Bugzilla ID: 794036
Bugzilla Summary: Enable EV for Firmaprofesional

CAs wishing to have their certificates included in Mozilla products must

1) Comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/)
2) Supply all of the information listed in http://wiki.mozilla.org/CA:Information_checklist.
   a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
   b. Review the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic_Practices

General information about the CA's associated organization

CA Company Name	Firmaprofesional, Ltd.
Website URL	www.firmaprofesional.com
Organizational type	Commercial CA in Spain
Primark Market / Customer Base	Firmaprofesional is a commercial CA in Spain that issues certificates to professional corporations, companies and other institutions. 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.
CA Contact Information	CA Email Alias: info@firmaprofesional.com CA Phone Number: +34 93 477 42 45 Title / Department: Director Técnico de Firmaprofesional

Technical information about each root certificate

Certificate Name	Autoridad de Certificacion Firmaprofesional CIF A62634068

Certificate Issuer Field	CN = Autoridad de Certificacion Firmaprofesional CIF A62634068
	C = ES

Certificate Summary	This request is to enable EV for this root certificate that is currently included in NSS as per Bugzilla #521439.
Root Cert URL	http://crl.firmaprofesional.com/caroot.crt
SHA1 Fingerprint	AE:C5:FB:3F:C8:E1:BF:C4:E5:4F:03:07:5A:9A:E8:00:B7:F7:B6:FA
Valid From	2009-05-20
Valid To	2030-12-31
Certificate Version	3
Certificate Signature Algorithm	SHA-1
Signing key parameters	4096
Test Website URL	Please provide a url to a website whose EV SSL cert chains up to this root. Please test EV treatment and add screenshot to bug: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version
CRL URL	ARL: http://crl.firmaprofesional.com/fproot.crl CRL: http://crl.firmaprofesional.com/firmaprofesional1.crl (NextUpdate: 7 days) 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.

OCSP URL	http://servicios.firmaprofesional.com/ocsp Maximum expiration time of OCSP responses? (per EV guidelines)
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type	OV and EV
EV Policy OID	EV Policy OID

CA Hierarchy information for each root certificate

CA Hierarchy	CPS section 1.3.2 has a CA hierarchy diagram. Certificate Basic Constraints Extensions: Maximum number of intermediate CAs: 1 This root CA signs subordinate CAs that sign end-entity certificates. One sub-CA is used by Firmaprofesional, and other sub-CAs are issued for organizations -- professional corporations, companies or other institutions, which act as Registration Authorities and Certification Authorities in the hierarchy of certification Firmaprofesional. Translation of section 1.3.2, Subordinate Certificate Authorities It's called Delegate or certification authorities Subordinated to entities within the certification hierarchy issuing end-entity certificates and public key whose certificate has been digitally signed by the root certificate authority. Subordinated certificate authorities may be in the name of or on behalf of Firmaprofesional other entity. These other entities must be as Certification Service Providers and define its own Certification Practice Statement (CPS). Currently Firmaprofesional certification hierarchy is formed by two subordinate CA certificates themselves and for external Subordinate CA certificate: - Subordinate Certification Authority "AC Firmaprofesional - CA1" issues digital certificates to private corporations, in accordance with Law 59/2003 of 19 December on the electronic signature. - Subordinate Certification Authority "AC Firmaprofesional - AAPP" issues digital certificates to public corporations, as established in Law 11/2007 of 22 June, on electronic access of citizens to public services. - Subordinate Certification Authority "SIGNE Certification Authority" **is governed by its own practices and certification policies not outlined in this CPS,** which can be obtained directly from the home page of SIGNE: http://www.signe.es Please also explain the EV hierarchy. Can any third-party issuers issue EV certs?
Externally Operated SubCAs	Please provide the information listed here: https://wiki.mozilla.org/CA:SubordinateCA_checklist
Cross-Signing	List all other root certificates for which this root certificate has issued cross-signing certificates. List all other root certificates that have issued cross-signing certificates for this root certificate.
Technical Constraints on Third-party Issuers	Describe the technical constraints that are in place for all third-parties (CAs and RAs) who can directly cause the issuance of certificates. See #4 of https://wiki.mozilla.org/CA:Information_checklist#CA_Hierarchy_information_for_each_root_certificate

Verification Policies and Practices

Policy Documentation	Document Repository: http://www.firmaprofesional.com/cps CPS (Spanish): http://www.firmaprofesional.com/cps/FP_CPS_5.pdf CP (Spanish): http://www.firmaprofesional.com/cps/FP_CP_Gen_Servidor_Web_SSL_6.1.pdf CP (English): https://bugzilla.mozilla.org/attachment.cgi?id=664446
Audits	Audit Type: WebTrust Auditor: Ernst & Young WebTrust CA Seal: https://cert.webtrust.org/ViewSeal?id=946 (2011.09.16) WebTrust EV Seal: https://cert.webtrust.org/ViewSeal?id=1363 (2012.07.20)
Baseline Requirements (SSL)	CP section 1.1: The standard SSL certificates issued by Firmaprofesional comply with the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v1.0 of the CA/Browser Forum, in effect at the time of publication of this policy. The EV SSL certificates issued by Firmaprofesional comply with the Guidelines For the Issuance And Management Of Extended Validation Certificates, Version 1.3 of the same entity, in effect at the time of publication of this policy. The Requirements will have priority over this document in case of any incompatibility between this document and the published Requirements be the CA/Browser Forum.
SSL Verification Procedures	CP section 4.1: The organization must be the holder of the domain in order to apply for a SSL Secure Web Server Certificate. … Following verification 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: -- For "*.es" domains, consult the following authenticated WHOIS service: https://www.nic.es/sqnd/dominio/publicInformacionDominios.action -- 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. 3. The application, electronically signed by the legal representative, will be validated. If this is not possible the organization details will be validated through some of the following mechanisms: a. Contractual agreement between the organization and Firmaprofesional, previous to the application. b. Consult the Commercial Register. c. Manual verification of the organization's details through telephone call. CP section 4.1.e: Firmaprofesional will issue an EV SSL Web Server Certificate if the application is electronically signed with a Corporate Legal Representative 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	Please provide translations of the corresponding sections in the CP/CPS. I think CPS section 3.2 and 4.1.
Email Address Verification Procedures	Firmaprofesional RAs use a challenge/response mechanism to verify that the certificate subscriber has control of the email address to be included in the certificate when it is not the RA requesting the certificate. Alternatively, the organization acting as the RA may request a certificate on behalf of an individual and provide the individual's email address from their organization's database, where the email address is in the organization's domain and controlled by the organization. (CPS section 3.2.6) * CPS Section 3.2.6: In general, the signatories are people associated with the Registration Authority (eg, colleges, members of associations, etc.) In such cases it is not the signatory who is requesting a specific email address to be included in the certificate but the RA itself, by consulting its database, gets the address. In cases where the signer does not have any link with the RA, the control of the e-mail is verified by challenge and response to the requested address.
Code Signing Subscriber Verification Procedures	Where is the CP/CPS documentation regarding code signing certificates and verifying the identity and authority of the certificate subscriber?
Multi-factor Authentication	Confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance. See # 6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices Where is this documented?
Network Security	Confirm that you have performed the actions listed in #7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices Where is this documented?

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)

Publicly Available CP and CPS	Yes. CP section 3.1: Standard SSl Certificates: Between 1 and 5 years. If this is the case, then there must also be documentation about re-verifying the certificates… http://www.mozilla.org/projects/security/certs/policy/InclusionPolicy.html, section 6: "verify that all of the information that is included in SSL certificates remains current and correct at time intervals of **thirty-nine months or less;**"
CA Hierarchy	Yes. See above.
Audit Criteria	Yes. See above.
Document Handling of IDNs in CP/CPS	?
Revocation of Compromised Certificates	?
Verifying Domain Name Ownership	See above.
Verifying Email Address Control	See above.
Verifying Identity of Code Signing Certificate Subscriber	See above.
DNS names go in SAN	?
Domain owned by a Natural Person	?
OCSP	Yes. Tested.

Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)

Long-lived DV certificates	SSL certs are OV.
Wildcard DV SSL certificates	SSL certs are OV. Wildcard certs are allowed for non-EV SSL certs, see CP section 3.3.
Email Address Prefixes for DV Certs	SSL certs are OV
Delegation of Domain / Email validation to third parties	Delegation of domain verification to third parties? Delegation of email validation to third parties? * CPS Section 3.2.6: In general, the signatories are people associated with the Registration Authority (eg, colleges, members of associations, etc.) In such cases it is not the signatory who is requesting a specific email address to be included in the certificate but the RA itself, by consulting its database, gets the address. In cases where the signer does not have any link with the RA, the control of the e-mail is verified by challenge and response to the requested address. * CPS section 8.4.1: RAs have to pass a yearly-based audit perform by a third, independent party. The scope of that audit reaches from procedural issues since logical security points. Third party RAs can only issue certificates to end-entities closely related with the RA. Most of these RAs are professional association and they only can issue certificates to its members. * CPS section 1.3.3: The following may act as RA for Firmaprofesional: ** Schools, Professional Corporations and Professional Schools Councils, for their professional associations or for applicants who maintain some kind of relationship with the organization as employees, partners, customers or suppliers. Only Colleges or professional corporations may be registered for their college or members, because they have the capacity certification exclusively, on the peer or member status. *** Companies and private entities, for applicants who maintain some kind of relationship with the organization as employees, partners, customers or suppliers. *** Firmaprofesional directly regarding any type of certificate. **Firmaprofesional contractually formalize the relations between itself and each of the entities act as RA in the Firmaprofesional Certification System. ** Where the geographical location of subscribers represents a logistical problem for the subscriber identification and the application and presentation of certificates, the RA may delegate these functions to a trusted entity. This entity must have a special bond with the RA and a close relationship with the underwriters of the certificates to justify the delegation. ** The trusted entity must sign a partnership agreement with the RA on the acceptance of delegation of these functions. Firmaprofesional should know and explicitly authorize the agreement.
Issuing end entity certificates directly from roots	No.
Allowing external entities to operate subordinate CAs	?
Distributing generated private keys in PKCS#12 files	What about S/MIME certs? SSL CP section 4.1.d: Applicants shall deliver to Firmaprofesional, directly or through an authorized

	intermediary, a certificate request in PKCS #10.
Certificates referencing hostnames or private IP addresses	?
Issuing SSL Certificates for Internal Domains	?
OCSP Responses signed by a certificate under a different root	OCSP tested.
CRL with critical CIDP Extension	CRL tested.
Generic names for CAs	No.