**Bugzilla ID:** 849950
**Bugzilla Summary:** Add Entrust G2 and EC1 root certificate

CAs wishing to have their certificates included in Mozilla products must

1) Comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/)
2) Supply all of the information listed in http://wiki.mozilla.org/CA:Information_checklist.
    a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
    b. Review the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic_Practices

**General information about the CA's associated organization**

| | |
|---|---|
| CA Company Name | Entrust |
| Website URL | http://www.entrust.net/ |
| Organizational type, Primark Market / Customer Base | Entrust is a commercial CA serving the global market for SSL web certificates. Entrust also issues certificates to subordinate CAs for enterprise and commercial use. Entrust has enterprise subordinate CAs that issue certificates for SSL and S/MIME internal use. There are also commercial subordinate CAs that issue SSL certificates and S/MIME certificates to the public. |
| CA Contact Information | CA Email Alias: roots@entrust.com<br>CA Phone Number: 613-270-3400<br>Title / Department: Entrust Certificate Services |

**Technical information about each root certificate**

| | | |
|---|---|---|
| Certificate Name | Entrust Root Certification Authority - G2 | Entrust Root Certification Authority - EC1 |
| Certificate Issuer Field | CN = Entrust Root Certification Authority - G2<br>OU = "(c) 2009 Entrust, Inc. - for authorized use only"<br>OU = See www.entrust.net/legal-terms<br>O = "Entrust, Inc."<br>C = US | CN = Entrust Root Certification Authority - EC1<br>OU = (c) 2012 Entrust, Inc. - for authorized use only<br>OU = See www.entrust.net/legal-terms<br>O = Entrust, Inc.<br>C = US |
| Certificate Summary | This SHA-256 root certificate is intended to eventually replace Entrust's SHA-1 root certificates, and will be used for commercially issuing SSL, S/MIME, and Code Signing certificates. | This root is intended to support distribution of ECC certificates. |
| Root Cert URL | https://bugzilla.mozilla.org/attachment.cgi?id=767483 | https://bugzilla.mozilla.org/attachment.cgi?id=813664 |
| SHA1 | 8C:F4:27:FD:79:0C:3A:D1:66:06:8D:E8:1E:57:EF:BB:93:22:72:D4 | 20:D8:06:40:DF:9B:25:F5:12:25:3A:11:EA:F7:59:8A:EB:14:B5:47 |
| Valid From | 2009-07-07 | 2012-12-18 |
| Valid To | 2030-12-07 | 2037-12-18 |
| Cert Version | 3 | 3 |
| Cert Signature Algorithm | PKCS #1 SHA-256 With RSA Encryption | sha384ECDSA |
| Signing key parameters | 2048 | ECDSA_P384 |
| Test Website | Valid - https://validg2.entrust.net/ | Valid: https://validec.entrust.net |

| | | |
|---|---|---|
| | Expired – https://expiredg2.entrust.net<br>Revoked – https://revokedg2.entrust.net | Expired: https://expiredec.entrust.net<br>Revoked: https://revokedec.entrust.net |
| CRL URL | http://crl.entrust.net/g2ca.crl<br>CPS section 4.4.3: CRLs updated within 24 hours of revocation request.<br>CPS section 4.4.9: CRLs for end entities shall be issued at least once every seven days. | http://crl.entrust.net/ec1root.crl<br>CPS section 4.4.3: CRLs updated within 24 hours of revocation request.<br>CPS section 4.4.9: CRLs for end entities shall be issued at least once every seven days. |
| OCSP URL | http://ocsp.entrust.net/<br>CPS section 4.4.11: OCSP responses for end-entities issued at least every 4 days, with max expiration time of 10 days. | http://ocsp.entrust.net/<br>CPS section 4.4.11: OCSP responses for end-entities issued at least every 4 days, with max expiration time of 10 days. |
| Requested Trust Bits | Websites (SSL/TLS)<br>Email (S/MIME)<br>Code Signing | Websites (SSL/TLS)<br>Email (S/MIME)<br>Code Signing |
| SSL Validation Type | OV and EV | OV and EV |
| EV Policy OID | 2.16.840.1.114028.10.1.2<br>EV Tested:<br>https://bugzilla.mozilla.org/attachment.cgi?id=8513021 | 2.16.840.1.114028.10.1.2<br>EV Tested:<br>https://bugzilla.mozilla.org/attachment.cgi?id=8513829 |

**CA Hierarchy information for each root certificate**

| | |
|---|---|
| CA Hierarchy | These G2 and EC1 roots will have internally-operated subordinate CAs, and will eventually have externally-operated subordinate CAs.<br>The G2 root is intended to eventually replace Entrust's SHA-1 root certificates, so the externally-operated subordinate CAs will eventually be migrated to the new G2 CA hierarchy. |
| Externally Operated SubCAs | For the currently included Entrust root certificates, Entrust's Third Party Subordinate CA Disclosure:<br>http://www.entrust.net/about/third-party-sub-ca.htm<br><br>CPS Appendix B: Third Party Subordinate CAs are assessed to meet the requirements of the CP and/or CPS on an annual basis using one of the audit criteria specified in the Baseline Requirements.<br><br>According to Entrust's CPS, all subordinate CAs are required to be audited annually, whether they are technically constrained or not. |
| Cross-Signing | The G2 root has signed 2 Entrust issuing CAs and the EC1 root has signed 1 Entrust issuing CAs. |
| Technical Constraints on Third-party Issuers | In the case of Enterprise RAs, an administrator is authorized and assigned by the subscribing organization. The organization's account is technically limited as follows: two-factor authentication for administrator, domains pre-verified, and organizations names pre-verified.<br><br>CPS section 2.1.2: Independent third-party Registration Authorities shall remain responsible for the performance of such representatives or agents under the Entrust CPS, any Subscription Agreements, or any Relying Party Agreements. Entrust may |

| | |
|---|---|
| | appoint Resellers and Co-marketers for (i) Entrust Certificates, and (ii) services provided in respect to Entrust Certificates. Such Resellers and Co-marketers shall be responsible for their performance under the Entrust CPS, any Subscription Agreements, or any Relying Party Agreements.<br><br>CPS section 2.7.1: Entrust Certification Authorities, Entrust-operated Registration Authorities, and independent third-party Registration Authorities operating under the Entrust Certification Authorities shall be audited once per calendar year for compliance with the practices and procedures set forth in the Entrust CPS. If the results of an audit report recommend remedial action, Entrust or the applicable independent third-party Registration Authority shall initiate corrective action within thirty (30) days of receipt of such audit report.<br><br>CPS section 2.7.4: The compliance audit shall test compliance of Entrust Certification Authorities, Entrust-operated Registration Authorities, or independent third-party operated Registration Authorities under the Entrust Certification Authorities against the policies and procedures set forth in:<br>i. the Entrust CPS; and<br>ii. the WebTrust Program for Certification Authorities. |

**Third-Party Private (or Enterprise) Subordinate CAs**

| | |
|---|---|
| General description of the sub-CAs operated by third parties | For the currently included Entrust root certificates, Entrust's Third Party Subordinate CA Disclosure: http://www.entrust.net/about/third-party-sub-ca.htm |
| Selection criteria for sub-CAs | All cross-certificate issuance to third parties is reviewed and approved by Entrust President and CEO. |
| The CP/CPS that the sub-CAs are required to follow | CPS Appendix B: Entrust operated subordinate CAs are managed in accordance with this CPS or are operated in accordance with their own CP and/or CPS which meets the minimum requirements of this CPS. |
| Requirements (technical and contractual) for sub-CAs in regards to whether or not sub-CAs are constrained to issue certificates only within certain domains, and whether or not sub-CAs can create their own subordinates | CPS Appendix B: Third Party Subordinate CAs are assessed to meet the requirements of the CP and/or CPS on an annual basis using one of the audit criteria specified in the Baseline Requirements.<br><br>According to Entrust's CPS, all subordinate CAs are required to be audited annually, whether they are technically constrained or not.<br><br>In the past Sub-CAs domains were only constrained by contract. If Entrust plans to cross-certify Sub CAs with G2 or EC1, we will consider constraining the CAs with domain constraints.<br><br>In some cases sub-CAs are allowed to issue their own subordinates. This is assessed on a case-by-case basis. In practice many sub-CAs want to operate their own "root" that can be secured off-line. |
| Requirements (typically in the CP or CPS) for sub-CAs | Enterprise sub-CAs can only issue to Subscribers as defined in their contract. Subscribers of S/MIME client certificates are employees, groups of employees, or business partners that use the certificates for enterprise business purposes. |

| | |
|---|---|
| to take reasonable measures to verify the ownership of the domain name and email address for end-entity certificates chaining up to the root, as per section 7 of our Mozilla CA certificate policy. | Subscribers of SSL certificates are the enterprise or affiliate that has registered the domain name.<br>Enterprise sub-CAs are contractually bound only to issue SSL and/or S/MIME certificates with domains registered to the enterprise or enterprise affiliate.<br>All certificates issued by an enterprise sub-CA must contain the organization name of the enterprise or enterprise affiliate. Use of certificates must be restricted by EKU. |
| Description of audit requirements for sub-CAs (typically in the CP or CPS) | All enterprise sub-CAs are subject to an annual audit to be conducted by an independent security auditor. In the past, Entrust allowed audits to be conducted in accordance with criteria specified in the sub-CA agreement. Entrust has revised all agreements to require annual audits to be conducted in accordance with one of the four audit standards as specified in the Baseline Requirements. |

**Verification Policies and Practices**

| | |
|---|---|
| Policy Documentation | Documents are in English.<br>Document Repository: http://www.entrust.net/CPS<br>CPS: http://www.entrust.net/CPS/pdf/SSL-CPS-English-20140304-Version-2-11.pdf<br>EV CPS: http://www.entrust.net/CPS/pdf/EV-SSL-CPS-English-20140304-v1-6.pdf |
| Audits | Audit Type: WebTrust for CA, WebTrust for EV, and SSL Baseline Requirements<br>Auditor: Deloitte LLP, www.deloitte.ca<br>Audits: https://entrust.webtrust.org/ViewSeal?id=328 (2014.04.21) |
| Organization Verification Procedures | CPS section 3.1.8: Registration Authorities operating under the Entrust Certification Authorities shall perform a limited verification of any organizational identities that are submitted by an Applicant or Subscriber. Registration Authorities operating under the Entrust Certification Authorities shall determine whether the organizational identity, address, and domain name provided with an Entrust Certificate Application are consistent with information contained in third-party databases and/or governmental sources. The information and sources used for the limited verification of Entrust Certificate Applications may vary depending on the jurisdiction of the Applicant or Subscriber.<br>In the case of organizational identities that are not registered with any governmental sources, Registration Authorities operating under the Entrust Certification Authorities shall use commercially reasonable efforts to confirm the existence of the organization. Such commercially reasonable efforts may include site visits or third-party attestation letter. Registration Authorities operating under the Entrust Certification Authorities shall comply with all verification practices mandated by the Entrust Policy Authority.<br><br>CPS section 3.1.9: Registration Authorities operating under the Entrust Certification Authorities shall use reasonable means to verify any individual identities that are submitted by an Applicant or Subscriber.<br>SSL Certificates<br>An individual identity shall be verified by using a legible copy, which discernibly shows the Applicant's face, of at least one currently valid government-issued photo ID (passport, driver's license, military ID, national ID, or |

| | |
|---|---|
| | equivalent document type). The copy shall be inspected for any indication of alteration or falsification.<br>The Applicant's address shall be verified using a trusted form of identification such as a government ID, utility bill, or bank or credit card statement. The same government-issued ID that was used to verify the Applicant's name may be relied upon.<br>The request shall be verified by contacting the Applicant using a phone number that was provided from a third-party.<br>Class 1 Client Certificates<br>The identity asserted in Entrust Class 1 Client Certificates is an email address that represents the Subscriber.<br>Class 2 Client Certificates<br>The identity shall be authenticated by matching the identity provided by the Applicant or Subscriber to:<br>(i) information residing in the database of an identity proofing service approved by Entrust, such as a major credit bureau, or<br>(ii) information contained in the business records or databases (e.g. employee or customer directories) of a Registration Authority approving certificates to its own affiliated individuals. |
| SSL Verification Procedures | CPS section 1.4.2: Entrust Certificates issued to organizations are typically used for server authentication, SSL/TLS secure sessions, and code signing.<br><br>CPS 3.1.10 Authentication of Domain Name<br>Registration Authorities operating under the Entrust Certification Authorities shall use reasonable means to confirm the Applicant or Subscriber has control of the domain names to be included in the Entrust Certificate. The Registration Authority shall check the WHOIS record to determine who the top level domain (TLD) is registered to. The authorization to use the domain is done by contacting an authorization contact at the entity that registered the domain name or by contacting a user identified in the WHOIS record.<br>If contacting a user identified in the WHOIS record by email, then only the following emails addresses may be used:<br>(i) Supplied by the Domain Name Registrar;<br>(ii) Taken from the Domain Name Registrant's "registrant", "technical", or "administrative" contact information, as it appears in the Domain's WHOIS record; or;<br>(iii) By pre-pending a local part to a Domain Name as follows:<br>a. Local part - One of the following: 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster'; and<br>b. Domain Name – Formed by pruning zero or more components from the Registered Domain Name or the requested Fully-Qualified Domain Name. |
| Email Address Verification Procedures | CPS section 1.4:<br>Entrust Certificates issued to individuals are typically used to sign and encrypt e-mail and to authenticate to applications (client authentication).<br>Class 1 Certificates is considered to be low assurance, as the verification method simply confirms that the Subscriber controls the asserted email address. No verification checks of the Subscriber's identity are performed.<br>Class 2 Certificates provide a greater level of assurance over Class 1 Certificates, because in addition to email address control, basic verification steps are performed to confirm the identity of the Subscriber. |

| | |
|---|---|
| | CPS section 3.1.11 Authentication of Email Address<br>Registration Authorities operating under the Entrust Certification Authorities shall use reasonable means to confirm the Applicant or Subscriber has control of the e-mail address to be included in the Entrust Certificate. The e-mail address for Entrust Client Certificates is confirmed using the e-mail through the enrollment process. |
| Code Signing Subscriber Verification Procedures | From Entrust:<br>Entrust only issues Code Signing certificates to organizations. Organization identity information and authorization is verified the same as with Entrust EV SSL certificates less, of course, the domain information. |
| EV – Organization Verification | EV CPS section 3.1.8: Registration Authorities operating under the Entrust EV SSL Certification Authorities shall determine whether the organizational identity, legal existence, physical existence, operational existence, and domain name provided with an Entrust EV SSL Certificate Application are consistent with the requirements set forth in the Guidelines published by the CA/Browser Forum.<br>EV CPS section 3.1.9: Registration Authorities operating under the Entrust EV SSL Certification Authorities shall perform a verification of the identity and authority of the Contract Signer, the Certificate Approver, and the Certificate Requestor associated with EV SSL Certificate Applications that are submitted by an Applicant or Subscriber. In order to establish the accuracy of an individual identity, the Registration Authority operating under an Entrust EV SSL Certification Authority shall perform identity and authority verification consistent with the requirements set forth in the Guidelines published by the CA/Browser Forum.<br><br>From Entrust:<br>Entrust EV verification procedures are written directly from the EV Guidelines requirements. The EV Guidelines are very prescriptive and do offer a few options. Entrust takes advantage of most options as applicable to the Applicant. We feel that there is no reason to provide any more detail in the CPS which has not been an issue with our WebTrust auditor. In addition, referring to the EV Guidelines is lower maintenance as the Guidelines are under constant change, Entrust's practices can stay compliant without unnecessary changes to the CPS. |
| EV – Domain Name Verification | EV CPS section 3.1: Before issuing an EV SSL Certificate, the Entrust EV SSL Certification Authorities ensure that all Subject organization information in the EV SSL Certificate conforms to the requirements of, and has been verified in accordance with, the procedures prescribed in this CPS and the Guidelines published by the CA/Browser Forum and matches the information confirmed and documented by the Registration Authority pursuant to its verification processes. Such verification processes are intended accomplish the following:<br>(i) Verify the Applicant's existence and identity, including;<br>a. Verify the Applicant's legal existence and identity (as stipulated in the Guidelines),<br>b. Verify the Applicant's physical existence (business presence at a physical address), and<br>c. Verify the Applicant's operational existence (business activity).<br>(ii) Verify the Applicant is a registered holder or has exclusive control of the domain name to be included in the EV SSL Certificate; and<br>(iii) Verify the Applicant's authorization for the EV SSL Certificate, including;<br>a. Verify the name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester;<br>b. Verify that Contract Signer signed the Subscription Agreement; and<br>c. Verify that a Certificate Approver has signed or otherwise approved the EV SSL Certificate Request. |
| Multi-factor Authentication | Entrust RAs use smartcards as second-factor authentication in order to issue certificates.<br>Entrust third party RAs cannot directly issue SSL certificates. |

| | |
|---|---|
| | Entrust also has Enterprise administrator accounts that allow customers to issue certificates on demand for pre-verified domains and organization names. The software limits issuance to these pre-verified domains through technical means.<br>All Enterprise administrators authenticate with a second factor. |
| Network Security | Entrust has checks in place for to look for mis-issued certificates. Also, Entrust has implemented a black-list/white-list system to control the issuance of certificates for high-profile domains.<br>CPS section 6. |

**Response to Mozilla's CA Recommended Practices** (https://wiki.mozilla.org/CA:Recommended_Practices)

| | |
|---|---|
| Publicly Available CP and CPS | Yes |
| CA Hierarchy | Described above |
| Audit Criteria | Yes |
| Document Handling of IDNs in CP/CPS | Entrust does not issue certificates with IDNs |
| Revocation of Compromised Certificates | Yes, Entrust revokes certificates with compromised keys and with invalid subscriber information |
| Verifying Domain Name Ownership | Described above |
| Verifying Email Address Control | Described above |
| Verifying Identity of Code Signing Certificate Subscriber | Described above |
| DNS names go in SAN | We still use the Common Name, but we do put all DNS names into the SAN extension per the Baseline Requirements. |
| Domain owned by a Natural Person | Entrust puts the name of a natural person in the O field, but does not populate an OU field with "natural person" |
| OCSP | Entrust uses OCSP for all Entrust CAs. OCSP responses are generated every 8 hrs and are valid for 7 days. |

**Response to Mozilla's list of Potentially Problematic Practices** (https://wiki.mozilla.org/CA:Problematic_Practices)

| | |
|---|---|
| Long-lived DV certificates | SSL certs are OV or EV |
| Wildcard DV SSL certificates | Entrust only issues OV wildcard certificates |
| Email Address Prefixes for DV Certs | SSL certs are OV or EV. |
| Delegation of Domain / Email validation to third parties | **Entrust allows third party domain/email verification per the requirements above. All third party certificate requests are reviewed by Entrust before issuance. Third Party RAs are also audited annually by a third party auditor.** |
| Issuing end entity certificates directly from roots | N/A |
| Allowing external entities to operate subordinate CAs | Yes, as described above. |
| Distributing generated private keys in PKCS#12 files | Entrust generates keys for Subscribers only for Class 2 Client certificates. The P12 files are encrypted using a password provided by the applicant at time of enrollment. |
| Certificates referencing hostnames or | |

| | |
|---|---|
| private IP addresses | |
| Issuing SSL Certificates for Internal Domains | **Entrust does issue SSL certificates with internal host names and reserved IP addresses. We will be phasing this practice out in accordance with the Baseline Requirements.** |
| OCSP Responses signed by a certificate under a different root | N/A, all Entrust OCSP responses are signed with a certificate issued from the same CA that issued the end entity certificate being checked. |
| SHA-1 Certificates | Entrust is issuing SHA-2 end entity certificates. The default signing algorithm uses SHA-2. We do allow the certificate Subscriber to choose SHA-1 and we provide a warning that in the future it will have trust issues with some browsers. In December 2014, we will limit the SHA-1 validity period to 31 December 2016. As of 1 January 2016, we will stop issuing SHA-1 signed publicly trusted certificates. |
| Generic names for CAs | N/A |
| Lack of Communication With End Users | N/A |