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)?	Maximum expiration time of OCSP responses is from five (5) minutes up to one (1) day, as a maximum, depending on the server load. See attached OCPS Response.

CA Hierarchy information for each root certificate

Verification Policies and Practices

Response to Mozilla's CA Recommended Practices

Document Handling of IDNs in CP/CPS		The use of IDN is not allowed. An amendment will be done to the CPs in order to clarify this limitation. Proposed amendment: 3.4 USE OF INTERNATIONALIZED DOMAIN NAMES The use of IDN is not allowed under this Certificate Policy. This prevents from the homographic spoofing attack. The following sections of the CP will have to be re-numbered.
Revocation of Compromised Certificates		This topic is addressed in section “4.2 Revocation of the certificates” of the attached Certificate Policy.
DNS names go in SAN		Please, refer to “5.2 Certificate extensions” section, ROW “X509v3 Subject Alternative Name”. I would like to recall that in both “CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.1” and “CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates, v1.4” the use of “Subject Common Name Field” is discouraged, **but not prohibited**. Also, you can find the following comment in the “Mozilla's CA Recommended Practices - Domain owned by a Natural Person”: “*Its right, that the DNS to the CN is a deprecated solution, but the usage of the DNS in CN field is still popular*”

		We are making a smooth transition from “Subject Common Name Field” to “Subject Alternative Name Extension”
Domain owned by a Natural Person		The issuance of SSL certificates including domain names owned by natural persons is not allowed under the SSL Secure Web Server Certificate Policy.

Response to Mozilla's list of Potentially 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;”	We will add this verification in our SSL lifecycle management procedure and the correspondent amendment will be done to the CPs. Proposed amendment: 4.3 LONG-LIFE INFORMATION VERIFICATION The information included in SSL certificates older than three (3) years will be verified according to “4.1 CERTIFICATE ISSUANCE PROCESS”, “b) Acceptance of the Application” subsection, point 1.