Bugzilla ID: 794036
Bugzilla Summary: Enable-EV-for-Firmaprofesional

Technical information about each root certificate

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	<* Work In Progress *>
OCSP URL	Maximum expiration time of OCSP responses? (per EV guidelines)?	<* Work In Progress *>
EV Policy OID	EV Policy OID	EV Policy OID: 1.3.6.1.4.1.13177.10.1.3.10, as can be seen at section 1.2 Identification of the document, in the previously provided (and translated) CP

CA Hierarchy information for each root certificate

CA Hierarchy	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: Please also explain the EV hierarchy. Can any thirddparty issuers issue EV certs?	No, only AC Firmaprofesional - CA1 can issue SSL certificates, EV or not. It is stated at section 2.1 Certification Authorities. The term “CA1” is only written in the Spanish version. I missed it in the translation. Anyway, no subordinated CA not governed directly by Firmaprofesional can issue EV certs.
Externally Operated SubCAs	Please provide the information listed here: https://wiki.mozilla.org/CA:SubordinateCA_checklist	I think this not apply, because externally operated SubCAs are not allowed to issue EV certs, as stated at 2.1 Certification Authorities section of the CP
Cross Signing	List all other root certificates for which this root certificate has issued crossdsigning certificates. List all other root certificates that have issued crossdsigning certificates for this root certificate	There is no RootCA cross-certified
Technical Constraints on Thirddparty Issuers	Describe the technical constraints that are in place for all thirddparties CAs and RAs) who can directly cause theissuance of certificates. See #4 of https://wiki.mozilla.org/CA:Information_checklist#CA_Hierarchy_information_for_each_root_certificate	No external third party can directly cause the issuance of EV certificates. 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."

Verification Policies and Practices

Organization Verification Procedures	Please provide translations of the	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,

	corresponding sections in the CP/CPS. I think CPS section 3.2 and 4.1.	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 ***3.2.6 Email validation*** 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	Where is the CP/CPS documentation regarding code signing certificates and verifying the identity and authority of thecertificate subscriber?	Sincerely. I do not see the point on asking about Code Signing certificates when we are applying for EV. Of course we have a Code Signing CP, that you can find (in Spanish) at: http://www.firmaprofesional.com/cps/FP_CP_Gen_Firma_Codigo_5.pdf

Multifactor 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?	It is not publi-facing documented, but RA Operators authenticate to the system and sign every transaction with a certificate within a Smart Card. I did not mentioned it explicitly in the bug #521439, but 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	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?	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*). Find here a translation of the mentioned post: Firmaprofesional is committed to security beyond what is legally required, as evidenced by WebTrust Extended Validation and WebTrust for CA seals. Another example of this commitment to security and also to transparency are the measures that Firmaprofesional took in response to incidents of Certification Service Providers that occurred during the past 2011 year, as the DigiNotar case. Firmaprofesional approach in response to the events discussed covers three areas of action, namely: 1. Tracking all information related to incidents, with particular emphasis on cases Comodo (March 25, 2011) and DigiNotar (July 10, 2011.) 2. Close collaboration in research work from different software vendors, industry groups and authorities. 3. Strengthening security measures Firmaprofesional applies to the process and systems lifecycle management of certificates. **Tracking information of incidents** This tracking allows us to detect which vulnerabilities have been exploited, whether procedural, basic software, and network infrastructure or the certificates lifecycle management software. The main sources of information were: 1. DigiNotar case report of ICT security consultancy Fox-IT. 2. Comodo hacker's own information (The Comodo hacker releases his manifesto, Hi again! I strike back again, huh?), which proved to be the same as the case of DigiNotar, GlobalSign and the Starcom. 3. Report of renowned cryptography expert Peter Gutman. 4. Report of the Information Security Group, Royal Holloway, University of London on the DigiNotar case. 5. The GlobalSign own internal report. The conclusions are that the systems and procedures of DigiNotar had significant shortcomings, including: 1. The most critical servers contain malicious software that can normally be detected by an antivirus. 2. All CA servers belonged to one Windows domain, which made it possible to access all of them getting a single user / password. 3. The administrative password was not robust and easy to get through brute force. 4. The software installed on the public web servers was outdated and had not timely patched. 5. No antivirus protection on servers investigated. 6. The certificate issuing system is fully automated, without human intervention. None of the above deficiencies affecting Firmaprofesional since we already had countermeasures to these problems, as will be explained later. **Collaboration in research tasks** Firmaprofesional has worked closely and openly with all entities that have requested it, to try to identify the author or authors of the attacks, the *modus operandi* and the circumstances that arose to carry attacks.

		On one hand, the Mozilla Foundation asked to Firmaprofesional for a series of checks and collaboration in September 2011, to which Firmaprofesional replied diligently point by point. At that time, Firmaprofesional had received several unusual and suspicious SSL certificates requests, about what we informed the Mozilla Foundation. Here began a collaboration coordinated by the Mozilla Foundation putting in touch Firmaprofesional with StartCom company and he Dutch Secret Service staff, with the CA Browser Forum and the latter with the FBI. Meanwhile, Microsoft also made contact with us, on the same dates, in confidence according to its terms. Again Firmaprofesional answered promptly on the information required. **<u>Strengthening security measures Firmaprofesional</u>** 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 uodate 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.)** With all this, since we are certain Firmaprofesional have systems and procedures adequately protected.

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

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..[...]	Here you are referring to CPS only, that is a general framework, and you are not taking into account the CPThat is, CP states that: **"2.2 REGISTRATION AUTHORITIES (RA)** The management o f applications and issuances of the certificates **will be carried out by Firmaprofesional** or by an authorized intermediary. The **authorized intermediaries** will b**e 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.
Allowing external entities to operate subordinate CAs	¿?	Yes, SIGNE is an external entity that operatea a 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 inPKCS#12 files	What about S/MIME certs? SSL CP section 4.1.d: Applicants shall deliver to Firmaprofesional, directly or through an authorized	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. Firmaprofesional receives a PKCS#10 certification request.
Certificates referencing hostnames orprivate IP addresses	¿?	Firmaprofesional only issue SSL certificates (EV or not) to public ascertainable domains such as firmaprofesional.com indenpemdently 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 indenpemdently if a specific domain (e.g. private.firmaprofesional.com) is not publicly accessible. Firmaprofesional does not issue SSL certificates to private IP addresses