The document summarizes the information gathered and verified for two requests from GeoTrust.
Bugzilla ID #409236 -- Add GeoTrust's ECC root
Bugzilla ID #484899 -- Add GeoTrust's SHA2 root

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.

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

Info Needed	**Data - #409236**	**Data - #484899**
Certificate Name	GeoTrust Primary Certificate Authority - G2	GeoTrust Primary Certification Authority - G3
Cert summary / comments	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 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.
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
Requested Trust Bits	Websites Email Code Signing	Websites Email
Test Website	https://ecc-test-valid.geotrust.com We do not have EV test certs for the G2 root as we do not have this root enabled in a production environment yet.	https://ptnr-geotrust256.bbtest.net We do not currently use this root for production level certificates, so this certificate was issued directly from the root. In production our plan will be to use this root to sign an intermediate CA that will issue the ee certs.

List or description of subordinate CAs operated by the CA organization associated with the root CA.	Planned sub-CAs for the G2 root: • Class 3 Secure Server CA (standard SSL certificates) • Class 3 Secure Intranet Server CA (intranet SSL certificates) • Class 3 Extended Validation SSL CA (EV SSL certificates) • Class 3 Code Signing (EV and non-EV Code Signing certificates) • OnSite Administrator CA - Class 3 (Enterprise portal Admin certificates) • Class 3 Open Financial Exchange CA - G2 (OFX SSL certificates) • Time Stamping Authority CA (time stamping certificates) • Class 3 Mobile CA (authentication of servers in the mobile space) • Class 3 WLAN CA (for Microsoft RADIUS/IAS servers) • Class 3 Organizational CA (S/MIME certs for organizations) All of these subordinate CAs are operated by the CA organization associated with the root CA.	This root CA has not yet issued any intermediate or subordinate CA certificates. It may be used to issue Subordinate CA certificates for SSL. It will also be used to sign CRLs. Planned sub-CAs for the G3 root: • Class 3 Secure Server CA (standard SSL certificates) • Class 3 Secure Intranet Server CA (intranet SSL certificates) • Class 3 Extended Validation SSL CA (EV SSL certificates)
subordinate CAs operated by third parties	None	
List any other root CAs that have issued cross-signing certificates for this root CA	None yet. However, 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 GeoTrust: Your interpretation is correct of our plans to create a new EV subca and cross-certify.	

CRL URL	**No CRL exists yet** GeoTrust has not yet issued any certificates from either of these roots, so they have yet to issue a CRL.
CRL Issuance Frequency	CPS Section 4.9.7 CRL Issuance Frequency GeoTrust shall post the CRL online at least weekly (but no later than twenty-four (24) hours after revocation of a Certificate) in a DER format except as otherwise provided in GeoTrust's Business Continuity Plan. CPS Apendix 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
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: DV, OV, and/or EV	DV, OV, EV (not requesting EV-enablement at this time) 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. 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. 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 conducted by GeoTrust, to another e-mail address containing the domain name that is listed as the Common Name in the enrollment form. 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.

EV policy OID	1.3.6.1.4.1.14370.1.6 (not requesting EV-enablement at this time) CPS Appendix A1, section 7, EV Certificate Policy Identification Requirements: (a) EV Subscriber Certificates Each EV Certificate issued by GeoTrust to a Subscriber will include GeoTrust’s EV OID in the certificate’s certificatePolicies extension. GeoTrust’s EV OID used for this purpose is 1.3.6.1.4.1.14370.1.6. This is the only GeoTrust EV certificate that contains this special GeoTrust EV OID since GeoTrust owns all CAs in the hierarchy. (b) EV On-line Subordinate CA Certificate The GeoTrust Extended Validation SSL CA contains the special anyPolicy OID (2.5.29.32.0) in the certificatePolicies extension. (c) EV Off-line Subordinate CA Certificate The GeoTrust Extended Validation SSL CA contains the special anyPolicy OID (2.5.29.32.0) in the certificatePolicies extension. (d) Root CA Certificates 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
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-Version1.1.1.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.

	Note: Not requesting EV-enablement at this time. It appears that neither of these roots have been part of a WebTrust EV Readiness audit. GeoTrust: GeoTrust did complete an EV readiness audit back in 2006 to be eligible to issue EV certificates. At that time the G2 root was not created so was not included in the EV readiness audit. Per the letter from KPMG (our auditor) attached to bugzilla 409236, our annual WebTrust for CAs reports for the GeoTrust cover the effectiveness of CA controls including the CA key generation process based on the WebTrust for CAs criteria. Each audit cycle, KPMG tests various CA key generation ceremonies and identify specific production CAs in their reports.

Review CPS sections dealing with subscriber verification
(section 7 of http://www.mozilla.org/projects/security/certs/policy/)

- Verify domain check for SSL
    - 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 conducted by GeoTrust, to another e-mail address containing the domain name that is listed as the Common Name in the enrollment form. 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.
            - 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
- Verify the email account associated with the email address in the cert is owned by the subscriber. In addition to verification of subscriber’s legal identity.
    - 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.
    - 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.

- Verify identity info in code signing certs is that of subscriber
    - 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).

Flag Problematic Practices
(http://wiki.mozilla.org/CA:Problematic_Practices)

- Long-lived DV certificates
    - GeoTrust issues DV certs up to 5 years.
    - CPS Appendix A1: "The maximum validity period for an EV Certificate is twenty-seven (27) months."
    - 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.
    - Comment #12: The proposed validity of the minimal guidelines Jay refers to is 27 month, the same like EV.
- 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 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
  - OCSP not provided yet for either of these roots.
  - 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.