

**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](http://wiki.mozilla.org/CA:Information_checklist).
  - a. Review the Recommended Practices at [https://wiki.mozilla.org/CA:Recommended\\_Practices](https://wiki.mozilla.org/CA:Recommended_Practices)
  - b. Review the Potentially Problematic Practices at [https://wiki.mozilla.org/CA:Problematic\\_Practices](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?<br>Are there particular vertical market segments in which it operates?<br>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 ( <a href="http://www.mozilla.org/projects/security/certs/included/">http://www.mozilla.org/projects/security/certs/included/</a> ). If your CA will be issuing certificates to the public or to a large number of websites, then please provide the following explanation.<br>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?<br>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) | <a href="https://wiki.mozilla.org/CA:Information_checklist#CA_Primary_Point_of_Contact_.28POC.29">https://wiki.mozilla.org/CA:Information_checklist#CA_Primary_Point_of_Contact_.28POC.29</a><br>POC direct email:<br>Email Alias:<br>CA Phone Number:<br>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 ... <b>The request must be made by an authorized representative of the subject CA...</b> "<br>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.  |
| 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)<br>Example Certificate (non-SSL) |   |
| CRL URL   | URL<br>NextUpdate for CRLs of end-entity certs, both actual value and what's documented in CP/CPS.<br>Test: Results of importing into Firefox browser   |
| OCSP URL (Required now)                                 | OCSP URI in the AIA of end-entity certs<br>Maximum expiration time of OCSP responses<br>Testing results<br>a) Browsing to test website with OCSP enforced in Firefox browser<br>b) If requesting EV: <a href="https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version">https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version</a><br><br>BR #13.2.2: "The CA SHALL update information provided via an Online Certificate Status Protocol..."<br>BR Appendix B regarding authorityInformationAccess in Subordinate CA Certificate and Subscriber Certificate: "With the exception of stapling ... this extension MUST be present ... and it MUST contain the HTTP URL of the Issuing CA's OCSP responder" |
| Requested Trust Bits                                    | One or more of:<br>Websites (SSL/TLS)<br>Email (S/MIME)<br>Code Signing   |
| SSL Validation Type                                     | e.g. DV, OV, and/or EV  |
| EV Policy OID(s)  |   |
| Non-sequential serial numbers and entropy in cert       | <a href="http://www.mozilla.org/projects/security/certs/policy/MaintenancePolicy.html">http://www.mozilla.org/projects/security/certs/policy/MaintenancePolicy.html</a><br>"9. We expect CAs to maintain current best practices to prevent algorithm attacks against certificates. As such, the following steps will be taken: ...<br>- all new end-entity certificates must contain at least 20 bits of unpredictable random data (preferably in the serial number)."<br><br>The purpose of adding entropy is to help defeat a prefix-chosen collision for non collision resistant hash  |

|  |   |
|--|---|
|  | <p>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.</p> <p>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.</p> |
|--|---|

### CA Hierarchy information for each root certificate

|  |  |
|--|--|
| CA Hierarchy                                 | List, description, and/or diagram of all intermediate CAs signed by this root.<br>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:<br><a href="https://wiki.mozilla.org/CA:SubordinateCA_checklist">https://wiki.mozilla.org/CA:SubordinateCA_checklist</a><br>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.<br>List all other root certificates that have issued cross-signing certificates for this root certificate.<br>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<br><a href="https://wiki.mozilla.org/CA:Information_checklist#CA_Hierarchy_information_for_each_root_certificate">https://wiki.mozilla.org/CA:Information_checklist#CA_Hierarchy_information_for_each_root_certificate</a>   |

### Verification Policies and Practices

|                                      |   |
|--------------------------------------|---|
| Policy Documentation                 | Language(s) that the documents are in:<br>CP:<br>CPS:<br>Relying Party Agreement:   |
| Audits                               | Audit Type:<br>Auditor:<br>Auditor Website:<br>URL to Audit Report and Management's Assertions:   |
| Baseline Requirements (SSL)          | 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.<br><br>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. |
| 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<br><a href="https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices">https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices</a>   |
| 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 <a href="https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices">https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices</a>        |
| 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 <a href="https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices">https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices</a> |
| Multi-factor Authentication                     | Confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance. See # 6 of <a href="https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices">https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices</a>                                   |
| Network Security                                | Confirm that you have performed the actions listed in #7 of <a href="https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices">https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices</a>  |

**Response to Mozilla's CA Recommended Practices** ([https://wiki.mozilla.org/CA:Recommended\\_Practices](https://wiki.mozilla.org/CA:Recommended_Practices))

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

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

|  |   |
|--|---|
| <a href="#">Long-lived DV certificates</a>                                 |   |
| <a href="#">Wildcard DV SSL certificates</a>                               |   |
| <a href="#">Email Address Prefixes for DV Certs</a>                        | If DV SSL certs, then list the acceptable email addresses that are used for verification. |
| <a href="#">Delegation of Domain / Email validation to third parties</a>   |   |
| <a href="#">Issuing end entity certificates directly from roots</a>        |   |
| <a href="#">Allowing external entities to operate subordinate CAs</a>      |   |
| <a href="#">Distributing generated private keys in PKCS#12 files</a>       |   |
| <a href="#">Certificates referencing hostnames or private IP addresses</a> |   |

|   |  |
|---|--|
| <a href="#">Issuing SSL Certificates for Internal Domains</a>                 |  |
| <a href="#">OCSP Responses signed by a certificate under a different root</a> |  |
| <a href="#">CRL with critical CIDP Extension</a>                              |  |
| <a href="#">Generic names for CAs</a>   |  |
| <a href="#">Lack of Communication With End Users</a>                          |  |