Bugzilla ID: 601950
Bugzilla Summary: Turn on the code signing trust bit for the Thawte Primary Root CA

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.
CA's are also encouraged to review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices.

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: 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**
Certificate Name	thawte Primary Root CA
Cert summary / comments	This request is to enable the code signing trust bit. This root was included in NSS as per bug #407163.
Root Cert URL	https://bugzilla.mozilla.org/attachment.cgi?id=306736
SHA-1 fingerprint	91:C6:D6:EE:3E:8A:C8:63:84:E5:48:C2:99:29:5C:75:6C:81:7B:81
Valid from	2006-11-17
Valid to	2036-07-16
Cert Version	3
Modulus length / key length	2048
Test Website	https://www.thawte.com/
CRL URL	http://crl.thawte.com/ThawteEVCA2006.crl (NextUpdate: 7 days) CPS 4.4.9 CRL Issuance Frequency: For end-entity certs, the CRLs are issued "At Least Daily"
OCSP Responder URL	http://ocsp.thawte.com
CA Hierarchy	This root has the following subordinate CAs: - thawte Extended Validation SSL CA - thawte Extended Validation SSL SGC CA - Thawte SSL CA

	- Thawte DV SSL CA - Thawte Code Signing CA – G2
Externally operated subCAs	None
Cross-Signing	None
Requested Trust Bits	Requesting that the Code Signing trust bit be enabled. The Websites trust bit is currently enabled.
SSL Validation Type	DV, OV, and EV
If DV – email addresses used for verification	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
EV policy OID(s)	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
AUDIT	Auditor: KPMG Audit Type: WebTrust CA and WebTrust EV 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	Not requesting email trust bit.
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 Authentication of the Identity of Organizational End-User Subscribers 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 Comment #4: Thawte issues all the certificates. Organization administrators can only approve certificates for the Organization name verified for that account.
Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices)

- 1.1 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.
- 1.2 Wildcard DV SSL certificates
  - N/A. Wildcard certs are OV.
- 1.3 Email Address Prefixes for DV Certs
  - See list above.
- 1.4 Delegation of Domain / Email validation to third parties
  - N/A
- 1.5 Issuing end entity certificates directly from roots
  - N/A
- 1.6 Allowing external entities to operate subordinate CAs
  - N/A
- 1.7 Distributing generated private keys in PKCS#12 files
  - N/A
- 1.8 Certificates referencing hostnames or private IP addresses
  - OV non-EV certs may contain a host name.
  - CPS Sectgion 3.1, Table 14: 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
- 1.9 Issuing SSL Certificates for Internal Domains
  - OV non-EV certs may be issued for internal domains.
- 1.10 OCSP Responses signed by a certificate under a different root
  - N/A
- 1.11 CRL with critical CIDP Extension
  - N/A
- 1.12 Generic names for CAs
  - N/A
- 1.13 Lack of Communication With End Users
  - N/A