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			
CA Email Alias 2			
Company Website	www.firmaprofesional.com	**Verified?**	Verified
Organizational Type	Public Corporation	**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	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	Comment #3: I have reviewed Mozilla's list of Recommended Practices, and confirm that we follow those 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	* We allow external entities to operate subordinate CAs. But none of those CAs is allowed to issue SSL, EV nor CS certificates. * Server CP section 4.3: The information included in SSL certificates older than three (3) years will be verified according to “4.1 CERTIFICATE ISSUANCE PROCESS”, “b) Acceptance of the Application” subsection, point 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

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	This is the SHA-256 version of the currently include "Autoridad de Certificacion Firmaprofesional CIF A62634068" root cert.This new root has the 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
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	https://www.firmaprofesional.com	**Verified?**	Verified
CRL URL(s)	http://crl.firmaprofesional.com/fproot.crl http://crl.firmaprofesional.com/infraestructura.crl 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?**	Verified
OCSP URL(s)	http://ocsp.firmaprofesional.com	**Verified?**	Verified
Revocation Tested	http://certificate.revocationcheck.com/www.firmaprofesional.com NEED: Please resolve the Errors (in red on the website): - OCSP signing certificate does not contain the OCSP No Check extension - OCSP signing certificate does not contain the OCSP No Check extension	**Verified?**	Need Response From CA
Trust Bits	Code; Email; Websites	**Verified?**	Verified
SSL Validation Type	OV; EV	**Verified?**	Verified
EV Policy OID(s)	1.3.6.1.4.1.13177.10.1.3.10	**Verified?**	Verified
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
Root Stores Included In		**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

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	The old and new roots will have the same CA Hierarchy. See https://bugzilla.mozilla.org/show_bug.cgi?id=1012744 - CA 1: Certs for private corporations. SSL certs. - Cualificados: Qualified certs for electronic signature. - AAPP: Certs for Spanish Public Administration - CFEA: Certs electronic signature services. No SSL certs. - OTC: Certs valid for one day that can sign a single document. - SEU: not issuing certs, using CA 1 instead	**Verified?**	Verified

	- SIGNE - SANTANDER: not issuing certs		
Externally Operated SubCAs	SIGNE is governed by its own certification policies: https://www.signe.es/signe-ac/dpc 1. RA software is the same used by the other RA's bound to Firmaprofesional. 2. SIGNE and Firmaprofesional have signed a service agreement by which, Firmaprofesional hosts SIGNE Subordinate CA server and keys (HSM) and technically manage and maintain them 3. SIGNE Subordinate CA is not allowed to issue SSL Certificates.	**Verified?**	Verified
Cross Signing	None	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	CPS section 1.3.2.2: All SSL and SSL-EV certificates issued under the Firmaprofesional Certification Hierarchy are issued by this CA. Therefore, any other Subordinate CA under the Firmaprofesional Certification Hierarchy (public, private or to other PSC) cannot issue SSL or SSL-EV certificates. Firmaprofesional has a network of more than 70 Registration Authorities located throughout Spain. See CPS section 8.4.1 https://bugzilla.mozilla.org/show_bug.cgi?id=794036#c45	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	http://www.firmaprofesional.com/cps Documents are in Spanish. Certain CP CPS documents translated into English. CPS: https://www.firmaprofesional.com/images/pdfs/CPS/151005-CPS_151005.pdf Server CP: https://www.firmaprofesional.com/images/pdfs/CPS/FP_CP_Servidor_Web_SSL_6.3.pdf	**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/151005-CPS_151005-EN.pdf	**Verified?**	Verified
Other Relevant Documents	Code Signing CPS: https://www.firmaprofesional.com/images/pdfs/CPS/FP_CP_Firma_Codigo_6.0.pdf	**Verified?**	Verified
Auditor Name	Auren	**Verified?**	Verified
Auditor Website	https://cpacanada.ca/	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified

Standard Audit	https://cert.webtrust.org/SealFile?seal=1846&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	3/11/2015	**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	https://cert.webtrust.org/SealFile?seal=1847&file=pdf	**Verified?**	Verified
EV Audit Type	WebTrust	**Verified?**	Verified
EV Audit Statement Date	3/11/2015	**Verified?**	Verified
BR Commitment to Comply	Server CP section 1.1	**Verified?**	Verified
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 Server CP section 4.1 b:Following verifications must be done in order to guarantee that the requesting organization has control over the domain (URL) that is requested to be included in a certificate. This is carried out without detriment to what is established in the corresponding Certification Practice Statement (CPS) of Firmaprofesional: 1. The following authenticated whois services are consulted: o For “*.es” domains, consult the following authenticated WHOIS service: https://www.nic.es/sgnd/dominio/publicInformacionDominios.action o For the rest of the domains consult on http://www.iana.org/domains/root/db/ which is the authenticated WHOIS server to look for information about the domain, depending on the Top Level Domain (TLD), or said in another way, depending on whether the domain ends in .com, .org, .net, … 2. The details of the applicant will be validated as “Administrative Contact” of the domain.	**Verified?**	Verified
EV SSL Verification Procedures	Server CP section 4.1e: Firmaprofesional will issue an EV SSL Web Server Certificate if the application is electronically signed with a Corporate Legal Representative	**Verified?**	Verified

	Certificate of Firmaprofesional; in other case it will be issued a standard SSL Web Server Certificate. Additionally, the EV SSL Web Server Certificate's issuance requires the approval of two people: the RA Operator responsible for managing the request and the Technical Department Manager responsible for issuing the certificate.		
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	Translation of Code Signing CPS section 4.1, ISSUE OF CERTIFICATES: The steps for obtaining the certificate are: a) Request: Applications for these certificates should be made directly to Firmaprofesional addressing any partner acting as a Firmaprofesional's RA. In cases where Firmaprofesional had previously verified the identity of the Person Legal and the applicant, additional verifications will not be required. Specifically: - If the applicant has a Corporate Certificate of Legal Representative issued by Firmaprofesional. - If the Corporation acts as a Firmaprofesional's RA to issue their own certificates. b) Acceptance of the application: Firmaprofesional verify the personal data of the applicant and the organization to be to issue the certificate.	**Verified?**	Verified
Multi-Factor Authentication	RA operators are required to use Secure Signature-Creation Devices. CPS section 6.2.1: "The keys of the subscribers of SSCD (DSCF in Spanish) qualified certificates and the keys of operators and administrators are generated securely by the party concerned using a CC EAL4+, FIPS 140-1 level 3, ITSEC E4 High cryptographic device or other equivalent device."	**Verified?**	Verified
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 -- both the old	**Verified?**	Verified

SHA-1 and the new SHA-256 root certs
will have the same CA hierarhcy.