Print this page

Mozilla - CA Program

Case Information

Case Number	00000052	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owners/Certificate Name	Entrust	**Request Status**	In Public Discussion

Additional Case Information

Subject	Inclusion request for G2 and EC1 roots	**Case Reason**	New Owner/Root inclusion requested

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=849950

General information about CA's associated organization

Company Website	http://www.entrust.net/	**Verified?**	Verified
Organizational Type	Public Corporation	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Primary 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.	**Verified?**	Verified
Impact to Mozilla Users	These new root certificates are intended to eventually replace Entrust's currently included SHA-1 root certificates.	**Verified?**	Verified

Response to Mozilla's list of Recommended Practices

Recommended Practices	https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's list of Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Recommended Practices	Entrust does not issue certificates with IDNs Entrust revokes certificates with compromised keys and with invalid subscriber information We still use the Common Name, but we do put all DNS names into the SAN extension per the Baseline Requirements. Entrust puts the name of a natural person in the O field, but does not populate an OU field with “natural person” Entrust uses OCSP for all Entrust CAs. OCSP responses are generated every 8 hrs and are valid for 7 days.	**Verified?**	Verified

Response to Mozilla's list of Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices	**Problematic Practices Statement**	I have reviewed Mozilla's list of Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below
CA's Response to Problematic Practices	SSL certs are OV or EV Entrust only issues OV wildcard certificates Entrust allows third party domain/email verification. All third party certificate requests are reviewed by Entrust before issuance. Third Party RAs are also audited annually by a third party auditor. 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. 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. All Entrust OCSP responses are signed with a certificate issued from the same CA that issued the end entity certificate being checked. 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.	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Case No	R00000018	**Case Number**	00000052
Request Status	In Public Discussion	**Root Certificate Name**	Entrust Root Certification Authority - G2

Additional Root Case Information

Subject	Include Entrust Root Certification Authority - G2 root

Technical Information about Root Certificate

O From Issuer Field	Entrust, Inc.	**Verified?**	Verified
OU From Issuer Field	(c) 2009 Entrust, Inc.-for authorized use only	**Verified?**	Verified
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.	**Verified?**	Verified
Root Certificate Download URL	https://bugzilla.mozilla.org/attachment.cgi?id=567059	**Verified?**	Verified
SHA-1 Fingerprint	8C:F4:27:FD:79:0C:3A:D1:66:06:8D:E8:1E:57:EF:BB:93:22:72:D4	**Verified?**	Verified
SHA-256 Fingerprint	43:DF:57:74:B0:3E:7F:EF:5F:E4:0D:93:1A:7B:ED:F1:BB:2E:6B:42:73:8C:4E:6D:38:41:10:3D:3A:A7:F3:39	**Verified?**	Verified
Valid From	2009 Jul 07	**Verified?**	Verified

Valid To	2030 Dec 07	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-256	**Verified?**	Verified
Signing Key Parameters	2048	**Verified?**	Verified
Test Website URL (SSL)	https://validg2.entrust.net/	**Verified?**	Verified
CRL URL(s)	http://crl.entrust.net/g2ca.crl 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.	**Verified?**	Verified
OCSP URL(s)	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.	**Verified?**	Verified
Trust Bits	Code; Email; Websites	**Verified?**	Verified
SSL Validation Type	OV; EV	**Verified?**	Verified
EV Policy OID(s)	2.16.840.1.114028.10.1.2	**Verified?**	Verified
EV Tested	// 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 "2.16.840.1.114028.10.1.2", "Entrust EV OID", SEC_OID_UNKNOWN, { 0x43, 0xDF, 0x57, 0x74, 0xB0, 0x3E, 0x7F, 0xEF, 0x5F, 0xE4, 0x0D, 0x93, 0x1A, 0x7B, 0xED, 0xF1, 0xBB, 0x2E, 0x6B, 0x42, 0x73, 0x8C, 0x4E, 0x6D, 0x38, 0x41, 0x10, 0x3D, 0x3A, 0xA7, 0xF3, 0x39 }, "MIG+MQswCQYDVQQGEwJVUzEWMBQGA1UEChMNRW50cnVzdCwgSW5jLjEoMCYGA1UE" "CxMfU2VlIHd3dy5lbnRydXN0Lm5ldC9sZWdhbC10ZXJtczE5MDcGA1UECxMwKGMp" "IDIwMDkgRW50cnVzdCwgSW5jLiAtIGZvciBhdXRob3JpemVkIHVzZSBvbmx5MTIw" "MAYDVQQDEylFbnRydXN0IFJvb3QgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkgLSBH" "Mg==", "SlOMKA==", Success!	**Verified?**	Verified
Browsers Included In	Internet Explorer	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	This G2 root will have internally-operated subordinate CAs, and will eventually have externally-operated subordinate CAs. This 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.	**Verified?**	Verified
Externally Operated SubCAs	For the currently included Entrust root certificates, Entrust’s Third Party Subordinate CA Disclosure: http://www.entrust.net/about/third-party-sub-ca.htm	**Verified?**	Verified

	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. 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.	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	Enterprise RAs: the organization’s account is technically limited as follows: two-factor authentication for administrator, domains pre-verified, and organizations names pre-verified. CPS, 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.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Documents are in English	**Verified?**	Verified
CA Document Repository	http://www.entrust.net/CPS	**Verified?**	Verified
CP Doc Language	English		
CP	http://www.entrust.net/CPS	**Verified?**	Verified
CP Doc Language	English		
CPS	http://www.entrust.net/CPS	**Verified?**	Verified
Other Relevant Documents	EV CPS: http://www.entrust.net/CPS/pdf/EV-SSL-CPS-English-20140304-v1-6.pdf	**Verified?**	Verified
Auditor Name	Deloitte LLP	**Verified?**	Verified
Auditor Website	http://www2.deloitte.com/ca/en.html	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified
Standard Audit	https://entrust.webtrust.org/SealFile?seal=328&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	4/21/2014	**Verified?**	Verified
BR Audit	https://entrust.webtrust.org/SealFile?seal=328&file=pdf	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	4/21/2014	**Verified?**	Verified
EV Audit	https://entrust.webtrust.org/SealFile?seal=328&file=pdf	**Verified?**	Verified

EV Audit Type	WebTrust	**Verified?**	Verified
EV Audit Statement Date	4/21/2014	**Verified?**	Verified
BR Commitment to Comply	CPS section 1.1	**Verified?**	Verified
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.	**Verified?**	Verified
EV SSL Verification Procedures	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	**Verified?**	Verified

	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.		
Organization Verification Procedures	CPS sections 3.1.8 and 3.1.9	**Verified?**	Verified
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.	**Verified?**	Verified
Code Signing Subscriber Verification Pro	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.	**Verified?**	Verified
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.	**Verified?**	Verified
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. CPS section 6.	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	http://www.entrust.net/about/third-party-sub-ca.htm	**Verified?**	Verified

Root Case Record # 2

Root Case Information

Root Case No	R00000019	**Case Number**	00000052
Request Status	In Public Discussion	**Root Certificate Name**	Entrust Root Certification Authority - EC1

Additional Root Case Information

Subject	Include Entrust Root Certification Authority - EC1 root

Technical Information about Root Certificate

O From Issuer Field	Entrust, Inc.	**Verified?**	Verified
OU From Issuer Field	(c) 2012 Entrust, Inc. - for authorized use only	**Verified?**	Verified
Certificate Summary	This root is intended to support distribution of ECC certificates.	**Verified?**	Verified
Root Certificate Download URL	https://bugzilla.mozilla.org/attachment.cgi?id=813664	**Verified?**	Verified
SHA-1 Fingerprint	20:D8:06:40:DF:9B:25:F5:12:25:3A:11:EA:F7:59:8A:EB:14:B5:47	**Verified?**	Verified
SHA-256 Fingerprint	02:ED:0E:B2:8C:14:DA:45:16:5C:56:67:91:70:0D:64:51:D7:FB:56:F0:B2:AB:1D:3B:8E:B0:70:E5:6E:DF:F5	**Verified?**	Verified
Valid From	2012 Dec 18	**Verified?**	Verified
Valid To	2037 Dec 18	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	ECC	**Verified?**	Verified
Signing Key Parameters	ECC P-384	**Verified?**	Verified
Test Website URL (SSL)	https://validec.entrust.net	**Verified?**	Verified
CRL URL(s)	http://crl.entrust.net/ec1root.crl 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.	**Verified?**	Verified
OCSP URL(s)	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.	**Verified?**	Verified
Trust Bits	Code; Email; Websites	**Verified?**	Verified
SSL Validation Type	OV; EV	**Verified?**	Verified
EV Policy OID(s)	2.16.840.1.114028.10.1.2	**Verified?**	Verified
EV Tested	// CN=Entrust Root Certification Authority - EC1,OU="(c) 2012 Entrust, Inc. - for authorized use only",OU=See www.entrust.net/legal-terms,O="Entrust, Inc.",C=US "2.16.840.1.114028.10.1.2", "Entrust EV OID", SEC_OID_UNKNOWN, { 0x02, 0xED, 0x0E, 0xB2, 0x8C, 0x14, 0xDA, 0x45, 0x16, 0x5C, 0x56, 0x67, 0x91, 0x70, 0x0D, 0x64, 0x51, 0xD7, 0xFB, 0x56, 0xF0, 0xB2, 0xAB, 0x1D, 0x3B, 0x8E, 0xB0, 0x70, 0xE5, 0x6E, 0xDF, 0xF5 }, "MIG/MQswCQYDVQQGEwJVUzEWMBQGA1UEChMNRW50cnVzdCwgSW5jLjEoMCYGA1UE" "CxMfU2VlIHd3dy5lbnRydXN0Lm5ldC9sZWdhbC10ZXJtczE5MDcGA1UECxMwKGMp"	**Verified?**	Verified

"IDIwMTIgRW50cnVzdCwgSW5jLiAtIGZvciBhdXRob3JpemVkIHVzZSBvbmx5MTMw"
"MQYDVQQDEypFbnRydXN0IFJvb3QgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkgLSBF"
"QzE=",
"AKaLeSkAAAAAUNCR+Q==",
Success!

Browsers Included In	Internet Explorer	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	This EC1 root will have internally-operated subordinate CAs, and will eventually have externally-operated subordinate CAs.	**Verified?**	Verified
Externally Operated SubCAs	This EC1 root will eventually have externally-operated subordinate CAs.	**Verified?**	Verified
Cross Signing	The EC1 root has signed 1 Entrust issuing CA.	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	Enterprise RAs: the organization's account is technically limited as follows: two-factor authentication for administrator, domains pre-verified, and organizations names pre-verified. CPS, 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.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Documents are in English	**Verified?**	Verified
CA Document Repository	http://www.entrust.net/CPS	**Verified?**	Verified
CP Doc Language	English		
CP	http://www.entrust.net/CPS	**Verified?**	Verified
CP Doc Language	English		
CPS	http://www.entrust.net/CPS	**Verified?**	Verified
Other Relevant Documents	EV CPS: http://www.entrust.net/CPS/pdf/EV-SSL-CPS-English-20140304-v1-6.pdf	**Verified?**	Verified
Auditor Name	Deloitte LLP	**Verified?**	Verified
Auditor Website	http://www2.deloitte.com/ca/en.html	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified
Standard Audit	https://entrust.webtrust.org/SealFile?seal=328&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified

Standard Audit Statement Date	4/21/2014	**Verified?**	Verified
BR Audit	https://entrust.webtrust.org/SealFile?seal=328&file=pdf	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	4/21/2014	**Verified?**	Verified
EV Audit	https://entrust.webtrust.org/SealFile?seal=328&file=pdf	**Verified?**	Verified
EV Audit Type	WebTrust	**Verified?**	Verified
EV Audit Statement Date	4/21/2014	**Verified?**	Verified
BR Commitment to Comply	CPS section 1.1	**Verified?**	Verified
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.	**Verified?**	Verified
EV SSL Verification Procedures	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;	**Verified?**	Verified

	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.		
Organization Verification Procedures	CPS sections 3.1.8 and 3.1.9	**Verified?**	Verified
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.	**Verified?**	Verified
Code Signing Subscriber Verification Pro	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.	**Verified?**	Verified
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.	**Verified?**	Verified
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. CPS section 6.	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed &	http://www.entrust.net/about/third-party-	**Verified?**	Verified

Audited subCAs	sub-ca.htm