

The document summarizes the information gathered and verified for two requests from Thawte.

**Bugzilla ID:** 409237

**Bugzilla Summary:** add new Thawte root CA certificate

**Bugzilla ID:** 484903

**Bugzilla Summary:** 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](http://wiki.mozilla.org/CA:Information_checklist).

General Information	Data
CA Name	thawte
Website URL (English version)	<a href="http://www.thawte.com/">http://www.thawte.com/</a>
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	<a href="https://bugzilla.mozilla.org/attachment.cgi?id=335551">https://bugzilla.mozilla.org/attachment.cgi?id=335551</a>	<a href="https://bugzilla.mozilla.org/attachment.cgi?id=369000">https://bugzilla.mozilla.org/attachment.cgi?id=369000</a>
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	<a href="https://ecc-test-valid.thawte.com">https://ecc-test-valid.thawte.com</a>	Need website whose cert chains up to this root.
CRL	<b>No CRL URL exists yet.</b> 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	Need: CRL(s) for end-entity certs issued from this root

	CPS 4.4.9 CRL Issuance Frequency: For end-entity certs, the CRLs are issued "At Least Daily"	
OCSP	None	Is there OCSP for this root?
List or description of subordinate CAs operated by the CA organization associated with the root CA.	<p>Planned sub-CAs for thawte Primary Root CA - G2:</p> <ul style="list-style-type: none"> <li>• Class 3 Secure Server CA (standard SSL certificates)</li> <li>• Class 3 Secure Intranet Server CA (intranet SSL certificates)</li> <li>• Class 3 Extended Validation SSL CA (EV SSL certificates)</li> <li>• Class 3 Code Signing (EV and non-EV Code Signing certificates)</li> <li>• OnSite Administrator CA - Class 3 (Enterprise portal Admin certificates)</li> <li>• Class 3 Open Financial Exchange CA - G2 (OFX SSL certificates)</li> <li>• Time Stamping Authority CA (time stamping certificates)</li> <li>• Class 3 Mobile CA (authentication of servers in the mobile space)</li> <li>• Class 3 WLAN CA (for Microsoft RADIUS/IAS servers)</li> <li>• Class 3 Organizational CA (S/MIME certs for organizations)</li> </ul> <p>All subordinate CAs are operated by the CA organization associated with the root CA.</p>	<p>Please provide a description of the CA hierarchy for this thawte Primary Root CA - G3 root.</p> <p>Can SSL123 certs be issued under this root?</p>
subordinate CAs operated by third parties	None and none planned.	Are, or will there be, subordinate CAs operated by third parties?
List any other root CAs that have issued cross-signing certificates for this root CA	None and none planned.	Has this G3 root been involved in cross-signing with another root?
Requested Trust Bits One or more of: <ul style="list-style-type: none"> <li>• Websites (SSL/TLS)</li> <li>• Email (S/MIME)</li> <li>• Code Signing</li> </ul>	Websites Code	Websites Code

<p>If SSL certificates are issued within the hierarchy rooted at this root CA certificate: DV, OV, and/or EV</p>	<p>DV, OV</p> <p>Thawte's SSL123 certificates are of Medium Assurance, which is DV.</p> <p>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.</p> <p>CPS Section 1.1:</p> <p><b>thawte</b> High Assurance Certificates are issued to organizations (including sole proprietors) to provide authentication; message, software, and content integrity; and confidentiality encryption.</p> <p><b>thawte</b> 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.</p> <p><b>thawte</b> 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.</p> <p><b>thawte</b> Medium Assurance SSL123 Certificates are issued to Domains to provide confidentiality encryption. <b>thawte</b> 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.</p> <p>CPS Section 3.1.8 Authentication of Organization Identity</p>	
<p>EV policy OID</p>	<p>Not EV</p>	<p>Are you requesting EV for the thawte Primary Root CA - G3 root?</p>
<p>CP/CPS</p>	<p>Thawte Documents: <a href="http://www.thawte.com/repository">http://www.thawte.com/repository</a></p> <p>CPS: <a href="http://www.thawte.com/cps/index.html">http://www.thawte.com/cps/index.html</a></p>	
<p>AUDIT</p>	<p>Auditor: KPMG</p> <p>Audit Type: WebTrust CA</p> <p>Audit Report &amp; Management Assertions: <a href="https://cert.webtrust.org/SealFile?seal=527&amp;file=pdf">https://cert.webtrust.org/SealFile?seal=527&amp;file=pdf</a></p> <p>2008-11-30</p>	

#### 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.

### Flag Problematic Practices

([http://wiki.mozilla.org/CA:Problematic Practices](http://wiki.mozilla.org/CA:Problematic_Practices))

- Long-lived DV certificates
  - SSL123 certs are DV. It looks like they can be valid for 4 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 .
- 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](#)
  - ?
- [Allowing external entities to operate unconstrained subordinate CAs](#)
  - ?
- [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](#)
  - ?
- [OCSP Responses signed by a certificate under a different root](#)
  - ?
- [CRL with critical CIDP Extension](#)
  - ?
- [Generic names for CAs](#)
  - The CA names are not generic.

### Verify Audits

- Validate contact info in report, call to verify that they did indeed issue this report.
  - Posted on cert.webtrust.org
- For EV CA’s, verify current WebTrust EV Audit done.
  - N/A
- Review Audit to flag any issues noted in the report
  - No issues noted