Bugzilla ID: 539255
Bugzilla Summary: EV enable GeoTrust ECC and SHA256 root certificates

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	GeoTrust
Website URL	http://www.geotrust.com/
Organizational type	Commercial
Primary market / customer base	GeoTrust is a commercial CA with worldwide operations and customer base; it is a subsidiary of VeriSign, Inc.
CA Contact Information	CA Email Alias: practices@verisign.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 – G2**	**Data – G3**
Certificate Name	GeoTrust Primary Certificate Authority - G2	GeoTrust Primary Certification Authority - G3
Cert summary / comments	This ECC root is currently included in NSS. Inclusion bug #409236 This CA 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.	This SHA256 root is currently included in NSS. Inclusion bug #484899 This CA 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.
OPEN ACTION ITEMS	From bug #484899 – Please post updates directly in bug #484899. ACTION: GeoTrust will remove the following email addresses from their list of options for domain validated certs: is, it, mis, ssladministrator, sslwebmaster. GeoTrust has committed to notifying their customers according to their 6-month SLAs, and then complete the changes in the February/March 2010 timeframe. ACTION: GeoTrust will update their list to meet the CAB/Forum guidelines of acceptable email addresses for domain validated certs, when the CAB/Forum guidelines are provided. ACTION: GeoTrust will update their CPS to clarify the domain verification procedures as per this discussion. Note that the clarification is not significant enough to warrant requiring another audit, and the changes will be covered in their annual audit.	
Root CA URL	https://bugzilla.mozilla.org/attachment.cgi?id=294057	https://bugzilla.mozilla.org/attachment.cgi?id=368997
SHA-1 fingerprint	8D:17:84:D5:37:F3:03:7D:EC:70:FE:57:8B:51:9A:99:E6:10:D7:B0	03:9E:ED:B8:0B:E7:A0:3C:69:53:89:3B:20:D2:D9:32:3A:4C:2A:FD

Valid from	2007-11-04	2008-04-01
Valid to	2038-01-18	2037-12-01
Cert Version	3	3
Modulus length or type of signing key	SECG elliptic curve secp384r1 (aka NIST P-384)	2048 SHA-256
Trust Bits	Websites Email Code Signing	Websites Email Code Signing
Test Website	Please provide the url to a website whose EV SSL cert chains up to this root.	Please provide the url to a website whose EV SSL cert chains up to this root.
CA Hierarchy	Please provide a description and/or diagram of the CA hierarchy under this root (current and planned), especially noting EV sub-CAs and certificates.	Please provide a description and/or diagram of the CA hierarchy under this root (current and planned), especially noting EV sub-CAs and certificates.
Sub-CAs operated by 3rd parties	None, and none planned.	None, and none planned.
Cross-Signing	Please clarify plans for each root From the root inclusion requests: These roots may be involved in cross-signing for EV or other. We have not decided on the implementation details at this point. Based on the CPS, when either the G2 or G3 root provide EV, an EV sub-CA will be created which is cross-signed by the off-line GeoTrust EV SSL CA root. CPS Appendix A1, section 7.d: There are two GeoTrust EV Root certificates. 1 – The off-line GeoTrust Extended Validation SSL CA will be signed by the Equifax Secure Certification Authority Root certificate. This Root CA does not contain the certificatePolicies or extendedKeyUsage fields. 2 – The On-line Extended Validation SSL CA certificate is signed by the EV off-line Subordinate CA, And it is also signed by the GeoTrust Primary Certificate Authority. The EVOffline subordinate CA and the GeoTrust EV Root CA both have the same subject DN and use the same key	
CRL URL	No CRL URL exists yet – Is this still the case?	No CRL URL exists yet – Is this still the case?
CRL Issuance Frequency	CPS Section 4.9.7 CRL Issuance Frequency CPS Appendix A1, section 26, EV Certificate Status Checking: GeoTrust maintains an online 24/7 Repository mechanism whereby Internet browsers can automatically check online the current status of all certificates. (1) 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	
SSL Verification Type	DV, OV, EV	
EV policy OID	1.3.6.1.4.1.14370.1.6	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-Version1.1.2.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.2.0.pdf GeoTrust Relying Party Agreement: http://www.geotrust.com/resources/cps/pdfs/gt_ssl_rpa_v.1.0.pdf GeoTrust Reseller Agreement: http://www.geotrust.com/resources/cps/pdfs/reseller_agreement_5.0.pdf GeoTrust EnterpriseSSL Agreement: http://www.geotrust.com/resources/cps/pdfs/enterprisessl_agreement.pdf	
AUDIT	Auditor: KPMG Audit Report and Management Assertions: https://cert.webtrust.org/SealFile?seal=650&file=pdf (2008.11.30) Type: This seal file contains two audit reports, one for WebTrust for CA and one for WebTrust for EV. No issues were noted in either audit report. Both the GeoTrust Primary Certificate Authority - G2 and the GeoTrust Primary Certification Authority - G3 roots are covered by the WebTrust for CA audit report. Neither of these roots have been part of a WebTrust EV Readiness audit.	
Organization Identity Verification	CP/CPS Section 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)	
Domain Name Ownership / Control	CPS Section 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 IDs and Enterprise SSL and Enterprise SSL Premium Certificates.	

	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. 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 enrollment 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 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* 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 list 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. Domain name control is performed for the products listed in the table below. • GeoTrust Power Server ID Certificates • GeoTrust QuickSSL Certificates • GeoTrust QuickSSL Premium Certificates
EV Validation	GeoTrust’s Information 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	GeoTrust: Our process for client certs is we send an email to the address applying for the cert and require them to respond to a link and enter a PIN we sent them. CPS Section 3.2.4, Authentication of individual identity An Applicant for a GeoTrust My Credential Certificate shall complete a GeoTrust My Credential enrollment application on behalf of Subscriber in a form prescribed by GeoTrust. All applications are subject to review, approval and acceptance by GeoTrust. All Applicants are required to include an e-mail contact address (“Contact Address”) and telephone number (“Telephone Number”) within the My Credential enrollment application and prove control over the Contact Address and Telephone Number as specified below. GeoTrust does not otherwise verify the accuracy of the information contained in the Applicant’s enrollment form or otherwise check for errors and omissions.

	True Credential Subscribers must provide the following data in or with the CSR: Common Name and E-mail Address of Subscriber. Company's Administrator will have sole responsibility for approving all Certificate requests for issuance. Once approved, GeoTrust will process the Certificate applications without confirming the information on the Certificates. Company will be required to agree to terms and conditions of use as necessary for issuance of Certificates through an enrollment agreement, and Subscribers receiving Certificates via the Service may be required to agree to additional terms and conditions of use as necessary to receive a Certificate authorized by the Administrator.
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.
Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices • Long-lived DV certificates o GeoTrust issues DV certs up to 5 years. o CPS Appendix A1: "The maximum validity period for an EV Certificate is twenty-seven (27) months." o GeoTrust: We do plan to issue domain validated certs from the GeoTrust Primary Certificate Authority - G2 roots, but have not decided with the GeoTrust Primary Certificate Authority - G3 root. For validity period, we plan to issue per the new minimum SSL guidelines being developed by the CAB Forum. o Comment #12: The proposed validity of the minimal guidelines Jay refers to is 27 month, the same like EV. • Wildcard DV SSL certificates o 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. o CPS Appendix A1: "Wildcard certificates are not allowed for EV certificates." • Delegation of Domain / Email validation to third parties o GeoTrust does not delegate any piece of the validation process to third parties. • Issuing end entity certificates directly from roots o All certs will be issued through subordinate CAs • Allowing external entities to operate unconstrained subordinate CAs o GeoTrust does not allow external entities to operate unconstrained sub CAs off any of their roots. • Distributing generated private keys in PKCS#12 files o 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 o 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 o OCSP not provided yet for either of these roots. o GeoTrust does not use OCSP responses signed by a certificate under a different root. • CRL with critical CIDP Extension o GeoTrust's CRLs do not have the CIDP extension. • Generic names for CAs o No.