



OATI Application for the Mozilla Root Certificate Program

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:

Indicate whether the CA is operated by a private or public corporation, government agency, international organization, academic institution or consortium, NGO, etc. Note that in some cases the CA may be of a hybrid type, e.g., a corporation established by the government. For government CAs, the type of government should be noted, e.g., national, regional/state/provincial, or municipal.

[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:

Which types of customers does the CA serve?

[See "Impact to Mozilla Users" below.](#)

Are there particular vertical market segments in which it operates?

[See "Impact to Mozilla Users" below.](#)

Does the CA focus its activities on a particular country or other geographic region?

[See "Impact to Mozilla Users" below.](#)

Impact to Mozilla Users:

Describe the types of Mozilla users who are likely to encounter your root certificate as relying parties while web browsing (HTTPS servers doing SSL), sending/receiving email to their own MTA (SMTPS, IMAPS servers doing SSL), sending/receiving S/MIME email (S/MIME email certs), etc.

[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\) of 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 \(including some of Apple's largest customers and best known third party application providers\).](#)

Mobile Applications:

With the release of its webMobile product, OATI aims to usher in a new era of securing mobile applications with digital certificates and PIN's. OATI's patent-pending process will help mobile application developers eliminate the security risks associated with use of usernames and passwords by replacing them with digital certificates and PINs.

Wholesale Energy:

OATI primary business focus is providing secure applications for Wholesale Energy Industry participants. OATI provides online Software as a Service (SaaS) applications to more than 1,200 entities in the North American energy industry including market participants, regulators, governmental and quasi-governmental entities, transmission providers, generators, and all other entities participating in the market. OATI is an industry leader in providing large scale SaaS over SSL/TLS AND mandating two-factor authentication using SSL/TLS client certificates. The company has successfully rolled out its root, issuing and client certificates to every Wholesale Energy Industry end-user. OATI's PKI client/server certificate infrastructure is used to authenticate transactions involving critical infrastructure. As these end-users move from desktop browsers to mobile devices, the number of digital certificates required will increase exponentially.

Retail (Home & Business) Energy/Smart Grid:

OATI is leveraging its Wholesale Energy, experience to assist Wholesale Energy Industry users within Retail (Home & Business) Energy/Smart Grid Industry operations, over a multitude of emerging smart consumer products including meters, appliances, chargers, thermostats and other smart devices, each of which can be monitored through the use of a mobile field device. A range of estimates show smart grid-connected devices and the need for associated digital certificates growing from 20 to 60 million in 2013 to 200 to 600 million in 2020.

OATI is also working with Retail (Home & Business) Energy/Smart Grid groups to develop standards for server and client certificates. These standards will establish mechanisms to authenticate Smart Grid devices and secure traffic between them. In many cases, the certificates will be installed during the manufacturing process similar to what is done on a smaller scale in the cable set top box industry. OATI estimates that the need will grow exponentially in the near future.

OATI is also involved in developing 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. Now that a digital certificate requirement has been added to the standard, OATI expects that 5 to 10 million

certificates will be needed in the first year, with exponential growth in future years.

Amateur Sports:

OATI has been serving amateur sports organizations since 2006 with its HangAStar application (www.hangastar.com). Users we currently work with include USA Weightlifting, USA Taekwondo, USA Volleyball, National Senior Games Association, and the World Taekwondo Federation. The World Taekwondo Federation extends to 200 countries and 100,000 users. HangAStar users number approximately 200,000 with growth estimated at 50,000 per year. At this point in time, only administrators require certificates; however we expect to move away from username/passwords to client certificates for all users.

CA Contact Information

CA Email Alias:

CA Phone Number:

Title / Department:

1. PKIMonitor@oati.net

763.201.2000

Patrick Tronnier - Senior Director Quality Assurance, Customer Support and webCARES Principal Security Architect

2. cio@oati.net

763.201.2000

David Heim - Chief Information Officer

Technical information about each root certificate

Certificate Name:

Friendly name to be used when displaying information about the root. Usually the CN.

OATI WebCARES Root CA

Certificate Issuer Field:

The Organization Name and CN in the Issuer must have sufficient information about the CA Organization.

CN = OATI WebCARES Root CA

O = Open Access Technology International Inc

L = Minneapolis

S = MN

C = US

Certificate Summary:

A summary about this root certificate, its purpose, and the types of certificates that are issued under it.

The OATI webCARES PKI is used to secure four 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.

A high percentage of OATI certificates are issued as client-authentication certificates used in SSL/TLS to provide multi-factor authentication to secure any application implementing SSL/TLS. All OATI applications require a client-authentication certificate to properly authenticate the user.

In addition the North American Electric Standards Board (NAESB), North American Electric Reliability Corporation (NERC), Federal Energy Regulatory Commission (FERC), Department of Homeland Security (DHS), and many other regulatory agencies are adopting standards which will require the use of our SSL/TLS client certificates. Please see “Impact to Mozilla Users” (starting on page 1 of this document) for more details.

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:

YYYY-MM-DD
2008-06-03

Valid To:

YYYY-MM-DD
2038-06-03

Certificate Version:

V3

Certificate Signature Algorithm:

sha1RSA

Signing key parameters:

RSA modulus length; e.g. 2048 or 4096 bits. Or ECC named curve, e.g. NIST Curve P-256, P-384, or P-512.
RSA (4096 Bits)

Test Website URL (SSL):

<https://www.oaticerts.com/>

Example Certificate (non-SSL):

OATI does not issue non-SSL certificates.

CRL URL:

URL: <http://certs.oaticerts.com/repository/OATIIA2.crl>

NextUpdate for CRLs of end-entity certs, both actual value and what's documented in CP/CPS.

Test: Results of importing into Firefox browser

NextUpdate: Every 24 hours.

OCSP URL:

OCSP URI in the AIA of end-entity certs

Maximum expiration time of OCSP responses

Testing results

a. *Browsing to test website with OCSP enforced in Firefox browser*

b. *If requesting EV:*

https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version

[OATI does not use OCSP.](#)

Requested Trust Bits:

One or more of:

Websites (SSL/TLS) [Yes](#)

Email (S/MIME) [Yes](#)

Code Signing [No](#)

SSL Validation Type:

e.g. DV, OV, and/or EV

[Currently OATI only issues Domain Validated \(DV\) Certificates.](#)

EV Policy OID(s): [OATI does not issue extended validation certificates.](#)

CA Hierarchy information for each root certificate

CA Hierarchy:

List, description, and/or diagram of all intermediate CAs signed by this root.

Identify which subCAs are internally-operated and which are externally operated.

[Currently OATI only has one intermediate CA called "OATI webCARES Issuing CA" \(<http://www.oaticerts.com/repository/OATIIA2.crt>\) and it is operated internally.](#)

Externally Operated SubCAs:

If this root has subCAs that are operated by external third parties, then provide the information listed here:

https://wiki.mozilla.org/CA:SubordinateCA_checklist

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

[OATI does not have any externally operated SubCA's.](#)

Cross-Signing:

List all other root certificates for which this root certificate has issued cross-signing certificates.

List all other root certificates that have issued cross-signing certificates for this root certificate.

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.

[OATI's webCARES Root Certificate Authority does not cross-sign with any other root certificates.](#)

Technical Constraints:

Describe the technical constraints that are in place for all third-parties (CAs and RAs) who can directly cause the issuance of certificates. See #4 of https://wiki.mozilla.org/CA:Information_checklist#CA_Hierarchy_information_for_each_root_certificate

The subject of each certificate issued by our Registration Authorities is pre-determined by the organizational data submitted and verified during the application authorization process. Pre-filled in 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:

Language(s) that the documents are in: English

CP: None

CPS: <http://www.oaticerts.com/repository/OATI-webCARES-CPS.pdf>

Relying Party Agreement: None

Audits:

Audit Type:

- 1) AICPA/CICA Trust Services Principles and Criteria for Certification Authorities Version 2.0 (WebTrust for Certification Authorities Principles and Criteria).*
- 2) North American Energy Standards Board (NAESB) Wholesale Electric Quadrant (WEQ) Public Key Infrastructure (PKI) for Authorized Certification Authorities (ACA) standards and the NAESB Accreditation Requirements for Authorized Certification Authorities (collectively "WEQ-012 Business Practice Standards") NOTE: The NAESB WEQ-012 Standards and accompanying accreditation specification set forth the requirements a certificate authority must meet to become an Authorized Certificate Authority (ACA). Only ACAs may provide certificate authority services to certain shared applications relied upon in the operation of the North American energy industry.*

Auditor: Schellman & Company, LLC (SCLLC), an affiliate of BrightLine

Auditor Website:

WebTrust: <https://cert.webtrust.org/ViewSeal?id=1447>

WEQ-012: http://www.naesb.org/pdf4/ac_authorities_041012.pdf

SSL Verification Procedures:

If you are requesting to enable the Websites Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #3 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices

Please see our CPS at www.oaticerts.com/repository/OATI-webCARES-CPS.pdf

Organization Verification Procedures:

Please see our CPS at www.oaticerts.com/repository/OATI-webCARES-CPS.pdf

Email Address Verification Procedures:

If you are requesting to enable the Email Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #4 of

https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices

Please see our CPS at www.oaticerts.com/repository/OATI-webCARES-CPS.pdf

Code Signing Subscriber Verification Procedures:

If you are requesting to enable the Code Signing Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #5 of

https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices

OATI does not issue Code signing certificates.

Confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance. See # 6 of

https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices

Multi-factor authentication including username, password and digital client certificates are required to access OATI's CA and issue certificates.

Network Security:

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

OATI does not issue Network Security certificates.

Response to Mozilla's CA Recommended Practices

(https://wiki.mozilla.org/CA:Recommended_Practices)

Publicly Available CP and CPS:

OATI's Practice Statement (CPS) contains sufficient information to determine whether and how OATI complies with the Mozilla policy requirements. Please see our CPS at www.oaticerts.com/repository/OATI-webCARES-CPS.pdf

CA Hierarchy:

OATI's PKI of a single root with only one intermediate CA (subCA) follows the preferred hierarchical structure and our single top-level root's public certificate was supplied for Mozilla's root list.

Audit Criteria:

OATI has provided evidence of our being evaluated according to one or more of the criteria accepted as suitable per the Mozilla policy. Please refer to the "Audits" section on page 6.

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:

OATI relies on public documentation and audits of those documented processes to ascertain that the requirements of section 7 of the Mozilla CA Certificate Policy are met. Please see our CPS at www.oaticerts.com/repository/OATI-webCARES-CPS.pdf

Verifying Email Address Control:

For a certificate to be used for digitally signing and/or encrypting email messages, OATI takes detailed measures to verify that the entity submitting the request controls the email account associated with the email address referenced in the certificate. Please see our CPS at www.oaticerts.com/repository/OATI-webCARES-CPS.pdf

Verifying Identity of Code Signing Certificate Subscriber:

OATI does not issue Code Signing Certificates.

DNS names go in SAN:

OATI does not use the SAN for server certificates.

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: OATI does not use OCSP

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:

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

OATI does not issue DV certificates.

Delegation of Domain / Email validation to third parties:

OATI does not delegate Domain/Email validation to third parties.

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:

OATI does not use OCSP.

CRL with critical CIDP Extension:

OATI does not currently use partitioned CRL's and does not put critical CIDP extensions into full CRLs.

Generic names for CAs:

OATI incorporates an organizational name (OATI) and product brand name (webCARES) sufficiently unique to allow relatively straightforward identification of its CA. In addition, the issuer and subject information in the root certificate provides clear indication about who owns or operates the certificate.

CN = OATI WebCARES Root CA

O = Open Access Technology International Inc

L = Minneapolis

S = MN

C = US

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.