Print this page

Mozilla - CA Program

Case Information

Case Number	00000124	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Example CA Owner	**Request Status**	Initial Request Received

Additional Case Information

Subject	Include Example Root	**Case Reason**	

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=1234567

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		**Verified?**	Need Response From CA
Organizational Type (Others)	Organization Type choices: - 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	**Verified?**	Need Response From CA

	geographic region?		
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

Required and Recommended Practices

Recommended Practices	https://wiki.mozilla.org/CA/Required_or_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's lists of Required and 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: CAs response to each of the items listed in https://wiki.mozilla.org/CA/Required_or_Recommended_Practices	**Verified?**	Need Response From CA

Forbidden and Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org/CA/Forbidden_or_Problematic_Practices	**Problematic Practices Statement**	I have reviewed Mozilla's lists of Forbidden and 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/Forbidden_or_Problematic_Practices	**Verified?**	Need Response From CA

Root Case Record # 1

Root Case Information

Root Certificate Name	Example Root Cert Common Name	**Root Case No**	R00000208
Request Status	Initial Request Received	**Case Number**	00000124

Certificate Data

Certificate Issuer Common Name	
O From Issuer Field	
OU From Issuer Field	
Valid From	
Valid To	
Certificate Serial Number	
Subject	
Signature Hash Algorithm	
Public Key Algorithm	
SHA-1 Fingerprint	
SHA-256 Fingerprint	
Certificate Fingerprint	
Certificate Version	

Technical Information about Root Certificate

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
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
Trust Bits	Email; Websites	**Verified?**	Need Response From CA
SSL Validation Type	DV; OV; EV	**Verified?**	Need Response From CA
EV Policy OID(s)	2.23.140.1.2.2	**Verified?**	Need Response From CA
Root Stores Included In		**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. https://dxr.mozilla.org/mozilla-central/source/security/nss/lib/certdb/genname.c#1551	**Verified?**	Need Response From CA

Test Websites or Example Cert

Test Website - Valid		**Verified?**	Need Response From CA
Test Website - Expired			
Test Website - Revoked			
Example Cert			
Test Notes	NEED: - If requesting Websites trust bit provide 3 URLs to 3 test websites (valid, expired, revoked) whose TLS/SSL cert chains up to this root. - If only requesting the Email trust bit, then attach an example S/MIME cert to the bug.		

Test Results (When Requesting the SSL/TLS Trust Bit)

Revocation Tested	NEED: Test with http://certificate.revocationcheck.com/ make sure there aren't any errors.	**Verified?**	Need Response From CA
CA/Browser Forum Lint Test	NEED: The CA MUST check that they are not issuing certificates that violate any of the CA/Browser Forum Baseline Requirements (BRs). BR Lint Test: https://github.com/awslabs/certlint	**Verified?**	Need Response From CA
Test Website Lint Test	NEED: The CA MUST check that they are not issuing certificates that violate any of the X.509 rules. X.509 Lint Test: https://github.com/kroeckx/x509lint	**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

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/Subordinate_CA_Checklist - If the CA functions as a super CA such their CA policies and auditing don't apply to the subordinate CAs, then those subordinate CAs must apply for inclusion themselves as separate trust anchors.	**Verified?**	Need Response From CA
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 the CA/Browser Forum's Baseline Requirements - Mozilla's Root Store Policy	**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: Audit statements meeting the requirements of Mozilla's Root Store Policy.	**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 per Mozilla's Root Store Policy.	**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: If requesting EV treatment, then also need an EV audit as per Mozilla's Root Store Policy.	**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: If requesting Websites trust bit, need section in the CP/CPS that has the commitment to comply with the BRs as described in section 2.2 of the CA/Browser Forum's Baseline Requirements.	**Verified?**	Need Response From CA
BR Self Assessment	NEED: If requesting Websites trust bit, attach BR Self Assessment (https://wiki.mozilla.org/CA/BR_Self-Assessment) to the Bugzilla Bug.	**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. CP/CPS must clearly specify the procedures that the CA employs. Each documented procedure should state which subsection of BR section 3.2.2.4 it is complying with.	**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.	**Verified?**	Need Response From CA

Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	NEED section number of the CP/CPS that states that multi-factor authentication is enforced for all accounts capable of directly causing certificate issuance. (reference section 6.5 of the BRs)	**Verified?**	Need Response From CA
Network Security	NEED section number(s) of the CP/CPS dealing with Network Security.	**Verified?**	Need Response From CA