Print this page

Mozilla - CA Program

Case Information

Case Number	00000043	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Symantec / GeoTrust	**Request Status**	Need Information from CA

Additional Case Information

Subject	Enable EV for GeoTrust ECC root	**Case Reason**	New Owner/Root inclusion requested

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=834004

General information about CA's associated organization

CA Email Alias 1	dl-eng-root-certificate-management@symantec.com		
CA Email Alias 2			
Company Website	http://www.geotrust.com/	**Verified?**	Verified
Organizational Type	Commercial Organization	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	Global	**Verified?**	Verified
Primary Market / Customer Base	Symantec/GeoTrust is a major commercial CA with worldwide operations and customer base.	**Verified?**	Verified
Impact to Mozilla Users	Enable EV for already-included root.	**Verified?**	Verified

Response to Mozilla's list of Recommended Practices

Recommended Practices	https://wiki.mozilla.org /CA:Recommended_Practices#CA_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's list of Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Recommended Practices	NEED response to each item listed in https://wiki.mozilla.org /CA:Recommended_Practices#CA_Recommended_Practices	**Verified?**	Need Response From CA

Response to Mozilla's list of Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org /CA:Problematic_Practices#Potentially_problematic_CA_practices	**Problematic Practices Statement**	I have reviewed Mozilla's list of Potentially Problematic Practices, and confirm that we

			do not do those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Problematic Practices	NEED response to each items listed in https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices	**Verified?**	Need Response From CA

Root Case Record # 1

Root Case Information

Root Certificate Name	GeoTrust Primary Certification Authority - G2	**Root Case No**	R00000058
Request Status	Need Information from CA	**Case Number**	00000043

Additional Root Case Information

Subject	Enable EV for GeoTrust Primary Certification Authority - G2

Technical Information about Root Certificate

O From Issuer Field	GeoTrust Inc.	**Verified?**	Verified
OU From Issuer Field	(c) 2007 GeoTrust Inc. - For authorized use only	**Verified?**	Verified
Certificate Summary	Enable EV treatment for the GeoTrust Primary Certification Authority - G2 root that was included via Bugzilla Bug #409236.	**Verified?**	Verified
Root Certificate Download URL	Already Included	**Verified?**	Verified
Valid From	2007 Nov 05	**Verified?**	Verified
Valid To	2038 Jan 18	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	ECC	**Verified?**	Verified
Signing Key Parameters	ECC P-384	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://ssltest42.ssl.symclab.com/	**Verified?**	Verified
CRL URL(s)	http://crl.geotrust.com/GeoTrustPCA-G2.crl	**Verified?**	Verified
OCSP URL(s)	http://ocsp.geotrust.com Maximum expiration time of OCSP responses: 7 days	**Verified?**	Verified
Revocation Tested	NEED: Resolve all errors reported by https://certificate.revocationcheck.com/ssltest42.ssl.symclab.com	**Verified?**	Need Response From CA
Trust Bits	Code; Email; Websites	**Verified?**	Verified
SSL Validation Type	OV; EV	**Verified?**	Verified
EV Policy OID(s)	1.3.6.1.4.1.14370.1.6	**Verified?**	Verified

EV Tested	NEED: update the test website to have an EV SSL cert that is not signed directly by the root. https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version#Running_the_test_locally Results in: Verifying the certificate at 'ssltest42.ssl.symclab.com:443' failed. The following additional output may be informative: BuildCertChain failed: SEC_ERROR_POLICY_VALIDATION_FAILED Cert chain fails policy validation It appears be the case that the end-entity certificate was issued directly by the root. There should be at least one intermediate in the certificate issuance chain.	**Verified?**	Need Response From CA
Root Stores Included In	Microsoft; Mozilla	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	8D:17:84:D5:37:F3:03:7D:EC:70:FE:57:8B:51:9A:99:E6:10:D7:B0	**Verified?**	Verified
SHA-256 Fingerprint	5E:DB:7A:C4:3B:82:A0:6A:87:61:E8:D7:BE:49:79:EB:F2:61:1F:7D:D7:9B:F9:1C:1C:6B:56:6A:21:9E:D7:66	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	Root will be used to issue internally-operated SubCAs which will issue end-entity certificates.	**Verified?**	Verified
Externally Operated SubCAs	NEED Clarification: Can this root have externally-operated subordinate CAs?	**Verified?**	Need Clarification From CA
Cross Signing	NEED Clarification: Has this root been involved in any cross-signing? If yes, with which other root(s)?	**Verified?**	Need Clarification From CA
Technical Constraint on 3rd party Issuer	NEED Clarification: Can external RAs directly cause the issuance of certs in this CA hierarchy? What types of certs can they issue? What technical and contractual constraints are in place regarding the issuance of certs by external parties?	**Verified?**	Need Clarification From CA

Verification Policies and Practices

Policy Documentation	GeoTrust is a subsidiary of Symantec https://www.symantec.com/about/profile/policies/repository.jsp	**Verified?**	Verified
CA Document Repository	https://www.geotrust.com/resources/repository/legal/	**Verified?**	Verified
CP Doc Language	English		
CP	https://www.geotrust.com/resources/cps/pdfs/GeoTrustCPS-Version1.1.17.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://www.geotrust.com/resources/cps/pdfs/GeoTrustCPS-Version1.1.17.pdf	**Verified?**	Verified
Other Relevant Documents	Subscriber Agreement: https://www.geotrust.com/resources/cps/pdfs/ssl_SA_v9.0.pdf	**Verified?**	Verified

Auditor Name	KPMG	**Verified?**	Verified
Auditor Website	http://www.us.kpmg.com/	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified
Standard Audit	https://cert.webtrust.org/SealFile?seal=1567&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	5/5/2015	**Verified?**	Verified
BR Audit	http://www.symantec.com/content/en/us/about/media/repository/symantec-webtrust-audit-report.pdf	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	5/5/2015	**Verified?**	Verified
EV Audit	https://cert.webtrust.org/SealFile?seal=1567&file=pdf	**Verified?**	Verified
EV Audit Type	WebTrust	**Verified?**	Verified
EV Audit Statement Date	5/5/2015	**Verified?**	Verified
BR Commitment to Comply	CPS section 1.1	**Verified?**	Verified
SSL Verification Procedures	CPS section 3.2.3: 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 ... 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 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 listed in the whois. Upon receipt of a confirming e-mail message authorizing issuance of the Certificate, GeoTrust will issue the Certificate...	**Verified?**	Verified
EV SSL Verification Procedures	NEED Clarification: CPS refers to non-existent supplemental validation procedures for EV SSL certs. CPS section 3.2.2: Extended Validation (EV) Certificates Additional Procedures - Extended Validation (EV) Certificates - Supplemental validation procedures for issuing EV SSL Certificates are described in Appendix A1 to this CPS. CPS Appendix A1 does not exist Appendix B1 says: "The current version of the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation (EV) SSL Certificates can be accessed at https://cabforum.org/extended validation/	**Verified?**	Need Clarification From CA

	o submit, the EV Certificate" so, doesn't say anything useful		
Organization Verification Procedures	CPS section 3.2.2 -- Authentication of Organization Identity section 3.2.4 - Authentication of individual identity section 3.2.6 - Validation of Authority	**Verified?**	Verified
Email Address Verification Procedures	NEED Clarification: Currently the Email trust bit is also turned on for this root. If you will not be issuing Email (S/MIME) certs in this CA hierarchy, then we should turn off the email trust bit for this root. Please confirm. If the email trust bit is to remain enable for this root, then please provide documentation in the CP/CPS about what steps are taken to verify that the email address to be included in the certificate is owned/controlled by the certificate subscriber. See https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Email_Address_Control and https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices items #4	**Verified?**	Need Clarification From CA
Code Signing Subscriber Verification Pro	NEED Clarification: CPS refers to non-existent supplemental validation procedures for EV Code Signing certs. CPS section 3.2.2: Extended Validation (EV) Certificates Additional Procedures Extended Validation (EV) Certificates Supplemental validation procedures for issuing EV Code-Signing Certificates are described in Appendix B to this CPS. Appendix B is not about Code Signing certs. Appendix C says: "The current version of the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation (EV) Code Signing Certificates can be accessed at https://cabforum.org/ev-code-signing-certificate-guidelines/" So, doesn't say anything useful.	**Verified?**	Need Clarification From CA
Multi-Factor Authentication	NEED response to item #6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices CPS section 6.5.1.1: EV SSL Certificates, EV Code Signing, and domain validated and organization validated SSL Certificates conform to the CA /Browser Forum requirements as set forth in the GeoTrust Supplemental Procedures, Appendix B1, Appendix C and Appendix D, respectively. Where is the "GeoTrust Supplemental Procedures"? Mozilla process depends on public-facing docs.	**Verified?**	Need Response From CA
Network Security	Confirm that you have performed the actions listed in #7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices We confirm that we have done the above, and continue to do them on a regular basis.	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	https://bugzilla.mozilla.org/show_bug.cgi?id=1019860	**Verified?**	Verified