Bugzilla ID:
Bugzilla Summary:

CAs wishing to have their certificates included in Mozilla products must

1) Comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/)
2) Supply all of the information listed in http://wiki.mozilla.org/CA:Information_checklist.
    a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
    b. Review the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic_Practices

General information about the CA's associated organization

CA Company Name	
Website URL	
Organizational type	
Primark Market / Customer Base	
Impact to Mozilla Users	
CA Contact Information	CA Email Alias: CA Phone Number: Title / Department:

Technical information about each root certificate

Certificate Name	Friendly name to be used when displaying information about the root. Usually the CN.
Certificate Issuer Field	The Organization Name and CN in the Issuer must have sufficient information about the CA Organization.
Certificate Summary	A summary about this root certificate, it's purpose, and the types of certificates that are issued under it.
Root Cert URL	
SHA1 Fingerprint	
Valid From	YYYY-MM-DD
Valid To	YYYY-MM-DD
Certificate Version	
Certificate Signature Algorithm	
Signing key parameters	RSA modulus length; e.g. 2048 or 4096 bits. Or ECC named curve, e.g. NIST Curve P-256, P-384, or P-512.
Test Website URL (SSL) Example Certificate (non-SSL)	

CRL URL	URL NextUpdate for CRLs of end-entity certs, both actual value and what’s documented in CP/CPS. Test: Results of importing into Firefox browser
OCSP URL	OCSP URI in the AIA of end-entity certs Maximum expiration time of OCSP responses Testing results a) Browsing to test website with OCSP enforced in Firefox browser b) If requesting EV: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version
Requested Trust Bits	One or more of: Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type	e.g. DV, OV, and/or EV
EV Policy OID(s)	

CA Hierarchy information for each root certificate

CA Hierarchy	List, description, and/or diagram of all intermediate CAs signed by this root. Identify which subCAs are internally-operated and which are externally operated.
Externally Operated SubCAs	If this root has subCAs that are operated by external third parties, then provide the information listed here: https://wiki.mozilla.org/CA:SubordinateCA_checklist 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	List all other roots for which this root CA has issued cross-signing certificates. List all other root CAs that have issued cross-signing certificates for this root CA. Note whether the roots in question are already included in the Mozilla root store or not.

Verification Policies and Practices

Policy Documentation	Language(s) that the documents are in: CP: CPS: Relying Party Agreement:
Audits	Audit Type: Auditor: Auditor Website: URL to Audit Report and Management’s Assertions: Date of completion of last audit:

SSL Verification Procedures	If you are requesting to enable the Websites Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #3 of https://wiki.mozilla.org/CA:Information_checklist#Technical_information_about_each_root_certificate
Organization Verification Procedures	
Email Address Verification Procedures	If you are requesting to enable the Email Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #4 of https://wiki.mozilla.org/CA:Information_checklist#Technical_information_about_each_root_certificate
Code Signing Subscriber Verification Procedures	If you are requesting to enable the Code Signing Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #5 of https://wiki.mozilla.org/CA:Information_checklist#Technical_information_about_each_root_certificate

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)

Publicly Available CP and CPS	
CA Hierarchy	
Audit Criteria	
Document Handling of IDNs in CP/CPS	
Revocation of Compromised Certificates	
Verifying Domain Name Ownership	
Verifying Email Address Control	
Verifying Identity of Code Signing Certificate Subscriber	
DNS names go in SAN	
Domain owned by a Natural Person	
OCSP	

Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)

Long-lived DV certificates	
Wildcard DV SSL certificates	
Email Address Prefixes for DV Certs	If DV SSL certs, then list the acceptable email addresses that are used for verification.
Delegation of Domain / Email validation to third parties	
Issuing end entity certificates directly from roots	
Allowing external entities to operate subordinate CAs	

Distributing generated private keys in PKCS#12 files	
Certificates referencing hostnames or private IP addresses	
Issuing SSL Certificates for Internal Domains	
OCSP Responses signed by a certificate under a different root	
CRL with critical CIDP Extension	
Generic names for CAs	
Lack of Communication With End Users	