**Bugzilla ID:** 539257
**Bugzilla Summary:** EV enable thawte ECC and SHA256 root certificates

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. |
| CA Contact Information | CA Email Alias: practices@verisign.com<br>CA Phone Number: 1 650.961.7500<br>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 – G2 | Data – G3 |
|---|---|---|
| Certificate Name | thawte Primary Root CA - G2 | thawte Primary Root CA - G3 |
| Cert summary / comments | This ECC root is currently included in NSS.<br>Inclusion bug #409237<br><br>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 SHA256 root is currently included in NSS.<br>Inclusion bug #484903<br><br>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. |
| OPEN ACTION ITEMS | From bug #484903 – Please post updates directly in bug #484903.<br>ACTION: Thawte will remove the following email addresses from their list of options for domain validated certs: is, it, mis, ssladministrator, sslwebmaster. Thawte has committed to notifying their customers according to their 6-month SLAs, and then complete the changes in the February/March 2010 timeframe. | |
| 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<br>SHA-256 |
| Test Website | Please provide the url to a website whose EV SSL cert chains up to this root. | Please provide the url to a website whose EV SSL cert chains up to this root. |
| CRL | No CRL URL exists yet – Is this still the case? | No CRL URL exists yet – Is this still the case? |
| 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 |

| | | |
|---|---|---|
| CA Hierarchy | Thawte will have this root offline and create sub CAs that issue the end-entity certs.<br><br>Planned sub-CAs for thawte Primary Root CA - G2:<br>• Class 3 Secure Server CA (standard SSL certificates)<br>• Class 3 Secure Intranet Server CA (intranet SSL certificates)<br>• Class 3 Extended Validation SSL CA (EV SSL certificates)<br>• Class 3 Code Signing (EV and non-EV Code Signing certificates)<br>• OnSite Administrator CA - Class 3 (Enterprise portal Admin certificates)<br>• Class 3 Open Financial Exchange CA - G2 (OFX SSL certificates)<br>• Time Stamping Authority CA (time stamping certificates)<br>• Class 3 Mobile CA (authentication of servers in the mobile space)<br>• Class 3 WLAN CA (for Microsoft RADIUS/IAS servers)<br>• Class 3 Organizational CA (S/MIME certs for organizations) | 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.<br><br>Thawte plans to issue SSL123 certs off a Sub CA chained to this root.<br><br>Please clarify hierarchy in regards to EV-SSL certs.<br>From CPS it looks like the "thawte Primary Root CA – G3" will sign an intermediate CA "thawte Extended Validation SSL CA" which will sign the end-entity EV SSL certs. |
| SubCAs operated by 3rd parties | None and none planned.<br>Thawte does not allow 3rd parties to operate sub CAs from Thawte roots. | |
| Cross-signing | None and none planned. | |
| Trust Bits | Websites<br>Code | Websites<br>Code |
| SSL Verification Type | DV, OV, EV<br>Thawte's SSL123 certificates are of Medium Assurance, which is DV.<br>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 | 2.16.840.1.113733.1.7.48.1 |
| CP/CPS | Thawte Documents: http://www.thawte.com/repository<br>CPS: http://www.thawte.com/cps/index.html -- Appendix A1 has Supplemental Validation Procedures EV SSL Certificates | |
| AUDIT | Audit Type: WebTrust CA<br>Auditor: KPMG<br>Audit Report & Management Assertions: https://cert.webtrust.org/SealFile?seal=527&file=pdf (2008-11-30)<br>Both of the roots in this request are included in the WebTrust for CA audit report.<br>Neither of these roots are included in the Webtrust EV Audit. | |
| Levels of Verfication | CPS Section 1.1:<br>***thawte's*** Certification Authorities (CAs) offer four distinct classes of end user subscriber certificates – High Assurance with extended validation, High Assurance, Medium Assurance and Low Assurance. The distinction between these classes of | |

| | |
|---|---|
| | Certificates is the level of Subscriber identification and authentication performed (*See* CPS §§ 3.1.8, 3.1.9). In addition, specific types of certificates within these classes have specific intended uses (*See* CPS §1.3.4) and certificate profiles (*See* CPS §7.1).<br>***thawte*** High Assurance with extended validation Certificates are certificates issued by thawte in conformance with the Guidelines for Extended Validation Certificates published by the a forum consisting of major certification authorities and browser vendors.<br>***thawte*** High Assurance Certificates are issued to organizations (including sole proprietors) to provide authentication; message, software, and content integrity; and confidentiality encryption.<br>***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.<br>***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.<br>***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.<br>***thawte*** Low Assurance Certificates are individual Certificates, whose validation procedures are based on assurances that the Subscriber's e-mail address is associated with a public key. They are appropriate for digital signatures, encryption, and access control for non-commercial or low-value transactions where proof of identity is unnecessary. In addition, thawte also offers Freemail Web of Trust individual certificates, which include confirmation of the Subscriber's identity. *See* CPS §3.1.9 for more information.<br>CPS Table 1: Assurance Levels<br>SSL Web Server Certificates with EV – High with extended validation<br>SSL Web Server Certificates – High (OV)<br>Wildcard SSL Certificates – High (OV)<br>High Assurance Premium Server Gated Cryptography SSL Certificates – High (OV)<br>Code Signing Certificates – High (OV)<br>SSL 123 Certificates – Medium (DV)<br>Personal E-Mail Certificates – Low |
| Organization Identity Verification | See CPS Section 3.1.8 -- Authentication of Organization Identity |
| Domain Name Ownership / Control | CPS Section 1.1:<br>• SSL123 Certs are Medium Assurance (DV)<br>• SSL Web Server Certificates, SSL Wildcard Certificates and SGC SuperCerts are High Assurance (OV)<br>• SSL Web Server Certificates with EV are High Assurance with extended validation (EV)<br>*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.<br><br>CPS Section 3.1.8.1 Authentication of the Identity of Organizational End-User Subscribers<br>• 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<br>• 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. |
| EV Validation | CPS Appendix A1, Sections:<br>14. Verification of Applicant's Legal Existence and Identity<br>15. Verification of Applicant's Legal Existence and Identity – Assumed Name<br>16. Verification of Applicant's Physical Existence<br>17. Verification of Applicant's Operational Existence<br><br>18. Verification of Applicant's Domain Name<br>***thawte*** verifies Applicant's registration of the domain name(s) to be listed in the EV Certificate, satisfy the following requirements:<br>(1) The domain name is registered with an Internet Corporation for Assigned Names and Numbers (ICANN)- approved registrar or a registry listed by the Internet Assigned Numbers Authority (IANA);<br>(2) Domain registration information in the WHOIS database SHOULD be public and SHOULD show the name, physical address, and administrative contact information for the organization.<br>For Government Entity Applicants, the CA MAY rely on the domain name listed for that entity in the records of the QGIS in Applicant's Jurisdiction to verify Domain Name.<br>(3) The Applicant is the registered holder of the domain name or has been granted the exclusive right to use the domain name by the registered holder of the domain name<br>(4) The Applicant is aware of its registration or exclusive control of the domain name;<br><br>***thawte*** performs a WHOIS inquiry on the Internet for the domain name supplied by the Applicant, to verify that the Applicant is the entity to whom the domain name is registered. Where the WHOIS record indicates otherwise, ***thawte*** will require the WHOIS record to be updated to reflect the Applicant as the registered holder of the domain. Confirmation that the registered owner of the domain name is a Parent/Subsidiary Company of Applicant, or a registered trading name of Applicant is sufficient to establish that Applicant is the registered owner of the domain name.<br><br>In cases where Applicant is not the registered holder of the domain name, or domain registration information cannot be obtained from WHOIS, ***thawte*** may obtain positive confirmation from the registered domain holder that the applicant has been granted the exclusive right to use the requested Fully Qualified Domain Name (FQDN). In these circumstances, ***thawte*** also verifies the Applicant's exclusive right to use the domain name using one of the following methods:<br>(A) Relying on a Verified Legal Opinion to the effect that the Applicant has the exclusive right to use the specified domain name in identifying itself on the Internet; or<br>(B) Relying on a representation from the Contract Signer, or the Certificate Approver if expressly authorized in a mutually agreed upon contract, that it controls the confirmed domain name.. ...<br>In cases where the registered domain holder cannot be contacted, ***thawte*** shall:<br>o Rely on a Verified Legal Opinion to the effect that the Applicant has the exclusive right to use the specified domain name in identifying itself on the Internet, ***and***<br>o Rely on a representation from the Contract Signer, or the Certificate Approver if expressly authorized in a mutually agreed upon contract, coupled with a practical demonstration by the Applicant establishing that it controls the confirmed domain name by making an agreed-upon change in information found online on a web page identified by a uniform resource identifier |

| | |
|---|---|
| | containing the Applicant's FQDN;<br>***thawte*** may verify the Applicant is aware that it has exclusive control and/or ownership of the domain name by obtaining a Confirmation from Corporate Contact verifying that the Applicant is aware that it has exclusive control of the 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<br>CPS Section 3.1.8.1:<br>*thawte* confirms the identity of a Certificate Applicant for a High Assurance Server or Code Signing Certificate by:<br>• 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<br>• 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<br>• Long-lived DV certificates<br>o **SSL123 certs are DV. They can be valid for up to 5 years.**<br>▪ 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.<br>o 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.<br>• Wildcard DV SSL certificates<br>o Wildcard SSL certs are High Assurance, which means OV.<br>o 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.<br>• Delegation of Domain / Email validation to third parties<br>o 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.<br>• Issuing end entity certificates directly from roots<br>o Thawte will have these roots offline and create sub CAs that issue the end-entity certs.<br>• Allowing external entities to operate unconstrained subordinate CAs |

| | |
|---|---|
| | ○ Thawte does not allow 3rd parties to operate sub CAs from Thawte roots.<br>• Distributing generated private keys in PKCS#12 files<br>○ 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.<br>• Certificates referencing hostnames or private IP addresses<br>○ 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.<br>• OCSP Responses signed by a certificate under a different root<br>○ 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).<br>• CRL with critical CIDP Extension<br>○ The Thawte CRLs do not use extensions at all.<br>• Generic names for CAs<br>○ The CA names are not generic. |