Bugzilla ID: 539257
Bugzilla Summary: EV enable thawte SHA256 root certificate

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	Symantec thawte Authentication Services
Website URL	http://www.symantec.com http://www.thawte.com
Organizational type	Commercial
Primary market / customer base	Thawte is a subsidiary of Symantec. Symantec acquired the VeriSign Authentication Services and root certificates, and is a major commercial CA with worldwide operations and customer base.
CA Contact Information	CA Email Alias: practices@verisign.com CA Phone Number: 1 650.961.7500 Title/Department: 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 – G3**
Certificate Name	thawte Primary Root CA - G3
Cert summary / comments	This SHA256 root is currently included in NSS. Inclusion bug #484903. This request is to EV-enabled this root.
Root CA cert URL	https://bugzilla.mozilla.org/attachment.cgi?id=369000
SHA-1 fingerprint	F1:8B:53:8D:1B:E9:03:B6:A6:F0:56:43:5B:17:15:89:CA:F3:6B:F2
Valid from	2008-04-02
Valid to	2037-12-01
Cert Version	3
Modulus length or type of signing key	2048 SHA-256
Test Website	https://ssltest8.bbtest.net/
CRL	http://crl.thawte.com/ThawtePCA-G3.crl CPS 4.4.9 CRL Issuance Frequency: For end-entity certs, the CRLs are issued "At Least Daily"
OCSP	None yet – must be in place before being approved for EV.
CA Hierarchy	Thawte will have this root offline and create sub CAs that issue the end-entity certs. The sub CAs will sign certificates for SSL-enabled servers, and may in the future be used to sign certificates for digitally-signed executable code objects. "thawte Primary Root CA – G3" will sign an intermediate CA "thawte Extended Validation SSL CA" which will sign the end-entity EV SSL certs. Thawte plans to issue SSL123 certs off a subCA chained to this "thawte Primary Root CA - G3" root.

SubCAs operated by 3rd parties	None and none planned. Thawte does not allow 3rd parties to operate sub CAs from Thawte roots.
Cross-signing	None and none planned.
Trust Bits	Websites Code
SSL Verification Type	DV, OV, EV Thawte's SSL123 certificates are of Medium Assurance, which is DV. Thawte's SSL Web Server Certificates, Wildcard Certificates, and Server Gated Cryptography (SGC) SSL certificates are of High Assurance – both the domain ownership and the organization are verified.
EV policy OID	2.16.840.1.113733.1.7.48.1
CP/CPS	Thawte Documents: http://www.thawte.com/repository CPS: http://www.thawte.com/cps/index.html -- Appendix A1 has Supplemental Validation Procedures EV SSL Certificates
AUDIT	Audit Type: WebTrust CA and WebTrust EV Auditor: KPMG Audit Report & Management Assertions: https://cert.webtrust.org/SealFile?seal=527&file=pdf (2010.11.30)
Levels of Verification	CPS Section 1.1: There are two levels of verification for SSL certificates, High Assurance (both the Organization and the domain are verified) and Medium Assurance (only the domain is verified, not the organization). Thawte High Assurance Certificates are: SSL Web Server Certificates with EV, SSL Web Server Certificates, Wildcard SSL Certificates, SGC SuperCerts, and Code Signing Certificates. Thawte Medium Assurance Certificates are: SSL123 Certificates.
Organization Identity Verification	See CPS Section 3.1.8 -- Authentication of Organization Identity
Domain Name Ownership / Control	CPS Section 3.1.8.1 Authentication of the Identity of Organizational End-User Subscribers • 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 • SSL 123 Certs: thawte validates the Certificate Applicants 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. Thawte's acceptable e-mail aliases for DV-verification are listed here: https://search.thawte.com/support/ssl-digital-certificates/index?page=content&id=SO5555&actp=search&viewlocale=en_US&searchid=1287593215908 They are: - admin@yourdomain - administrator@yourdomain - hostmaster@yourdomain - root@yourdomain - webmaster@yourdomain - postmaster@yourdomain CPS section 1.1: Thawte Certificate Center Enterprise (TCCE): TCCE Customers approve or deny certificate requests using the TCCE Account system functionality. Customers manage the life cycle of certificates themselves and thus have full control of revocation and renewal of certificates. As with other certificates, thawte performs the back-end

	certificate issuance. Customers only issue certificates for SSL Web Server, SGC SuperCerts and Code Signing Certificates within their own organizations. (Table 19: TCCE customers cannot approve EV SSL certs or SSL123 certs).
EV Validation	CPS Appendix A1, Sections: 14. Verification of Applicant’s Legal Existence and Identity 15. Verification of Applicant’s Legal Existence and Identity – Assumed Name 16. Verification of Applicant’s Physical Existence 17. Verification of Applicant’s Operational Existence 18. Verification of Applicant’s Domain Name
Email Address Ownership / Control	Email trust bit is not enabled.
Identity of Code Signing Subscriber	CPS Section 1.1, the table indicates that Code Signing Certificates are of High Assurance CPS Section 3.1.8.1: *thawte* confirms the identity of a Certificate Applicant for a High Assurance Server or Code Signing Certificate by: • Verifying that the organization exists through the use of at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government that confirms the existence of the organization and • Confirming with an appropriate Organizational contact by telephone, postal mail, or a comparable procedure certain information about the organization, that the organization has authorized the Certificate Application, and that the person submitting the Certificate Application on behalf of the Organization is authorized to do so
Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices • Long-lived DV certificates ○ **SSL123 certs are DV. They can be valid for up to 5 years.** ○ CPS section 6.3.2 footnote 1: At a minimum, the Distinguished Name of 4 and 5 year validity SSL certificates is re-verified after three years from date of issuance. There is no requirement to re-verify the Distinguished Name of 4 and 5 year SSL123 certificates during the validity period of the certificate. • Wildcard DV SSL certificates ○ Wildcard SSL certs are High Assurance, which means OV. ○ CPS Section 1.1: *thawte* High Assurance Certificates for servers (SSL Web Server Certificates, SSL Wildcard Certificates and SGC SuperCerts) also provide assurances that the Subscriber is entitled to use the domain name listed in the Certificate Application. • Delegation of Domain / Email validation to third parties ○ CPS Section 1.3.2: *thawte* performs the RA function for all high assurance certificates, medium assurance certificates and for low assurance “Freemail”certificates, which do not include the subscriber’s name. SPKI Customers perform identification and authentication of high assurance Certificate subscribers within the SPKI Customer’s organization as described in CPS §1.1. *thawte’s* Web of Trust Notaries perform the RA function for low assurance “Freemail Web of Trust certificates which contain the subscriber’s authenticated name. • Issuing end entity certificates directly from roots ○ Thawte will have these roots offline and create sub CAs that issue the end-entity certs.

	• Allowing external entities to operate unconstrained subordinate CAs ○ Thawte does not allow 3rd parties to operate sub CAs from Thawte roots. • Distributing generated private keys in PKCS#12 files ○ CPS Section 3.1.7 Method to Prove Possession of Private Key: *thawte* verifies the Certificate Applicant's possession of a private key through the use of a digitally signed certificate request pursuant to PKCS #10, another cryptographically-equivalent demonstration, or another *thawte*-approved method. • Certificates referencing hostnames or private IP addresses ○ CPS Section 3.1.8, SSL123 for Intranet Certificate: *thawte* validates that the Server or Intranet name or IP are not publicly accessible via the World Wide Web. When an IP address is used *thawte* validates that the IP address is within the private range for intranets as specified by RFC 1597. • OCSP Responses signed by a certificate under a different root ○ Thawte's practice is to sign OCSP responses with a cert signed by the same root (the one that signed the end-entity cert in question). • CRL with critical CIDP Extension ○ The Thawte CRLs do not use extensions at all. • Generic names for CAs ○ The CA names are not generic.