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**	Information Verification In Process

Additional Case Information

Subject	Include OATI Root	**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).	**Verified?**	Verified
Geographic Focus	USA	**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.	**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 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	1. Publicly Available CP and CPS: CPS section 2.3 1.1 Revision Table, updated annually: ??? NEED: revision table in the CPS as per https://wiki.mozilla.org/CA/Required_or_Recommended_Practices#CP.2FCPS_Revision_Table 1.2 CAA Domains listed in CP/CPS: CPS section 4.6 1.3 BR Commitment to Comply statement in CP/CPS: CPS section 2.1 2. Audit Criteria: CPS section 10.1 3. Revocation of Compromised Certificates: CPS section 3.4.6 4. Verifying Domain Name Ownership: CPS section 3.2.1 5. Verifying Email Address Control: CPS section 3.2.1 6. DNS names go in SAN: CPS section 7.1.5 7. OCSP: CPS sections 3.4.10 - OCSP SHALL NOT respond "Good" for unissued certs: CPS section 7.3 8. Network Security Controls: CPS section 5.4	**Verified?**	Need Response From CA

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 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	1. Long-lived Certificates: CPS section 7.1.2 2. Non-Standard Email Address Prefixes for Domain Ownership Validation: CPS section 3.2.1 3. Issuing End Entity Certificates Directly From Roots: CPS section 2.10 4. Distributing Generated Private Keys in PKCS#12 Files: CPS section 5.2 5. Certificates Referencing Local Names or Private IP Addresses: CPS section 7.1.5.2 6. Issuing SSL Certificates for .int Domains: CPS section 7.1.5.2 7. OCSP Responses Signed by a Certificate Under a Different Root: CPS	**Verified?**	Verified

section 3.4.10
8. Issuance of SHA-1 Certificates: CPS section 5.1.3
9. Delegation of Domain / Email Validation to Third Parties: CPS section 2.5

Root Case Record # 1

Root Case Information

Root Certificate Name	webCARES Root CA 2018	**Root Case No**	R00000036
Request Status	Information Verification In Process	**Case Number**	00000032

Certificate Data

Certificate Issuer Common Name	webCARES Root CA 2018
O From Issuer Field	Open Access Technology International Inc
OU From Issuer Field	
Valid From	2018 Apr 19
Valid To	2038 Apr 19
Certificate Serial Number	4ED6823AB7CAC3B74AB3B9EBA04BCDA5
Subject	CN=webCARES Root CA 2018; OU=; O=Open Access Technology International Inc; C=US
Signature Hash Algorithm	SHA512WithRSA
Public Key Algorithm	RSA 4096 bits
SHA-1 Fingerprint	CDFD54F28E8E44CFA6D8848809530C65D80F452C
SHA-256 Fingerprint	F0B6883DDEEDF22E674555F98F638738E0CCE44519FBC97FFA8C8C9F7E1DED5B
Subject + SPKI SHA256	E7A50E7CB0826F996725B1466602527E7AD299BF7B5F29B530E6F108B30EB094
Certificate Version	3

Technical Information about Root Certificate

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	**Verified?**	Verified

	both Server Authentication and the optional Client Side Authentication.		
Root Certificate Download URL	https://bugzilla.mozilla.org/attachment.cgi?id=8970886	Verified?	Verified
CRL URL(s)	http://certs.oaticerts.com/repository/Root2018.crl, http://certs.oati.net/repository/Root2018.crl CPS section 7.5: 12 hours for end-entity CRL	Verified?	Not Verified
OCSP URL(s)	http://ocsp.oaticerts.com/ocsp	Verified?	Not Verified
Mozilla Trust Bits	Email; Websites	Verified?	Verified
SSL Validation Type	DV	Verified?	Verified
Mozilla EV Policy OID(s)	Not EV	Verified?	Not Applicable
Root Stores Included In	Microsoft	Verified?	Verified
Mozilla Applied Constraints	None	Verified?	Verified

Test Websites or Example Cert

Test Website - Valid	https://www.oaticerts.com/	Verified?	Need Response From CA
Test Website - Expired	https://expired.oaticerts.com		
Test Website - Revoked	https://revoked.oaticerts.com		
Example Cert			
Test Notes	NEED: Three test websites (valid, expired, revoked) whose SSL certs chain up to the new 'webCARES Root CA 2018' root.		

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

Revocation Tested	https://certificate.revocationcheck.com/www.oaticerts.com NEED: Revocation check of a valid test website whose SSL cert chains up to the new 'webCARES Root CA 2018' root.	Verified?	Need Response From CA
CA/Browser Forum Lint Test	https://bugzilla.mozilla.org/show_bug.cgi?id=848766#c61	Verified?	Verified
Test Website Lint Test	https://bugzilla.mozilla.org/show_bug.cgi?id=848766#c61	Verified?	Verified
EV Tested	Not requesting EV treatment.	Verified?	Not Applicable

CA Hierarchy Information

CA Hierarchy	CPS section 2.10: "OATI webCARES PKI is implemented with the following hierarchical structure: 1. OATI Root 2. OATI IA 3. Company SOs 4. End Entities Additionally, the OATI CA will operate a Repository and OATI will initially act as an NA for webCARES system users."	**Verified?**	Verified
Externally Operated SubCAs	OATI does not have and does not allow externally operated SubCAs. CPS section 2.4: "OATI webCARES acts as a CA providing certificate services within the webCARES PKI. OATI webCARES CA will: - Issue and publish OATI webCARES Digital Certificates in accordance with this CPS. ..."	**Verified?**	Verified
Cross Signing	CPS section 2.11.4: "OATI webCARES currently does not cross certify any other CA and has not issued any cross certificates."	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	CPS section 2.5: "The OATI RA may delegate RA duties to LRAs. The RA and/or LRA, where applicable, is responsible for performing the OATI webCARES 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."	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	NEED: Remove all "CONFIDENTIAL" notices and text from the publicly-posted CPS. Mozilla requires CAs to publicly post non-confidential CP/CPS documents.	**Verified?**	Need Response From CA
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	Schellman & Company, Inc.	Verified?	Verified
Auditor Location	United States	Verified?	Verified
Standard Audit	https://www.cpacanada.ca/webtrustseal?sealid=2419	Verified?	Verified
Standard Audit Type	WebTrust	Verified?	Verified
Standard Audit Statement Date	2/13/2018	Verified?	Verified
BR Audit	https://www.cpacanada.ca/webtrustseal?sealid=2420	Verified?	Verified
BR Audit Type	WebTrust	Verified?	Verified
BR Audit Statement Date	2/13/2018	Verified?	Verified
EV SSL Audit	Not requesting EV treatment	Verified?	Not Applicable
EV SSL Audit Type		Verified?	Not Applicable
EV SSL Audit Statement Date		Verified?	Not Applicable
BR Commitment to Comply	CPS section 2.1	Verified?	Verified
BR Self Assessment	https://bugzilla.mozilla.org/attachment.cgi?id=8866959	Verified?	Verified
SSL Verification Procedures	CPS section 3.2.1	Verified?	Verified
EV SSL Verification Procedures	Not requesting EV treatment	Verified?	Not Applicable
Organization Verification Procedures	CPS sections 3.2.1, 3.2.2	Verified?	Verified
Email Address Verification Procedures	CPS section 3.2.1	Verified?	Verified
Code Signing Subscriber Verification Pro	Not requesting the code signing trust bit.	Verified?	Not Applicable
Multi-Factor Authentication	CPS section 5.1.1	Verified?	Verified
Network Security	CPS section 5.4	Verified?	Verified