OPEN ACCESS TECHNOLOGY INTERNATIONAL, INC.
3660 Technology Drive NE | Minneapolis, MN 55418
Phone 763.201.2000 | Fax 763.201.5333
www.oati.com

Mozilla Root CA Certificate Application

Follow up Questions

Below please find Open Access Technology International, Inc's (OATI's) responses to issues raised by Mozilla in attachment 779413, "Initial CA Information Document" posted for Bug 848766 which requests Mozilla to admit the OATI Root Certificate Authority (CA) Certificate into the Mozilla Root Certificate Program. OATI affirms that the responses provided below are true and accurate as of effective date, March 25, 2014.

1. OSCP URL (Required now by Baseline Requirements)

Mozilla comment:

OCSP is now required as per the CA/Browser Forum's Baseline Requirement #13.2.2

OATI Response:

OATI has fully implemented OCSP for its webCARES Digital Certificate Public Key Infrastructure (PKI). OCSP responders are now available for OATI's Root, Issuer, and End Entity Certificates using the standard OCSP protocol.

2. Policy Documentation

Mozilla comment:

Why does the first page of the Certification Practice Statement (CPS) say "Proprietary and Confidential"? And the second page says: "TRADE SECRET…"

OATI Response:

This is standard language provided on all OATI internal and external facing documents. The most current version of OATI's CPS is always posted publically on OATI's website and access to this document is not restricted.

3. Baseline Requirements (SSL)

Mozilla comment:

The document(s) and section number(s) where the "Commitment to Comply" with the Certificate Authority (CA)/Browser Forum Baseline Requirements may be found for Secured Socket Layer (SSL) Certificate issuance, as per BR #8.3.

Audits performed after January 2013 need to include verification of compliance with the CA/Browser Forum Baseline Requirements if SSL Certificates may be issued within the CA hierarchy, and the audit statement shall indicate the results.

OATI response:

Please refer to Section 9 of the OATI Certificate Practice Statement v2.5 which states, "The practices in this CPS are designed to meet or exceed the requirements of generally accepted industry standards, including the latest versions of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (CA/B Forum), the North American Energy Standards Board (NAESB) Wholesale Electric Quadrant Public Key Infrastructure for Authorized Certification Authorities Standards (WEQ-012), and the American Institute of Certified Public Accountants (AICPA)/Canadian Institute of Chartered Accountants (CICA) WebTrust Program for CAs (WebTrust).

OATI undergoes an annual audit by an independent external auditor to assess OATI's compliance with this CPS, WebTrust and WEQ-012 criteria. The audit covers OATI's systems, processes and procedures regarding the OATI webCARES Digital Certificate PKI operations, and its compliance with applicable guidelines and standards."

4. Registration Authorities (RAs)

Mozilla comment:

Can Local Registration Authorities (LRAs) issue SSL Certificates?

OATI response:

LRAs can generate requests for SSL Certificates. The webCARES System validates the request and if successful issues the SSL Certificate.

5. SSL Verification Procedures

Mozilla comments:

If you are requesting to enable the Websites Trust Bit, then provide the information requested in #3 (SSL Verification Procedures) of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices.

OATI response:

Please refer to section 3.2.1. of the OATI webCARES CPS and the OATI webCARES Business Representative Application Form (BRAF); both documents can be found at: http://www.oaticerts.com/repository/. The identity proofing requirements used are defined by NIST SP800-63 version 1.0.2 section *7.2.1 Registration of Identity Proofing Requirements*.

Additionally, each applicant for an OATI webCARES Digital Certificate must complete and submit a BRAF to OATI. Upon receipt of a completed BRAF, OATI webCARES personnel follow a formal process that includes steps to ensure that the organizational information to be included in the Certificate has been verified, the identity of the individual (the person requesting the Certificate) has been verified, if the request is on behalf of an organization, then the authority of the individual to make that request has been verified, and the identity and organization validation are tied together so that there is reasonable assurance that

someone cannot submit forged or stolen documents and receive a certificate in his name (or that of a company).

The verification process may include, but is not limited to:

- Calling the applicant's contacts provided on the BRAF.
- Verifying the Data Universal Numbering System (DUNS) number provided, and researching the applicant's company.
- Verifying applicant control over e-mail addresses that will be included in certificates by sending an e-mail and requiring a response from the receiver.
- Verifying Domain Name Ownership by one or more of the following methods defined by the CA/Browser Forum Baseline Requirements, v. 1.1.6.1:
  1. Confirming the Applicant as the Domain Name Registrant directly with the Domain Name Registrar;
  2. Communicating directly with the Domain Name Registrant using an address, email, or telephone number provided by the Domain Name Registrar;
  3. Communicating directly with the Domain Name Registrant using the contact information listed in the WHOIS record's "registrant," "technical," or "administrative" field;
  4. Communicating with the Domain's administrator using an email address created by pre-pending 'admin,' 'administrator,' 'webmaster,' 'hostmaster,' or 'postmaster' in the local part, followed by the at-sign ("@"), followed by the Domain Name, which may be formed by pruning zero or more components from the requested FQDN;
  5. Relying upon a Domain Authorization Document;
  6. Having the Applicant demonstrate practical control over the FQDN by making an agreed-upon change to information found on an online Web page identified by a uniform resource identifier containing the FQDN; or
  7. Using any other method of confirmation, provided that the OATI is able to maintain documented evidence that the method of confirmation establishes that the Applicant is the Domain Name Registrant or has control over the FQDN to at least the same level of assurance as those methods previously described.

6. Email Address Verification Procedures

Mozilla comments:

If you are requesting to enable the Email Trust Bit, then provide the information requested in #4 (Email Address Verification Procedures) of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices.

OATI response:

To verify the e-mail of a Certificate request, OATI sends an e-mail to the address specified in the request and requires the receiver to verify receipt of the e-mail before a Certificate is issued.

[1] CA/Browser Forum Baseline Requirements, v. 1.1.6
https://cabforum.org/wp-content/uploads/Baseline_Requirements_V1_1_61.pdf.

7. Network Security

Mozilla comments:

Confirm that you have performed the actions listed in #7 (Network Security) of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices.

OATI response:

OATI has reviewed the actions listed in item #7 of the Verification Policies and Practices and confirms that it has performed all actions listed. OATI has also reviewed the CA/Browser Forum's Network and Certificate System Security Requirements and confirms that OATI network security controls meet these standards.

8. DNS names go in Storage Area Network (SAN)

Mozilla comments:

Please see Baseline Requirement #9.2.1.

OATI response:

OATI enforces subjectAltName and Subject Common Name containing the Fully-Qualified Domain Name or an IPAddress containing the IP address of a server.

9. Email Address Prefixes for DV Certs

Mozilla comments:

If DV SSL certs, then list the acceptable email addresses that are used for verification.

OATI response:

If OATI ever uses emails to verify Domain Ownership, 'admin,' 'administrator,' 'webmaster,' 'hostmaster,' or 'postmaster' will be used.