x45, 0x9D, 0x2A, 0x46, 0x97, 0x2F, 0x1F, 0x24, 0x40, 0x32, 0x9B, 0x39, 0x0B, 0x89, 0x57, 0x49, 0xAD, 0x45 }, "MIIBCjELMAkGA1UEBhMCRVMxEjAQBgNVBAgMCUJhcmNlbG9uYTFYMFYGA1UEBwxP" "QmFyY2Vsb25hIChzZWUgY3VycmVudCBhZGRyZXNzIGF0IGh0dHA6Ly93d3cuYW5m" "LmVzL2VzL2FkZHJlc3MtZGlyZWNjaW9uLmh0bWwgKTEnMCUGA1UECgweQU5GIEF1" "dG9yaWRhZCBkZSBDZXJ0aWZpY2FjaW9uMRcwFQYDVQQLDA5BTkYgQ2xhc2UgMSBD" "QTEaMBgGCSqGSIb3DQEJARYLaW5mb0BhbmYuZXMxEjAQBgNVBAUTCUc2MzI4NzUx" "MDEbMBkGA1UEAwwSQU5GIEdsb2JhbCBSb290IENB", "AT8vMXfm", Success!	**Verified?**	Verified
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	26:CA:FF:09:A7:AF:BA:E9:68:10:CF:FF:82:1A:94:32:6D:28:45:AA	**Verified?**	Verified
SHA-256 Fingerprint	E3:26:8F:61:06:BA:8B:66:5A:1A:96:2D:DE:A1:45:9D:2A:46:97:2F:1F:24:40:32:9B:39:0B:89:57:49:AD:45	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	The “ANF Global Root CA” certificate has the following internally-operated sub-CAs: - ANF High Assurance EV CA1 (SHA1 and SHA256): Issues technical certificates for authentication services SSL, SSL EV, Encryption and Code Signing. - ANF High Assurance AP CA1 (SHA1 and SHA256): Issues end-entity certificates for Public Administrations. - ANF Global CA1 (SHA1 and SHA256): Issues certificates for the management and administration of the PKI of ANF AC. - ANF Assured ID CA1 (SHA1 and SHA256): Issues end-entity in accordance with the provisions of Electronic Signature Law 59/2003.	**Verified?**	Verified
Externally Operated SubCAs	None. None planned.	**Verified?**	Verified
Cross Signing	None. None planned.	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	According to CPS section 1.3.1.4: Issuance Report Managers (staff attached to ANF AC's Legal Department) check the documents provided by the RA, and issue the certificates.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Documents are provided in Spanish and English. Document repository (ES): http://www.anf.es/es/politicas/psc-acreditado/documentos-publicados	**Verified?**	Verified
CA Document Repository	http://www.anf.es/en/	**Verified?**	Verified
CP Doc Language	English		
CP	https://www.anf.es/es/pdf/PC_SSL_Sede_EV_EN.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://www.anf.es/es/pdf/DPC_ANF_AC_EN.pdf	**Verified?**	Verified
Other Relevant Documents	SSL CP (Spanish): http://www.anf.es/es/pdf/PC_SSL_Sede_EV.pdf Declaración de Prácticas de Certificación: http://www.anf.es/es/politicas/psc-acreditado/declaracion-practicas-certificacion.html CPS (Spanish): http://www.anf.es/es/pdf/DPC_ANF_AC.pdf	**Verified?**	Verified
Auditor Name	Auren	**Verified?**	Verified
Auditor Website	http://www.auren.com/	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified

Standard Audit	https://cert.webtrust.org/SealFile?seal=1833&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	1/26/2015	**Verified?**	Verified
BR Audit	https://cert.webtrust.org/SealFile?seal=1833&file=pdf	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	1/26/2015	**Verified?**	Verified
EV Audit	https://cert.webtrust.org/SealFile?seal=1834&file=pdf	**Verified?**	Verified
EV Audit Type	WebTrust	**Verified?**	Verified
EV Audit Statement Date	1/26/2015	**Verified?**	Verified
BR Commitment to Comply	CPS section 1	**Verified?**	Verified
SSL Verification Procedures	CPS section 1.3.1.4, Issuance Report Managers: These are staff attached to ANF AC's Legal Department, responsible for checking the documentation provided by the Registration Authorities. They determine whether the documents are sufficient or not, they check the reliability of the information, and, if they consider it necessary, order further investigations. CPS, section 5.2.1.8 Issuance reports and certificates revocation manager They are required to have worked at least one year in a related role. 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.	**Verified?**	Verified
EV SSL Verification Procedures	SSL CP section 4.2.2.3, SSL EV y and Electronic Office EV Certificates: In the process of verification of the information and documentation received, the following means may be used: - Consultation to official public records in which the entity must be registered in order to check availability, effect of charges and other legal issues such as activity and date of establishment. - Official Journals of national or regional public bodies belonging to public bodies and enterprises. - With regard to Internet addresses and domains, ANF AC consult recorders	**Verified?**	Verified

	attached only by ICANN / IANA domain names and addresses associated with the certificate. In this query, it is verified verify: -- That the holder (registrant) agrees with the subscriber. -- People and contact information associated with that domain registration. - One of the contact persons listed in the whois query shall be reached in order to verify compliance of the certificate issuance request associated with that domain.		
Organization Verification Procedures	SSL CP section 4.2.1 provides a description of the process for performing identification and authentication functions for verifying the certificate subscriber's identity, organization, and authority to request the certificate on behalf of the organization.	**Verified?**	Verified
Email Address Verification Procedures	Not requesting Email trust bit.	**Verified?**	Not Applicable
Code Signing Subscriber Verification Pro	Not requesting Code Signing trust bit	**Verified?**	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.	**Verified?**	Verified
Network Security	CPS section 6	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	http://www.anf.es/es/certificados-de-ca-intermedias.html	**Verified?**	Verified