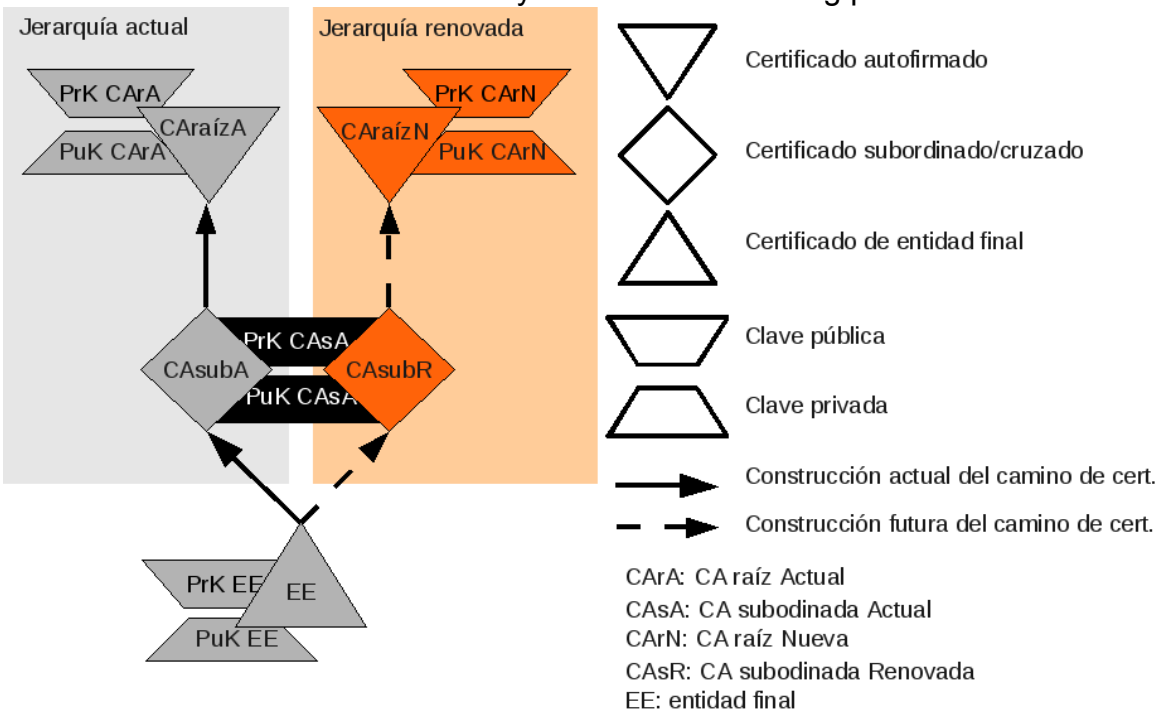
- Test Website: For testing purposes, please provide a URL to a website whose SSL cert chains up to this root.

Beside the new CA root certificate we have cross-certificate the subordinate CA, that is, we have resign the same data of the sub-CA only changing the validity period. I attach the renews sub-CA. You can acces to https://www.firmaprofesional.com and build the cert chains with this sub-CA and the new root CA. It validates correctly. Look at the following picture how it works.



- Sub-CAs operated by third parties: Are the organization sub-CAs operated by external third parties? Or are they operated internally by Firmaprofesional, and the sub-CAs organizations just act as RAs?.

Sub-CA's are internally operated by Firmaprofesional. In fact, currently there is onlu one sub-CA called ""

- Requested Trust Bits: Code Signing? – Do you want to enable the Code Signing trust bit for this root?

Yes, please.

- SSL Validation Type: Do you perform identity/organization verification for all SSL certificates?

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. The following documentation is needed (from pg 7 of http://www.firmaprofesional.com/cps/FP_CP_SSL_4.pdf):

- The authorization of the applicant organization to the individual 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.

In addition we also use whois services.

- DV, OV, and/or EV: Is it ever the case for SSL certs that the ownership of the domain name is verified, but the identity/organization of the subscriber is not verified?

No

- CP/CPS: Email (S/MIME) CP: Which CP should I look at for the info about certs that can be used for S/MIME?

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.

- Domain Name Ownership / Control: It's not clear to me how the ownership of the domain name is verified. Does the RA check the domain ownership using a third-party source, such as whois?
    - The ownership of the domain name, certified by a legal representative of the organization.

Responsible declaration by a legal representative of the company

- Email Address Ownership / Control: Please provide translations into English of the sections of the appropriate CP document(s) that describe the procedures for verifying that the email account associated with the email address in the cert is owned/controlled by the subscriber. Please also list the corresponding document(s) and section or page numbers containing the original text.

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.

- Potentially Problematic Practices: Please review the list of Potentially Problematic Practices (http://wiki.mozilla.org/CA:Problematic_Practices). When applicable, please provide further information and translations into English of the relevant CP/CPS.

SSL cert. are 3 or less years valid, what it is not very long. Additionally they seem to be OV, according with the definition in https://wiki.mozilla.org/CA:How_to_apply