ISSUE		STATUS		REPONSE
Case Information				
CA Owners/Certificate Name	Autoridad de Certificacion Firmaprofesional	**Request Status**	Need Information from CA	Organization name and tax number: Firmaprofesional, S.A., A62634068 Root CN: Autoridad de Certificacion Firmaprofesional CIF A62634068
Response to Mozilla's list of Recommended Practices				
CA's Response to Recommended Practices	Please review and respond to Mozilla's list of Recommended Practices: https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices	**Verified?**	Need Response From CA	Verified. I have reviewed Mozilla's list of Recommended Practices, and confirm that we follow those practices.
Response to Mozilla's list of Potentially Problematic Practices				
CA's Response to Problematic Practices	Please review and respond to Mozilla's list of Potentially Problematic Practices: https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices	**Verified?**	Need Response From CA	I have reviewed Mozilla's list of Potentially Problematic Practices, and confirm that we do not follow those practices, except that we allow external entities to operate subordinate CAs. But none of those CAs is allowed to issue SSL, EV nor CS certificates.
Technical Information about Root Certificate				
Certificate Summary	Will this root eventually replace the currently include "Autoridad de Certificacion Firmaprofesional CIF A62634068" root cert? Will this root eventually have the same CA hierarchy as the old root?	**Verified?**	Need Response From CA	This root will have the same CA hierarchy as the old root. In fact, it has the same key pair and DN, so validation can be performed with either of them interchangeably.
Test Website URL (SSL) or Example Cert	Provide test website whose SSL cert chains up to this root.	**Verified?**	Need Response From CA	Validation can be performed with either of them interchangeably. https://www.firmaprofesi
CRL URL(s)	Need CRL URLs. 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?**	Need Response From CA	Validation can be performed with either of them interchangeably. http://crl.firmaprofesional.com/fproot.crl
OCSP URL(s)	Will it be http://servicios.firmaprofesional.com/ocsp for this CA hierarchy? CPS section 4.10.3: The use of OCSP services is not public and requires specific licensing. CONCERN: I don't think this meets the requirements of the CA/Browser Forum's Baseline Requirements.	**Verified?**	Need Response From CA	Yes, it'll be. Regarding "OCSP services is not public", in fact, it is public.
Trust Bits	Code; Email; Websites	**Verified?**	Need Response From CA	Yes, please, as the SHA1 root.
SSL Validation Type	OV	**Verified?**	Need Response From CA	Yes, please, as the SHA1 root.
EV Policy OID(s)	EV?	**Verified?**	Need Response From CA	Yes, please, as the SHA1 root.
EV Tested	If requesting EV treatment for this root, then provide successful output from the EV Cert Test: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version	**Verified?**	Need Response From CA	Validation can be performed with either of them interchangeably.
Root Stores Included In		**Verified?**	Need Response From CA	This root CA has the same key pair and DN than the SHA1 root CA already included, so validation can be performed with either of them interchangeably. Nevetheless Mozilla Root Store is the first root store we are dealing with.
Mozilla Applied Constraints	Should Mozilla apply constraints to certain TLDs for certs issued in this CA hierarchy?	**Verified?**	Need Response From CA	Not currently.
CA Hierarchy Information				
CA Hierarchy	Please describe the planned CA Hierarchy for this root	**Verified?**	Need Response From CA	The same than the current SHA1 root CA (see answers above).

ISSUE		STATUS		REPONSE
Externally Operated SubCAs	Will all subCAs in this CA hierarchy be internally operated? Are there any plans to have or allow for externally operated SubCAs? It looks like the CPS allows for externally-operated subCAs, so will need to understand how they are constrained or audited/disclosed according to sections 8 through 10 of https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/inclusion/	**Verified?**	Need Response From CA	There are externally operatd subca's but they are not alllow no issue SSL, EV nor CS certificates.
Cross Signing	Has this root been cross-signed with another root? Will it be?	**Verified?**	Need Response From CA	No and, not currently (who knows, maybe with FBCA?)
Technical Constraint on 3rd party Issuer	Firmaprofesional has a network of more than 70 Registration Authorities located throughout Spain. Please describe how these Registration Authorities are constrained or audited/disclosed per sections 8 through 10 of https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/inclusion/ see also https://wiki.mozilla.org/CA:CertificatePolicyV2.1#Frequently_Asked_Questions	**Verified?**	Need Response From CA	Currently Firmaprofesional does not technically constraint subordinate CAs. On the other hand see https://bugzilla.mozilla.org/show_bug.cgi?id=1012744 for further information on Firmaprofesional's subordinate CAs. See also 8.4.1 Registration authority auditing. Currently audits are annual or maximun biennal. Additionally we use a data model where RA operators belong to a RA, and a RA is allowed to issue a determined set of Certificate Policy. This allowance is a positive one, that is, when you create a new RA this RA can not issue any certificate at all and two RA administrators have to add one by one the CPs allowed to this new RA (see https://bugzilla.mozilla.org/show_bug.cgi?id=794036).
Verification Policies and Practices				
Auditor Qualifications	I did not find DNB in the Webtrust list here: http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx#Spain	**Verified?**	Need Response From CA	Neither do I, so I emailed to CPA, email that was never answered. Nevertheless the seals has been released by CPA so DNB should be a licensed practitioner.
BR Audit	Need	**Verified?**	Need Response From CA	Works will start in January
BR Audit Type		**Verified?**	Need Response From CA	First audit
BR Audit Statement Date		**Verified?**	Need Response From CA	Works will start in January
EV Audit	EV?	**Verified?**	Need Response From CA	Renewal will start in January
EV Audit Type		**Verified?**	Need Response From CA	Renewal
EV Audit Statement Date		**Verified?**	Need Response From CA	<**> Work-in-progress
BR Commitment to Comply	Please carefully review this with your auditors: https://wiki.mozilla.org/CA:BaselineRequirements Also, see BRs section 8.3	**Verified?**	Need Response From CA	<**> Work-in-progress
EV SSL Verification Procedures		**Verified?**	Need Response From CA	<**> Work-in-progress

ISSUE		STATUS		REPONSE
Code Signing Subscriber Verification Pro	It's not clear to me from the CPS how the identity and authority of the code signing certificate subscriber is verified. Please see https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Identity_of_Code_Signing_Certificate_Subscriber	**Verified?**	Need Response From CA	Unortunately the specific CS CP (http://goo.gl/QVL2vt) is not translated into English. I'll translate 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.
Multi-Factor Authentication	BR #16.5: The CA SHALL enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.	**Verified?**	Need Response From CA	RA operators are required to use Secure Signature-Creation Devices. See CPs section "6.2.1 Standards for cryptographic modules": "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."
Link to Publicly Disclosed and Audited subordinate CA Certificates				
Publicly Disclosed & Audited subCAs	https://bugzilla.mozilla.org/show_bug.cgi?id=1012744 -- Is the CA hierarchy for this new root also represented here?	**Verified?**	Need Response From CA	Yes (see answers above)