Bugzilla ID: 848766
Bugzilla Summary: Please Add OATI's Root CA Certificate to Mozilla's trusted root list

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	Open Access Technology International, Inc. (OATI)
Website URL	http://www.oati.com/
Organizational type	The CA (OATI webCARES) is owned and operated by Open Access Technology International, Inc. ("OATI"). OATI is a private corporation incorporated under laws of the State of Minnesota.
Primary Market / Customer Base and Impact to Mozilla Users	The scope of OATI's Public Key Infrastructure (PKI) operations can be broken down into four primary user communities: 1) Mobile Applications consumers, Markets, & products; 2) Wholesale Energy; 3) Retail (Home & Business) Energy/Smart Grid consumers, Markets, & Products; and 4) Amateur Sports participants. OATI anticipates massive growth in each of these user communities spurred by: 1) User activities expansion from desktop to mobile devices/tablets, 2) Proliferation of Smart Grid standards and the resulting devices requiring client certificates, and 3) A critical mass of industries switching to two-factor authentication using client certificates 4) Key Smart Grid standards to include PKI and a limited number of trusted Root CAs. These standards are currently in use in more than 600 electric cooperatives, investor-owned utilities, municipal utilities, and public power districts in at least 15 different countries, and total market penetration is growing significantly every year.
Inclusion in other major browsers	Microsoft accepted OATI's root inclusion request.
CA Contact Information	PKIMonitor@oati.net, 763.201.2000 Patrick Tronnier – Senior Director Quality Assurance, Customer Support and webCARES Principal Security Architect cio@oati.net, 763.201.2000 David Heim - Chief Information Officer

Technical information about each root certificate

Certificate Name	OATI WebCARES Root CA

Certificate Issuer Field	CN = OATI WebCARES Root CA
	O = Open Access Technology International Inc
	L = Minneapolis
	ST = MN
	C = US

Certificate Summary	OATI issues certificates to be used for identity authentication purposes for S/MIME and within an SSL/TLS session for both Server Authentication and the optional Client Side Authentication.
Root Cert URL	http://www.oaticerts.com/repository/OATICA2.crt
SHA1 Fingerprint	4B:6B:D2:D3:88:4E:46:C8:0C:E2:B9:62:BC:59:8C:D9:D5:D8:40:13
Valid From	2008-06-03
Valid To	2038-06-03
Certificate Version	3
Certificate Signature Algorithm	PKCS #1 SHA-1 With RSA Encryption
Signing key parameters	4096
Test Website URL (SSL)	https://www.oaticerts.com/ The SSL cert does not have an OCSP URI in the AIA.
CRL URL	http://certs.oaticerts.com/repository/OATICA2.crl http://certs.oaticerts.com/repository/OATIIA2.crl (NextUpdate: 24 hours)
OCSP URL (Required now by Baseline Requirements)	**Need OCSP URI from the AIA of the AAL cert in the test website.** 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.
Requested Trust Bits	Websites (SSL/TLS) Code Signing (need verification procedures regarding code signing certs documented in CPS, see below) Email (S/MIME)
SSL Validation Type	DV
EV Policy OID(s)	Not applicable, not requesting EV treatment

CA Hierarchy information for each root certificate

CA Hierarchy	OATI currently has one internally-operated intermediate CA called "OATI webCARES Issuing CA"
Externally Operated SubCAs	OATI does not have any externally operated SubCAs.
Cross-Signing	OATI's webCARES Root Certificate Authority does not cross-sign with any other root certificates.
Technical Constraints on Third-party Issuers	The subject of each certificate issued by OATI's Registration Authorities is pre-determined by the organizational data submitted and verified during the application authorization process. Pre-filled fields and form dropdowns provide the technical constraints necessary to prevent issuance of certificates with misleading or incorrect information.

Verification Policies and Practices

Policy Documentation	Document Repository: http://www.oaticerts.com/repository/ CPS (English): http://www.oaticerts.com/repository/OATI-webCARES-CPS.pdf Why does the first page of the 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.

Audits	Audit Type: WebTrust for CA Auditor: Schellman & Company, LLC (SCLLC), an affiliate of BrightLine Auditor Website: WebTrust Seal: https://cert.webtrust.org/ViewSeal?id=1447 (2013.01.09) – when do you expect the new audit statement?
Baseline Requirements (SSL)	BR audit statement https://wiki.mozilla.org/CA:CertificatePolicyV2.1#Time_Frames_for_included_CAs_to_comply_with_the_new_policy “Any Certificate Authority being considered for root inclusion after February 15, 2013 must comply with Version 2.1 or later of Mozilla's CA Certificate Policy. This includes having a Baseline Requirements audit performed if the websites trust bit is to be enabled. Note that the CA's first Baseline Requirements audit may be a Point in Time audit.” CPS section 9: 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 NAESB WEQ-012, and the AICPA/CICA WebTrust Program for Certification Authorities (WebTrust). OATI receives annual audits by an independent external auditor to assess OATI's compliance with this CPS, WebTrust and WEQ-012 criteria. The audits cover OATI’s systems, processes and procedures regarding the OATI webCARES Digital Certificate PKI operations, and its compliance with applicable guidelines and standards.
Registration Authorities	LRAs can generate requests for SSL Certificates. The webCARES System validates the request and if successful issues the SSL Certificate. How does the webCARES System validate the request? Is there some software that automatically checks certain things? If yes, what exactly does the software check? CPS section 2.5: The OATI Registration Authority (RA) may delegate RA duties to Local Registration Authorities (LRAs). The RA and/or LRA, where applicable, is responsible for performing the OATI webCARES Subscriber Identification and Verification Procedure (SIVP) or other acceptable methods of identity verification in conformance with applicable standards. This procedure is documented and ensures that OATI issues webCARES digital certificates to entities that are verified using commercially reasonable industry practices and procedures. CPS section 3.3.1: The role of Security Officer, otherwise known as a Local Registration Authority (LRA), is mandatory for every organization or entity subscribing to the OATI webCARES System. A Security Officer (SO) will be responsible for managing the Digital Certificates within his or her Organizational Unit. A SO will be responsible to use the OATI webCARES System to perform the SO’s duties and responsibilities described in this CPS. A SO is delegated the right to serve as a LRA. The SOs duties and obligations include, for example, identity proofing; issuing, revoking, renewing, and tracking Digital Certificates for his or her End Users; and revoking digital certificates which are compromised or for employees who leave the company. A SO will be provided personal access to the OATI webCARES System to perform his or her role.
Organization Verification	CPS section 3.2.1.1: Security Officers can verify the identity of Subscribers in one of three ways.

Procedures	1. The Security Officer can validate a Subscriber's identity in person by having the Subscriber present a valid and current Government Issued picture ID. 2. The Security Officer can validate a Subscriber's identity remotely through the Subscriber's presenting a valid and current Government Issued picture ID and a financial account number that can be confirmed. 3. Security Officer's issuing Digital Certificates to internal employees may perform identity verification through their company's Human Resources background screening performed upon employment, a corporate issued picture ID and/or an online processes where notification is sent via the distribution channels normally used for sensitive, personal communications. 3.2.2 Eligible Entities The following describes the types of entities eligible for OATI webCARES access. 3.2.2.1 Business Representative To verify a Subscriber as a Business Representative for a specific organization, the identity of both the organization for which the Subscriber claims to work and the Security Officer for that organization must be verified by the Registration Authority. 3.2.2.2 Unaffiliated Individual An Unaffiliated Individual may apply for an OATI webCARES Digital Certificate for his or her own personal use. An Unaffiliated Individual, by definition, will not be applying for a webCARES Digital Certificate as the Agent of an Organization. Therefore, unlike a Business Representative, the Unaffiliated Individual must be identified and verified solely using his or her own personal information. 3.2.2.3 Machine/Server/Applications In the case of a machine, server, or application a person at the organization where the machine, server or application resides will need to apply for and be named an SO for his or her organization. Therefore, the person who will manage the Digital Certificate(s) for the machine, server, or application must submit both the organziation and personal information to be identified and verified.
SSL Verification Procedures	CPS section 3.2.1: The SIVP includes, 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 fully qualified

	domain name (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 CA maintains 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.
Email Address Verification Procedures	CPS section 3.2.1: The SIVP includes, but is not limited to: … 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. 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.
Code Signing Subscriber Verification Procedures	If you are requesting to enable the Code Signing Trust Bit, then provide pointers to where the verification procedures for Code Signing certificates are documented in the CPS, as described in #5 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices
Multi-factor Authentication	Multi-factor authentication including username, password and digital client certificates are required to access OATI's CA and issue certificates.
Network Security	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.

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

Publicly Available CP and CPS	Yes, see above
CA Hierarchy	See above
Audit Criteria	See above
Document Handling of IDNs in CP/CPS	OATI does not allow the use of internationalized domain names (IDNs) in certificates.
Revocation of Compromised Certificates	OATI revokes certificates with private keys that are known to be compromised, or for which verification of subscriber information is known to be invalid.
Verifying Domain Name Ownership	See above
Verifying Email Address Control	See above
Verifying Identity of Code Signing Certificate Subscriber	Not applicable
DNS names go in SAN	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.
Domain owned by a Natural Person	OATI does not issue certificates to external individuals. Every certificate is issued to a business representative of a verified organization. Thus, for every certificate issued by OATI O = name of the verified organization OU = the organizational unit the individual belongs to
OCSP	See above

Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)

Long-lived DV certificates	OATI certificates expire every 24 months. Upon renewal, each certificate is verified to confirm set is included in SSL certificates remains current and correct.
Wildcard DV SSL certificates	OATI does not issue Wildcard DV SSL certificates.
Email Address Prefixes for DV Certs	OATI response: If OATI ever uses emails to verify Domain Ownership, ‘admin,’ ‘administrator,’ ‘webmaster,’ ‘hostmaster,’ or ‘postmaster’ will be used.
Delegation of Domain / Email validation to third parties	**Yes. See LRA information above.**
Issuing end entity certificates directly from roots	OATI does not allow issuance of end-entity certificates directly from its root.
Allowing external entities to operate subordinate CAs	OATI does not allow external entities to operate subordinate CAs.
Distributing generated private keys in PKCS#12 files	OATI does not generate key pairs for subscribers.
Certificates referencing hostnames or private IP addresses	OATI does not allow Registration Authorities or subscribers to issue certificates referencing hostnames or private IP addresses within its CA hierarchy. In some instances, OATI uses internal domain names for its development activities, but this is strictly confined to internal OATI developer servers.
Issuing SSL Certificates for Internal Domains	OATI does not allow Registration Authorities or subscribers to issue certificates for internal domains within its CA hierarchy. In some instances, OATI will use internal domain names for its development activities, but this is strictly confined to internal OATI developer servers.
OCSP Responses signed by a certificate under a different root	See above.
CRL with critical CIDP Extension	CRLs imported into Firefox without error.
Generic names for CAs	CN not generic
Lack of Communication With End Users	OATI operates a 24x7x365 Helpdesk support center which allows it to be contacted by, and accept and act upon complaints made by, those relying on its assertions of identity. This includes being responsive to members of the general public, including people who have not purchased products from OATI.