Print this page

Mozilla - CA Program

Case Information

Case Number	00000044	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Symantec / Thawte	**Request Status**	Need Information from CA

Additional Case Information

Subject	Enable EV-treatement for thawte Primary Root CA - G2	**Case Reason**	New Owner/Root inclusion requested

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=833998

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.thawte.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/Thawte is a major commercial CA with worldwide operations and customer base.	**Verified?**	Verified
Impact to Mozilla Users	Enable EV treatment on an included root cert.	**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 item 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	thawte Primary Root CA - G2	**Root Case No**	R00000059
Request Status	Need Information from CA	**Case Number**	00000044

Additional Root Case Information

Subject	Enable EV for thawte Primary Root CA - G2

Technical Information about Root Certificate

O From Issuer Field	thawte, Inc."	**Verified?**	Verified
OU From Issuer Field	(c) 2007 thawte, Inc. - For authorized use only"	**Verified?**	Verified
Certificate Summary	Enable EV treatment for already-included root.	**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://ssltest40.ssl.symclab.com/	**Verified?**	Verified
CRL URL(s)	http://crl.geotrust.com/ThawtePCA-G2.crl	**Verified?**	Verified
OCSP URL(s)	http://ocsp.thawte.com	**Verified?**	Verified
Revocation Tested	NEED: Resolve errors listed here: https://certificate.revocationcheck.com /ssltest40.ssl.symclab.com	**Verified?**	Need Response From CA
Trust Bits	Code; Websites	**Verified?**	Verified
SSL Validation Type	OV; EV	**Verified?**	Not Applicable

EV Policy OID(s)	2.16.840.1.113733.1.7.48.1	**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 'ssltest40.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	AA:DB:BC:22:23:8F:C4:01:A1:27:BB:38:DD:F4:1D:DB:08:9E:F0:12	**Verified?**	Verified
SHA-256 Fingerprint	A4:31:0D:50:AF:18:A6:44:71:90:37:2A:86:AF:AF:8B:95:1F:FB:43:1D:83:7F:1E:56:88:B4:59:71:ED:15:57	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	This root is used to issue internally-operated SubCAs which issue CodeSigning, SSL, and TimeStamping certificates.	**Verified?**	Verified
Externally Operated SubCAs	This root does not and will not have any subCAs that are operated by external third parties.	**Verified?**	Verified
Cross Signing	None. None planned.	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	CPS section 3.2.2.1: With respect to thawte Certificate Center Enterprise (TCCE), formerly SPKI, Customers, the identity confirmation process begins with thawte's confirmation of the identity of the TCCE Customer itself in accordance with this section. Following such confirmation, the TCCE Customer is responsible for approving the issuance of SSL Web Server and Code Signing Certificates within its own organization by ensuring that the server designated as the Subject of a SSL Web Server Certificate actually exists.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Documents are in English.	**Verified?**	Verified
CA Document Repository	http://www.thawte.com/repository	**Verified?**	Verified

CP Doc Language	English		
CP	http://www.thawte.com/repository	**Verified?**	Verified
CP Doc Language	English		
CPS	http://www.thawte.com/cps/index.html	**Verified?**	Verified
Other Relevant Documents	Relying Party Agreement: http://www.thawte.com/assets/documents/repository/agreements/cpsrelyingparty.pdf	**Verified?**	Verified
Auditor Name	KPMG	**Verified?**	Verified
Auditor Website	http://www.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=1566&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	5/5/2015	**Verified?**	Verified
BR Audit	https://cert.webtrust.org/SealFile?seal=1566&file=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=1566&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	**Verified?**	Verified
SSL Verification Procedures	NEED documentation in the CPS about what steps are taken to verify that the domain name to be included in the SSL certificate is owned/controlled by the certificate subscriber. See https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Domain_Name_Ownership The only information along these lines currently in the CPS is only for SSL 123. CPS section 1.1: thawte Medium Assurance SSL123 Certificates are issued to Domains to provide confidentiality encryption. thawte validates that the person enrolling for the certificate has control of the domain by requiring the person to respond to an e-mail hosted at that domain. No organization authentication is performed on the owner of the domain. CPS section 3.2.2.1: Where a domain name or e-mail address is included in the certificate thawte authenticates the Organization's right to use that domain name. Confirmation of an organization's right to use a domain name is not performed for SSL123 Certificates. For these certificates, validation of domain control only is performed, as described in Table 12 below. SSL123 Certificate -- thawte validates the Certificate Applicant's control of a domain by requiring the person to answer an e-mail sent to the e-mail address listed or predetermined for that domain.	**Verified?**	Need Response From CA
EV SSL Verification Procedures	NEED information in the CPS that says what Thawte actually does regarding verification for EV SSL certs. CPS section 3.2.2.1: SSL Web Server Certificates with EV - thawte's procedures for issuing Extended Validation SSL Certificates are described in Appendix B1 to this CPS." 3.2.2.1.1 CABF Verification Requirements for Organization Applicants EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated	**Verified?**	Need Response From CA

	SSL Certificates conform to the CA / Browser Forum requirements as set forth in the thawte Supplemental Procedures, Appendix B1, Appendix C and Appendix D, respectively. Appendix B1: "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/" This doesn't say what Thawte does.		
Organization Verification Procedures	CPS section 3.2.2 - Authentication of Organization Identity	**Verified?**	Verified
Email Address Verification Procedures	Email trust bit is not set.	**Verified?**	Not Applicable
Code Signing Subscriber Verification Pro	NEED information in the CPS that says what Thawte actually does regarding verification for code signing certs. It is *not* sufficient to merely refer to other documents. See https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Identity_of_Code_Signing_Certificate_Subscriber	**Verified?**	Need Response From CA
Multi-Factor Authentication	Need response to item #6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Network Security	Need response to item #7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	https://bugzilla.mozilla.org/show_bug.cgi?id=1019863	**Verified?**	Verified