**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>.
   1. Review the Recommended Practices at <https://wiki.mozilla.org/CA:Recommended_Practices>
   2. Review the Potentially Problematic Practices at <https://wiki.mozilla.org/CA:Problematic_Practices>

**General information about the CA’s associated organization**

|  |  |
| --- | --- |
| CA Company Name | Symantec Corporation |
| Website URL | www.thawte.com |
| Organizational type | Commercial |
| Primary Market / Customer Base | Symantec is a major commercial CA with worldwide operations and customer base. |
| Impact to Mozilla Users | Firefox users may encounter SSL certs that chain up to some of these roots, and Thunderbird users may encounter S/MIME certificates that chain up to some of these roots. |
| CA Contact Information | CA Email Alias: DL-ENG-Root-Certificate-Management@symantec.com  CA Phone Number: Gautam Kanaparthi, 650-527-7181  Title / Department: Senior Product Manager, Enterprise Security Group |

**Technical information about each root certificate**

|  |  |
| --- | --- |
| Certificate Name | thawte Primary Root CA - G2 |
| Certificate Issuer Field | C = US  O = thawte, Inc.  OU = (c) 2007 thawte, Inc. - For authorized use only  CN = thawte Primary Root CA - G2 |
| Certificate Summary | NOTE: This Root is already in Mozilla’s store – we want to update the trust bits only.  Root is offline. Used only to issue SubCAs, CRLs every quarter (or as needed), and OCSP certificates. |
| Root Cert URL | https://www.thawte.com/roots/index.html |
| SHA1 Fingerprint | aadbbc22238fc401a127bb38ddf41ddb089ef012 |
| Valid From | 11/05/2007 |
| Valid To | 01/18/2038 |
| Certificate Version | 3 |
| Certificate Signature Algorithm | SHA384withECC |
| Signing key parameters | P384 |
| Test Website URL (SSL)  Example Certificate (non-SSL) | <https://ssltest40.ssl.symclab.com> |
| CRL URL | URL: <http://crl.geotrust.com/ThawtePCA-G2.crl> |
| OCSP URL | URL: <http://ocsp.thawte.com>  *Maximum expiration time of OCSP responses*: 7 days  *Testing results*  *a) Browsing to test website with OCSP enforced in Firefox browser* - TBD  *b) If requesting EV:* - TBD |
| Requested Trust Bits | Websites (SSL/TLS)  Code Signing |
| SSL Validation Type | OV and/or EV |
| EV Policy OID(s) | 2.16.840.1.113733.1.7.48.1 |

**CA Hierarchy information for each root certificate**

|  |  |
| --- | --- |
| CA Hierarchy | Root will be used to issue internally-operated SubCAs which will issue CodeSigning, SSL, and TimeStamping certificates. |
| Externally Operated SubCAs | This root does not and will not have any subCAs that are operated by external third parties. |
| Cross-Signing | n/a |
| Technical Constraints on  Third-party Issuers | No third parties can issue certificates signed by this root. |

**Verification Policies and Practices**

|  |  |
| --- | --- |
| Policy Documentation | *Language(s) that the documents are in*: English  CP: We don’t have a separate CP for this brand.  CPS: <http://www.thawte.com/cps/index.html> Relying Party Agreement: <http://www.thawte.com/assets/documents/repository/agreements/cpsrelyingparty.pdf> |
| Audits | Audit Type: WebTrust for CA  Auditor: KPMG  Auditor Website: https://cert.webtrust.org/  URL to Audit Report and Management’s Assertions: <http://www.thawte.com> Click on WebTrust icon in lower left corner |
| Baseline Requirements (SSL) | *What is your status in regards to complying with the CAB Forum Baseline Requirements? (*[*https://www.cabforum.org/Baseline\_Requirements\_V1.pdf*](https://www.cabforum.org/Baseline_Requirements_V1.pdf)*)* Since 1 July, 2012, Symantec has issued certificates in full compliance with the CAB Forum Baseline Requirements.  *As per the CAB Forum Baseline Requirement # 8.3, where is the “Commitment to Comply” statement that should be in your CP or CPS?* In Section 1, Introduction, of the CPS. |
| 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*](https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices)   * *URLs and section/page number information pointing directly to the sections of the CP/CPS documents that describe the procedures for verifying that the domain referenced in an SSL cert is owned/controlled by the subscriber.*    + See <http://www.thawte.com/cps/index.html> Section 3.2Initial Identity Validation * If a challenge-response mechanism via email is used to confirm the ownership/control of the domain name, then provide the list of email addresses that are used for verification.   + See <http://www.thawte.com/cps/index.html> Section 3.2.2.1.1 CABF Verification Requirements for Organization Applicants. This list includes “admin‟, “administrator‟, “webmaster‟, “hostmaster‟, and “postmaster‟. * *Confirm that you have automatic blocks in place for high-profile domain names (including those targeted in the DigiNotar and Comodo attacks in 2011).* We confirm that we have such automatic blocks in place.   + *Specify the procedure for additional verification of a certificate request that is blocked*. If our automatic check detects a high-profile domain name, it flags the order for manual review. A trained Authentication Specialist must review the order details and clear the flag if the order is legitimate. * *If OV verification is performed, then provide URLs and section/page number information pointing directly to the sections of the CP/CPS documents that describe the procedures for verifying the identity, existence, and authority of the organization to request the certificate.*    + See <http://www.thawte.com/cps/index.html> Section 3.2.2Authentication of Organization Identity * 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.   + See <http://www.thawte.com/cps/index.html> Appendix B1 |
| Organization Verification Procedures | See above |
| 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*](https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices)   * N/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* [*https://wiki.mozilla.org/CA:Information\_checklist#Verification\_Policies\_and\_Practices*](https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices)   * *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.*   + See <http://www.thawte.com/cps/index.html> Section 3.2.2Authentication of Organization Identity |
| Multi-factor Authentication | *Confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance or specify the technical controls that are implemented by the CA to restrict certificate issuance through the account to a limited set of pre-approved domains or email addresses.*   * *For each account that can access the certificate issuance system, do you have the log-in procedure require something in addition to username/password?* Yes. * *Specify the form factor that you use. Examples of multi-factor authentication include smartcards, client certificates, one-time-passwords, and hardware tokens.* Client certificate and username/password are required. * *This must apply to all accounts that can cause the approval and/or issuance of end-entity certificates, including your RAs and sub-CAs, unless there are technical controls that are implemented and controlled by the CA to restrict certificate issuance through the account to a limited set of pre-approved domains or email addresses.* This applies to all accounts that can cause the approval and/or issuance of end-entity certificates. * *If technical controls are used instead of multi-factor auth for any accounts, then specify what those technical controls are.* No additional technical controls are used for those accounts.   + See <http://www.thawte.com/cps/index.html> Section 6.5.1.1CABF Requirements for System Security |
| Network Security | *Confirm that you have performed the actions listed in #7 of* [*https://wiki.mozilla.org/CA:Information\_checklist#Verification\_Policies\_and\_Practices*](https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices)  *Confirm that you have done the following, and will do the following on a regular basis:*   * *Check for mis-issuance of certificates, especially high-profile domains.* * *Review network infrastructure, monitoring, passwords, etc. for signs of intrusion or weakness.* * *Ensure Intrusion Detection System and other monitoring software is up-to-date.* * *Confirm that you will be able to shut down certificate issuance quickly if you are alerted of intrusion.*   We confirm that we have done the above, and continue to do them on a regular basis. |

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

|  |  |
| --- | --- |
| [Publicly Available CP and CPS](https://wiki.mozilla.org/CA:Recommended_Practices#Publicly_Available_CP_and_CPS) | See above |
| [CA Hierarchy](https://wiki.mozilla.org/CA:Recommended_Practices#CA_Hierarchy) | <https://www.thawte.com/roots/index.html> |
| [Audit Criteria](https://wiki.mozilla.org/CA:Recommended_Practices#Audit_Criteria) | See above (**Verification Policies and Practices:** Audits) |
| [Document Handling of IDNs in CP/CPS](https://wiki.mozilla.org/CA:Recommended_Practices#Document_Handling_of_IDNs_in_CP.2FCPS) | Symantec’s automated domain ownership process uses various ‘whois’ services to find the owner of a particular domain. We believe that in most cases of homographic spoofing, that automated process will fail, resulting in the order being flagged for manual review. Our authentication representatives who perform manual review are trained to reject any domain name made up of multiple scripts within one domain name label.  Symantec actively participates in the CA/Browser Forum, which has recently debated standards for IDN certificates. We intend to fully comply with whatever standards are drafted by that body.  Symantec will update its CPS by March 31, 2012 to reflect this policy. |
| [Revocation of Compromised Certificates](https://wiki.mozilla.org/CA:Recommended_Practices#Revocation_of_Compromised_Certificates) | See Section 4.9 Certificate Revocation and Suspension in the CPS mentioned above. |
| [Verifying Domain Name Ownership](https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Domain_Name_Ownership) | * See <http://www.thawte.com/cps/index.html> Section 3.2.2Authentication of Organization Identity |
| [Verifying Email Address Control](https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Email_Address_Control) | N/A |
| [Verifying Identity of Code Signing Certificate Subscriber](https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Identity_of_Code_Signing_Certificate_Subscriber) | * See <http://www.thawte.com/cps/index.html> Section 3.2.2Authentication of Organization Identity |
| [DNS names go in SAN](https://wiki.mozilla.org/CA:Recommended_Practices#DNS_names_go_in_SAN) | * See <http://www.thawte.com/cps/index.html> Section 3.1.1.3.5 CABF Naming Requirements |
| [Domain owned by a Natural Person](https://wiki.mozilla.org/CA:Recommended_Practices#Domain_owned_by_a_Natural_Person) | Mozilla’s recommendation conflicts with CAB Forum’s Baseline Requirements (<https://cabforum.org/Baseline_Requirements_V1_1.pdf>) Section 9.2.4 Subject Distinguished Name Fields. Symantec complies with the latest version of the CAB Forum Baseline Requirements. |
| [OCSP](https://wiki.mozilla.org/CA:Recommended_Practices#OCSP) | Symantec provides OCSP support for all certificates. OCSP service is updated at least every 3.5 days, and OCSP responses are valid for no more than 7 days. |

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

|  |  |
| --- | --- |
| [Long-lived DV certificates](https://wiki.mozilla.org/CA:Problematic_Practices#Long-lived_DV_certificates) | Symantec complies with section 6 of the Mozilla CA Certificate Inclusion Policy |
| [Wildcard DV SSL certificates](https://wiki.mozilla.org/CA:Problematic_Practices#Wildcard_DV_SSL_certificates) | Symantec does not issue such certificates under its Thawte brand |
| [Email Address Prefixes for DV Certs](https://wiki.mozilla.org/CA:Problematic_Practices#Email_Address_Prefixes_for_DV_Certs) | * See <http://www.thawte.com/cps/index.html> Section 3.2.2.1.1CABF Verification Requirements for Organization Applicants * When using the Internet mail system to confirm that the Applicant has authorization from the Domain Name Registrant to obtain a Certificate for the requested Fully-Qualified Domain Name, Symantec uses a mail system address formed in one of the following ways:   + 1. Supplied by the Domain Name Registrar;   + 2. Taken from the Domain Name Registrant‟s “registrant”, “technical”, or “administrative” contact information, as it appears in the Domain‟s WHOIS record; or;   + 3. By pre-pending a local part to a Domain Name as follows:     - a. Local part - One of the following: “admin”, “administrator”, “webmaster”, “hostmaster”, or “postmaster”; and     - b. Domain Name – Formed by pruning zero or more components from the Registered Domain Name or the requested Fully-Qualified Domain Name. |
| [Delegation of Domain / Email validation to third parties](https://wiki.mozilla.org/CA:Problematic_Practices#Delegation_of_Domain_.2F_Email_validation_to_third_parties) | * See <http://www.thawte.com/cps/index.html> Section 1.3.2 Registration Authorities   Symantec does not delegate the RA functions for EV Code Signing Certificates. |
| [Issuing end entity certificates directly from roots](https://wiki.mozilla.org/CA:Problematic_Practices#Issuing_end_entity_certificates_directly_from_roots) | Symantec issues a limited number of end-entity certificates directly from GeoTrust- and Thawte-branded roots for test purposes, and to provide business continuity for customers in exceptional circumstances (e.g., when mission-critical software does not support certificate chaining). |
| [Allowing external entities to operate subordinate CAs](https://wiki.mozilla.org/CA:Problematic_Practices#Allowing_external_entities_to_operate_subordinate_CAs) | Symantec does not allow any external entities to operate subordinate CAs signed by any Thawte root. |
| [Distributing generated private keys in PKCS#12 files](https://wiki.mozilla.org/CA:Problematic_Practices#Distributing_generated_private_keys_in_PKCS.2312_files) | Symantec does not engage in this problematic practice. |
| [Certificates referencing hostnames or private IP addresses](https://wiki.mozilla.org/CA:Problematic_Practices#Certificates_referencing_hostnames_or_private_IP_addresses) | Symantec fully complies with the CAB Forum Baseline Requirements concerning certificates with non-FQDN or private IP addresses. |
| [Issuing SSL Certificates for Internal Domains](https://wiki.mozilla.org/CA:Problematic_Practices#Issuing_SSL_Certificates_for_Internal_Domains) | Symantec’s Authentication Team is aware that .int is a valid TLD. Symantec has issued certificates to .int, and we have verified that the subscriber owns the domain name. Symantec correctly identifies internal and external domain names and verifies that subscribers own/control the domain name to be included in their certificate. |
| [OCSP Responses signed by a certificate under a different root](https://wiki.mozilla.org/CA:Problematic_Practices#OCSP_Responses_signed_by_a_certificate_under_a_different_root) | Symantec does not sign OCSP responses under a different root. |
| [CRL with critical CIDP Extension](https://wiki.mozilla.org/CA:Problematic_Practices#CRL_with_critical_CIDP_Extension) | Symantec issues only “full” CRLs. |
| [Generic names for CAs](https://wiki.mozilla.org/CA:Problematic_Practices#Generic_names_for_CAs) | Symantec does not use generic names in its root and intermediate CA certificates. |
| [Lack of Communication With End Users](https://wiki.mozilla.org/CA:Problematic_Practices#Lack_of_Communication_With_End_Users) | Symantec maintains a continuous 24x7 ability to accept and respond to certificate problem reports via Technical Support numbers, posted prominently on all corporate web portals. |