Print this page

Mozilla - CA Program

Case Information

Case Number	00000053	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/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

CA Email Alias 1	info@firmaprofesional.com		
CA Email Alias 2			
Company Website	http://www.firmaprofesional.com/	**Verified?**	Verified
Organizational Type	Commercial Organization	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	Spain	**Verified?**	Verified
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	Root Renewal	**Verified?**	Verified

Required and Recommended Practices

Recommended Practices	https://wiki.mozilla.org/CA/Required_or_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	1. Publicly Available CP and CPS: CPS section 2.1, Server CP section 1.2 1.1 Revision Table, updated annually: CP/CPS page 2 1.2 CAA Domains listed in CP/CPS: NEED: What section is the required CAA information in? https://wiki.mozilla.org/CA/Required_or_Recommended_Practices#CAA_Domains_listed_in_CP.2FCPS 1.3 BR Commitment to Comply statement in CP/CPS: Server CP section 1.1 2. Audit Criteria: CP section 8 3. Revocation of Compromised Certificates: CPS section 4.9 4. Verifying Domain Name Ownership: Server CP section 4.1, CPS section 3.2.5 5. Verifying Email Address Control: CPS section 3.2.6 6. DNS names go in SAN: Server CP section 5.1 7. OCSP: CPS section 7.3 - OCSP SHALL NOT respond "Good" for unissued certs: 8. Network Security Controls: CPS section 6.7	**Verified?**	Need Response From CA

Forbidden and Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org/CA/Forbidden_or_Problematic_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	1. Long-lived Certificates: Server CP section 3.1 (see version published 19/07/2018) 2. Non-Standard Email Address Prefixes for Domain Ownership Validation: Server CP section 4.1 3. Issuing End Entity Certificates Directly From Roots: CPS section 1.3.2 4. Distributing Generated Private Keys in PKCS#12 Files: Server CP section 4.1 5. Certificates Referencing Local Names or Private IP Addresses: Server CP section 3.4 6. Issuing SSL Certificates for .int Domains: Server CP section 3.4 7. OCSP Responses Signed by a Certificate Under a Different Root: CPS section 7.3 8. Issuance of SHA-1 Certificates: CPS section 1.3.2.1 9. Delegation of Domain / Email Validation to Third Parties: CPS section 8.4.1	**Verified?**	Verified

Root Case Record # 1

Root Case Information

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

Certificate Data

Certificate Issuer Common Name	Autoridad de Certificacion Firmaprofesional CIF A62634068
O From Issuer Field	
OU From Issuer Field	
Valid From	2014 Sep 23
Valid To	2036 May 05
Certificate Serial Number	1B70E9D2FFAE6C71
Subject	CN=Autoridad de Certificacion Firmaprofesional CIF A62634068; OU=; O=null; C=ES
Signature Hash Algorithm	SHA256WithRSA
Public Key Algorithm	RSA 4096 bits
SHA-1 Fingerprint	0BBEC2272249CB39AADB355C53E38CAE78FFB6FE
SHA-256 Fingerprint	57DE0583EFD2B26E0361DA99DA9DF4648DEF7EE8441C3B728AFA9BCDE0F9B26A
Subject + SPKI SHA256	B5DAFFA4766010AC1693044AFF780C954BC71DBE5ABB16E3ADA0DCC6C7FE550F
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	This is the SHA-256 version of the SHA-1 "Autoridad de Certificacion Firmaprofesional CIF A62634068" root cert that was included via Bugzilla #794036. Same key pair and DN as the old root, and will have the same CA hierarchy as the old root.	**Verified?**	Verified
Root Certificate Download URL	http://crl.firmaprofesional.com/caroot256.crt	**Verified?**	Verified
CRL URL(s)	http://crl.firmaprofesional.com/fproot.crl http://crl.firmaprofesional.com/infraestructura.crl http://crl2.firmaprofesional.com/infraestructura.crl CPS section 4.9.6: valid for 7 days, issued every 24 hours.	**Verified?**	Verified
OCSP URL(s)	http://ocsp.firmaprofesional.com	**Verified?**	Verified
Mozilla Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	OV; EV	**Verified?**	Verified
Mozilla EV Policy OID(s)	1.3.6.1.4.1.13177.10.1.3.10	**Verified?**	Verified
Root Stores Included In		**Verified?**	Not Applicable
Mozilla Applied Constraints	None	**Verified?**	Not Applicable

Test Websites or Example Cert

Test Website - Valid	https://www.firmaprofesional.com	**Verified?**	Verified
Test Website - Expired	https://testexpiredsslev.firmaprofesional.com		
Test Website - Revoked	https://testrevokedsslev.firmaprofesional.com		
Example Cert			
Test Notes	Turn off trust bit of old root in order to test chain up to this new root.		

Test Results (When Requesting the SSL/TLS Trust Bit)

Revocation Tested	http://certificate.revocationcheck.com/www.firmaprofesional.com OK	**Verified?**	Verified
CA/Browser Forum Lint Test	NEED: Explain/resolve all lint test errors: https://crt.sh/?caid=430&opt=cablint,zlint,x509lint&minNotBefore=2014-01-01 https://crt.sh/?caid=994&opt=cablint,zlint,x509lint&minNotBefore=2014-01-01	**Verified?**	Need Response From CA
Test Website Lint Test	see above.	**Verified?**	Not Applicable
EV Tested	// CN=Autoridad de Certificacion Firmaprofesional CIF A62634068,C=ES "1.3.6.1.4.1.13177.10.1.3.10", "Firmaprofesional EV OID", SEC_OID_UNKNOWN, { 0x57, 0xDE, 0x05, 0x83, 0xEF, 0xD2, 0xB2, 0x6E, 0x03, 0x61, 0xDA, 0x99, 0xDA, 0x9D, 0xF4, 0x64, 0x8D, 0xEF, 0x7E, 0xE8, 0x44, 0x1C, 0x3B, 0x72, 0x8A, 0xFA, 0x9B, 0xCD, 0xE0, 0xF9, 0xB2, 0x6A }, "MFExCzAJBgNVBAYTAkVTMUIwQAYDVQQDDDlBdXRvcmlkYWQgZGUgQ2VydGlmaWNh" "Y2lvbiBGaXJtYXByb2Zlc2lvbmFsIENJRiBBNjI2MzQwNjg=", "G3Dp0v+ubHE=", Success!	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	See CPS section 1.3. The old and new roots will have the same CA Hierarchy, which is disclosed in the CCADB.	**Verified?**	Verified
Externally Operated SubCAs	See CPS section 1.3.2.2 External subCAs are allowed, but their subCA certs are operated by Firmaprofesional. "... all CAs within the Firmaprofesional Certification Hierarchy must be operated technically by Firmaprofesional, within the infrastructure of Firmaprofesional."	**Verified?**	Verified
Cross Signing	None	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	Firmaprofesional has a network of more than 70 Registration Authorities located throughout Spain. See CPS section 8.4.1	**Verified?**	Verified

https://bugzilla.mozilla.org/show_bug.cgi?id=794036#c45

Verification Policies and Practices

Policy Documentation	Documents are in Spanish, with certain CP/CPS documents translated into English.	**Verified?**	Verified
CA Document Repository	http://www.firmaprofesional.com/cps	**Verified?**	Verified
CP Doc Language	English		
CP	https://www.firmaprofesional.com/images/pdfs/CPS/FP_CP_Servidor_Web_SSL-171121-EN.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://www.firmaprofesional.com/images/pdfs/CPS/FP_CPS-171121-EN.pdf	**Verified?**	Verified
Other Relevant Documents	Current Documents in Spanish: https://www.firmaprofesional.com/images/pdfs/CPS/FP_CP_Servidor_Web_SSL-180719-ES.pdf https://www.firmaprofesional.com/images/pdfs/CPS/FP_CPS-180704-ES.pdf Historical Audit Reports: https://bugzilla.mozilla.org/show_bug.cgi?id=1412950	**Verified?**	Verified
Auditor	Auren	**Verified?**	Verified
Auditor Location	Spain	**Verified?**	Verified
Standard Audit	https://bug1412950.bmoattachments.org/attachment.cgi?id=8938788	**Verified?**	Need Response From CA
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	12/20/2017	**Verified?**	Verified
BR Audit	https://bugzilla.mozilla.org/attachment.cgi?id=8938790	**Verified?**	Need Response From CA
BR Audit Type		**Verified?**	Verified
BR Audit Statement Date	12/20/2017	**Verified?**	Verified
EV SSL Audit	https://bugzilla.mozilla.org/attachment.cgi?id=8938792	**Verified?**	Need Response From CA
EV SSL Audit Type	WebTrust	**Verified?**	Verified
EV SSL Audit Statement Date	12/20/2017	**Verified?**	Verified
BR Commitment to Comply	Server CP section 1.1	**Verified?**	Verified

BR Self Assessment	https://bugzilla.mozilla.org/attachment.cgi?id=8977789	**Verified?**	Verified
SSL Verification Procedures	Server CP section 4.1, CPS section 3.2.5	**Verified?**	Verified
EV SSL Verification Procedures	Server CP section 3.2, 4.1,	**Verified?**	Verified
Organization Verification Procedures	CPS sections 3.2.2, 3.2.3,	**Verified?**	Verified
Email Address Verification Procedures	CPS section 3.2.6	**Verified?**	Verified
Code Signing Subscriber Verification Pro	N/A Mozilla does not enable the Code Signing trust bit anymore.	**Verified?**	Not Applicable
Multi-Factor Authentication	CPS section 6.2	**Verified?**	Verified
Network Security	CPS section 6.7	**Verified?**	Verified