Print this page

Mozilla - CA Program

Case Information

Case Number	00000070	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Example Owner	**Request Status**	Denied

Additional Case Information

Subject	Include Example Root	**Case Reason**	

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=647959

General information about CA's associated organization

CA Email Alias 1	alias@example.org		
CA Email Alias 2			
Company Website	NEED: URL to company website	**Verified?**	Need Response From CA
Organizational Type	Public Corporation	**Verified?**	Need Response From CA
Organizational Type (Others)	Organization Type pull-down list: - Private Corporation - Public Corporation - Government Agency - Commercial Organization - International Organization - Non-Profit Organization - Academic Institution - Consortium - NGO	**Verified?**	Need Response From CA
Geographic Focus	NEED: Country or geographic region where CA typically sells certs.	**Verified?**	Need Response From CA
Primary Market / Customer Base	NEED: - Which types of customers does the CA serve? - Are there particular vertical market segments in which it operates? - Does the CA focus its activities on a particular country or other geographic region?	**Verified?**	Need Response From CA
Impact to Mozilla Users	NEED: Why does the CA need to have their root certificate directly included in Mozilla's products, rather than being signed by another CA's root certificate that is already included in NSS? Mozilla CA certificate policy: We require that all CAs whose certificates are distributed with our software product ... provide some service relevant to typical users of our software products	**Verified?**	Need Response From CA

Response to Mozilla's list of Recommended Practices

Recommended Practices	https://wiki.mozilla.org /CA:Recommended_Practices#CA_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's list of Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Recommended Practices	NEED CA's response to each of the items listed in https://wiki.mozilla.org /CA:Recommended_Practices#CA_Recommended_Practices	**Verified?**	Need Response From CA

Response to Mozilla's list of Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org /CA:Problematic_Practices#Potentially_problematic_CA_practices	**Problematic Practices Statement**	I have reviewed Mozilla's list of Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Problematic Practices	NEED CA's response to each of the items listed in https://wiki.mozilla.org /CA:Problematic_Practices#Potentially_problematic_CA_practices	**Verified?**	Need Response From CA

Root Case Record # 1

Root Case Information

Root Certificate Name	Example Root Cert	**Root Case No**	R00000098
Request Status	Denied	**Case Number**	00000070

Additional Root Case Information

Subject	Include Example Root Cert

Technical Information about Root Certificate

O From Issuer Field		**Verified?**	Need Response From CA
OU From Issuer Field		**Verified?**	Need Response From CA
Certificate Summary		**Verified?**	Need Response From CA
Root Certificate Download URL	NEED: A public URL through which the CA certificate can be directly downloaded.	**Verified?**	Need Response From CA
Valid From		**Verified?**	Need Response From CA
Valid To		**Verified?**	Need Response From CA
Certificate Version	3	**Verified?**	Need Response From CA
Certificate Signature Algorithm	ECC	**Verified?**	Need Response From CA
Signing Key Parameters	ECC P-384	**Verified?**	Need Response From CA
Test Website URL (SSL) or Example Cert	NEED: - If requesting Websites trust bit: URL to a website whose SSL cert chains up to this root. Note that this can be a test site. - If requesting Email trust bit: attach	**Verified?**	Need Response From CA

	an example cert to the bug		
CRL URL(s)	NEED CRL URLs and CRL issuing frequency for subscriber certs, with reference to where this is documented in the CP/CPS	**Verified?**	Need Response From CA
OCSP URL(s)	NEED OCSP URL and maximum OCSP expiration time, with reference to where this is documented in the CP/CPS	**Verified?**	Need Response From CA
Revocation Tested	NEED: Test with http://certificate.revocationcheck.com/ make sure there aren't any errors.	**Verified?**	Need Response From CA
Trust Bits	Code; Email; Websites	**Verified?**	Need Response From CA
SSL Validation Type	DV; OV; EV	**Verified?**	Need Response From CA
EV Policy OID(s)	1.3.6.1.4.1.13769.9.1	**Verified?**	Need Response From CA
EV Tested	NEED: If EV treatment is being requested, then provide successful output from EV Testing as described here https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version	**Verified?**	Need Response From CA
Root Stores Included In	Adobe; Apple; Google; Microsoft; Mozilla; Opera	**Verified?**	Need Response From CA
Mozilla Applied Constraints	NEED: Mozilla has the ability to name constrain root certs; e.g. to *.gov or *.mil. CAs should consider if such constraints may be applied to their root certs.	**Verified?**	Need Response From CA

Digital Fingerprint Information

SHA-1 Fingerprint	F9:7E:62:42:4E:38:79:96:CA:87:71:2A:F8:51:38:C8:16:92:5C:A7	**Verified?**	Need Response From CA
SHA-256 Fingerprint	12:CB:98:6C:FB:27:8C:A2:30:C6:54:C5:B4:AA:02:0C:61:C5:07:FB:FD:4C:C5:E3:45:77:E4:83:EC:68:43:C9	**Verified?**	Need Response From CA

CA Hierarchy Information

CA Hierarchy	NEED: A description of the PKI hierarchy rooted at or otherwise associated with this root CA certificate. - List and/or describe all of the subordinate CAs that are signed by this root. - Identify which of the subordinate CAs are internally-operated; e.g. list the subordinate CAs that operated by the CA organization associated with the root CA. For example, this might include subordinate CAs created to issue different classes or types of end entity certificates to the general public: Class 1 vs. class 2 certificates, qualified vs. non-qualified certificates, EV certificates vs. non-EV certificates, SSL certificates vs. email certificates, and so on. - It might also include subordinate CAs operated for the benefit of specific third parties. In this case note that we do not require that the CA submit a complete customer list; rather we are interested in the general type and nature of the third-party arrangements	**Verified?**	Need Response From CA
Externally Operated SubCAs	NEED: - If this root has any subordinate CA certificates that are operated by external third parties, then provide the information listed in the Subordinate CA Checklist, https://wiki.mozilla.org/CA:SubordinateCA_checklist	**Verified?**	Need Response From CA

	- If the CA functions as a super CA such their CA policies and auditing don't apply to the subordinate CAs, then those CAs must apply for inclusion themselves as separate trust anchors.		
Cross Signing	NEED: - List all other root certificates for which this root certificate has issued cross-signing certificates. - List all other root certificates that have issued cross-signing certificates for this root certificate. - If any such cross-signing relationships exist, it is important to note whether the cross-signing CAs' certificates are already included in the Mozilla root store or not.	**Verified?**	Need Response From CA
Technical Constraint on 3rd party Issuer	NEED: CP/CPS documentation describing the technical and contractual controls over any 3rd party who may issue certs in this CA Hierarchy. This includes external RAs as well as External subCAs. References: - section 7.1.5 of version 1.3 of the CA/Browser Foruom's Baseline Requirements - https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/inclusion/ - https://wiki.mozilla.org/CA:CertificatePolicyV2.1#Frequently_Asked_Questions	**Verified?**	Need Response From CA

Verification Policies and Practices

Policy Documentation	NEED: Languages that the CP/CPS and other documents are provided in.	**Verified?**	Need Response From CA
CA Document Repository		**Verified?**	Need Response From CA
CP Doc Language			
CP		**Verified?**	Need Response From CA
CP Doc Language			
CPS		**Verified?**	Need Response From CA
Other Relevant Documents		**Verified?**	Need Response From CA
Auditor Name		**Verified?**	Need Response From CA
Auditor Website		**Verified?**	Need Response From CA
Auditor Qualifications		**Verified?**	Need Response From CA
Standard Audit	NEED: for all root inclusion/change requests. Reference section 2 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Standard Audit Type		**Verified?**	Need Response From CA

Standard Audit Statement Date		**Verified?**	Need Response From CA
BR Audit	NEED: If requesting Websites trust bit, then also need a BR audit as described here: https://wiki.mozilla.org/CA:BaselineRequirements	**Verified?**	Need Response From CA
BR Audit Type		**Verified?**	Need Response From CA
BR Audit Statement Date		**Verified?**	Need Response From CA
EV Audit	NEED only if requesting EV treatment	**Verified?**	Need Response From CA
EV Audit Type		**Verified?**	Need Response From CA
EV Audit Statement Date		**Verified?**	Need Response From CA
BR Commitment to Comply	NEED section in the CP/CPS that has the commitment to comply with the BRs as described in section 2.2 of version 1.3 of the CA/Browser Forum's Baseline Requirements.	**Verified?**	Need Response From CA
SSL Verification Procedures	NEED if Websites trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the domain name to be included in the SSL/TLS cert. As per section 3 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices https://wiki.mozilla.org/CA:BaselineRequirements#CA_Conformance_to_the_BRs It is not sufficient to simply reference section 11 of the CA/Browser Forum's Baseline Requirements (BR). BR #11.1.1 lists several ways in which the CA may confirm that the certificate subscriber owns/controls the domain name to be included in the certificate. Simply referencing section 11 of the BRs does not specify which of those options the CA uses, and is insufficient for describing how the CA conforms to the BRs. The CA's CP/CPS must include a reasonable description of the ways the CA can verify that the certificate subscriber owns/controls the domain name(s) to be included in the certificate. https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Domain_Name_Ownership	**Verified?**	Need Response From CA
EV SSL Verification Procedures	NEED: If EV verification is performed, then provide URLs and section/page number information pointing directly to the sections of the CP/CPS documents that pertain to EV and describe the procedures for verifying the ownership/control of the domain name, and the verification of identity, existence, and authority of the organization to request the EV certificate. The EV verification documentation must meet the requirements of the CA/Browser Forum's EV Guidelines, and must also provide information specific to the CA's operations.	**Verified?**	Need Response From CA
Organization Verification Procedures	NEED: CP/CPS sections that describe identity and organization verification procedures for cert issuance.	**Verified?**	Need Response From CA
Email Address Verification Procedures	NEED if Email trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the email address to be included in the cert. As per section 4 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Email_Address_Control	**Verified?**	Need Response From CA
Code Signing Subscriber Verification Pro	NEED: If you are requesting to enable the Code Signing trust bit... - URLs and section/page number information pointing directly to the sections of the CP/CPS documents that describe the procedures for verifying the certificate subscriber's identity and authority, and the organization's identity and existence. https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Identity_of_Code_Signing_Certificate_Subscriber	**Verified?**	Need Response From CA

Multi-Factor Authentication	NEED CA response (and corresponding CP/CPS sections/text) to section 6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Network Security	NEED CA response (and corresponding CP/CPS sections/text) to section 7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	NEED URL to publicly disclosed subordinate CA certificates that chain up to certificates in Mozilla's CA program, as per Items #8, 9, and 10 of Mozilla's CA Certificate Inclusion Policy.	**Verified?**	Need Response From CA