The document summarizes the information gathered and verified for two requests from GeoTrust.
**Bugzilla ID:** 409236
**Bugzilla Summary:** Add GeoTrust's ECC root
**Bugzilla ID:** 484899
**Bugzilla Summary:** 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<br>or type of signing key | SECG elliptic curve secp384r1 (aka NIST P-384) | 2048<br>SHA-256 |
| Test Website | https://ecc-test-valid.geotrust.com | Need website whose cert chains up to this root. |
| CRL | **No CRL URL exists yet.**<br>GeoTrust does not yet have a CRL URL for this root, because they are not yet actively issuing certificates from this root. They are trying to get this root into the NSS database in anticipation of a market in the near future | Need: CRL(s) for end-entity certs issued from this root |

| | | |
|---|---|---|
| | CPS Section 4.9.7 CRL Issuance Frequency<br>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. | |
| OCSP | none | Is there OCSP for this G3 root? |
| List or description of subordinate CAs operated by the CA organization associated with the root CA. | Planned sub-CAs for the G2 root:<br>• Class 3 Secure Server CA (standard SSL certificates)<br>• Class 3 Secure Intranet Server CA (intranet SSL certificates)<br>• Class 3 Extended Validation SSL CA (EV SSL certificates)<br>• Class 3 Code Signing (EV and non-EV Code Signing certificates)<br>• OnSite Administrator CA - Class 3 (Enterprise portal Admin certificates)<br>• Class 3 Open Financial Exchange CA - G2 (OFX SSL certificates)<br>• Time Stamping Authority CA (time stamping certificates)<br>• Class 3 Mobile CA (authentication of servers in the mobile space)<br>• Class 3 WLAN CA (for Microsoft RADIUS/IAS servers)<br>• Class 3 Organizational CA (S/MIME certs for organizations)<br>All of these subordinate CAs are operated by the CA organization associated with the root CA. | Please provide a description of the CA hierarchy for this root. |
| subordinate CAs operated by third parties | None and none planned. | Are, or will there be, subordinate CAs operated by third parties? |
| List any other root CAs that have issued cross-signing certificates for this root CA | None and none planned. | Has this G3 root been involved in cross-signing with another root? |
| Requested Trust Bits<br>• Websites (SSL/TLS)<br>• Email (S/MIME)<br>• Code Signing | Websites<br>Code Signing | Which trust bits are you requesting for this root? |

| | | |
|---|---|---|
| If SSL certificates are issued within the hierarchy rooted at this root CA certificate: DV, OV, and/or EV | DV, OV<br>CPS 3.2.3 Authentication of Domain Name<br>CPS 3.2.2 Authentication of Organization Identity | DV, OV<br>CPS 3.2.3 Authentication of Domain Name<br>CPS 3.2.2 Authentication of Organization Identity |
| EV policy OID | Not EV | Are you requesting EV for this root? |
| CP/CPS | Current and Archived GeoTrust Documentation: http://www.geotrust.com/resources/repository/legal.asp<br>GeoTrust Certification Practice Statement: http://www.geotrust.com/resources/cps/pdfs/GeoTrustCPS-Version1.1.1.pdf<br>GeoTrust Subscriber Agreement: http://www.geotrust.com/resources/cps/pdfs/gt_ssl_SA_v.2.0.pdf<br>GeoTrust Relying Party Agreement: http://www.geotrust.com/resources/cps/pdfs/gt_ssl_rpa_v.1.0.pdf<br>GeoTrust Reseller Agreement: http://www.geotrust.com/resources/cps/pdfs/reseller_agreement_5.0.pdf<br>GeoTrust EnterpriseSSL Agreement: http://www.geotrust.com/resources/cps/pdfs/enterprisessl_agreement.pdf | |
| AUDIT | Auditor: KPMG<br>Type: WebTrust for CA<br>Audit Report and Management Assertions: https://cert.webtrust.org/SealFile?seal=650&file=pdf<br>2008-01-31<br>Is there a more recent audit? If not, when do you expect to do your next audit? | |

**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.
    - Not Applicable, Not requesting e-mail trust bit.
- 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
    - ?
- 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.
- Delegation of Domain / Email validation to third parties
    - ?

- Issuing end entity certificates directly from roots
    - All certs issued through subordinate CAs
- Allowing external entities to operate unconstrained subordinate CAs
    - ?
- 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
    - ?
- CRL with critical CIDP Extension
    - ?
- Generic names for CAs
    - No.

**Verify Audits**

- Validate contact info in report, call to verify that they did indeed issue this report.
    - On WebTrust site
- For EV CA’s, verify current WebTrust EV Audit done.
    - N/A
- Review Audit to flag any issues noted in the report
    - No issues noted