WEBCARES CERTIFICATION PRACTICE STATEMENT v3.3

OPEN ACCESS TECHNOLOGY INTERNATIONAL, INC.

OCTOBER 2017

PROPRIETARY AND CONFIDENTIAL

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

TRADE SECRET

This document and attachments contain confidential and proprietary information of Open Access Technology International, Inc. This information is not to be used, disseminated, distributed, or otherwise transferred without the expressed written permission of Open Access Technology International, Inc.

PROPRIETARY NOTICE

Table of Contents

1. Acronyms and Glossary

1.1 Acronyms

ACA	Authorized Certificate Authority
AICPA	American Institute of Certified Public Accountants, Inc.
AO	Audit Officer
BRAF	Business Representative Application Form
BES	Bulk Electric System
CA	Certificate Authority
CAA	Certification Authority Authorization
CA/B Forum	CA Browser Forum
CA/B Forum BRs	CA/Browser Forum's Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates
ccTLD	Country code Top-Level Domain
CICA	Canadian Institute of Chartered Accountants
CIP	Critical Infrastructure Protection
CNAME	Canonical Name
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
CST	Central Standard Time
DN	Distinguished Name
DNS	Domain Name Service
DSS	Digital Signature Standard
DUNS	Data Universal Numbering System
FQDN	Fully Qualified Domain Name
gTLD	Generic Top-Level Domain
HSM	Hardware Security Module
IA	(Certificate) Issuing Authority
ICANN	Internet Corporation for Assigned Names and Numbers
LRA	Local Registration Authority
NA	Naming Authority
NAESB	North American Energy Standards Board
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
OATI	Open Access Technology International, Inc.
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organizational Unit
PKI	Public Key Infrastructure
RA	Registration Authority
SIVP	Subscriber Identification and Verification Procedure
SO	Security Officer
SOA Record	Start of Authority Record
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator
WebTrust	Requirements found within the AICPA/CICA WebTrust Program for Certification Authorities

webCARES	OATI web-based Certificate Administration, Renewal, and Enrollment System
WEQ-012	NAESB Business Practice Standards for Public Key Infrastructure
X.509	The ITU-T standard for Certificates and corresponding authentication framework

1.2 Glossary

Agent: An entity authorized by another to act on its behalf.

Applicant: An organization, person, or entity that has applied for, but has not yet been issued a webCARES Digital Certificate.

Application Software Supplier: A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.

Audit Officer: A person designated within an organization to oversee and audit the actions of the SO as they pertain to issuing and managing webCARES Digital Certificates.

Authorization Domain Name: The Domain Name used to obtain authorization for certificate issuance for a given FQDN. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If the FQDN contains a wildcard character, then the CA must remove all wildcard labels from the left most portion of requested FQDN. The CA may prune zero or more labels from left to right until encountering a Base Domain Name and may use any one of the intermediate values for the purpose of domain validation.

Authorized Certificate Authority: A CA that meets NAESB's Business Practice Standards related to PKI (WEQ-012), meets the Accreditation Specification requirements and has been credentialed by NAESB as an ACA.

Authorized Port: One of the following ports: 80 (http), 443 (http), 115 (sftp), 25 (smtp), 22 (ssh).

Base Domain Name: The portion of an applied-for FQDN that is the first domain name node left of a registry-controlled or public suffix plus the registry-controlled for public suffix (e.g. "example.co.uk" or "example.com"). For FQDNs where the right-most domain name node is a gTLD having ICANN Specification 13 in its registry agreement the gTLD itself may be used as the Base Domain Name.

Business Representative: An Agent of an Organization who applies for access to the OATI webCARES system for the purpose of issuing and managing OATI webCARES Digital Certificates for End Users within the Organization. See also Security Officer.

Certificate Authority: The CA manages the Certificate lifecycle, which includes generation and issuance, distribution, renewal, rekey, and revocation of Certificates.

Certificate Authority Operations: Include the management of the Certificate lifecycle, which includes generation and issuance, distribution, renewal and reissuance, and revocation of Certificates.

Certificate Manufacturing Authority (Issuing Authority): An entity responsible for Signing and Issuing webCARES Digital Certificates to SOs and End Users.

Certification Practice Statement: A statement outlining the practices and procedures that a CA employs in issuing and signing Digital Certificates.

Critical Certificate Authority Operations: Includes the management of the Digital Certificate life cycle, which includes generation and issuance, distribution, renewal and reissuance, and revocation of the CA's root and subordinate Certificates.

Cross Certificate: A certificate issued by one CA to another CA that contains a CA signature key used for issuing certificates. The issuer and subject are different and show a trust relationship between the two CAs.

OATI webCARES Digital Certificate: An electronic record produced from the OATI webCARES system that lists a Public Key and confirms that the prospective signer identified in the electronic record holds the corresponding Private Key.

Digital Signatures: The transformation of a message using asymmetric cryptography such that the recipient of the message can use the sender's Public Key to accurately determine whether the message was created using the sender's corresponding Private Key. A Digital Signature allows a recipient to determine if the message has been altered or changed after the Digital Signature was created.

Distinguished Name: The set of information that identifies a person or entity in the real world. The format of an OATI webCARES DN is as follows: Country/State (or Province)/City/Organization/Organizational Unit/End Entity Name/End Entity E-Mail (or IP Address).

Domain Authorization Document: Documentation provided by, or a CA's documentation of a communication with, a Domain Name Registrar, the Domain Name Registrant, or the person or entity listed in WHOIS as the Domain Name Registrant (including any private, anonymous, or proxy registration services) attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace.

Domain Contact: The Domain Name Registrant, technical contact,or administrative contract (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA Record.

Domain Name: The label assigned to a node in the Domain Name System.

Domain Namespace: The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.

Domain Name Registrant: Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.

End Entity: The recipient of an OATI webCARES Digital Certificate. The End Entity is designated in the DN assigned to the Digital Certificate. End Entities include End Users, Relying Parties, and Subscribers.

End User: See End Entity.

Enterprise RA: An employee or agent of an organization unaffiliated with the CA who authorizes issuance of Certificates to that organization. See also LRA and SO.

Fully-Qualified Domain Name: A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.

Hash Function: An algorithm that maps or translates a set of data into another set of data in a fixed length, which is generally shorter than the original data set. A Hash Function outputs the same result every time the same data set is used as input; it is computationally unfeasible for the data set to be derived from the Hash Function output; and it is extremely improbable that two distinct data sets would produce the same Hash result.

High Impact Bulk Electric System Cyber Systems: Cyber system(s) essential to the operation of OATI Production Systems and the grouping of the BES Cyber Assets listed in the IT Device Management Component of webSupport. Please see NERC CIP-002-5.1 standard for the detailed description of High Impact BES Cyber Systems. OATI lists all of their BES Cyber Assets as High Impact.

Key Pair: A pair of mathematically derived keys made up of both a Public and Private Key.

Naming Authority: An entity responsible for assigning and managing DNs within a PKI. The NA is also responsible to ensure that all DNs assigned within the PKI are unique.

Local Registration Authority: A delegation of the RA functions by the CA to external registration authorities that may or may not be part of the same legal entity as the CA. See also Security Officer or Enterprise RA.

Private Key: A mathematical key that is kept secret and used to create Digital Signatures. A Private Key may also be used to decrypt data or communications encrypted using its corresponding Public Key.

Public Key: A mathematical key that can be made public and is used to verify Digital Signatures created with its corresponding Private Key. A Public Key may also be used to encrypt data or communications that can then be decrypted only using the corresponding Private Key. The Public Key of a key pair is typically made public by including the Public Key on the holder's Digital Certificate.

Public Key Infrastructure: The term describing a managed infrastructure for the distribution and management of Public Keys and Digital Certificates. This includes the architecture, organization, techniques, practices, and procedures that are integrated to support the operation of a PKI.

Qualifying Relying Party: A server or application that requires valid Digital Certificates from those entities or persons requesting access to the server or application. A Qualifying Relying Party will utilize an OATI webCARES Digital Certificate to establish the necessary SSL or TLS session with the entity or person requesting access.

Random Value: A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.

Registration Authority: The RA assumes delegated responsibilities from the CA to verify the identity of Subscribers to Digital Certificates.

Registration Authority Operations: RA operations include the identification and authentication of Subscribers.

Relying Parties: An organization, person, or entity that relies on or uses a webCARES Digital Certificate and/or any other information in the webCARES repository to verify the webCARES CA Public Keys when verifying the identity of a Subscriber.

Repository: A publically available read-only website containing documentation and information relevant to the operation of a PKI. This includes all copies of the relevant Policy Statement, CPS, CRLs, Certification Authority Certificates, and other appropriate information. OATI's repository is located at www.oaticerts.com/repository.

Request Token: A value derived in a method specified by the CA which binds this demonstration of control to the certificate request. The Request Token shall incorporate the key used in the certificate request. A Request Token may include a timestamp to indicate when it was create. A Request Token may include other information to ensure its uniqueness. A Request Token that includes a timestamp shall remain valid for no more than 30 days from the time of creation. A Request Token that includes a timestamp shall be treated as invalid if its timestamp is in the future. A Request Token that does not include a timestamp is valid for a single use and the OATI will NOT re-use it for a subsequent validation. The binding shall use a digital signature algorithm or cryptographic hash algorithm at least as strong as that to be used in signing the certificate request.

Required Website Content: Either a Random Value or a Request Token, together with additional information that uniquely identifies the Subscriber, as specified by the CA.

Security Officer: A person contractually responsible for issuing and managing OATI webCARES Digital Certificates within an Organizational Unit or an Unaffiliated Individual with access to the OATI webCARES solution. Each individual designated as a SO must have his/her identity verified using the OATI SIVP before he/she will be granted access the OATI webCARES system or receive an OATI webCARES Digital Certificate. See also Local Registration Authority and Enterprise RA.

Shared Network: A local network over which information and/or devices can be remotely accessed.

Subscribers: An organization, person, or device that has been issued a webCARES Digital Certificate.

Subscriber Identification and Verification Procedure: The complete verification process OATI webCARES personnel follow before an Applicant is granted access to the OATI webCARES system.

Test Certificate: A Certificate with a maximum validity period of 30 days and which: (i) includes a critical extension with the specified Test Certificate CABF OID, or (ii) is issued under a CA where there are no certificate paths/changes to a root certificate subject to these Requirements.

Trusted Employee (Trusted Role): A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously.

Unaffiliated Individual: A person applying for access to the OATI webCARES system for the purpose of issuing and managing OATI webCARES Digital Certificates for his or her personal use. An Unaffiliated Individual who is approved through the OATI SIVP and is given access to the OATI webCARES system will be termed an SO, and will assume all duties and obligations of a LRA.

OATI webCARES system: The OATI web-based Certificate Management System that allows an SO to issue, revoke and renew webCARES Digital Certificates for an Organization, and an AO to audit webCARES Digital Certificates for an Organization.

WHOIS: a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system, but is also used for a wider range of other information.

2. OATI webCARES

2.1 OATI webCARES Overview

This document is the OATI webCARES (Certificate Administration, Renewal, and Enrollment System) CPS. This CPS outlines the legal, commercial, and technical principles and practices related to OATI webCARES Certificate services. This CPS applies to all persons, entities, and organizations participating in or using OATI webCARES services.

This CPS describes the practices that webCARES follows in issuing Digital Certificates in accordance with requirements found within the AICPA, CICA, WebTrust Program for Certification Authorities (WebTrust Principles & Criteria for Certification Authorities – SSL Baseline with Network Security), and in accordance with other applicable industry standards.

2.2 Certification Practice Statement

This document was approved for publication following OATI standard processes.

The purpose of this CPS is to: 1) document procedures and practices that the OATI CA and, to the extent delegated to, a RA or LRA, will follow to create, sign, issue, validate, revoke, renew, and generally manage OATI webCARES Digital Certificates; 2) inform Subscribers about the OATI webCARES service of their rights and responsibilities; 3) outline the rights and responsibilities of the OATI CA, RA, and LRA; and 4) instill public confidence in the OATI CA through the disclosure of industry accepted policies, practices, and procedures that ensure the creation of a secure and trusted PKI.

2.3 Certification Practice Statement Management

The maintenance of the OATI Certification Practice Statement will be managed by the OATI Compliance Department and designees. The CPS is always publically available on the OATI webCARES Repository and will be reviewed at least annually and updated as necessary to reflect changes to applicable industry standards including, but not limited to, NAESB WEQ-012, WebTrust for CA's, and CA/B Forum BRs .

2.4 Certification Authorities

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.
- Revoke OATI webCARES Digital Certificates issued for use upon receipt of a valid request or reason to revoke.
- Issue and publish CRLs in a timely manner.
- Conform with other applicable industry standards.

2.5 Registration Authorities

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.

2.6 CPS Amendments and Publication

Amendments to this CPS may be published from time to time. Continued use of OATI webCARES Digital Certificates presumes knowledge and acceptance of changes contained in CPS amendments. All changes to this CPS will be published appropriately in the webCARES Repository.

2.7 Other Practice Statements and Agreements

OATI may issue from time to time other practice statements and agreements affecting use of OATI webCARES Digital Certificates.

2.8 Compliance with Applicable Standards and Laws

This CPS and the practices described within it meet or exceed the generally accepted industry standards for CA found in the AICPA/CICA WebTrust Program for CAs along with other industry related standards. The OATI webCARES CA complies with applicable laws and licensing requirements in each jurisdiction where OATI issues OATI webCARES Digital Certificates.

2.9 Certificate Authority Assets

OATI categorizes CA assets as High Impact BES Cyber Systems pursuant to NERC CIP requirements.

2.10 OATI webCARES PKI Hierarchy

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.

2.11 OATI Naming Authority

The OATI NA coordinates the creation and issuance of DN for all certificates issued to SOs and End Users. OATI webCARES Digital Certificates issued within the OATI PKI will contain a unique X.500 DN. The DN assigned by the OATI NA will clearly identify the official Company Name, the Company's Entity code, the name of the End Entity or machine ID, and the e-mail address of the person responsible for the Digital Certificate, as applicable. By combining all of these elements into the DN, OATI assures that every DN assigned will be unique and will clearly identify the party using the Certificate.

2.11.1 Enhanced Naming and Extensions

OATI webCARES Certificates are based upon the X.509 v3 structure and extensions. The X.509, Amendment 1 to ISO/IEC 9594-8:1995 provides for a number of extensions. These extensions allow various management and administrative controls that are useful for OATI webCARES purposes.

2.11.2 Anonymous Digital Certificates

OATI webCARES will not issue anonymous Digital Certificates.

2.11.3 Pseudonymous and Role OATI webCARES Digital Certificates

OATI webCARES may issue pseudonymous or role based OATI webCARES Digital Certificates provided that such certificates are not prohibited by applicable policy and name uniqueness is preserved.

2.11.4 Cross Certificates

OATI webCARES currently does not cross certify any other CA and has not issued any cross certificates.

2.12 Contact Details

The webCARES CPS is administered by the OATI Compliance Department. The contact information for questions about OATI webCARES Digital Certificates is:

Open Access Technology International, Inc.
ATTN: OATI Compliance Department
3660 Technology Drive NE
Minneapolis, MN 55418
Telephone: 763.201.2000
Email: Compliance@oati.net

3. OATI webCARES Digital Certificates Practice and Procedures

3.1 Types of webCARES Non-CA Certificates

- OATI webCARES Server Certificates – Any certificate where EKU = Server Authentication
- OATI webCARES Client Certificates – Any certificate where EKU = Client Authentication

3.2 Certificate Application

3.2.1 webCARES Application Process

OATI customers will designate employees to perform the roles of SO and AO. The applicant shall complete and return a notarized BRAF to OATI as part of OATI's SIVP.

OATI webCARES personnel follow an extensive SIVP prior to issuing Digital Certificates. The SIVP begins with an applicant completing the BRAF. The BRAF requires an applicant to provide detailed information about themselves, their company, domain names owned by the applicant, and the purpose for which the Digital Certificate will be used.

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 for any applicable use including: Server and Client Authentication. The SIVP includes, but is not limited to:

- Calling the applicant's contacts provided on the BRAF.
- Verifying the 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 making sure registration information returned from third party databases exactly match contract information OATI has for existing customers. If

there is not an exact match, domain ownership is done by making an agreed-upon change to the applicant's website.

3.2.1.1 Identity Proofing Requirements

To conform to SIVP, identity verification shall be performed prior to the issuance of all OATI webCARES Digital Certificates.

To meet the requirements SOs can verify the identity of Subscribers in one of three ways.

1. The SO can validate a Subscriber's identity in person by having the Subscriber present a valid and current government issued picture ID.
2. The SO can validate a Subscriber's identity remotely through the Subscriber presenting a valid and current government issued picture ID and a financial account number that can be confirmed.
3. SO's issuing OATI webCARES 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 process where notification is sent via the distribution channels normally used for sensitive, personal communications.

All Server Certificate requests are verified against Google's Safe Browsing Lookup API to screen for High Risk Requests including subsequent suspicious requests. Any requests identified by Google's Safe Browsing Lookup API as potentially containing malicious code or phishing attempts will be considered by OATI to be a High Risk Request, and as such, will be rejected and logged in the database.

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 for a specific organization, the identity of both the organization for which the Subscriber claims to work and the SO 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 individual, non-organizational information.

3.2.2.3 Machine/Server/Role/Applications

In the case of a machine, server, role, 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, role, or application must submit both the organization and Subscriber information to be identified and verified.

3.3 User Roles

3.3.1 Security Officer/Local Registration Authority

The role of SO, otherwise known as a LRA, is mandatory for every organization or entity subscribing to the OATI webCARES system. A SO will be responsible for managing the Digital Certificates within his or her Organizational Unit. A SO will be responsible for using 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 contractual obligations include issuing, revoking, renewing, tracking OATI webCARES Digital Certificates for his or her End Users, and revoking OATI webCARES Digital Certificates. A SO will be provided personal access to the OATI webCARES system to perform his or her role. All SOs must follow CA/B Forum BRs or risk revocation of their Digital Certificate.

3.3.2 Audit Officer

Designation of an organization AO is strongly recommended by OATI. An AO will have Read Only access to the OATI webCARES system for the purposes of monitoring audit logs and oversight of the SO.

3.3.3 End User

An End User uses Digital Certificates for identity authentication purposes.

3.3.4 Non-Enterprise RA

OATI does not use Non-Enterprise RAs.

3.4 Non-CA Digital Certificate Life Cycle Management

Digital Certificate Life Cycle Management refers to functions that include:

- Verification of the identity of an Applicant
- Issuing Digital Certificates
- Revoking Digital Certificates
- Listing Digital Certificates
- Distributing Digital Certificates
- Storing Digital Certificates
- Testing Digital Certificates

3.4.1 OATI webCARES Digital Certificate Issuance

OATI webCARES issues OATI webCARES Digital Certificates after the SIVP has been completed. The OATI webCARES Digital Certificates are generated and issued in a manner that protects the OATI webCARES Digital Certificate and CA from unauthorized access.

3.4.2 OATI webCARES Digital Certificate Distribution

Once issued, OATI webCARES Digital Certificates are distributed to Subscribers and Relying Parties via TLS or similar secure transfer mechanisms.

3.4.3 OATI webCARES Digital Certificate Use

OATI webCARES Digital Certificates can be used for secure website access, in-house applications, internal client/device (mobile, Smart Grid, etc.) authentication, and encrypting and digitally signing documents.

OATI webCARES Digital Certificates are not intended, and shall not be used for any transaction or data transfer that violates any applicable law or regulation. Any compromise or falsification

of data or information provided to or in webCARES may result in prosecution, fines, or imprisonment.

3.4.4 OATI webCARES Digital Certificate Suspension

OATI webCARES Digital Certificates may be suspended for reasons including, but not limited to, non-payment, activities in violation with this CPS, activities in violation of the law, and/or activities in violation of standard industry practices.

3.4.5 OATI webCARES Digital Certificate Revocation

Revocation of an OATI webCARES Digital Certificate permanently ends the operational period of the OATI webCARES Digital Certificate prior to the end of the OATI webCARES Digital Certificate's stated validity period. OATI webCARES can revoke an OATI webCARES Digital Certificate at any time. An SO can also revoke any OATI webCARES Digital Certificates they have issued to End Entities.

3.4.6 Conditions Requiring OATI webCARES Digital Certificate Revocation

Where the following conditions or circumstances occur, an OATI webCARES Digital Certificate issued by the OATI webCARES system must be immediately revoked within twenty four hours for Subscriber certificates and seven days for Subscriber CA certifcates . An SO is primarily responsible to revoke the Subscriber's Digital Certificates with respect to any of the SO's users. Alternatively the OATI webCARES Administrator may also revoke the OATI webCARES Digital Certificate of an End Entity or SO:

- When NAESB recommends that an ACA issued OATI webCARES Digital Certificate be revoked.
- When the ACA reasonably suspects or becomes aware that the Private Key, or the media holding the Private Key, is suspected to be compromised or actually is compromised.
- When the ACA becomes aware of an emergency which, if the OATI webCARES Digital Certificate is not revoked, may have material commercial impact to parties operation in accordance with the NAESB WEQ-012 Standards.
- When the SO or Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization.
- When a party listed as the SO no longer represents a Business Organization.

- When a device, server, or application is no longer active or no longer affiliated with the Subscriber's organization.
- When a contract is terminated with OATI webCARES.
- When requested, in writing, by an SO.
- The CA obtains evidence that the Certificate was misused.
- The CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name).
- The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name.
- The CA is made aware of a material change in the information contained in the Certificate.
- The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement.
- The CA determines that any of the information appearing in the Certificate is inaccurate or misleading.
- The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate.
- The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository.
- The CA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate.
- Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement.
- If a certificate is being used to promote malware or unwanted software OATI will revoke the certificate within a commercially-reasonable timeframe not to exceed two (2) business days from the date the request was received.
- The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use.
- The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g., a deprecated

cryptographic/signature algorithm or key size might present an unacceptable risk and need to be revoked and replaced by CAs within a given period of time).

OATI specifically reserves the right to revoke any OATI webCARES Digital Certificate issued by the OATI webCARES system for any issue relating to security or other national interest. Additionally, OATI reserves the right to provide federal, state and local agencies information relating to the application for, use of, and misconduct associated with any OATI webCARES Digital Certificate issued through the OATI webCARES system.

3.4.7 Request for Revocation

An End Entity may request revocation of his/her/its OATI webCARES Digital Certificate at any time for any reason. The request must be written (i.e., email, fax, postal mail, etc.) and presented to the End Entity's SO, or OATI's Help Desk, who approves the request and revokes the certificate via the webCARES User Interface. The End Entity's SO, or OATI's Help Desk, will begin an investigation request for revocation within 24 hours of receipt, and decide whether revocation or other appropriate action is warranted based on at least the following criteria:

1. The nature of the reported problem.
2. The number of Certificate Problem Reports received about a particular Certificate or Subscriber.
3. The entity making the complaint (for example, a complaint from a law enforcement official shall carry more weight than a complaint from an End Entity alleging the information in their certificates is wrong).
4. Relevant legislation.

3.4.8 Effect of Revocation

Revocation of an OATI webCARES Digital Certificate immediately terminates the operation period of that OATI webCARES Digital Certificate. The serial number of the revoked OATI webCARES Digital Certificate will be placed within the CRL within ten minutes of revocation and the serial number will remain on the CRL until after the end of the OATI webCARES Digital Certificate's validity period.

3.4.9 CRL and OCSP Revocation Data

The serial numbers of revoked OATI webCARES Digital Certificates are published to the CRL. The CRL is published in the 24x7 OATI repository: http://www.oaticerts.com/repository/.

OATI maintains webCARES CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

3.4.10 OCSP Responses

OATI webCARES OCSP responses conform to RFC6960 and/or RFC5019, are signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked. The OCSP signing Certificate contains an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960. OATI does not rely on Stapling to distribute OCSP responses. OATI webCARES OCSP responses do not respond with a "good" status for Certificates that have not been issued.

3.5 Renewal

Renewal application requirements and procedures rely on the verification of the data provided for the previously issued Certificate. The BRAF-verified SO must confirm by clicking the designated checkbox that the information in the Certificate issued 825 days or less prior to the Certificate renewal is still current and valid for new OATI webCARES Digital Certificates. By checking this checkbox, the SO confirms that they have verified the identity and legitimacy of the person, machine, or device being granted the Digital Certificate in accordance with the OATI CPS and CA/B Forum BRs. No data or documentation older than 39 months will be accepted for verification purposes. Renewed OATI webCARES Digital Certificates have a new validity period but the exact same information in the subject field as the original OATI webCARES Digital Certificate.

A new Certificate must be created for any incongruent or outdated information and a new BRAF must be verified by OATI.

3.5.1 Identification for Renewal

When a Subscriber seeks renewal for an OATI webCARES Digital Certificate, the RA/LRA will authenticate the identity of the Subscriber prior to renewing his or her OATI webCARES Digital Certificate. Once renewed, the previous OATI webCARES Digital Certificate is allowed to expire.

3.5.2 Renewal After Revocation

In the event an OATI webCARES Digital Certificate has been revoked, the Subscriber's identity shall be re-authenticated by the RA/LRA as a new Subscriber.

3.6 Notice Prior to Expiration

OATI webCARES RAs shall make reasonable efforts to notify Subscribers via e-mail of an upcoming expiration of an OATI webCARES Digital Certificate. Notice will ordinarily be provided within a 30-day period prior to the expiration date of the respective OATI webCARES Digital Certificate.

3.7 Retiring Key Pairs

OATI will not issue any OATI webCARES Digital Certificates that exceed beyond the end validity date of the subordinate Root Certificate.

3.8 Notifications

OATI will notify Subscribers in the event any of the following incidents occur

- Reasonably suspected or detected compromise of the ACA private key(s).
- Successful physical or electronic penetration of the ACA system(s).
- Successful denial of service attack on ACA components.
- An incident prevents the ACA from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL.

3.8.1 Business Continuity following a Disaster

As part of OATI's Business Continuity Plan, OATI webCARES will notify Subscribers in the event of a disaster that damages the ACA and destroys all copies of the ACA signature keys.

3.8.2 Certificate Authority Termination

In the event OATI webCARES ceases operation Subscribers will be given as much advance notice as circumstances permit prior to the ACA revoking all OATI webCARES Digital Certificates.

OATI webCARES will provide 90 days advice notice prior to voluntary withdrawal from any official certification program.

3.8.3 Incident Review and Notification

OATI maintains a process to identify and remediate possible security risks. In the event of a security incident, OATI will notify Subscribers. OATI will notify law enforcement agencies as applicable based on the OATI Cyber Security Incident Response Plan.

3.9 Refusal to Issue a Certificate

OATI reserves the right to refuse to issue an OATI webCARES Digital Certificate.

4. Facility, Management, and Operational Controls

4.1 Physical Access

The OATI webCARES infrastructure is located within OATI Data Centers. Physical access to the Data Centers is secured by multi-layered security. Access to the Data Centers is secured with biometrics, in addition to proximity card access controls.

Access authority is granted to OATI employees on a need basis only in accordance with OATI written processes and procedures. All access points are integrated into the OATI Data Center monitoring and alarm systems, which provide alarming notification both to OATI employees and a third party monitoring company in the event of unauthorized access. All OATI employees must display official OATI pictured security badges and use these badges to gain entrance beyond designated visitor areas of the OATI facilities.

The physical location of the webCARES infrastructure is within a production level Data Center environment, additionally secured within a six walled locked environment. An access log to the webCARES CA is maintained and periodically inspected. The webCARES CA is supported by redundant power and cooling. In the event commercial power was interrupted, on site generation will provide sufficient uninterrupted power.

Gaining physical access to the cryptographic module requires a minimum of two OATI trusted employees.

4.2 Personnel Controls

OATI screens all employees working with or having access to the webCARES infrastructure. The personnel background investigation includes a criminal background check, employment and reference verification, and social security verification. In addition, OATI employs a system of "separation of powers" by assigning webCARES personnel to no more than one critical position each, thus, ensuring that no single employee has the opportunity to compromise the system.

OATI provides all personnel performing information verification duties with skills-training and certification that covers basic Public Key Infrastructure knowledge, authentication, and vetting policies and procedures (including this Certification Practice Statement), common threats to the information verification process (including phishing and other social engineering tactics), and these Requirements. In addition, those in the Administrator role receive training and

certification on CA key lifecycle management including secure HSM operations. Each employee assigned to a critical position will have appropriate personnel assigned and trained for backup purposes. Trusted roles are established to guarantee role separation.

4.2.1 Trusted Roles

OATI webCARES operations are handled by multiple PKI personnel in trusted roles.

4.3 Audit Logging Procedures

OATI webCARES audit logs are compiled and archived in a confidential manner. The audit logs are automatically compiled daily for predefined events relating to the security of the webCARES CA. OATI will review the audit logs monthly and as required for cause.

OATI webCARES audit logs detail the actions taken to process a certificate request and to issue a certificate, including all information generated and documentation received in connection with the certificate request; the time and date; and the personnel involved. OATI makes these records available to its Qualified Auditor as proof of their compliance with these Requirements.

OATI records at least the following events and entries include the following elements: Date and time of event, identity of the person or process performing the event, and a description of the event.

1. CA key lifecycle management events, including:
   A. Key generation, backup, storage, recovery, archival, and destruction; and
   B. Cryptographic device lifecycle management events.
2. CA and Subscriber Certificate lifecycle management events, including:
   A. Certificate requests, renewal and re-key requests, and revocation;
   B. All verification activities stipulated in these Requirements and the CA's Certification Practice Statement;
   C. Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
   D. Acceptance and rejection of certificate requests;
   E. Issuance of Certificates; and
   F. Generation of Certificate Revocation Lists and OCSP entries.

3. Security events, including:
   A. Successful and unsuccessful PKI system access attempts;
   B. PKI and security system actions performed;
   C. Security profile changes;
   D. System crashes, hardware failures, and other anomalies;
   E. Firewall and router activities; and
   F. Entries to and exits from the CA facility.

4.3.1 Physical Access Logs

OATI webCARES physical access logs (paper and electronic) shall be reviewed quarterly.

4.3.2 Backup Procedure

OATI webCARES audit logs shall be backed up at a minimum once per month to an off-site location.

4.4 Records Retention Policy

OATI retains, according to generally accepted industry practices, all records associated with OATI webCARES Digital Certificates after an OATI webCARES Digital Certificate is revoked or expires. Records will be retained in electronic format where applicable, all other retained records will be in a physical medium. Physical records will be retained in a secure fashion, for time periods required by applicable standards including, but not limited to, WebTrust, CA/B Forum BRs and NAESB WEQ-012.

4.4.1 Records Archive

OATI webCARES Auditor(s) will verify, package, transmit, and store physical archive information in accordance with the applicable industry standards for each assurance level. The contents of the OATI webCARES archive shall not be released except as required by law or applicable regulations and standards.

Data to be archived include:

- Record of CA Renewal and Reissuance
- Other data or applications to verify archive contents

- Compliance Auditor Reports
- Any changes to audit parameters
- Any attempt to delete or modify the log
- Destruction of cryptographic modules
- All Digital Certificate compromise notifications
- Remedial action taken as a result of violations of physical security
- Violations of the OATI CPS
- Shipment receipt of cryptographic hardware (i.e., HSM modules, tokens, etc.)
- All changes to trusted public keys
- All Private Key relevant messages that are received by the system

4.5 Business Continuity Plan

OATI has developed and documented a Business Continuity Plan that exists to minimize the risk, cost, and duration of a catastrophic disruption to business processes in the event of damage to, failure of, loss of, corruption of, or discontinuance of a strategic component of the critical infrastructure that supports OATI services to customers. OATI maintains multiple geographically diverse locations; in the event of a disastrous disruption to one site, webCARES operations would continue at another other site with minimal disruption.

4.5.1 Computing Resources

When computing resources, software, and/or data are corrupted, the ACA shall respond as follow

- Before returning to operation OATI will ensure the webCARES system integrity has been restored.
- If the CA signature keys are not destroyed, CA operations shall be reestablished, giving priority to the ability to generate OATI webCARES Digital Certificate status information within the CRL issuance schedule.
- If the CA signature keys are destroyed, CA operations shall be reestablished as quickly as possible, giving priority to the generation of a new CA key pair.

4.6 CAA Records

As part of the issuance process, WebCares checks for a CAA record for the URL specified in the Common Name field (which is also used in the subjectAltName extension of the certificate to be issued) according to the procedure in RFC 6844, following the processing instructions set down in RFC 6844 for any records found. If this check (and all others) pass, WebCares will issue a certificate for this URL within the next 5 minutes.

OATI validates this FQDN against the domain's CAA records. If a CAA record exists that does not list oaticerts.com as an authorized CA, OATI will not issue the certificate. Additional CAA record processing rules include:

- Only the issue CAA tag is supported.
- The “iodef” and “issuewild” properties are not acted upon (i.e., OATI does not issue wildcard certificates, nor does it dispatch reports of such issuance requests to the contact(s) stipulated in the CAA iodef record(s)).
- No additional property tags are supported.
- All relevant CAA record processing actions taken, if any, are audited.

5. Technical Controls

5.1 Key Pair Generation and Installation

5.1.1 Key Pair Generation

OATI enforces multi-factor authentication for all accounts capable of directly causing certificate issuance. OATI webCARES CA key(s) are securely generated using Federal Information Processing Standards (FIPS) 140-2 Level 3 standards and take the applicable standard industry precautions to prevent the compromise or unauthorized use of the system. OATI Subscriber keys are securely generated after a multi-factor login to the webCARES system which includes a unique username, strong password, and client authentication certificate.

5.1.1.1 Logging

OATI webCARES key generation activities will be logged in accordance with the applicable industry standards.

5.1.1.2 Security

OATI webCARES key generation activities will take place in a physically secure environment.

5.1.1.3 Witnesses

OATI will engage an independent third party to witness and validate the key generation ceremony and/or OATI will video tape the ceremony.

5.1.2 CA Public Key Delivery to Users

CA Certificates, including public keys, are available for download from the Repository.

5.1.3 Key Sizes

OATI webCARES issues OATI webCARES Digital Certificates using a 2048 bit RSA key with Secure Hash Algorithm 2 (SHA-256) or greater.

5.1.4 Key Usage Purposes

An OATI webCARES Digital Certificate shall only be used in accordance with the terms, conditions and restrictions found in this CPS and applicable laws.

5.2 Private Key Protection

Subscribers are responsible for protecting the Private Key associated with the Public Key in the Subscriber's OATI webCARES Digital Certificate at all times. Subscribers must promptly notify their OATI webCARES SO, or OATI Help Desk, upon suspicion of loss or compromise of their private keys.

Parties other than the Subscriber or the Subscriber's SO SHALL NOT archive the Subscriber Private Key without written authorization by the Subscriber sent to the Subscriber's SO or the OATI Help Desk. If a Private Key is generated on behalf of the Subscriber it is encrypted during transport to the Subscriber.

If the CA or any of its designated RAs become aware that a Subscriber's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subscriber, then OATI will revoke all certificates that include the Public Key corresponding to the communicated Private Key.

5.2.1 Activation Data Protection

Data used to unlock Private Keys is protected from disclosure by a combination of cryptographic and physical access control mechanisms at each level of assurance associated with the activation of the cryptographic module. Mechanisms include, but are not limited to requiring password memorization and the temporary lock out and/or termination of the application after 10 failed login attempts.

5.3 Certificate Authority Key Usage

OATI Root CA key pairs are used for self-signed certificates to represent the Root CA itself and signing certificates for Subordinate CAs.

OATI non-root CA key pairs are issued for the purposes of issuing of Digital Certificates and CRLs. A periodic review of CA key pairs can confirm that each CA key pair has only been used for its intended purpose(s).

5.4 Network Security Controls

The OATI webCARES CA operates on a network of systems secured by multiple firewalls, virus and malware protection, and an intrusion detection system. Actions taken by OATI in response to attempted network attacks are recorded.

5.5 Cryptographic Module Engineering Controls

OATI webCARES cryptographic modules for its CA private keys are validated to FIPS 140-2 Level 3 standards. Subscribers must protect their Private Keys in accordance with the applicable guidelines on Private Key protection.

5.6 Time Stamping

The OATI webCARES system will time stamp and record all actions taken on an OATI webCARES Digital Certificate. OATI will time stamp OATI webCARES Digital Certificate issuance, renewal, revocation, and expiration. In addition to time stamping all actions taken on OATI webCARES Digital Certificates, the webCARES system will time stamp CRLs. The OATI webCARES system will operate on CST.

5.7 webCARES CA Infrastructure

OATI webCARES Digital Certificate services provided by webCARES CA are delivered on trustworthy infrastructure systems. The computer hardware, software, servers, and procedures used by webCARES CA provide a reasonable level of availability and reliability while maintaining a secure environment in enforcement of the OATI security policies and procedures.

5.7.1 Anti-Virus

An anti-virus scan will be run on the webCARES server infrastructure automatically at least once every week.

5.7.2 webCARES CA Key Archival

Retired, revoked, and expired Key Pairs are stored indefinitely.

5.7.3 Procedures Employed for webCARES CA Key Changeover

OATI CA Key Pairs have a lifetime of up to 20 years and are retired from service thereafter. OATI will retire the Root Certificate in a manner that renders the Root Certificate, and all OATI webCARES Digital Certificates issued under it, useless. OATI has the ability to stop issuing OATI webCARES Digital Certificates at any time, thereby rendering the CA retired before the Key Pair lifetime.

5.8 Key Archival and Destruction

OATI webCARES CA Private Keys are securely and confidentially stored. Once a Key Pair is retired it will never be put back into Production. If OATI were to decide to destroy a Key Pair at the end of its lifecycle, the Key Pair would be completely and confidentially destroyed in accordance with industry standards.

6. External Party Obligations

6.1 Reliance on Unverified Digital Signatures

Parties relying on Digital Signatures are responsible for verifying the validity of the OATI webCARES Digital Certificate against the relevant CRL published by OATI webCARES. An unverified Digital Signature cannot be assigned as a valid signature of the Subscriber and is used at the risk of the Relying Party.

6.2 Subscriber Obligations

OATI webCARES Subscribers shall be responsible for obligations as required by the CA/Browser Forum BRs which include, but are not limited to, the following:

- To minimize internal risk of private key compromise.
- To ensure the Public Key corresponds to the Private Key used.
- To provide accurate and up to date information in its communications with webCARES.
- To refrain from tampering with an OATI webCARES Digital Certificate.
- To make reasonable efforts to prevent the modification, disclosure, compromise, loss, or unauthorized use of the Private Key.
- To cease using an OATI webCARES Digital Certificate if any information is invalid, obsolete, or misleading.
- To cease using an OATI webCARES Digital Certificate if the OATI webCARES Digital Certificate is expired or revoked.
- To request a revocation for an OATI webCARES Digital Certificate in the occurrence the integrity of the OATI webCARES Digital Certificate is materially affected.
- To cease using the OATI webCARES Digital Certificate if the Subscriber has no legitimate business purpose to use it.
- To not share their personal OATI webCARES Digital Certificates.
- To respond to OATI instructions regarding a compromise to the Private Key or misuse of the OATI webCARES Digital Certificate.

6.3 Representations by Subscriber upon Acceptance

By accepting an OATI webCARES Digital Certificate, a Subscriber represents to OATI webCARES and other Relying Parties that at the time of acceptance and until further notice:

- Subscriber has reviewed and verified the contents of the OATI webCARES Digital Certificate for accuracy.
- Subscriber has installed the OATI webCARES Digital Certificate only on servers that are accessible at the subjectAltName(s) listed in the OATI webCARES Digital Certificate.
- OATI webCARES Digital signatures created using the Private Key corresponding to the Public Key included in the OATI webCARES Digital Certificate is the Digital Signature of the Subscriber and the OATI webCARES Digital Certificate has been accepted and is properly operational at the time the Digital Signature is created.
- No unauthorized person has ever had access to the Subscriber's Private Key.
- All representations made by the Subscriber to webCARES regarding the information contained in the OATI webCARES Digital Certificate are accurate and true.
- The OATI webCARES Digital Certificate is used consistent with this CPS and exclusively for authorized and legal purposes.

6.4 Obligations of a Relying Party

To reasonably rely on the OATI webCARES Digital Certificate, a Relying Party must:

- Trust an OATI webCARES Digital Certificate only if it is valid and has not been revoked or expired.
- Verify the entire OATI webCARES Digital Certificate validation/trust chain to the issuing webCARES Root Certificate is intact and valid.
- Minimize the risk of relying on an invalid, revoked, or expired OATI webCARES Digital Certificate by acquiring sufficient knowledge about using OATI webCARES Digital Certificates and signatures.
- Read and agree with the terms of this CPS.
- Verify the validity of the OATI webCARES Digital Certificate by referring to the relevant CRL.

6.5 Legality of Information

Subscribers are solely responsible, in any jurisdiction where such content may be used or viewed, for the legality of the information they provide for use in OATI webCARES Digital Certificate issuance under this CPS.

6.6 Subscriber Liability to Relying Parties

Subscribers are liable for any misrepresentations that they make in OATI webCARES Digital Certificates to third parties that reasonably rely on the representations contained therein. This does not limit other Subscriber obligations stated in this CPS.

6.7 Use of Agents

With regard to OATI webCARES Digital Certificates issued at the request of a Subscriber's Agent, both the Agent and the Subscriber shall jointly and severally indemnify OATI, its officers, employees, agents, customers, and contractors for damage related to the issued OATI webCARES Digital Certificates.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

OATI Certificates conform to RFC 5280, Internet X.509 PKI Certificate and CRL Profile. Certificate extensions and their criticality, as well as cryptographic algorithm object identifiers, are populated according to RFC 5280 and in cases where stipulations of RFC 5280 and the applicable CA/Browser Forum BRs differ, the BRs notion will be adhered to. Only field's mentioned in this CPS are allowed in OATI Certificates.

7.1.1 Version Number(s)

Subscriber certificates issued by OATI will be X.509 Version 3.

7.1.2 Validity Period(s)

Subscriber certificates issued by OATI have a Validity Period of two years.

7.1.3 Certificate Extensions

7.1.3.1 Root CA Certificate

- certificatePolicies: Present and NOT marked critical.
- basicConstraints: Present and marked as critical with the cA field set to True.
- keyUsage: Present and marked critical with bit positions for keyCertSign and cRLSign set.
- extendedKeyUsage: Present and NOT marked critical.
- subject Information: Present, NOT marked as critical, and contains at minimum the following:
  - countryName (OID 2.5.4.6).
  - organizationName (OID 2.5.4.10).

7.1.3.2 Issuing CA Certificate

- certificatePolicies: Present and NOT marked critical.
- basicConstraints: Present and marked as critical with the cA field set to True.

- cRLDistributionPoints: Present, NOT marked as critical, and at minimum contains the HTTP URL of OATI webCARES's CRL service.
- authorityInformationAccess: Present, NOT marked as critical, and contains at minimum the HTTP URL of OATI's Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1) and the HTTP URL of OATI's Issuing CA certificate (accessMethod = 1.3.6.1.5.5.7.48.2).
- basicConstraints: Present and marked as critical with the cA field set to True.
- keyUsage: Present and marked critical with bit positions for keyCertSign and cRLSign set.
- subject Information: Present, NOT marked as critical, and contains at minimum the following:
  - countryName (OID 2.5.4.6).
  - organizationName (OID 2.5.4.10).

7.1.3.3 Subscriber Certificate

- certificatePolicies: Present and NOT marked critical.
- basicConstraints: Must NOT be present.
- cRLDistributionPoints: Present, NOT marked as critical, and contains at minimum the HTTP URL of OATI's CRL service.
- authorityInformationAccess: Present, NOT marked as critical, and contains at minimum the HTTP URL of OATI's Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1) and the HTTP URL of OATI's Issuing CA certificate (accessMethod = 1.3.6.1.5.5.7.48.2).
- keyUsage: Not present.
- Subject Information: Present, NOT marked as critical, and contains at minimum the following:
  - countryName (OID 2.5.4.6).
  - organizationName (OID 2.5.4.10).

7.1.3.4 All Certificates

All other fields and extensions are set in accordance with RFC 5280.

OATI will not issue a Certificate with extensions that do not apply in the context of the public Internet (such as an extendedKeyUsage value for a service that is only valid in the context of a privately managed network), unless:

- Such value falls within an OID arc for which the Applicant demonstrates ownership, or

- The Applicant can otherwise demonstrate the right to assert the data in a public context, or
- Semantics that, if included, will not mislead a Relying Party about the certificate information verified by OATI.
- Serial Numbers are generated with non-sequential numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG.

7.1.3.5 Application of RFC 5280

For purposes of clarification, a Pre-certificate, as described in RFC 6962 – Certificate Transparency, shall not be considered to be a "certificate" subject to the requirements of RFC 5280 - Internet X.509 PKI Certificate and CRL Profile under these Baseline Requirements.

7.1.4 Algorithm Object identifiers

Effective January 01, 2016, OATI will not issue any new Subscriber certificates, Subordinate CA certificates, or certificates to verify OCSP responses using the SHA-1 hash algorithm.

7.1.5 Name Forms

7.1.5.1 Issuer Information

The content of the Certificate Issuer DN field matches the Subject DN of the OATI certificate to support name chaining as specified in RFC 5280, Section 4.1.2.4.

7.1.5.2 Subject Information

By issuing the Certificate, OATI represents that it followed the procedure set forth in this CPS to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate. OATI does not issue Certificates containing IP Addresses or Internal Names in the Subject Information.

7.1.5.2.1 Subject Alternative Name Extension

Certificate Field: extensions:subjectAltName

Required/Optional: Required

Contents: For server certificates this extension will contain at minimum a dNSName containing the FQDN. OATI confirms that the Applicant controls the FQDN or has been granted the right to use it by the Domain Name Registrant, as appropriate.

For client certificates this extension will contain at minimum an email address which conforms to RFC822 "Standard for ARPA Internet Text Messages."

7.1.5.2.2 Subject Distinguished Name Fields

- subject:commonName (OID 2.5.4.3)
  Required/Optional: Optional but discouraged.

  Contents: If present, for server certificates this field shall contain a single FQDN that is one of the values contained in the Certificate's subjectAltName extension (see Section 7.1.4.2.1 of the BRs).

  Certificate Field: For client certificates there are no restrictions.

- subject:organizationName (OID 2.5.4.10)
  Required/Optional: Required.

  Contents: The subject:organizationName field shall contain either the Subject's Organization's name or DBA as verified under Section 3.2.2.2 of the BRs. OATI may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that OATI documents the difference and any abbreviations used are locally accepted abbreviations; e.g., if the official record shows "Company Name Incorporated," OATI MAY use "Company Name Inc." or "Company Name."

- **Certificate Field:** subject:streetAddress (OID: 2.5.4.9)
  Required/Optional: Optional.

  Contents: The subject:streetAddress field shall contain the Subject's street address information as verified under Section 3.2.2.1 of the BRs.

- **Certificate Field:** subject:localityName (OID: 2.5.4.7)
  Required/Optional: Required

Contents: If present, the subject:localityName field shall contain the Subject's locality information as verified under Section 3.2.2.1 of the BRs.

- **Certificate Field:** subject:stateOrProvinceName (OID: 2.5.4.8)
  Required/Optional: Required

  Contents: The subject:stateOrProvinceName field shall contain the Subject's state or province information as verified under Section 3.2.2.1 of the BRs.

- **Certificate Field:** subject:postalCode (OID: 2.5.4.17)
  Required/Optional: Optional

  Contents: If present, the subject:postalCode field shall contain the Subject's zip or postal information as verified under Section 3.2.2.1 of the BRs.

- **Certificate Field:** subject:countryName (OID: 2.5.4.6)
  Required/Optional: Required

  Contents: The subject:countryName shall contain the two-letter ISO 3166-1 country code associated with the location of the Subject verified under Section 3.2.2.1 of the BRs.

- **Certificate Field: subject:organizationalUnitName:**
  Required/Optional: Optional

  Contents: OATI implements a process that prevents an OU attribute from including anything but a designated Entity Code for the Organization verified under Section 3.2.2.1 of the BRs.

  subject:emailAddress (OID: 1.2.840.113549.1.9.1)
  Required/Optional: Optional

  Contents: The subject:emailAddress field will contain the Subject's email address information as verified under Section 3.2.2.1 of the BRs.

- **Other Subject Attributes**

All other optional attributes, when present within the subject field, shall contain information that has been verified by OATI. Optional attributes shall NOT contain information that indicates the value is absent, incomplete, or not applicable.

7.1.5.3 Subject Information – Subordinate CA Certificates

By issuing a Subordinate CA Certificate, OATI represents that it followed the procedure set forth in this CPS to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

7.1.6 Name Constraints

OATI does not issue Subordinate CA Certificates to external parties and its internal Issuing CA is currently not technically constrained.

7.1.7 Certificate Policy Object Identifier

The certificates issued by OATI contain a Policy Identifier which identifies the use of this CPS as the governing policy for certificate issuance. The certificates issued by OATI may also contain the Organization Validated policy defined in the CA/B Forum BRs, {joint-iso-itut(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baselinerequirements(2) organization-validated(2)} (2.23.140.1.2.2).

7.1.7.1 Reserved Certificate Policy Identifiers

The Subscriber certificates issued by OATI contain a Policy Identifier representing the NAESB WEQ-012 Assurance Level.

[1]Certificate Policy:
    Policy Identifier=2.16.840.1.114505.1.12.2.2
    [1,1]Policy Qualifier Info:
        Policy Qualifier Id=CPS
        Qualifier:
            http://www.naesb.org/PKI/AssuranceLevel

7.1.7.2 Root CA Certificates

No stipulation.

7.1.7.3 Subordinate CA Certificates

No Stipulation.

7.1.7.4 Subscriber Certificates

No Stipulation.

7.1.8 Usage of Policy Constraints extension

The PolicyConstraints extension shall be empty.

7.1.9 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.10 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profile

CRLs issued by OATI conform to RFC 5280 standards.

7.2.1 Version Number(s)

No stipulation.

7.2.2 CRL and CRL Entry Extensions

No stipulation.

7.3 OCSP Profile

OATI supports OCSP, and its responders conform to the RFC 6960 standard. OATI identifies the OCSP responder within the AuthorityInformationAccess (AIA) extension via an OCSP responder URL. The responder does not respond with a “good” status on certificates which have not been issued.

7.3.1 Version Number(s)

No stipulation.

7.3.2 OCSP Extensions

No stipulation.

7.4 OATI webCARES Operational Redundancy

The OATI webCARES system can function from multiple Data Center sites. In the event of a Data Center site becoming unavailable, the OATI webCARES backup system shall be operational within a reasonable time.

7.5 OATI CRL Publishing

The CRL published by the OATI webCARES Root CA has a validity period of three months. The OATI webCARES Root CA publishes a new CRL prior to the expiration of the existing CRL, when a certificate is revoked, and on regular intervals to assure availability. OATI webCARES Digital Certificates can be validated by any entity against the CRL.

The CRL published by the OATI webCARES Issuing CA has a validity period of twelve hours. The OATI webCARES Issuing CA publishes a new CRL prior to the expiration of the existing CRL, when a Certificate is revoked, and on regular intervals to assure availability. Both the OATI webCARES Root and Issuing CA CRLs are published in the OATI Repository at the following URL: www.oaticerts.com/repository.

8. Legal Information

8.1 Conditions of Usage of the webCARES Repository and Website

Any Subscriber or Relying Party accessing the webCARES official website(s) or Repository shall abide by the provisions of this CPS and any other usage conditions made by webCARES and/or OATI.

Parties confirm acceptance of the conditions of usage in the CPS by using an OATI webCARES-issued OATI webCARES Digital Certificate. Failure to comply with the CPS conditions of usage of the webCARES repository and/or web site(s) may result in the termination of the relationship between OATI and the non-compliant party. This may result in immediate revocation of the non-compliant party's OATI webCARES Digital Certificate(s), and termination of access to the OATI webCARES system. This CPS may be amended from time to time, and continued use of webCARES is an affirmation of acceptance of any such amendment(s).

8.2 Accuracy of Information

OATI and SOs serving as LRAs shall make all reasonable efforts to ensure that the parties accessing webCARES repositories receive accurate information. OATI, webCARES, and SOs serving as LRAs do not accept liability beyond the limits of this CPS.

8.3 Warranties of Fitness for a Particular Purpose and Merchantability

OATI, webCARES, and the SOs serving as LRAs hereby disclaim any and all warranties or obligations of any kind; including but not limited to any warranty of merchantability and/or fitness for a particular purpose, as well as any warranty regarding the accuracy of non-verified information.

8.4 Other Warranties

Except as otherwise provided in Section 8.3 herein above and as provided in the CA/B Forum BRs, OATI makes no other warranties of any kind.

8.5 Exclusion of Certain Elements of Damages

OATI specifically excludes liability for special damages, including but not limited to, indirect, punitive, or consequential damages arising out of the use, non-use, or inability to use webCARES, even if advised of the possibility of such damages.

8.6 Damage and Loss Limitations

Except as otherwise provided herein, under no circumstances will OATI or webCARES be liable to any party for any damages or for any loss of profits or data arising out of, or relating to, the use of OATI webCARES Digital Certificates or Digital Signatures.

8.7 Indemnification by Subscribers

By accepting an OATI webCARES Digital Certificate, the Subscriber agrees, to the extent permitted by law, to indemnify and hold OATI and webCARES harmless from any acts or omissions resulting in liability, any loss or damage, and any suits or expenses that OATI may incur that are caused by the use or publication of an OATI webCARES Digital Certificate, and that arises from: (1) any misrepresentation or omission of data supplied by the Subscriber or agent; (2) the Subscriber's breach of the webCARES agreement or this CPS; (3) the Subscriber's failure to protect their Private Key; (4) violation of any applicable laws or regulations; or (5) Subscriber's misuse of the OATI webCARES Digital Certificate.

8.8 Indemnification by CA

OATI shall defend, indemnify, and hold harmless an Application Software Supplier to the extent required by the CA/B Forum BRs.

8.9 webCARES Intellectual Property Rights

OATI owns all intellectual property rights associated with its websites, databases, OATI webCARES Digital Certificates, and any publications used in providing webCARES services. OATI webCARES Digital Certificates are and remain the property of OATI.

The Private Keys for End Entity OATI webCARES Digital Certificates will be treated as property of the End Entity identified in the OATI webCARES Digital Certificate; however, Private Keys have no monetary value on their own.

8.10 Ownership

Subscribers hereby agree not to make any claim of right, title, or ownership in or to OATI webCARES.

8.11 Confidentiality

8.11.1 Confidentiality of Business Information

OATI webCARES information that does not require protection may be made publicly available.

8.11.2 Private Information

OATI webCARES shall treat the information of its Subscriber's as private and protect the information from unauthorized disclosure.

8.11.3 Public Information

OATI webCARES private information does not include CRLs, public certificates, or the data included therein.

8.11.4 Responsibility to Protect Private Information

OATI webCARES personnel are required to handle private information with due care. Private information is securely stored and may be released only in accordance with stipulations as previously in the OATI Data Protection Policy.

8.12 Governing Law

This CPS shall be governed, construed, interpreted, and enforced in accordance with the laws of the state of Minnesota. Regardless of the place of residence or place of use of an OATI webCARES Digital Certificate, Subscribers hereby agree to a venue of Minnesota.

8.13 Successors and Assigns

OATI reserves the right to assign OATI webCARES to successors and/or assigns without consent of any OATI webCARES Subscribers.

8.14 Severability

Any provision contained in this CPS that is held to be unenforceable shall not affect the other provisions in this CPS which shall be considered independent from the severable provision, and this CPS shall remain in full force and effect.

8.15 Interpretation

Captions are for convenience only and shall not be deemed part of the contents of this Agreement.

8.16 Electronic Agreement

THE USE OF ELECTRONIC SIGNATURES, CONTRACTS, ORDERS AND OTHER RECORDS AND ELECTRONIC DELIVERY OF NOTICES, POLICIES AND RECORDS OF TRANSACTIONS INITIATED OR COMPLETED THROUGH THE SERVICES PROVIDED BY OATI. BY UTILIZING webCARES YOU ARE AGREEING TO BE BOUND BY THE TERMS AND CONDITIONS SET FORTH IN THIS CPS. Further, You hereby waive any rights or requirements under any statutes, regulations, rules, ordinances or other laws in any jurisdiction which require an original signature or delivery or retention of non-electronic records, or to payments or the granting of credits by other than electronic means.

8.17 No Waiver

The waiver of any of the rights or remedies arising pursuant to this CPS on any occasion by any entity shall not constitute a waiver of any rights or remedies in respect to any subsequent breach or default of the terms of this Agreement.

8.18 Notice

Notice to OATI regarding issues found in this CPS may be sent to:

Open Access Technology International, Inc.
ATTN: webCARES Administrator
3660 Technology Drive, NE
Minneapolis, MN 55418

8.19 Fees

OATI will establish and may modify fees for use of OATI webCARES. Current pricing of OATI webCARES Digital Certificates is available online or by contacting Support@oati.net.

8.20 Refund Policy

OATI does not issue refunds in association with OATI webCARES Digital Certificate(s) or their use.

9. OATI 24x7x365 Customer Support

The OATI Help Desk provides full support 24x7x365. Customers are encouraged to contact the OATI Help Desk by telephone, email, postal mail, and OATI application messaging systems. Operational emergencies must be reported by telephone to 763.201.2020. OATI webSupport utilizes Tickets to track customer inquiries, issues relating to OATI services, and the OATI infrastructure including hardware, networks, and communications. Tickets can be classified as Low, Medium, High, or Critical and each status has its own process for timely resolution. Critical Tickets are addressed within 30 minutes on a 24x7x365 basis.

10. Compliance Audits

10.1 External Audits

The practices in this CPS are designed to meet or exceed the requirements of generally accepted industry standards, including the latest versions of NAESB WEQ-012, and the AICPA/CICA WebTrust Program for Certification Authorities (WebTrust). This CPS also conforms to the current version of the CA/B Forum BRs published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

OATI receives annual audits by an independent external auditor to assess OATI's compliance with this CPS, CA/B Forum BRs, 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.

10.2 Internal Audits

OATI also monitors adherence to its CPS, CA/B Forum BRs, NAESB WEQ-012 and WebTrust requirements and strictly controls its service quality by performing self-audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the webCARES Digital Certificates issued by OATI during the period commencing immediately after the previous self-audit sample was taken.

11. Copyright Statement