CA Owner Name: Entrust

-- General information about CA's associated organization --

CA Email Alias 1: *bruce.morton@entrustdatacard.com*

CA Email Alias 2: *roots@entrustdatacard.com*

Company Website: *www.entrustdatacard.com*

Organizational Type : *Manufacturing and Service*

Organizational Type (Others) :

Organization Type choices:
- Private Corporation

Geographic Focus: *Global CA with a focus on North America*

Primary Market / Customer Base:
- Which types of customers does the CA serve? High focus on enterprise customers which procure many types of certificates to protect many sites and perform other signing and encryption
- Are there particular vertical market segments in which it operates? Not specific market although Entrust has many government and financial customers
- Does the CA focus its activities on a particular country or other geographic region? Global CA, but majority of customers are in North America

Impact to Mozilla Users:
Why does the CA need to have their root certificate directly included in Mozilla's products, rather than being signed by another CA's root certificate that is already included in NSS? Entrust is already a root CA in the Mozilla program and would like to add this new 4096-bit root to support on going business.
Mozilla CA certificate policy: We require that all CAs whose certificates are distributed with our software product ... provide some service relevant to typical users of our software products – Entrust provides certificates to servers which support access by Mozilla Firefox.

-- Required and Recommended Practices --

Recommended Practices: https://wiki.mozilla.org/CA/Required_or_Recommended_Practices

Do You, as an official representative of this CA agree to the following Recommended Practices Statement?
Yes

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:
CAs response to each of the items listed in https://wiki.mozilla.org/CA/Required_or_Recommended_Practices

-- Forbidden and Potentially Problematic Practices --

Potentially Problematic Practices:
https://wiki.mozilla.org/CA/Forbidden_or_Problematic_Practices

Do You, as an official representative of this CA agree to the following Problematic Practices Statement?
Yes
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 Practice:
CA's response to each of the items listed in https://wiki.mozilla.org/CA/Forbidden_or_Problematic_Practices

- Policies and Practices -

Policy Documentation:
Languages that the CP/CPS and other documents are provided in.

CA Document Repository: *https://www.entrustdatacard.com/resource-center/licensing-and-agreements*

CP: *No CP*

CPS: *https://www.entrustdatacard.com/-/media/documentation/licensingandagreements/ssl-cps-english-20180531-version-30.pdf?la=en&hash=96C51D12E417D569CE5EA857117CC6B9EE74B373*

Other Relevant Documents:

Auditor Name: *Deloitte*

Auditor Website: *https://www2.deloitte.com/ca/en.html*

Auditor Qualifications: *WebTrust*

Standard Audit URL: *https://www.entrustdatacard.com/-/media/documentation/licensingandagreements/entrust_wforca_2018.pdf?la=en&hash=8FAB5940EB08D3D47DCB24C1B8FA5C0D5BFA93BA*

Standard Audit Type: *WebTrust for CA*

Standard Audit Statement Date: *21 May 2018*

BR Audit URL: *https://www.entrustdatacard.com/-/media/documentation/licensingandagreements/entrust_baselinerequirements_2018.pdf?la=en&hash=BC08BAF5AE81B2EE66A2146EE7710FB2F4F33BA6*
If requesting Websites trust bit, then also need a BR audit as per Mozilla's Root Store Policy.

BR Audit Type: *WebTrust*

BR Audit Statement Date: *21 May 2018*

EV SSL Audit URL: *https://www.entrustdatacard.com/-/media/documentation/licensingandagreements/entrust_wforevssl_2018.pdf?la=en&hash=B7F759CB298E973AB9A53F28AAED22AD9C7BE145*
If requesting EV treatment, then also need an EV audit as per Mozilla's Root Store Policy.

EV SSL Audit Type: *WebTrust*

EV SSL Audit Statement Date: *21 May 2018*

BR Commitment to Comply:
If requesting Websites trust bit, need section in the CP/CPS that has the commitment to comply with the BRs as described in section 2.2 of the CA/Browser Forum's Baseline Requirements.
Section 1.1

BR Self Assessment:
If requesting Websites trust bit, attach BR Self Assessment (https://wiki.mozilla.org/CA/BR_Self-Assessment) to the Bugzilla Bug.

SSL Verification Procedures:
if Websites trust bit requested...
Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the domain name to be included in the SSL/TLS cert.
CP/CPS must clearly specify the procedures that the CA employs. Each documented procedure should state which subsection of BR section 3.2.2.4 it is complying with.
CPS section 3.2.2.4 and sub-sections define all BR section 3.2.2.4 methods that Entrust supports for domain verification.

EV SSL Verification Procedures:
If EV verification is performed, then provide URLs and section/page number information pointing directly to the sections of the CP/CPS documents that pertain to EV and describe the procedures for verifying the ownership/control of the domain name, and the verification of identity, existence, and authority of the organization to request the EV certificate.
The EV verification documentation must meet the requirements of the CA/Browser Forum's EV Guidelines, and must also provide information specific to the CA's operations.
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 4.1.

Organization Verification Procedures:
CP/CPS sections that describe identity and organization verification procedures for cert issuance.
CPS 3.2.2.1 (Organization) and CPS 3.2.3 (Individual)

Email Address Verification Procedures:
if Email trust bit requested...
Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the email address to be included in the cert.
CPS 3.2.2.9

Multi-Factor Authentication:
section number of the CP/CPS that states that multi-factor authentication is enforced for all accounts capable of directly causing certificate issuance. (reference section 6.5 of the BRs)
CPS 6.5.1

Network Security:
section number(s) of the CP/CPS dealing with Network Security.
CPS 5 and 6.7

-- Technical Information about each Root Certificate --
Provide the following information for each root cert for which you are requesting inclusion or change.

-- Root Certificate #1 --

Root Certificate Name: *Example Root Cert Common Name*

- Certificate Data -

Root Certificate Download URL:
A public URL through which the CA certificate can be directly downloaded.

Certificate Issuer Common Name: *Entrust Root Certification Authority - G4*
O From Issuer Field: *Entrust, Inc.*
OU From Issuer Field: *(c) 2015 Entrust, Inc. - for authorized use only*
See www.entrust.net/legal-terms
SHA-256 Fingerprint:
DB:35:17:D1:F6:73:2A:2D:5A:B9:7C:53:3E:C7:07:79:EE:32:70:A6:2F:B4:AC:42:38:37:24:60:E6:F0:1E:88

CRL URL(s): *http://crl.entrust.net/g4ca.crl*
CRL URLs and CRL issuing frequency for subscriber certs, with reference to where this is documented in the CP/CPS - CPS 4.9.7, at least once every twelve months or with 24 hours after revoking a Subordinate CA Certificate

OCSP URL(s): *http://ocsp.entrust.net*
OCSP URL and maximum OCSP expiration time, with reference to where this is documented in the CP/CPS CPS 4.9.10 (i) OCSP responses for Certificates issued to Subordinate CAs shall be issued at least once every twelve months or within 24 hours after revoking a Subordinate CA Certificate

Mozilla Trust Bits:
Email; Websites Entrust requests both Email and Websites trust bits

SSL Validation Type:
DV; OV; EV Entrust requests DV, OV and EV validation types

Mozilla EV Policy OID(s):
2.23.140.1.2.2 Entrust EV policy OID is 2.16.840.1.114028.10.1.2

Root Stores Included In: *This root is not included in any other root stores.*

Mozilla Applied Constraints
Mozilla has the ability to name constrain root certs; e.g. to *.gov or *.mil. CAs should consider if such constraints may be applied to their root certs. *This does not apply to this root.*
https://dxr.mozilla.org/mozilla-central/source/security/nss/lib/certdb/genname.c#1551

- Test Websites or Example Cert -

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

If requesting Websites trust bit provide 3 URLs to 3 test websites (valid, expired, revoked) whose TLS/SSL cert chains up to this root. - If only requesting the Email trust bit, then attach an example S/MIME cert to the bug.

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

Revocation Tested:
Test with http://certificate.revocationcheck.com/ make sure there aren't any errors.

CA/Browser Forum Lint Test:
The CA MUST check that they are not issuing certificates that violate any of the CA/Browser Forum Baseline Requirements (BRs).

BR Lint Test:
https://github.com/awslabs/certlint - Passed test

Test Website Lint Test :
The CA MUST check that they are not issuing certificates that violate any of the X.509 rules.

X.509 Lint Test: https://github.com/kroeckx/x509lint - *Passed test*

EV Tested:
If EV treatment is being requested, then provide successful output from EV Testing as described here https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version
Passed test see, https://screenshots.firefox.com/dtc2pt2wY1Ondhc9/tls-observatory.services.mozilla.com

- CA Hierarchy Information -

CA Hierarchy:
A description of the PKI hierarchy rooted at or otherwise associated with this root CA certificate.
- List and/or describe all of the subordinate CAs that are signed by this root.
CN = Entrust Certification Authority - L1N
- Identify which of the subordinate CAs are internally-operated; e.g. list the subordinate CAs that operated by the CA organization associated with the root CA. For example, this might include subordinate CAs created to issue different classes or types of end entity certificates to the general public: Class 1 vs. class 2 certificates, qualified vs. non-qualified certificates, EV certificates vs. non-EV certificates, SSL certificates vs. email certificates, and so on.
The L1N subordinate CA is internally operated. There is only one subordinate CA which has been set up for testing. It has been configured for EV SSL certificates. There will be move subordinate CAs once the root has been embedded.
- It might also include subordinate CAs operated for the benefit of specific third parties. In this case note that we do not require that the CA submit a complete customer list; rather we are interested in the general type and nature of the third-party arrangements

Externally Operated SubCAs:
- If this root has any subordinate CA certificates that are operated by external third parties, then provide the information listed in the Subordinate CA Checklist, https://wiki.mozilla.org/CA/Subordinate_CA_Checklist
This root does not have any subordinate CAs operated by third parties.

- If the CA functions as a super CA such their CA policies and auditing don't apply to the subordinate CAs, then those subordinate CAs must apply for inclusion themselves as separate trust anchors.
Not applicable

Cross Signing:
- List all other root certificates for which this root certificate has issued cross-signing certificates.
No cross-signed certificates.
- List all other root certificates that have issued cross-signing certificates for this root certificate.
No cross-signed certificates.
- If any such cross-signing relationships exist, it is important to note whether the cross-signing CAs' certificates are already included in the Mozilla root store or not.
Not applicable.

Technical Constraint on 3rd party Issuer:
CP/CPS documentation describing the technical and contractual controls over any 3rd party who may issue certs in this CA Hierarchy. This includes external RAs as well as External subCAs.
References:
- section 7.1.5 of the CA/Browser Forum's Baseline Requirements
- Mozilla's Root Store Policy
There are no third party operated CAs. Entrust only plans to have subordinate CAs that will be operated by Entrust.
Third party RA's are really only information providers. All information is provided to an Entrust Verification Specialist, who then performs verification. All manual verification is reviewed by a Verification Auditor which can then approve or reject. All validated information for all certificates resides in the Entrust database and is subject to audit during the annual Entrust compliance audit.

-- End Root Certificate #1 --