Bugzilla ID: 694536
Bugzilla Summary: Add Entrust Root Certificates to NSS

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)**	**Entrust Root Certification Authority - G2**

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
		CN = Entrust Root Certification Authority - G2
		OU = "(c) 2009 Entrust, Inc. - for authorized use only"
		OU = See www.entrust.net/legal-terms
		O = "Entrust, Inc."
		C = US

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 achor for commercially issuing SSL, S/MIME, and Code Signing certificates.	This is a new root which has been signed with the SHA-256 algorithm. This root is intended to eventually replace Entrust's SHA-1 signed roots. This root is intended to be used for commercially issuing SSL, S/MIME, and Code Signing certs.
Root Cert URL	https://bugzilla.mozilla.org/attachment.cgi?id=567058	https://bugzilla.mozilla.org/attachment.cgi?id=567059
SHA1	50:30:06:09:1D:97:D4:F5:AE:39:F7:CB:E7:92:7D:7D:65:2D:34:31	8C:F4:27:FD:79:0C:3A:D1:66:06:8D:E8:1E:57:EF:BB:93:22:72:D4
Valid From	1999-12-24	2009-07-07
Valid To	2029-07-24	2030-12-07
Cert Version	3	3
Cert Signature Algorithm	SHA-1	SHA-256
Signing key parameters	2048	2048

Test Website	https://2048test.entrust.net/	https://validg2.entrust.net/ **Have to turn off OCSP, because this root isn't in production yet. The test cert is signed by the root, because the intermediate issuing CA hasn't yet been created.**
CRL URL	http://crl.entrust.net/2048ca.crl http://crl.entrust.net/level1c.crl (NextUpdate: 7 days) CRL issuing frequency for end-entity certificates: CRL is issued every 24 hrs, valid for 7 days	http://crl.entrust.net/g2ca.crl **CRL doesn't exist yet, because root is not yet in use.** CRL issuing frequency for end-entity certificates: CRL is issued every 24 hrs, valid for 7 days
OCSP URL	http://ocsp.entrust.net/	http://ocsp.entrust.net/ **OCSP not yet operational for this root. EV-enablement final approval will not be given until OCSP support and the EV issuing CA are in place.** EV CPS section 4.4.11: OCSP responses at least once every twenty-four (24) hours with a validity period of seven (7) days.
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing	Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type	OV and EV	OV and EV
EV Policy OID	2.16.840.1.114028.10.1.2	2.16.840.1.114028.10.1.2

CA Hierarchy information for each root certificate

CA Hierarchy	List, description, and/or diagram of all intermediate CAs signed by this root. Identify which subCAs are internally-operated and which are externally operated.	Please explain the hierarchy that is planned for this root.
Externally Operated SubCAs	If this root has subCAs that are operated by external third parties, then provide the information listed here: https://wiki.mozilla.org/CA:SubordinateCA_checklist	If this root will have subCAs that are operated by external third parties, then provide the information listed here: https://wiki.mozilla.org/CA:SubordinateCA_checklist
Cross-Signing	List all other root certificates for which this root certificate has issued cross-signing certificates. List all other root certificates that have issued cross-signing certificates for this root certificate.	List all other root certificates for which this root certificate will issue cross-signing certificates. List all other root certificates will issue cross-signing certificates for this root certificate.
Technical Constraints on Third-party Issuers	Describe the technical constraints that are in place for all third-parties (CAs and RAs) who can directly cause the issuance of certificates. See #4 of https://wiki.mozilla.org/CA:Information_checklist#CA_Hierarchy_information_for_each_root_certificate	

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-english-28-02-11-v2-6.pdf EV CPS: http://www.entrust.net/CPS/pdf/evssl_cps_english280211-v1-3.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	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	Please provide all the information requested in #3 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices
Email Address Verification Procedures	CPS section 3.1.10: 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. Please provide more information about the mechanics of doing this, as per #4 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices
Code Signing Subscriber Verification Procedures	Please see #5 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices And https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Identity_of_Code_Signing_Certificate_Subscriber
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. This really just defers to EV Guidelines… Is there a CP or something with more information?
EV – Domain Name Verification	EV CPS just defers to EV Guidelines… Is there a CP or something with more information about how the domain name is verified for EV certs?
Multi-factor Authentication	Confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance. See # 6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices
Network Security	Confirm that you have performed the actions listed in #7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices

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

Publicly Available CP and CPS	Yes
CA Hierarchy	?
Audit Criteria	Yes
Document Handling of IDNs in CP/CPS	?
Revocation of Compromised Certificates	?
Verifying Domain Name Ownership	?
Verifying Email Address Control	?
Verifying Identity of Code Signing Certificate Subscriber	?
DNS names go in SAN	?
Domain owned by a Natural Person	?
OCSP	?

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	SSL certs are OV or EV. Are wildcard certs issued?
Email Address Prefixes for DV Certs	SSL certs are OV or EV.
Delegation of Domain / Email validation to third parties	?
Issuing end entity certificates directly from roots	N/A
Allowing external entities to operate	?

subordinate CAs	
Distributing generated private keys in PKCS#12 files	?
Certificates referencing hostnames or private IP addresses	?
Issuing SSL Certificates for Internal Domains	?
OCSP Responses signed by a certificate under a different root	?
CRL with critical CIDP Extension	N/A
Generic names for CAs	N/A
Lack of Communication With End Users	N/A