Bugzilla ID: 539255
Bugzilla Summary: EV enable GeoTrust SHA256 root certificate

CAs wishing to have their certificates included in Mozilla products must comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/) and must supply the information necessary to determine whether or not the policy's requirements have been satisfied, as per http://wiki.mozilla.org/CA:Information_checklist.

General Information	Data
CA Name	Symantec GeoTrust Authentication Services
Website URL	http://www.symantec.com http://www.geotrust.com/
Organizational type	Commercial
Primary market / customer base	GeoTrust is a subsidiary of Symantec. Symantec acquired the VeriSign Authentication Services and root certificates, and is a major commercial CA with worldwide operations and customer base.
CA Contact Information	CA Email Alias: DL-ENG-Root-Certificate-Management@symantec.com CA Phone Number: 1 650.961.7500 Title / Department: The Certificate Policy Manager

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	Data – G3
Certificate Name	GeoTrust Primary Certification Authority - G3
Cert summary / comments	This request is to enable EV for this SHA256 root is currently included in NSS, as per bug #484899. This CA will sign intermediate CAs that will be used to sign certificates for SSL-enabled servers, and may in the future be used to sign certificates for digitally-signed executable code objects.
Root CA URL	https://bugzilla.mozilla.org/attachment.cgi?id=368997
SHA-1 fingerprint	03:9E:ED:B8:0B:E7:A0:3C:69:53:89:3B:20:D2:D9:32:3A:4C:2A:FD
Valid from	2008-04-01
Valid to	2037-12-01
Cert Version	3
Modulus length or type of signing key	2048 SHA-256
Trust Bits	Websites Email Code Signing
Test Website	https://ssltest21.bbtest.net/ Before approval, need test website whose EV SSL cert chains up to the intermediate issuing CA, chaining up to this root.
CA Hierarchy	An EV intermediate CA will be created under this root for EV issuance
Sub-CAs operated by 3rd parties	None, and none planned.
Cross-Signing	There is no intention to have this root be involved with cross signing with another root, but it is possible it may be involved in a cross-signing to another GeoTrust Root for backward compatibility.
CRL URL	http://evsecure-crl.geotrust.com/GeoTrustPCA-G3.crl No end-entity CRL URL exists yet, because this root is not yet in use.
CRL Issuance Frequency	CPS Section 4.9.7: GeoTrust shall post the CRL online at least weekly (but no later than twenty-four (24) hours after revocation of a Certificate)

	CPS Appendix A1, section 26: For EV Certificates: (A) CRLs are be updated and reissued at least every seven (7) days, and the nextUpdate field value SHALL NOT be more than ten (10) days; or (B) OCSP. If used, GeoTrust's Online Certificate Status Protocol (OCSP) is updated at least every four (4) days, and with a maximum expiration time of ten (10) days.
OCSP	None yet – must be in place before these roots may be approved for EV. EV testing must also be completed before approval: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version
SSL Verification Type	DV, OV, EV
EV policy OID	1.3.6.1.4.1.14370.1.6
CP/CPS	Current and Archived GeoTrust Documentation: http://www.geotrust.com/resources/repository/legal.asp GeoTrust Certification Practice Statement: http://www.geotrust.com/resources/cps/pdfs/GeoTrustCPS-Version1.1.6.pdf Appendix A1: Supplemental Validation Procedures for Extended Validation SSL Certificates GeoTrust Subscriber Agreement: http://www.geotrust.com/resources/cps/pdfs/gt_ssl_SA_v.3.0.pdf GeoTrust Relying Party Agreement: http://www.geotrust.com/resources/cps/pdfs/gt_ssl_rpa_v.2.0.pdf GeoTrust Reseller Agreement: http://www.geotrust.com/resources/cps/pdfs/reseller_agreement_6.1.pdf GeoTrust EnterpriseSSL Agreement: http://www.geotrust.com/resources/cps/pdfs/enterprisessl_agreement-3.0.pdf
AUDIT	Audit Type: WebTrust CA and WebTrust EV Auditor: KPMG Audit Report and Management Assertions: https://cert.webtrust.org/SealFile?seal=650&file=pdf (2010.11.30)
Organization Identity Verification	CP/CPS Section 3.2.2, Authentication of Organization Identity
Domain Name Ownership / Control	CPS Section 3.2.3, Authentication of Domain Name
EV Validation	GeoTrust's EV SSL Verification Requirements are in Appendix A of the CPS. Sections 14 and 15: Verification of Applicant's Legal Existence and Identity Section 16: Verification of Applicant's Physical Existence Section 17: Verification of Applicant's Operational Existence Section 18: Verification of Applicant's Domain Name (starts on page 64)
Email Address Ownership / Control	CPS Section 3.2.4 of GeoTrust's CPS states that GeoTrust requires the certificate applicant to prove control over the Contact Address, which is the email address to be included in the cert. GeoTrust's process for proving control over the email address is to send an email to the Contact Address requiring the applicant to respond to a link and enter a PIN that is also sent via email.
Identity of Code Signing Subscriber	Section 3.2.2 of GeoTrust's CPS describes the steps taken to verify the identity of the certificate subscriber. CPS section 3.2.6 describes the steps taken to validate the authority of the cert subscriber to make the request.

Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices
	• Long-lived DV certificates
	  ○ CPS Appendix A1: "The maximum validity period for an EV Certificate is twenty-seven (27) months."
	• Wildcard DV SSL certificates
	  ○ CPS Section 1.4: GeoTrust may issue Wildcard Certificates, which are X.509 Certificates with SSL Extensions that are vetted to a specified level domain and may be used in connection with all next level higher domains that contain the specified vetted level domain.

	○ CPS Appendix A1: "Wildcard certificates are not allowed for EV certificates." • Delegation of Domain / Email validation to third parties ○ GeoTrust does not delegate any piece of the validation process to third parties. • Issuing end entity certificates directly from roots ○ All certs will be issued through internally-operated subordinate CAs • Allowing external entities to operate unconstrained subordinate CAs ○ GeoTrust does not allow external entities to operate unconstrained sub CAs off any of their roots. • Distributing generated private keys in PKCS#12 files ○ CPS Section 3.2.1 Method to Prove Possession of Private Key ▪ The certificate applicant must demonstrate that it rightfully holds the private key corresponding to the public key to be listed in the Certificate. The method to prove possession of a private key shall be PKCS #10, another cryptographically equivalent demonstration, or another GeoTrustapproved method. This requirement does not apply where a key pair is generated by a CA on behalf of a Subscriber, for example where pregenerated keys are placed on smart cards. • Certificates referencing hostnames or private IP addresses ○ CPS Section 3.2.3: True Business ID Certificates may contain an IP address in the CommonName field. GeoTrust Verifies the Organization's ownership of the IP address in these circumstances. • OCSP Responses signed by a certificate under a different root ○ GeoTrust does not use OCSP responses signed by a certificate under a different root. • CRL with critical CIDP Extension ○ GeoTrust's CRLs do not have the CIDP extension. • Generic names for CAs ○ No.