Print this page

Mozilla - CA Program

Case Information

Case Number	00000332	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Entrust	**Request Status**	In Detailed CP/CPS Review

Additional Case Information

Subject	Add Entrust G4 Root	**Case Reason**	

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=1480510

General information about CA's associated organization

CA Email Alias 1	roots@entrust.com		
CA Email Alias 2			
Company Website	https://www.entrustdatacard.com/	**Verified?**	Verified
Organizational Type	Private Corporation	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Verified
Geographic Focus	North America, Global	**Verified?**	Verified
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	High focus on enterprise customers, and has many government and financial customers. Root renewal.	**Verified?**	Verified

Required and Recommended Practices

Recommended Practices	https://wiki.mozilla.org /CA/Required_or_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's lists of Required and

			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	1. Publicly Available CP and CPS: CPS section 2 1.1 Revision Table, updated annually: CPS Revision History and section 2.3 1.2 CAA Domains listed in CP/CPS: CPS section 3.2.2.8, entrust.net 1.3 BR Commitment to Comply statement in CP/CPS: CPS section 1.1 2. Audit Criteria: CPS section 8 3. Revocation of Compromised Certificates: CPS section 4.9.1 4. Verifying Domain Name Ownership: CPS section 3.2.2.4 5. Verifying Email Address Control: CPS 3.2.2.9 6. DNS names go in SAN: Appendix A 7. OCSP: CPS section 4.9.9 - OCSP SHALL NOT respond "Good" for unissued certs: CPS section 4.9.10 8. Network Security Controls: CPS section 6.7	**Verified?**	Verified

Forbidden and Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org/CA/Forbidden_or_Problematic_Practices	**Problematic Practices Statement**	I have reviewed Mozilla's lists of Forbidden and 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	1. Long-lived Certificates: CPS section 6.3.2 2. Non-Standard Email Address Prefixes for Domain Ownership Validation: CPS section 3.2.2.4 3. Issuing End Entity Certificates Directly From Roots: CPS section 1.3.1 4. Distributing Generated Private Keys in PKCS#12 Files: CPS sections 6.1.1.3, 6.2.5, 6.2.11 5. Certificates Referencing Local Names or Private IP Addresses: CPS section 3.2.2.5 6. Issuing SSL Certificates for .int Domains: CPS section 7.1.4.2 7. OCSP Responses Signed by a Certificate Under a Different Root: CPS section 4.9.9 8. Issuance of SHA-1 Certificates: CPS section 7.1.3 9. Delegation of Domain / Email	**Verified?**	Verified

Validation to Third Parties: CPS sections 3.2.2.4, 7.1.6.3

Root Case Record # 1

Root Case Information

Root Certificate Name	Entrust Root Certification Authority - G4	**Root Case No**	R00000656
Request Status	In Detailed CP/CPS Review	**Case Number**	00000332

Certificate Data

Certificate Issuer Common Name	Entrust Root Certification Authority - G4
O From Issuer Field	Entrust, Inc.
OU From Issuer Field	See www.entrust.net/legal-terms, (c) 2015 Entrust, Inc. - for authorized use only
Valid From	2015 May 27
Valid To	2037 Dec 27
Certificate Serial Number	00D9B5437FAFA9390F000000005565AD58
Subject	CN=Entrust Root Certification Authority - G4; OU=See www.entrust.net/legal-terms, (c) 2015 Entrust, Inc. - for authorized use only; O=Entrust, Inc.; C=US
Signature Hash Algorithm	SHA256WithRSA
Public Key Algorithm	RSA 4096 bits
SHA-1 Fingerprint	14884E862637B026AF59625C4077EC3529BA9601
SHA-256 Fingerprint	DB3517D1F6732A2D5AB97C533EC70779EE3270A62FB4AC4238372460E6F01E88
Subject + SPKI SHA256	47E10321DE2408B5CEFCF90497B92C4A771F73983A75FEC54EB615311F11840E
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	This is the next generation Entrust root. Previous Entrust roots were included via Bugzilla Bug #382352 and #849950.	**Verified?**	Verified
Root Certificate Download URL	https://bug1480510.bmoattachments.org/attachment.cgi?id=8997105	**Verified?**	Verified

CRL URL(s)	http://crl.entrust.net/g4ca.crl http://crl.entrust.net/level1n.crl	**Verified?**	Verified
OCSP URL(s)	http://ocsp.entrust.net	**Verified?**	Verified
Mozilla Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	DV; OV; EV	**Verified?**	Verified
Mozilla EV Policy OID(s)	2.16.840.1.114028.10.1.2	**Verified?**	Verified
Root Stores Included In		**Verified?**	Verified
Mozilla Applied Constraints		**Verified?**	Not Applicable

Test Websites or Example Cert

Test Website - Valid	https://validg4.entrust.net/	**Verified?**	Verified
Test Website - Expired	https://expiredg4.entrust.net/		
Test Website - Revoked	https://revokedg4.entrust.net/		
Example Cert			
Test Notes			

Test Results (When Requesting the SSL/TLS Trust Bit)

Revocation Tested	https://certificate.revocationcheck.com/validg4.entrust.net No errors	**Verified?**	Verified
CA/Browser Forum Lint Test	https://crt.sh/?caid=96595&opt=cablint,zlint,x509lint&minNotBefore=2015-05-27	**Verified?**	Verified
Test Website Lint Test	CA performed lint testing	**Verified?**	Verified
EV Tested	ev-checker exited successfully: Success!	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	Section 1.3.1 of the CPS says: "This CPS covers all Certificates issued and signed by the following CAs." And it lists the Entrust root certificates (including this root) and their subCAs. The subCAs for the	**Verified?**	Verified

	other Entrust roots are disclosed in the CCADB. There is currently only one subordinate CA (Entrust Certification Authority - L1N) which has been set up for testing, and configured for EV SSL certificates. There will be more subordinate CAs once the root has been embedded.		
Externally Operated SubCAs	For this root Entrust only plans to have subordinate CAs that will be operated by Entrust. CPS section 7.1.6.3: "Subordinate CA Certificates issued to a Third Party Subordinate CA must include one or more explicit certificate policy object identifiers that indicates the Third Party Subordinate CA's adherence to and compliance with the requirements documented in its CP and/or CPS. For Third Party Subordinate CAs which issue SSL Certificates, these requirements must include adherence and compliance to the Baseline Requirements.	**Verified?**	Verified
Cross Signing	Currently no cross-signing with this root. CPS section 1.3.1 lists the externally issued cross certificates that are signed by other Entrust roots, and binds them to this CPS.	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	External RAs are allowed. CPS section 3.2.2.4: "The CA shall confirm that prior to issuance, the CA or the RA validated each Fully-Qualified Domain Name (FQDN) listed in the SSL or EV SSL Certificate using at least one of the methods listed below."	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	See the "ECS Legal Documents" tab of the Document Repository. No Certificate Policy. EV and OV CPS documents have been combined into one document in RFC 3647 format.	**Verified?**	Verified
CA Document Repository	https://www.entrustdatacard.com/resource-center/licensing-and-agreements	**Verified?**	Verified

CP Doc Language	English		
CP	https://www.entrustdatacard.com/-/media/documentation/licensingandagreements/ssl-cps-english-20181012-version-3_2.pdf?la=en&hash=6A125479A6A3C564F393D7811007DCF8AB551BA8	**Verified?**	Verified
CP Doc Language	English		
CPS	https://www.entrustdatacard.com/-/media/documentation/licensingandagreements/ssl-cps-english-20181012-version-3_2.pdf?la=en&hash=6A125479A6A3C564F393D7811007DCF8AB551BA8	**Verified?**	Verified
Other Relevant Documents	https://www.entrustdatacard.com/products/categories/ssl-certificates	**Verified?**	Verified
Auditor	Deloitte	**Verified?**	Verified
Auditor Location	Canada	**Verified?**	Verified
Standard Audit	https://www.entrustdatacard.com/-/media/documentation/licensingandagreements/entrust_wforca_2018.pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	5/21/2018	**Verified?**	Verified
BR Audit	https://www.entrustdatacard.com/-/media/documentation/licensingandagreements/entrust_baselinerequirements_2018.pdf?la=en&hash=BC08BAF5AE81B2EE66A2146EE7710FB2F4F33BA6	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	5/21/2018	**Verified?**	Verified
EV SSL Audit	https://www.entrustdatacard.com/-/media/documentation/licensingandagreements/entrust_wforevssl_2018.pdf?la=en&hash=B7F759CB298E973AB9A53F28AAED22AD9C7BE145	**Verified?**	Verified
EV SSL Audit Type	WebTrust	**Verified?**	Verified
EV SSL Audit Statement Date	5/21/2018	**Verified?**	Verified
BR Commitment to Comply	CPS Section 1.1	**Verified?**	Verified
BR Self Assessment	https://bugzilla.mozilla.org/attachment.cgi?id=8997108	**Verified?**	Verified
SSL Verification Procedures	CPS sections 3.2.2.4, 4.2.1	**Verified?**	Verified
EV SSL Verification Procedures	Identity – CPS 3.2.2.1 Domain – CPS 3.2.2.4 Authority – CPS 3.2.3 (identity of Contract Signer, Certificate Approver and Certificate Requester), CPS 3.2.5 and CPS	**Verified?**	Verified

	4.1.		
Organization Verification Procedures	CPS 3.2.2.1 (Organization) and CPS 3.2.3 (Individual)	**Verified?**	Verified
Email Address Verification Procedures	CPS 3.2.2.9	**Verified?**	Verified
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	CPS 6.5.1	**Verified?**	Verified
Network Security	CPS 5 and 6.7	**Verified?**	Verified