Bugzilla ID: 521439
Bugzilla Summary: Add renewed Firmaprofesional root CA cert

CAs wishing to have their certificates included in Mozilla products must comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/) and must supply the information necessary to determine whether or not the policy's requirements have been satisfied, as per http://wiki.mozilla.org/CA:Information_checklist.
CA's are also encouraged to review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices.

General Information	**Data**
CA Name	Firmaprofesional, Ltd.
Website URL	www.firmaprofesional.com
Organizational type	Commercial CA in Spain
Primary 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

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	**Data**
Certificate Name	Autoridad de Certificacion Firmaprofesional CIF A62634068
Cert summary / comments	The old root was evaluated for inclusion in bug #342426. Sub-CAs of the new root cross-sign end-entity certs with sub-CAs of the old root, in order to maintain business continuity.
The root CA certificate URL	http://crl.firmaprofesional.com/carootnew.crt
SHA-1 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
Cert Version	3
Modulus length / key length	4096
Test Website	https://www.firmaprofesional.com Sub-CA cert to perform SSL cert chain tests (AC Firmaprofesional - CA1): https://bugzilla.mozilla.org/attachment.cgi?id=407496
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 Responder URL	http://servicios.firmaprofesional.com/ocsp
List or description of subordinate CAs operated by the CA organization associated with the root CA.	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. Google Translation: Subordinate Certification Authorities It is called Certification Authorities Delegated or subordinate CAs to entities within the hierarchy of certification authority issuing certificates and issued with final key public has been digitally signed by the Root Certification Authority. Authorities Subordinate Certification can be in the name of Firmaprofesional or on behalf of another entity. Firmaprofesional uses a Subordinate Certification Authority (CA Sub) to issue own certificates to end users.
Sub-CAs operated by third parties	All of the Sub-CAs are internally operated by Firmaprofesional.
List any other root CAs that have issued cross-signing certificates for this root CA	Sub-CAs of the new root cross-sign end-entity certs with sub-CAs of the old root, in order to maintain business continuity. Google Translation of CPS section 1.3.2: All certificates issued before the publication of this CPS may be validated with both Root Certificates interchangeably through a process of "cross certification" of the Subordinated Certification Authorities. It is recommended for all users and organizations that include both root certificates in all Lists or repositories of trusted root certificates in their possession. It is noteworthy that both subordinate CA certificates using the same private key, same public key, CA the same name and share the same CRL. This model shared key certification is called "cross certification". As a result the end-user certificates issued to date can be validated both the hierarchy based on the CA that expires in 2013 and with the hierarchy based on the CA that expires 2030.
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type DV, OV, and/or EV	OV
EV policy OID(s)	Not EV
CP/CPS	All documents are in Spanish. Certification Policies and Practices: http://www.firmaprofesional.com/index.php?option=com_content&view=article&id=62&Itemid=75 CPS: http://www.firmaprofesional.com/cps/FP_CPS_4_1.pdf

	SSL CP: http://www.firmaprofesional.com/cps/FP_CP_SSL_4.pdf Code Signing CP: http://www.firmaprofesional.com/cps/FP_CP_FirmaCodigo_4.pdf There is no specific policy for S/MIME. All the personal certificates are allowed to be used for S/MIME purposes. See certification profiles: X509v3 Extended Key Usage - TLS Web Client Authentication and E-mail Protection.
AUDIT	Audit Type: WebTrust CA Auditor: Ernst & Young Auditor Website: http://www.ey.com/es Audit Report and Management's Assertions: https://cert.webtrust.org/ViewSeal?id=946 (2009.07.28)
Organization Identity Verification	Google Translations of CPS: http://www.firmaprofesional.com/cps/FP_CPS_4_1.pdf 1.3.3 Registration Authority (RA) A Registration Authority (RA in English or Registry Authority) within the Certification System Firmaprofesional, is the entity responsible for: • Process applications for certificates. • Identify and validate the applicant's personal circumstances of a signing certificate electronically. • Manage the issuance of certificates, only to groups of users that have a special connection. • Presenting the award to the subscriber. For the purposes of this CPS may act as RA 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. • The self 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. 3.2 INITIAL IDENTITY VALIDATION 3.2.1 Test Method for possession of private key When issuing a certificate on a hardware device, the private key is created in the moment prior to the certificate generation, in a manner which ensures confidentiality and its connection with subscriber's identity.

Each RA is responsible for ensuring delivery to the subscriber device safely.
In other cases, the method of proof of possession of the private key by the subscriber will be the delivery or a PKCS # 10 cryptographic equivalent test or other method approved by Firmaprofesional.

3.2.2 Authentication of the identity of a legal entity

The Registration Authority shall verify the following information to authenticate the identity of the Organization:

- The data relating to the name or trade name of the organization.
- The data relating to the constitution and legal status of the subscriber.
- Data on the extent and duration of the powers of representation applicant.
- Data on tax registration of the organization or equivalent code used in the country whose law is subject to the Subscriber.

Firmaprofesional reserves the right not to issue the certificate if it considers that the documentation provided is not sufficient or appropriate for the verification of the aforesaid information.

3.2.3 Authentication of the identity of an individual

The RA reliably verify the identity of the subscriber. For this, the subscriber must person and present the National ID card, residence, passport or other means recognized in law that identifies you.

Exceptionally, the RA will validate the identity of subscriber data transfer without impartiality need. In this case it is essential that the subscriber is authenticated by the use of electronic ID.

If the owner claims the modification of personal identifying information to register respect to the identification document presented, must submit the corresponding Civil Registration Certificate by entering the change.

The RA will verify, either through the exhibition of original documentation enough, along with their own sources of information, data and other attributes to include in the certificate (name awarded the certificate) and must keep the documentation proving the validity of those data can not verify through their own data sources.

Nothing in the preceding paragraphs may not be enforceable in certificates issued after the entry into force of Law 59/2003 of 19 December, electronic signature, in the following cases:

a) When the identity or other circumstances of applicants for permanent licenses the RA were highlighted by a pre-existing relationship, in which, for identification the person concerned had been used the means set out in the first paragraph and the period of time since the identification is less than five years.

b) When requesting a certificate to use another expedition had been identified as the signatory in the manner prescribed in the first paragraph and the RA is satisfied that the period of time elapsed since the identification is less than five years.

3.2.4 Authentication of the identity of the RA and RA operators

In the formation of a new RA, will undertake the following actions:

- Firmaprofesional verify the existence of the entity through their own sources of information.
- Signing of contract for the formation of RA. An authorized representative of the organization must sign a contract with Firmaprofesional, which will detail the aspects specific delegation and responsibilities of each agent.

In addition, the RA will require compliance with the following in respect of the operators:

- To verify and validate the identity of new entrants to the RA. The RA shall send a Firmaprofesional documentation for the new operator and its authorization to act as operator of RA.
- To secure that the RA operators have received adequate training for performance of their duties, attending at least one training session operator.
- To secure communication between the RA and Firmaprofesional is done safely using digital certificates operator.

4 OPERATIONAL REQUIREMENTS FOR THE LIFE CYCLE CERTIFICATES

4.1 APPLICATION FOR CERTIFICATION

4.1.1 Who may request a certificate (applicant)

You can request a certificate by the person concerned or a third party to represent him. In the second case, there must be expressly authorized by Firmaprofesional.

The subscriber must have the National ID card, residence, passport or otherwise recognized in law, which in any case must be valid.

The specific requirements for a specific certificate request will be included in the "Policy Certification ".

4.1.2 Process Certificate Request

The applicant must contact an RA to manage the license application, persons or phone according to the type of certificate you are applying.

The RA applicant will provide the following information:

- Documents needed to submit for processing your application and to verify the subscriber's identity.
- Availability to perform the registration process.
- Information on the process of issuing and revocation of custody of the private key, and as the responsibilities and conditions of using the certificate and the device.
- How to access and view this document and the certification policies.

4.2 PROCESSING OF APPLICATIONS FOR CERTIFICATES

4.2.1 Carrying out the identification and authentication functions

It is the responsibility of the RA reliably perform identification and authentication Subscriber. This process should be conducted prior to issuance of the certificate.

4.2.2 Approval or denial of license applications

Once the certificate request, the RA shall verify the information provided by the applicant, including the validation of a subscriber's identity.

If the information is not correct, the RA deny the request by contacting the applicant to communicate the reason.

If correct, shall sign a binding legal instrument between Subscriber and / or applicant and the CA-RA. It shall then issue the certificate.

4.3 ISSUANCE OF CERTIFICATES

	4.3.1 CA actions during certificate issuance Once approved, the application will proceed to issue the certificate, which must be submitted securely to the subscriber. For the issuance of certificates shall perform the following actions: a) For certified hardware support: • The RA will be delivered or verify that the subscriber has a meeting the DSCF requirements of law and a device to access it, if any (generally a card reader). In the event that the Subscriber make its own device, it must be approved by Firmaprofesional prior to use. The RA should have a list of approved devices. • Activation of the device. If the subscriber does not have them, generate activation data from the device and access to the private key contain. • Key pair generation. This shall be the generation of keys using the facility provided by the RA. b) for software licenses: • The subscriber shall generate the key pair in the browser, in the page indicated by the RA. • A turn key pair generated, the subscriber will get a code to be submit to the RA to proceed with the issue. c) The RA will check again the contents of the certificate request with documentation filed, and if the verification is correct validate the request with its operator's certificate digitally signed. d) Finally, be sent through a secure channel with the public key verified data AC PKCS10 format or equivalent. In such a case the generation of certificate in a procedure to be protection against counterfeiting and maintain the confidentiality of data exchanged. e) Surrender of certificate. The certificate generated will be sent to the RA, which puts it at available to the subscriber. During the generation of the certificates, the CA will add the remaining information established in Article 11 of Law 59/2003 of 19 December, electronic signature, in accordance with prescribed in the relevant section of this document or the associated policy certification.
Domain Name Ownership / Control	Comment from Firmaprofesional: Yes, by out-of-bound and off-line means we verify the identity of the requesting person and the binding between the organization and the domain. … In addition we also use whois services. Google Translations of SSL CP: http://www.firmaprofesional.com/cps/FP_CP_SSL_4.pdf 4.1 PROCESS OF ISSUE OF CERTIFICATES The RA is responsible for processing applications and issuing certificates of compliance always with the general terms described in the CPS. The steps for obtaining the license is detailed below: a) Request: Must be submitted by the applicant, meeting described in the CPS and presenting, at least the following documentation: • The authorization of the applicant organization to the person making the request for issuing the certificate. • The identity of the individual. • The ownership of the domain name, certified by a legal representative of the organization. • Accreditation by a reliable means of existence of the entity under Right.

	b) Acceptance of the application: The RA will verify the applicant's identity, its relationship with the entity, its existence and data to include in the certificate. c) Processing: Once the application is accepted, the RA will process the application for the license d) Key Generation:The signature keys will be generated in the systems of the applicant using its own applications compatible with PKI standards. The applicant shall deliver to the RA a certificate request in PKCS # 10. Typically, server applications that can be configured with the SSL protocol, as Microsoft IIS, include tools to generate keys and certificate requests. e) Certificate: The RA shall issue the certificate, signing the certificate request format PKCS # 10 and sending it to the CA. Once the certificate has been generated, and before the RA could deliver to the Subscriber, the latter shall: • Log in person before the RA, according to the procedure to communicate it. • Read, accept and sign the legally binding instrument with RA. f) Delivery: Finally, the RA will award the certificate to the subscriber downloads allowing its way safe from the Internet. 4.3 RENEWAL OF CERTIFICATES There are two procedures: a) face Renewal Process: The subscriber must contact your RA, and proceed to the generating a new certificate. b) Online Renewal Process: If the RA has the service and the subscriber has contracted renewal, it will receive a notification from the RA by email to start the renewal through the website of Firmaprofesional.
Email Address Ownership / Control	Comment from Firmaprofesional: There is not a explicit indication on that point, but the different policies are always bound to the membership to a company, professional association, and so. It is not the individual (the person whose personal data is going to be in the "subject field") who provides the data to be include in the certificate, but a legal representative. And this data is collected from de company's or professional association's database.
Identity of Code Signing Subscriber	Google Translations of the Code Signing CP: http://www.firmaprofesional.com/cps/FP_CP_FirmaCodigo_4.pdf 4.1 PROCESS OF ISSUE OF CERTIFICATES The RA is responsible for processing applications and issuing certificates of compliance with the procedures described in the CPS. The steps for obtaining the certificate are: a) Request: Must be submitted by the applicant, meeting described in the CPS and with the following: • The applicant must be authorized to request the certificate. • The applicant must submit the documentation required by the RA to process the application. b) Acceptance of the application: The RA will verify the applicant's identity and linking the subscriber with the entity and data to include in the certificate. c) Processing: Once accepted, the RA will process the application is submitted. d) Key Generation: The signature keys will be generated in the systems of the applicant using its own applications compatible with PKI standards. The applicant shall deliver to the RA a certificate request in PKCS # 10 Generally, the development tools that allow the use of code signing include tools to generate keys and certificate requests. For example, the JDK includes tools for Java "keytool" and "jarsigner.

	e) Certificate: Once the keys generated, the RA shall make the issuance of the certificate by signing the petition certificate generation and sending it to the CA. Once the generated certificate, and before the RA could deliver to the subscriber, the latter shall: • Log in person before the RA, according to the procedure to communicate it. • Read, accept and sign the legally binding instrument with RA. f) Delivery: Finally, the RA shall award the certificate to the subscriber.
Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices • Long-lived DV certificates o SSL certs are OV. o SSL CPS section 3.1: Secure Server Certificates have a validity period of 1, 2 or 3 years. • Wildcard DV SSL certificates o SSL certs are OV. o SSL CPS section 3.3: Secure Server Certificates Multidomain different URLs can validate the same domain with the same certificate. This functionality is achieved using "Character Wildcards" for URLs as defined in the standard RFC 2818 HTTP Over TLS ". Under this standard, are allowed to use the character "asterisk" as a wildcard in a URL. Thus, a certificate with the address "*.dominio.com" may be used for any subdomain as subdominio1.dominio.com "," subdominio2.domino.com "," www.dominio.com ", etc ... The use of "wildcards" in SSL Secure Server certificates is supported by major Internet browsers and is very useful when you have many subdomains of the same Internet domain and want to use a single certificate for all of them. • Delegation of Domain / Email validation to third parties o Domain/Email validation is delegated to third party RAs. See the CPS translations above. • Issuing end entity certificates directly from roots o The root only signs sub-CAs. The sub-CAs sign the end-entity certs. • Allowing external entities to operate unconstrained subordinate CAs o The sub-CAs are operated internally by Firmaprofesional. • Distributing generated private keys in PKCS#12 files o SSL CP indicates the private keys are generated via PKCS#10. • Certificates referencing hostnames or private IP addresses o Not found. • OCSP Responses signed by a certificate under a different root o The test website loads into Firefox without error when OCSP is enforced. • CRL with critical CIDP Extension o CRLs downloaded into Firefox browser without error. • Generic names for CAs o Root name contains “Firmaprofesional”