Print this page

Mozilla - CA Program

Case Information

Case Number	00000053	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owners/Certificate Name	Autoridad de Certificacion Firmaprofesional	**Request Status**	Need Information from CA

Additional Case Information

Subject	Add Renewed Autoridad de Certificacion Firmaprofesional root certificate	**Case Reason**	

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=1102143

General information about CA's associated organization

Company Website	www.firmaprofesional.com	**Verified?**	Verified
Organizational Type	Public Corporation	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Primary Market / Customer Base	Firmaprofesional is a commercial CA in Spain that issues certificates to professional corporations, companies and other institutions.	**Verified?**	Verified
Impact to Mozilla Users	Their main activity is the generation, transmission and distribution of digital certificates through professional corporations, companies or other institutions, which act as Registration Authorities and Certification Authorities in the hierarchy of certification Firmaprofesional. Firmaprofesional has a network of more than 70 Registration Authorities located throughout Spain.	**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	Please review and respond to Mozilla's list of Recommended Practices: https://wiki.mozilla.org /CA:Recommended_Practices#CA_Recommended_Practices	**Verified?**	Need Response From CA

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	Please review and respond to Mozilla's list of Potentially Problematic Practices: https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices	**Verified?**	Need Response From CA

Root Case Record # 1

Root Case Information

Root Case No	R00000070	**Case Number**	00000053
Request Status	Need Information from CA	**Root Certificate Name**	Autoridad de Certificacion Firmaprofesional CIF A62634068

Additional Root Case Information

Subject	Add Renewed Autoridad de Certificacion Firmaprofesional CIF A62634068 root

Technical Information about Root Certificate

O From Issuer Field	Autoridad de Certificacion Firmaprofesional	**Verified?**	Verified
OU From Issuer Field		**Verified?**	Verified
Certificate Summary	Will this root eventually replace the currently include "Autoridad de Certificacion Firmaprofesional CIF A62634068" root cert? Will this root eventually have the same CA hierarchy as the old root?	**Verified?**	Need Response From CA
Root Certificate Download URL	http://crl.firmaprofesional.com/caroot256.crt	**Verified?**	Verified
Valid From	2014 Sep 23	**Verified?**	Verified
Valid To	2036 May 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	Provide test website whose SSL cert chains up to this root.	**Verified?**	Need Response From CA
CRL URL(s)	Need CRL URLs CPS Section 4.9.6: CRL for end entity certificates are issued at least every 24 hours, or when there is a reversal, with a validity of 7 days.	**Verified?**	Need Response From CA

OCSP URL(s)	Will it be http://servicios.firmaprofesional.com/ocsp for this CA hierarchy? CPS section 4.10.3: The use of OCSP services is not public and requires specific licensing. CONCERN: I don't think this meets the requirements of the CA/Browser Forum's Baseline Requirements.	**Verified?**	Need Response From CA
Trust Bits	Code; Email; Websites	**Verified?**	Need Response From CA
SSL Validation Type	OV	**Verified?**	Need Response From CA
EV Policy OID(s)	EV?	**Verified?**	Need Response From CA
EV Tested	If requesting EV treatment for this root, then provide successful output from the EV Cert Test: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version	**Verified?**	Need Response From CA
Root Stores Included In		**Verified?**	Need Response From CA
Mozilla Applied Constraints	Should Mozilla apply constraints to certain TLDs for certs issued in this CA hierarchy?	**Verified?**	Need Response From CA

Digital Fingerprint Information

SHA-1 Fingerprint	0B:BE:C2:27:22:49:CB:39:AA:DB:35:5C:53:E3:8C:AE:78:FF:B6:FE	**Verified?**	Verified
SHA-256 Fingerprint	57:DE:05:83:EF:D2:B2:6E:03:61:DA:99:DA:9D:F4:64:8D:EF:7E:E8:44:1C:3B:72:8A:FA:9B:CD:E0:F9:B2:6A	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	Please describe the planned CA Hierarchy for this root	**Verified?**	Need Response From CA
Externally Operated SubCAs	Will all subCAs in this CA hierarchy be internally operated? Are there any plans to have or allow for externally operated subCAs? It looks like the CPS allows for externally-operated subCAs, so will need to understand how they are constrained or audited/disclosed according to sections 8 through 10 of https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/inclusion/	**Verified?**	Need Response From CA
Cross Signing	Has this root been cross-signed with another root? Will it be?	**Verified?**	Need Response From CA
Technical Constraint on 3rd party Issuer	Firmaprofesional has a network of more than 70 Registration Authorities located throughout Spain. Please describe how these Registration Authorities are constrained or audited/disclosed per sections 8 through 10 of https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/inclusion/ see also https://wiki.mozilla.org/CA:CertificatePolicyV2.1#Frequently_Asked_Questions	**Verified?**	Need Response From CA

Verification Policies and Practices

Policy Documentation	http://www.firmaprofesional.com/cps Documents are in Spanish. Certain CP CPS documents translated into English. CP v6.3 Translation in progress	**Verified?**	Verified
CA Document Repository	https://www.firmaprofesional.com/esp/cps-eng-2	**Verified?**	Verified
CP Doc Language	English		
CP	https://www.firmaprofesional.com/images/pdfs/FP_CP_Gen_Servidor_Web_SSL_6.2-EN.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://www.firmaprofesional.com/images/pdfs/CPS/FP_CPS_6.1_english.pdf	**Verified?**	Verified
Other Relevant Documents		**Verified?**	Not Applicable
Auditor Name	DNB	**Verified?**	Verified
Auditor Website	http://www.dnbcons.com/	**Verified?**	Verified
Auditor Qualifications	I did not find DNB in the Webtrust list here: http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx#Spain	**Verified?**	Need Response From CA
Standard Audit	https://cert.webtrust.org/SealFile?seal=1617&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	12/20/2013	**Verified?**	Verified
BR Audit	Need	**Verified?**	Need Response From CA
BR Audit Type		**Verified?**	Need Response From CA
BR Audit Statement Date		**Verified?**	Need Response From CA
EV Audit	EV?	**Verified?**	Need Response From CA
EV Audit Type		**Verified?**	Need Response From CA
EV Audit Statement Date		**Verified?**	Need Response From CA
BR Commitment to Comply	Please carefully review this with your auditors: https://wiki.mozilla.org/CA:BaselineRequirements Also, see BRs section 8.3.	**Verified?**	Need Response From CA
SSL Verification Procedures	CPS section 3.2.5: To guarantee that an applicant entity has control over the domain (URL) which it seeks to include in a certificate, two types of checks are performed: - Organizational checks: the ownership title of the domain name is requested and is certified by a legal representative of the organization. - Technical checks: the following authenticated WHOIS services are consulted: -- For "*.es" domains: https://www.nic.es/sgnd/dominio/publicInformacionDominios.action -- For all other domains: https://www.networksolutions.com/whois/index.jsp	**Verified?**	Verified
EV SSL Verification Procedures		**Verified?**	Need Response From CA

Organization Verification Procedures	CPS section 3.2.2 - Authentication of the identity of a legal person CPS section 3.2.3 - Authentication of the identity of a natural person CPS section 3.2.4 - Authentication of the identity of the RA and the RA's operators	**Verified?**	Verified
Email Address Verification Procedures	CPS section 3.2.6: In general, the signers are people linked to the Registration Authority (for example, associates, association members, etc.). In these cases it is not the signer who requests a specific email address to be included in the certificate but the RA itself which, by consulting its database, obtains the address. In cases where the signer has no connection with the RA, verification of the e-mail address is performed using a challenge-response mechanism	**Verified?**	Verified
Code Signing Subscriber Verification Pro	It's not clear to me from the CPS how the identity and authority of the code signing certificate subscriber is verified. Please see https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Identity_of_Code_Signing_Certificate_Subscriber	**Verified?**	Need Response From CA
Multi-Factor Authentication	BR #16.5: The CA SHALL enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.	**Verified?**	Need Response From CA
Network Security	CPS section 6.	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	https://bugzilla.mozilla.org/show_bug.cgi?id=1012744 -- Is the CA hierarchy for this new root also represented here?	**Verified?**	Need Response From CA