**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.geotrust.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. |
| 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 | GeoTrust Primary Certification Authority - G2 |
| Certificate Issuer Field | C = US  O = GeoTrust Inc.  OU = (c) 2007 GeoTrust Inc. - For authorized use only  CN = GeoTrust Primary Certification Authority - 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 | http://www.geotrust.com/resources/root-certificates/index.html |
| SHA1 Fingerprint | 8d1784d537f3037dec70fe578b519a99e610d7b0 |
| 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://ssltest42.ssl.symclab.com> |
| CRL URL | URL: <http://crl.geotrust.com/GeoTrustPCA-G2.crl> |
| OCSP URL | URL: <http://ocsp.geotrust.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) | 1.3.6.1.4.1.14370.1.6 |

**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.geotrust.com/resources/cps/pdfs/GeoTrustCPS-Version1.1.1.0.pdf](http://www.geotrust.com/resources/cps/pdfs/GeoTrustCPS-Version1.1.1.0.pdf%20) Relying Party Agreement: <https://www.geotrust.com/resources/cps/pdfs/gt_ssl_rpa_v.2.0.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.geotrust.com> Click on WebTrust icon in lower right 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.geotrust.com/resources/cps/pdfs/GeoTrustCPS-Version1.1.1.0.pdf](http://www.geotrust.com/resources/cps/pdfs/GeoTrustCPS-Version1.1.1.0.pdf%20) 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.geotrust.com/resources/cps/pdfs/GeoTrustCPS-Version1.1.1.0.pdf](http://www.geotrust.com/resources/cps/pdfs/GeoTrustCPS-Version1.1.1.0.pdf%20) Section 3.2.2.1 CABF Verification Requirements for Organization Applicants. The 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.geotrust.com/resources/cps/pdfs/GeoTrustCPS-Version1.1.1.0.pdf](http://www.geotrust.com/resources/cps/pdfs/GeoTrustCPS-Version1.1.1.0.pdf%20) 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.geotrust.com/resources/cps/pdfs/GeoTrustCPS-Version1.1.1.0.pdf](http://www.geotrust.com/resources/cps/pdfs/GeoTrustCPS-Version1.1.1.0.pdf%20) Appendix A1 |
| 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.*   + For GeoTrust certificates, see [http://www.geotrust.com/resources/cps/pdfs/GeoTrustCPS-Version1.1.1.0.pdf](http://www.geotrust.com/resources/cps/pdfs/GeoTrustCPS-Version1.1.1.0.pdf%20) 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.geotrust.com/resources/cps/pdfs/GeoTrustCPS-Version1.1.1.0.pdf](http://www.geotrust.com/resources/cps/pdfs/GeoTrustCPS-Version1.1.1.0.pdf%20) 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.geotrust.com/resources/root-certificates/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.geotrust.com/resources/cps/pdfs/GeoTrustCPS-Version1.1.1.0.pdf](http://www.geotrust.com/resources/cps/pdfs/GeoTrustCPS-Version1.1.1.0.pdf%20) Section 3.2.3Authentication of Domain Name |
| [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.geotrust.com/resources/cps/pdfs/GeoTrustCPS-Version1.1.1.0.pdf](http://www.geotrust.com/resources/cps/pdfs/GeoTrustCPS-Version1.1.1.0.pdf%20) 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.geotrust.com/resources/cps/pdfs/GeoTrustCPS-Version1.1.1.0.pdf> Section 3.1.1.1 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 issue wildcard DV certificates from GeoTrust roots |
| [Email Address Prefixes for DV Certs](https://wiki.mozilla.org/CA:Problematic_Practices#Email_Address_Prefixes_for_DV_Certs) | * See [http://www.geotrust.com/resources/cps/pdfs/GeoTrustCPS-Version1.1.1.0.pdf](http://www.geotrust.com/resources/cps/pdfs/GeoTrustCPS-Version1.1.1.0.pdf%20) Section 3.2.2.1CABF 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.geotrust.com/resources/cps/pdfs/GeoTrustCPS-Version1.1.1.0.pdf](http://www.geotrust.com/resources/cps/pdfs/GeoTrustCPS-Version1.1.1.0.pdf%20) 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 has a limited number of customers allowed to operate subordinate CAs. Answers to the Subordinate CA Checklist are provided below. |
| [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. |

Answers to the Subordinate CA Checklist are provided below:

1. General description of the sub-CAs operated by third parties.

These sub-CAs are operated under our GeoRoot product definition and guidelines. This product is geared toward large enterprises that operate their own certificate authority software and desire the ubiquity of a public root to issue their own client or server SSL and SMIME certificates. Enterprises are vetted to insure they meet the GeoRoot requirements for Net Worth, Errors and Omissions insurance, Certificate Practices Statement, minimum FIPS 140-2 HSM for key storage and approved CA product.

2. Selection criteria for sub-CAs

An application for GeoRoot must include Articles/Certificate of Incorporation and an incumbency certificate with a corporate seal attached. A enrolment form is completed by the customer and reviewed by the product manager to verify that each enterprise CA complies with the requirements. Each organization must maintain a CPS and Subscriber agreement which can be reviewed by Symantec. The template for such CPS is the GeoTrust CPS.

3. The CP/CPS that the sub-CAs are required to follow.

The GeoTrust CPS is at <http://www.geotrust.com/resources/repository/legal/>.

4. Requirements (technical and contractual) for sub-CAs in regards to whether or not sub-CAs are constrained to issue certificates only within certain domains, and whether or not sub-CAs can create their own subordinates.

Customers are contractually bound to issue certificates only to domains they own. Symantec has audit rights to insure enforcement of this rule. Sub-CAs cannot issue subordinate CAs.

5. Requirements (typically in the CP or CPS) for sub-CAs to take reasonable measures to verify the ownership of the domain name and email address for end-entity certificates chaining up to the root, as per section 7 of our [Mozilla CA certificate policy.](http://www.mozilla.org/projects/security/certs/policy/)

Sub-CA customers are contractually obligated to maintain authentication procedures that meet or exceed the requirements set forth in these sections of the GeoTrust CPS or AICPA WebTrust standards. Here’s an excerpt from the GeoTrust CPS:

**3.2.2 Authentication of Organization Identity**

Whenever an organization name is included in the Certificate, GeoTrust or the RA will take reasonable steps to establish that a Certificate request made on behalf of that Organization is legitimate and properly authorized. GeoTrust will ensure the following:

(a) the Organizational Name appears in conjunction with a country and possibly a state or province of other locality to sufficiently identify its place of registration or a place where it is currently doing business; and

(b) in the case of an Organization that could reasonably be expected to be registered with a local, state or national authority, in certain circumstances GeoTrust will obtain, view and verify copies of the registration documents. For instance, GeoTrust may

(a) verify the validity of the registration through the authority that issued it, or

(b) verify the validity of the registration through a reputable third party database or other resource, or

(c) verify the validity of the Organization through a trusted third party, or

(d) confirm that the Organization exists if such Organization is not the type that is typically registered or is capable of being verified under clause (b).

**3.2.3 Authentication of Domain Name**

When a domain name is included in a Certificate together with an organization name, GeoTrust or the RA will verify that the Subscriber had the right to use the domain name submitted by the Subscriber at the time it submitted its application. For instance, GeoTrust may perform this verification by confirming that the Subscriber is the same person or entity that holds the domain name registration from the relevant domain name registrar or that the Subscriber is otherwise authorized to use such domain name.

Domain name verification as described above is performed for **TrueBusiness ID, Enterprise SSL** and **Enterprise SSL Premium**, **RapidSSL Enterprise** and **FreeSSL Server** Certificates.

**True Business ID** Certificates may contain an IP address in the *CommonName* field. **RapidSSL Enterprise** Certificates may contain a private IP address in the *CommonName* field.

When a domain name is included in a Certificate without authentication of the entity owning the domain name, GeoTrust or an RA will verify that the Subscriber has control over such domain name at the time it submitted its enrolment form by accessing a third party database of domain names and their owners. To do this, GeoTrust will send an e-mail message to one of the following 7

e-mail addresses requesting confirmation of the Certificate order and authorization to issue the Certificate in the domain name:

(a) an e-mail address listed as the administrative or technical contact for the domain name in an official InterNIC domain name registry that includes the domain name,

(b) a limited list of the most commonly used generic e-mail addresses for authorized persons at domain names (e.g., “[*admin@domain.com*,“ or “*hostmaster@domain.com*](mailto:admin@domain.com,“%20or%20“hostmaster@domain.com)” for the domain name domain.com), or

(c) using a manual process of verification conducted by GeoTrust, to an e-mail address identified as the registered owner of the domain per the *whois* database. Optionally, a verification phone call may be substituted to the domain owner phone number listed in the *whois*.

Upon receipt of a confirming e-mail message authorizing issuance of the Certificate, GeoTrust will issue the Certificate as described below. Additionally, a confirmatory phone call to the applicant may be performed for Domain Control Certificate applications.

6. Description of audit requirements for sub-CAs (typically in the CP or CPS)

* Whether or not the root CA audit includes the sub-CAs. All current contracts with SubCA customers stipulate that Symantec has the right to require an audit.
* Who can perform the audits for sub-CAs. Audits will be performed by a Qualified Auditor that meets all the requirements set forth in Section 17.6 of the CA/Browser Forum Baseline Requirements.
* Frequency of the audits for sub-CAs. Audits must be performed on a yearly basis.