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	1.3.6.1.4.1.13177.10.1.3.10

CA Hierarchy information for each root certificate

CA Hierarchy	Only AC Firmaprofesional can issue SSL certificates, EV or not SSL CP 2.1 AUTORIDADES DE CERTIFICACIÓN (CA) Estos certificados deben ser emitidos por la CA Subordinada "AC Firmaprofesional - CA1". Translation: These certificates must be issued by the Subordinate CA "AC Firmaprofesional - CA1". 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
Externally Operated SubCAs	All of the intermediate certificates are internally operated by Firmaprofesional.
Cross-Signing	None
Technical Constraints on Third-party Issuers	No external third party can directly cause the issuance of SSL certificates.

Verification Policies and Practices

Policy Documentation	Document Repository: http://www.firmaprofesional.com/cps CPS (Spanish): http://www.firmaprofesional.com/cps/FP_CPS_5.pdf SSL CP (Spanish): http://www.firmaprofesional.com/cps/FP_CP_Gen_Servidor_Web_SSL_6.1.pdf SSL CP (English): https://bugzilla.mozilla.org/attachment.cgi?id=664446 Code Signing CP (Spanish): http://www.firmaprofesional.com/cps/FP_CP_Gen_Firma_Codigo_5.pdf
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)	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	Firmaprofesional does not delegate issuance of SSL certificates to third parties. According to CPS Section 3.2, Firmaprofesional verifies the organization requesting the certificate and domain name ownership. According to SSL CP section 4.1, Firmaprofesional performs a whois query to confirm that the certificate subscriber owns the domain name to be included in the certificate. SSL 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	Here you can find the CPS sections 3.2 and 4.1 translated. Take also into account that the CPS has a general approach and for a detailed explanation of tasks, refer to the CP, translated and provided during the bug opening: 3.2 Initial validation of identity 3.2.1 Method to prove possession of the private key When issuing a certificate on a hardware device, the private key is created in the moment immediately preceding certificate generation, in a procedure which ensures confidentiality and its link to the applicant's identity. Each RA is responsible for ensuring secure delivery of the applicant's device. In other cases, proof of the subscriber's possession of the private key is achieved through the delivery of PKCS#10 or equivalent cryptographic proof or other method approved by Firmaprofesional. 3.2.2 Authentication of the identity of a legal person The Registration Authority shall verify the following information to enable authentication of the organization's identity: - Data relating to the name or business name the organization. - Data relating to the constitution and legal status of the subscriber. - Data on the extent and validity of the applicant's powers of representation. - Data regarding the tax identification code of the organization or equivalent code as used in the country to whose law the subscriber is subject. Firmaprofesional reserves the right not to issue a certificate in the event that it considers that the documentation provided is insufficient or inappropriate for the purpose of verifying the data set out above. 3.2.3 Authentication of the identity of a natural person The RA shall reliably verify the identity of the person identified in the certificate. As such, the natural person should present themselves and present their National Identity Document, residency card, passport or other means of identification which is recognized in law. In the event that the subscriber seeks modification of the personal identification data to be registered in respect of the identification document presented, he/she shall be required to present the Civil Registration Certificate where the variation is recorded. The RA will verify, through the presentation of sufficient original documentation and by means of its own sources of information, the remaining data and attributes to be included in the certificate (distinguished name of the certificate), and is required to retain the documentation supporting the validity of such data as it is unable to prove using its own data sources. Application of the provisions of the preceding paragraphs may not be required with respect to certificates issued subsequent to the entry into force of Law 59/2003 of 19 December on electronic signatures, in the following cases: a) When the identity or other permanent circumstances of the certificate applicants has already been obtained by the RA as a result of a pre-existing relationship, in which, for the identification of the applicant, the steps stipulated in the first paragraph have been concluded and the time period elapsed since the performance of said identification is not more than

	five years. b) When, in applying for a certificate, use is made of another certificate which was issued pursuant to the identification of the signer in accordance with the procedures set out in the first paragraph and where the RA is satisfied that the period of time elapsed since the verification of identification is not more than five years. 3.2.4 Authentication of the identity of the RA and the RA's operators In the constitution of a new RA, the following actions shall be undertaken: - Firmaprofesional shall verify the existence of the entity using its own sources of information. - An authorized representative of the organization shall be required to sign a contract with Firmaprofesional, which contract shall set out the specific aspects of the delegation and the responsibilities of each party. Furthermore, and with respect to the RA's operators, the RA shall be bound to: - Verify and validate the identity of the RA's new operators. The RA shall send documentation to Firmaprofesional corresponding to the new operator and his/her authorisation to act as an operator of the RA. - Ensure that the RA operators have received adequate training to perform their duties, attending at least one operator training session. - Ensure that communication between the RA and Firmaprofesional is conducted securely using operator digital certificates. 3.2.5 Domain Validation 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
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 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
Code Signing Subscriber Verification Procedures	Code Signing CP (Spanish): http://www.firmaprofesional.com/cps/FP_CP_Gen_Firma_Codigo_5.pdf
Multi-factor Authentication	RA Operators authenticate to the system and sign every transaction with a certificate within a Smart Card. … it can be deduce from my following paragraph: "+ Physical Security (SEF): to assess archiving and custody of registration documentation and RA Operator's authentication devices that performs the RA and operators of registration.

	# Documentation archiving: facilities, security levels,... # RA Operator authentication device: device management, PIN management, ... # ..." Also, It must to be reminded that there is not a unique account capable of directly causing certificate issuance. See CP section 4.1 Certificate Issuance Process; e) Certificate Issuance: "Additionally, the issuance of EV SSL Web Server Certificates requires the approval of two people: the RA Operator responsible for managing the request and management of the Technical Department Manager responsible for issuing the certificate."
Network Security	This is a part of our Security Policy that is not public-facing, but regarding the 2011 incidents (Comodo, Diginotar) we made a writing to the Spanish Ministry of Indrustry, Energy and Tourism, who is the body responsible for regulating the activity of certification service providers. And we made public in our blog an abstract of our writing (ES). http://firmaprofesional.blogspot.com.es/2012/10/transparencia-y-seguridad-claves-de-la.htmla A translation of this blog post is provided in the attachment of Comment #2. Here is part of it: Strengthening security measures Firmaprofesional As a result of the above, Firmaprofesional acquired a deep knowledge of the attacks and vulnerabilities that led to them. In Firmaprofesional do not apply some of the vulnerabilities, such as: 1. Firmaprofesional systems run on Linux machines, which does not apply any of the vulnerabilities attributable to Microsoft software. 2. The process of issuing SSL certificates require manual processing of applications, ie, no certificates are issued by 100x100 automated processes. This ensures that at least one person processes the request data and that can detect unusual behavior. 3. Firmaprofesional have their systems protected by Sonicwall CGSS suite. However, as a result of the commitment to security that has always characterized Firmaprofesional, we took additional measures, such as: - As a precaution, change all administration passwords. - Weekly update of the systems. Earlier this update was done monthly. - Installing intrusion detection tool (IDS) to detect rootkits (rhunter, chkrootkit.) The whole process of management of the incidents and design and implementation of appropriate measures has been supervised by our technical director, Oscar Conesa (CISA, CISSP, CISM, Lead Auditor BS27000) and by an external auditor of the company iSigma, Chema Lopez (CISA.)

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

Publicly Available CP and CPS	Yes.
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. SSL 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**;"
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	Firmaprofesional does not delegate issuance of SSL certificates to third parties. See above regarding S/MIME certs. CP "2.2 REGISTRATION AUTHORITIES (RA) The management of applications and issuances of the certificates will be carried out by Firmaprofesional or by an authorized intermediary. The authorized intermediaries will be register domains's entities accredited by ICANN which has a collaboration agreement with Firmaprofesional. (In fact we currently do not have any collaboration agreement signed, so only Firmaprofesional itself acting as RA and, of course CA, manages the applications/requests.) 2.3 APPLICANT The person appearing as "Administrative contact" (in the official record of the domain) will be able to do the application...." Besides, I place you to read section 4.1 CERTIFICATE ISSUANCE PROCESS, in particular, points a) Application and b) Acceptance of the application.
Issuing end entity certificates directly from roots	No.
Allowing external entities to operate subordinate CAs	SIGNE is an external subordinate CA, with a number of caveats, namely: 1. RA software is the same used by the other RA's bound to Firmaprofeasional, 2**. SIGNE Subordinate CA server and keys (HSM) are hosted in the Firmaprofesional facilities**. In fact, 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. Last but not least SIGNE Subordinate CA is not allowed to issue SSL Certificates (EV or not.) See SIGNE CA CPS and CPs (in Spanish).
Distributing generated private keys in PKCS#12 files	Firmaprofesional do not generate end entity keypairs at all, neither S/MIME unique purpose certificates. Keypairs are always generated in the secure signature-creation device, or in the user side: browser, web server, etc.

	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	Firmaprofesional only issue SSL certificates (EV or not) to public ascertainable domains such as firmaprofesional.com independently if a specific domain (e.g. private.firmaprofesional.com) is not publicly accessible. Firmaprofesional does not issue SSL certificates to private IP addresses
Issuing SSL Certificates for Internal Domains	Firmaprofesional only issue SSL certificates (EV or not) to public ascertainable domains such as firmaprofesional.com independently if a specific domain (e.g. private.firmaprofesional.com) is not publicly accessible.
OCSP Responses signed by a certificate under a different root	OCSP tested.
CRL with critical CIDP Extension	CRL tested.
Generic names for CAs	No.