The document summarizes the information gathered and verified for two requests from Thawte.
Bugzilla ID: 409237 -- add new Thawte root CA certificate
Bugzilla ID: 484903 -- Add thawte'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	thawte
Website URL (English version)	http://www.thawte.com/
Organizational type	Commercial
Primary market / customer base	Thawte 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 - #409237**	**Data - #484903**
Certificate Name	thawte Primary Root CA - G2	thawte Primary Root CA - 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 cert URL	https://bugzilla.mozilla.org/attachment.cgi?id=335551	https://bugzilla.mozilla.org/attachment.cgi?id=369000
SHA-1 fingerprint	AA:DB:BC:22:23:8F:C4:01:A1:27:BB:38:DD:F4:1D:DB:08:9E:F0:12	F1:8B:53:8D:1B:E9:03:B6:A6:F0:56:43:5B:17:15:89:CA:F3:6B:F2
Valid from	11/4/2007	2008-04-02
Valid to	1/18/2038	2037-12-01
Cert Version	3	3
Modulus length or type of signing key	SECG elliptic curve secp384r1 (aka NIST P-384)	2048 SHA-256
Test Website	https://ecc-test-valid.thawte.com	https://ptnr-thawte256.bbtest.net
CRL	**No CRL URL exists yet.** thawte 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	**No CRL URL exists yet.** thawte 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.
CRL Issuing Frequency	CPS 4.4.9 CRL Issuance Frequency: For end-entity certs, the CRLs are issued "At Least Daily"	
OCSP	None yet. Certs issued off this root will support OCSP.	None

List or description of subordinate CAs operated by the CA organization associated with the root CA.	Thawte will have these roots offline and create sub CAs that issue the end-entity certs. Planned sub-CAs for thawte Primary Root CA - G2: • Class 3 Secure Server CA (standard SSL certificates) • Class 3 Secure Intranet Server CA (intranet SSL certificates) • Class 3 Extended Validation SSL CA (EV SSL certificates) • Class 3 Code Signing (EV and non-EV Code Signing certificates) • OnSite Administrator CA - Class 3 (Enterprise portal Admin certificates) • Class 3 Open Financial Exchange CA - G2 (OFX SSL certificates) • Time Stamping Authority CA (time stamping certificates) • Class 3 Mobile CA (authentication of servers in the mobile space) • Class 3 WLAN CA (for Microsoft RADIUS/IAS servers) • Class 3 Organizational CA (S/MIME certs for organizations)	Thawte will have these roots 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 plans to issue SSL123 certs off a Sub CA chained to this 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.	
Requested Trust Bits	Websites Code	Websites Code
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: DV, OV, and/or EV	DV, OV 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. CPS Section 1.1: ***thawte*** High Assurance Certificates are issued to organizations (including sole proprietors) to provide authentication; message, software, and content integrity; and confidentiality encryption. ***thawte*** High Assurance Certificates provide assurances of the identity of the Subscriber based on a confirmation that the Subscriber organization does in fact exist, that the organization has authorized the Certificate Application, and that the person	

	submitting the Certificate Application on behalf of the Subscriber was authorized to do so. ***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. ***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 3.1.8 Authentication of Organization Identity
EV policy OID	Not Requesting EV-enablement for these roots at this time
CP/CPS	Thawte Documents: http://www.thawte.com/repository CPS: http://www.thawte.com/cps/index.html
AUDIT	Auditor: KPMG Audit Type: WebTrust CA Audit Report & Management Assertions: https://cert.webtrust.org/SealFile?seal=527&file=pdf 2008-11-30 Both of the roots in this request are included in the WebTrust for CA audit report. No issues were noted in the audit report.

Review CPS sections dealing with subscriber verification
(section 7 of http://www.mozilla.org/projects/security/certs/policy/)

- Verify identity info in code signing certs is that of 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
- Verify domain check for SSL
    - 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.

        - *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 3.1.8.1 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
        - With respect to Starter PKI (SPKI) Customers, the identity confirmation process begins with *thawte's* confirmation of the identity of the Starter PKI Customer itself in accordance with this section. Following such confirmation, the Starter PKI 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.
- 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 requesting email trust bit at this time.

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 footnote to table 22: At a minimum, the Distinguished Name of 4 and 5 year validity SSL certificates is reverified after three years from date of issuance. There is no requirement to reverify the Distinguished Name of 4 and 5 year SSL123 certificates during the validity period of the certificate.
    - Comment #7, bug # 484903: Long lived DV certs are an item that is being addressed in the CAB Forum with the creation of SSL minimum guidelines. We will certainly restrict the validity period offered with these certs based on those requirements.
- 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.