Print this page

Mozilla - CA Program

Case Information

Case Number	00000032	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Open Access Technology International, Inc. (OATI)	**Request Status**	Need Information from CA

Additional Case Information

Subject	New Owner/Root inclusion requested	**Case Reason**	New Owner/Root inclusion requested

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=848766

General information about CA's associated organization

CA Email Alias 1	pkimonitor@oati.net		
CA Email Alias 2			
Company Website	http://www.oati.com/	**Verified?**	Verified
Organizational Type	Private Corporation	**Verified?**	Verified
Organizational Type (Others)	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.	**Verified?**	Verified
Geographic Focus	United States	**Verified?**	Verified
Primary Market / Customer Base	OATI's PKI serves 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.	**Verified?**	Verified
Impact to Mozilla Users	OATI anticipates growth spurred by: Proliferation of Smart Grid standards and the resulting devices requiring client certificates, and 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.	**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	* OATI does not allow the use of internationalized domain names (IDNs) in 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. * OATI enforces subjectAltName and Subject Common Name containing the Fully-Qualified Domain Name or an IPAddress containing the IP address of a server. * 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	**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	* OATI does have external RAs, per CPS sections 2.5 and 3.3.1. * OATI certificates expire every 24 months. Upon renewal, each certificate is verified to confirm set is included in SSL certificates remains current and correct. * OATI does not issue Wildcard DV SSL certificates. * If OATI ever uses emails to verify Domain Ownership, 'admin,' 'administrator,' 'webmaster,' 'hostmaster,' or 'postmaster' will be used. * OATI does not allow issuance of end-entity certificates directly from its root. * OATI does not allow external entities to operate subordinate CAs. * OATI does not generate key pairs for subscribers. * 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. * 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. * 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.	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Certificate Name	OATI WebCARES Root CA	**Root Case No**	R00000036
Request Status	Need Information from CA	**Case Number**	00000032

Additional Root Case Information

Subject	Include OATI WebCARES Root CA cert

Technical Information about Root Certificate

O From Issuer Field	Open Access Technology International Inc	**Verified?**	Verified
OU From Issuer Field		**Verified?**	Verified
Certificate Summary	OATI has internally-operated intermediate certificates that sign 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.	**Verified?**	Verified
Root Certificate Download URL	http://www.oaticerts.com/repository/OATICA2.crt	**Verified?**	Verified
Valid From	2008 Jun 03	**Verified?**	Verified
Valid To	2038 Jun 03	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-1	**Verified?**	Verified
Signing Key Parameters	4096	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://www.oaticerts.com/	**Verified?**	Verified
CRL URL(s)	http://certs.oaticerts.com/repository/OATICA2.crl http://certs.oaticerts.com/repository/OATIIA2013.crl	**Verified?**	Verified
OCSP URL(s)	http://ocsp.oaticerts.com/ocsp	**Verified?**	Verified
Revocation Tested	NEED: Fix errors https://certificate.revocationcheck.com/www.oaticerts.com - The Cache-Control max-age header outlives NextUpdate	**Verified?**	Need Response From CA
Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	DV	**Verified?**	Verified
EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
EV Tested	Not requesting EV treatment.	**Verified?**	Not Applicable
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	4B:6B:D2:D3:88:4E:46:C8:0C:E2:B9:62:BC:59:8C:D9:D5:D8:40:13	**Verified?**	Verified
SHA-256 Fingerprint	7A:77:C6:C6:1E:EE:B9:AA:65:C4:EA:41:0D:65:D8:95:B2:6A:81:12:32:83:00:9D:B1:04:B4:8D:E8:0B:24:79	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	OATI currently has one internally-operated intermediate CA called “OATI webCARES Issuing CA”	**Verified?**	Verified
Externally Operated SubCAs	OATI does not have and does not allow externally operated SubCAs.	**Verified?**	Verified
Cross Signing	OATI’s webCARES Root Certificate Authority does not cross-sign with any other root certificates.	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	OATI has LRAs. 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. CPS section 2.5: The OATI Registration Authority (RA) may delegate RA duties to Local Registration Authorities (LRAs). 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.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	The first page of the CPS says: “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 publicly on OATI’s website and access to this document is not restricted.	**Verified?**	Verified
CA Document Repository	http://www.oaticerts.com/repository/	**Verified?**	Verified
CP Doc Language	English		
CP	http://www.oaticerts.com/repository/OATI-webCARES-CPS.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	http://www.oaticerts.com/repository/OATI-webCARES-CPS.pdf	**Verified?**	Verified
Other Relevant Documents		**Verified?**	Not Applicable

Auditor Name	Schellman & Company	**Verified?**	Verified
Auditor Website	NEED URL to Auditor's website/qualifications	**Verified?**	Need Response From CA
Auditor Qualifications	NEED: I'm not finding the auditor in the webtrust list: http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Need Response From CA
Standard Audit	https://cert.webtrust.org/SealFile?seal=1802&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	1/2/2015	**Verified?**	Verified
BR Audit	https://bug848766.bmoattachments.org/attachment.cgi?id=8641438	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	11/15/2014	**Verified?**	Verified
EV Audit	Not requesting EV treatment	**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	CPS section 10.1.	**Verified?**	Verified
SSL Verification Procedures	CPS section 1.1: SIVP = Subscriber Identification and Verification Procedure CPS section 3.2.1: The SIVP includes, but is not limited to: ... Verifying Domain Name Ownership by one or more of the following methods defined by the CA/Browser Forum Baseline Requirements, v1.1.6.1: - Confirming the Applicant as the Domain Name Registrant directly with the Domain Name Registrar; - Communicating directly with the Domain Name Registrant using an address, email, or telephone number provided by the Domain Name Registrar; - Communicating directly with the Domain Name Registrant using the contact information listed in the WHOIS record’s “registrant,” “technical,” or “administrative” field; - 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); - Relying upon a Domain Authorization Document; - 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	**Verified?**	Verified

	- 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 ...		
EV SSL Verification Procedures	Not requesting EV treatment	**Verified?**	Not Applicable
Organization Verification Procedures	CPS section 3.2.1: Upon receipt of a completed BRAF, OATI webCARES personnel continue the SIVP that includes steps to ensure that the organizational information to be included in the certificate has been verified, the identity of the applicant (the person requesting the certificate) has been verified, if the request is on behalf of an organization, then the authority of the applicant 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/her name (or that of a company). The application process contained in Section 3.2, including the various verification and identity proofing processes, apply to all applications received for webCARES Digital Certificates section 3.2.1.1 - Identity Proofing Requirements section 3.2.2 - Eligible Entities	**Verified?**	Verified
Email Address 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.	**Verified?**	Verified
Code Signing Subscriber Verification Pro	Not requesting the code signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	Multi-factor authentication including username, password and digital client certificates are required to access OATI's CA and issue certificates.	**Verified?**	Verified
Network Security	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.	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed &	http://www.oaticerts.com/repository/	**Verified?**	Verified

Audited subCAs