Bugzilla ID: 694536
Bugzilla Summary: Replace Entrust.net Certification Authority (2048) 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 CA Phone Number: 613-270-3400 Title / Department: Entrust Certificate Services

Technical information about each root certificate

Certificate Name	**Entrust.net Certification Authority (2048)**

Certificate Issuer Field	CN = Entrust.net Certification Authority (2048)
	OU = (c) 1999 Entrust.net Limited
	OU = www.entrust.net/CPS_2048 incorp. by ref. (limits liab.)
	O = Entrust.net

Certificate Summary	This root is already included in NSS. It has been updated to extend the validity period and to correct the Basic Constraints extension. This root is Entrust's primary trust anchor for commercially issuing SSL, S/MIME, and Code Signing certificates.
Root Cert URL	https://bugzilla.mozilla.org/attachment.cgi?id=567058
SHA1	50:30:06:09:1D:97:D4:F5:AE:39:F7:CB:E7:92:7D:7D:65:2D:34:31
Valid From	1999-12-24
Valid To	2029-07-24
Cert Version	3
Cert Signature Algorithm	SHA-1
Signing key parameters	2048
Test Website	https://2048test.entrust.net/ https://evtest2048.entrust.net/
CRL URL	http://crl.entrust.net/2048ca.crl http://crl.entrust.net/level1c.crl (NextUpdate: 7 days) CPS section 4.4.3: CRLs updated within 24 hours of revocation request. CPS section 4.4.9: CRLs for end entities shall be issued at least once every seven days.

OCSP URL	http://ocsp.entrust.net/ 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) Email (S/MIME) Code Signing
SSL Validation Type	OV and EV
EV Policy OID	2.16.840.1.114028.10.1.2

CA Hierarchy information for each root certificate

CA Hierarchy	Level 1 CAs - Operated by Entrust - CN = Entrust Certification Authority - L1B - CN = Entrust Certification Authority - L1C - CN = Entrust Code Signing Certification Authority - L1D - CN = Entrust Class 1 Client CA - CN = Entrust Class 2 Client CA - CN = Entrust Managed Services Commercial Public Root CA - CN = The Walt Disney Company Root CA, OU = TWDC-PKI, DC = Disney, DC = com - CN = Experian Root CA, CN = AIA, CN = Public Key Services, CN = Services, CN = Configuration, DC = Experian, DC = local - OU = First Data Root CA, OU = Certification Authorities, O = First Data Corporation, C = US - CN = PGE Root CA, OU = Certification Authorities, O = Pacific Gas and Electric Company, C = US
Externally Operated SubCAs	This root has been used to sign both private and public third-party subordinate CAs as described below.

Cross-Signing	Cross-signed Roots in Mozilla Program
	OU = TDC Internet Root CA, O = TDC Internet, C = DK
	CN = SecureTrust CA, O = SecureTrust Corporation, C = US
	CN = DigiCert High Assurance EV Root CA, OU = www.digicert.com, O = DigiCert Inc, C = US

Technical Constraints on Third-party Issuers	Entrust does not allow third parties to directly issue certificates with the exception of Enterprise RAs. In the case of Enterprise RAs, an administrator is authorized and assigned by the subscribing organization. The organizations account is technically limited to a list of information that can be included in the subject distinguished name. The account is also limited to the domain names that can be populated in the common name or subject alternative name fields.

Third-Party Private (or Enterprise) Subordinate CAs

General description of the sub-CAs operated by third parties	Generally Enterprise sub-CAs are Entrust PKI software customers looking for public trust in the certificates they are issuing for enterprise business purposes.
Selection criteria for sub-CAs	Enterprise CAs have generally been allowed to have a cross-certificate as they are also Entrust PKI software customers. All cross-certificate issuance to third parties is reviewed and approved by Entrust President and CEO. Entrust is planning to stop the practice of issuing cross-certificates to third parties that operate their own CA. No new customers of this type will be added, and existing customers will be transitioned to a different solution.
The CP/CPS that the sub-	Third Party sub-CAs must develop their own CP/CPS documentation, which must be no less stringent than the Entrust

CAs are required to follow	CPS and meet the requirements of the cross-certificate agreement.
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	Sub-CAs domains are only constrained by contract. 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 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.	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. Subscribers of SSL certificates are the enterprise or affiliate that has registered the domain name. Enterprise sub-CAs are contractually bound only to issue SSL and/or S/MIME certificates with domains registered to the enterprise or enterprise affiliate. 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 Mozilla and Microsoft CA policies.

Third-Party Public Subordinate CAs

Entrust (2048) Root CA has cross-signed CAs from three (3) organizations that can issue sub-CA or end entity certificates to third parties. These are Comodo, DigiCert and LAWtrust. There are no plans for the Entrust G2 root CA to issue sub-CA certificates to any third parties.

As Comodo and DigiCert are also in the Mozilla root certificate program and operate their sub-CAs in accordance with the same CP/CPS document as their roots, we will not be providing all on the requested information for these sub-CAs.

LAWtrust issues client certificates to third parties and has been authorized to issue one enterprise sub-CA certificate. Below is the requested information for LAWtrust.

1. LAW Trusted Third Party Services (Pty) Ltd, aka LAWtrust
2. LAWtrust website - https://www.lawtrust.co.za/index.php

LAWtrust repository - https://www.lawtrust.co.za/index.php?option=com_content&view=article&id=70&Itemid=80

3. Sub-CA cert download page – see LAWtrust repository
4. LAWtrust has two CAs under the Entrust root. One CA issues only issues third party client certificates. The other sub-CA has only issued one enterprise sub-CA certificate which in turn only issues enterprise client certificates.
5. CPS link – see LAWtrust repository

6. Email address ownership control is done in accordance with paragraph 3.2.4 of the LAWtrust CPS. Here is the text: In cases where the LAWtrust Certificate will be used for digitally signing and/or encrypting eMail the LAWtrust RA shall establish reasonable proof that the person or entity submitting the certificate request controls the eMail account associated with the eMail address referenced in the LAWtrust Certificate.
7. LAWtrust does not issue SSL certificates.
8. Problematic Practices – none identified
9. LAWtrust is audited annually by KPMG according to the WebTrust for CA criteria.
10. LAWtrust issues a CRL at least every 24 hours valid for 24 per CPS 4.9.5. LAWtrust publishes revoked certificate serial numbers to the CRL within 48 hours of revocation request per CPS 4.9.3.
11. LAWtrust does not support OCSP.

Verification Policies and Practices

Policy Documentation	Documents are in English. Document Repository: http://www.entrust.net/CPS CPS: http://www.entrust.net/CPS/pdf/ssl-cps-250612-v2-8.pdf EV CPS: http://www.entrust.net/CPS/pdf/evssl_cps_english250612.pdf
Audits	Audit Type: WebTrust for CA and WebTrust for EV Auditor: Deloitte and Touche LLP Auditor Website: www.deloitte.ca Audit Report and Management's Assertions: https://entrust.webtrust.org/ViewSeal?id=328
Organization Verification Procedures	CPS section 1.4.3 Assurance Levels 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. 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 3.1.8: 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. 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. Class 1 Client Certificates The identity asserted in Entrust Class 1 Client Certificates is an email address that represents the Subscriber. Class 2 Client Certificates The identity shall be authenticated by matching the identity provided by the Applicant or Subscriber to: (i) information residing in the database of an identity proofing service approved by Entrust, such as a major credit bureau, or (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 3.1.10 Authentication of Domain Name 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. If contacting a user identified in the WHOIS record by email, then only the following emails addresses may be used: (i) Supplied by the Domain Name Registrar; (ii) Taken from the Domain Name Registrant's "registrant", "technical", or "administrative" contact information, as it appears in the Domain's WHOIS record; or; (iii) By pre-pending a local part to a Domain Name as follows: a. Local part - One of the following: 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster'; and 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 3.1.11 Authentication of Email Address 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: 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. 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. From Entrust: 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: (i) Verify the Applicant's existence and identity, including; a. Verify the Applicant's legal existence and identity (as stipulated in the Guidelines), b. Verify the Applicant's physical existence (business presence at a physical address), and c. Verify the Applicant's operational existence (business activity). (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 (iii) Verify the Applicant's authorization for the EV SSL Certificate, including; a. Verify the name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester; b. Verify that Contract Signer signed the Subscription Agreement; and 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. 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. 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. Entrust has recently under gone a thorough third party security review.

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 makes 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.
CRL with critical CIDP Extension	N/A
Generic names for CAs	N/A
Lack of Communication With End Users	N/A