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	Indicate whether the CA is operated by a private or public corporation, government agency, international organization, academic institution or consortium, NGO, etc. Note that in some cases the CA may be of a hybrid type, e.g., a corporation established by the government. For government CAs, the type of government should be noted, e.g., national, regional/state/provincial, or municipal.
Primark Market / Customer Base	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?
Impact to Mozilla Users	If your CA will only issue certificates within your organization or for a small number of websites, then rather than including your root certificate in NSS, please consider having your CA hierarchy cross-signed with one of the already-included CA certificates (http://www.mozilla.org/projects/security/certs/included/). If your CA will be issuing certificates to the public or to a large number of websites, then please provide the following explanation. Why does this 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? Describe the types of Mozilla users who are likely to encounter your root certificate as relying parties while web browsing (HTTPS servers doing SSL), sending/receiving email to their own MTA (SMTPS, IMAPS servers doing SSL), sending/receiving S/MIME email (S/MIME email certs), etc.
Inclusion in other major browsers	Does this CA have root certificates included in any other major browsers? If yes, which? If no, why not?
CA Primary Point of Contact (POC)	https://wiki.mozilla.org/CA:Information_checklist#CA_Primary_Point_of_Contact_.28POC.29 POC direct email: Email Alias: CA Phone Number: An official representative of the CA must submit and/or participate in the root inclusion request. According to Mozilla's CA Certificate Inclusion Policy: "To request that its certificate(s) be added to the default set a CA should submit a formal request by submitting a bug report into the mozilla.org Bugzilla system ... **The request must be made by an authorized representative of the subject CA**..." If the CA contracts to another organization to help with the root inclusion request, the official representative of the CA must clarify that relationship in the bug, and must provide clear information about who the ongoing points-of-contact will be for the CA.

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.
Mozilla Applied Constraints	Mozilla has the ability to apply Domain Name Constraints at the root level, such that Mozilla products would only recognize SSL certificates in the CA's hierarchy with domains in the listed constraints. Constraints may be at the country level such as *.us; and can include a list such as (*.gov.us, *.gov, *.mil). Please consider the types of SSL certificates that need to be issued within this CA hierarchy, and if applicable provide a list of names to constrain the CA hierarchy to.
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.
OCSP URL (Required now for end-entity certs)	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 Regarding Mozilla's revocation checking plans: - OCSP is (and will continue to be) required for end-entity certs. OCSP stapling is preferred. - For revocation checking of intermediate certs we will be moving towards a CRL push mechanism, so Mozilla will not be requiring OCSP for intermediate certs.
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)	
Non-sequential serial numbers and entropy in cert	http://www.mozilla.org/projects/security/certs/policy/MaintenancePolicy.html "9. We expect CAs to maintain current best practices to prevent algorithm attacks against certificates. As such, the following steps will be taken: ...

	- all new end-entity certificates must contain at least 20 bits of unpredictable random data (preferably in the serial number)."
	The purpose of adding entropy is to help defeat a prefix-chosen collision for non collision resistant hash functions. Using SHA256 without entropy isn't a problem in a near future. However, the Mozilla Policy doesn't say that; the entropy is mandatory for all new certificates, the used hash function isn't taken into consideration. This isn't a blocker for an inclusion request if SHA1 is forbidden in the CA hierarchy. However, the CP/CPS must clearly state that SHA1 isn't an acceptable hash algorithm for certificates in this hierarchy.
Response to Recent CA Communication(s)	https://wiki.mozilla.org/CA:Communications

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 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.
Technical Constraints on Third-party Issuers	Describe the technical constraints that are in place for all third-parties (CAs and RAs) who can directly cause the issuance of certificates. See #4 of https://wiki.mozilla.org/CA:Information_checklist#CA_Hierarchy_information_for_each_root_certificate

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:
Baseline Requirements (SSL)	URL to BR audit statement: The document(s) and section number(s) where the "Commitment to Comply" with the CA/Browser Forum Baseline Requirements may be found, as per BR #8.3.

	Audits performed after January 2013 need to include verification of compliance with the CA/Browser Forum Baseline Requirements if SSL certificates may be issued within the CA hierarchy, and the audit statement shall indicate the results. https://wiki.mozilla.org/CA:CertificatePolicyV2.1#Time_Frames_for_included_CAs_to_comply_with_the_new_policy "Any Certificate Authority being considered for root inclusion after February 15, 2013 must comply with Version 2.1 or later of Mozilla's CA Certificate Policy. This includes having a Baseline Requirements audit performed if the websites trust bit is to be enabled. Note that the CA's first Baseline Requirements audit may be a Point in Time 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#Verification_Policies_and_Practices
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#Verification_Policies_and_Practices
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#Verification_Policies_and_Practices
Multi-factor Authentication	Confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance. See # 6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices
Network Security	Confirm that you have performed the actions listed in #7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices

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	
Backdating the notBefore date	