WEBCARES CERTIFICATION PRACTICE STATEMENT v5.0

OPEN ACCESS TECHNOLOGY INTERNATIONAL, INC.

DECEMBER 2021

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

Revision History

Version	Date	Comments	Author(s)
1.0	04/25/2002	Original document	OATI
1.1	07/19/2012	Modification of webCARES CPS	OATI
1.2	11/02/2012	Updates	OATI
2.0	11/12/2012	Fully approved	OATI
2.1	11/27/2012	WebTrust Updates	OATI
2.2	11/29/2012	WEQ-012 Updates	OATI
2.3	09/12/2013	Updates to Section 7.2 OATI Issuing Authorities and Section 7.4 OATI CRL Publishing	OATI
2.4	12/02/2013	Updates	OATI
2.5	02/06/2014	Updates	OATI
2.6	07/01/2014	Updates to Section 3.2.1 and added Section 9.2	OATI
2.7	09/09/2014	CA/B Updates	OATI
2.8	10/28/2014	CA/B Updates	OATI
2.9	06/08/2015	Updates to template	OATI
3.0	08/22/2016	Updates reflecting the new CAB Forum Code Signing Baseline Requirements and Microsoft Root Program changes Updates to Section 1.1 Acronyms and Section 3.2.1 webCARES Application Process	OATI
3.1	02/14/2017	Updated to incorporate webCARES Update to webCARES version 5.1.0.1 changes	OATI
3.2	04/21/2017	Updated to incorporate updates to QA/Browser Forum Baseline Requirements through and including version 1.4.4	OATI
3.3	08/15/2017	Updated to remove references to Backup Security Officer (BSO) & NIST SP800-63 Updates required by CA/Browser Forum Baseline Requirements through and including 1.4.9	OATI
3.4	03/21/2018	Update to template Minor updates throughout including: • Faraday cage • Key archival	OATI

Version	Date	Comments	Author(s)
3.5	08/22/2018	Removed confidential notices throughout CPS Added Revision History to publicly-facing version	OATI
3.6	09/20/2018	Updates needed for CA/B Forum Baseline Requirements Ballot SC6 – Revocation Timeline Extension Added/Revised definitions	OATI
4.0	12/14/2018	Updated template per RFC 3647	OATI
4.1	10/16/2019	Added/Revised definitions and acronyms Cleaned up some areas Updated as needed per WebTrust and CAB Forum changes	OATI
4.2	04/15/2020 07/14/2020	Minor revisions to the following sections: • 1.6.2 – Remove Test Certificates definition • 3.2.2 - Removed notary requirement for the BRAF • 4.9.1 – Added reason for revocation • 5.4.8 – Revised “quarterly” to instead say “every three months” • 6.1.7 – Removed Email signing	OATI
4.3	11/06/2020 12/02/2020 12/09/2020	Updates throughout with settings for latest Root and Issuer. Updates for recent CAB Forum changes.	OATI
4.4	09/21/2021 10/14/2021	Updates throughout with settings for latest Root and Issuer. Updates for recent CAB Forum changes.	OATI
5.0	10/28/2021 12/02/2021	Updates for recent CAB Forum and Browser Program changes.	OATI

Table of Contents

1. Introduction

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 OATI webCARES follows in issuing Digital Certificates in accordance with requirements found within the CPA Canada WebTrust Program for Certification Authorities (WebTrust Principles & Criteria for Certification Authorities and the WebTrust Principles & Criteria for Certification Authorities - SSL Baseline with Network Security), and in accordance with other applicable industry standards such as NAESB WEQ-012 and the CA/B Forum.

1.1 OATI webCARES Overview

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 of OATI webCARES service about 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.

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 a NA for OATI webCARES system users.

1.2 Document Name and Identification

This document is the OATI CA CPS and can be located at https://www.oaticerts.com/repository/OATI-webCARES-CPS.pdf.

1.3 PKI Participants

1.3.1 Certification Authorities

OATI webCARES acts as a CA providing certificate services within the OATI 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 to applicable industry standards.

1.3.2 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 OATI webCARES Digital Certificates to entities that are verified using commercially reasonable industry practices and procedures.

1.3.3 Subscribers

The following describes the types of entities eligible for OATI webCARES access.

1.3.3.1 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 RA.

1.3.3.2 Unaffiliated Individual

An Unaffiliated Individual may apply for an OATI webCARES Client Digital Certificate for his or her own personal use. An Unaffiliated Individual, by definition, will not be applying for an OATI 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 and if approved will be issued a Client Certificate only.

1.3.3.3 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 as an SO.

1.3.4 Relying Parties

OATI employees and all OATI webCARES customers are considered a Relying Party. The following sections describe the types of user roles available within OATI webCARES CA.

1.3.4.1 User Roles

1.3.4.1.1 Security Officer/Local Registration Authority

The role of SO, otherwise known as an LRA, is mandatory for every organization or entity subscribing to the OATI webCARES system. An SO will be responsible for managing the Digital Certificates within his or her OU. An SO will be responsible for using the OATI webCARES system to perform the SO's duties and responsibilities described in this CPS. An SO is delegated the right to serve as an LRA. The SO's duties and contractual obligations include issuing, revoking, renewing, and tracking OATI webCARES Digital Certificates for his or her End-Users, and revoking OATI webCARES Digital Certificates. An 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 OATI webCARES Digital Certificate.

1.3.4.1.2 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.

1.3.4.1.3 End-User

An End-User uses Digital Certificates for identity authentication purposes.

1.3.4.1.4 Non-Enterprise RA

OATI does not use Non-Enterprise RAs.

1.3.5 Other Participants

OATI does not have any other participants.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

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

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

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

OATI non-Root Key Pairs are distributed for the purposes of issuing of Digital Certificates and CRLs. A periodic review of Key Pairs can confirm that each Key Pair has only been used for its intended purpose(s).

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.

1.4.2 Prohibited Certificate Uses

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 OATI webCARES may result in prosecution, fines, or imprisonment.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The maintenance of the OATI CPS 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 CAs, and CA/B Forum BRs.

1.5.2 Contact Details

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

1.5.2.1 OATI 24x7x365 Customer Support

The OATI Help Desk provides full support 24x7x365. Customers are encouraged to contact the OATI Help Desk by telephone, email (webCARESSupport@oati.net), 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.

1.5.3 Person Determining CPS Suitability for the Policy

The OATI Compliance department decides the applicability and conformance of this CPS based on the results and recommendations provided by a Qualified Auditor.

1.5.4 CPS Approval Procedures

This document was approved for publication following OATI standard processes.

1.6 Definitions and Acronyms

1.6.1 Acronyms

ACA	Authorized Certificate Authority
ADN	Authorization Domain Name

AIA	Authority Information Access
AO	Audit Officer
API	Application Program Interface
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
CIP	Critical Infrastructure Protection
CNAME	Canonical Name
CPA Canada	Chartered Professional Accountants of Canada
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSPRNG	Cryptographically Secure Pseudorandom Number Generator
CST	Central Standard Time
DBA	Doing Business As
DN	Distinguished Name
DNS	Domain Name Service
DUNS	Data Universal Numbering System
EKU	Enhanced or Extended Key Usage
FIPS	Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
gTLD	Generic Top-Level Domain
GUI	Graphical User Interface
HIDS	Host-based Intrusion Detection System
HSM	Hardware Security Module
IA	(Certificate) Issuing Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
LDAP	Lightweight Directory Access Protocol

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
NTP	Network Time Protocol
OATI	Open Access Technology International, Inc.
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organizational Unit
PAR	Physical Access Request
PED	Pin Entry Device
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request for Comments
RSA	Rivest-Shamir-Adleman (Public Key Cryptosystem)
SDLC	Software Development Life Cycle
SHA	Secure Hash Algorithm
SIVP	Subscriber Identification and Verification Procedure
SO	Security Officer
SOA Record	Start of Authority Record
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UPS	Uninterruptible Power Supply
URL	Uniform Resource Locator
VESDA	Very Early Smoke Detection Apparatus
WebTrust	Requirements found within the CPA Canada 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

1.6.2 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 an OATI 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 OATI webCARES Digital Certificates.

Authorization Domain Name: The FQDN used to obtain authorization for a given FQDN to be included in a Certificate. OATI may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. OATI may prune zero or more Domain Labels of the FQDN from left to right until encountering a Base Domain Name and may use any one of the values that were yielded by pruning (including the Base Domain Name itself) 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. OATI webCARES is an ACA.

Authorized Port: One of the following ports: 80 (http), 443 (https), 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.

Certification Authority Authorization: From RFC 8659 (http://tools.ietf.org/html/rfc8659): "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify one or more Certification Authorities (CAs) authorized to issue certificates for that domain name. CAA Resource Records allow a public CA to implement additional controls to reduce the risk of unintended certificate mis-issue."

Certificate Authority Operations: 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 OATI webCARES Digital Certificates to SOs and End-Users.

Certificate Problem Report: Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

Certificate Revocation List: A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by OATI.

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

Certificate Profile: A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7 of the Baseline Requirements.

Critical Certificate Authority Operations: Management of the Digital Certificate lifecycle, 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 / OU / End Entity Name / End Entity Email (or IP Address).

Domain Authorization Document: Documentation provided by, or OATI'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 contact (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA Record, or as obtained through direct contact with the Domain Name Registrar.

Domain Label: From RFC 8499 (http://tools.ietf.org/html/rfc8499): "An ordered list of zero or more octets that makes up a portion of a domain name. Using graph theory, a label identifies one node in a portion of the graph of all possible domain names."

Domain Name: An ordered list of one or more Domain Labels 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.

Domain Name Registrar: A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN),

(ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assignees).

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 Domain 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.

Internal Name: A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate that cannot be verified as globally unique within the public DNS at the time of certificate issuance because it does not end with a Top Level Domain registered in IANA's Root Zone Database.

Key Compromise: A Private Key is said to be compromised if its value has been disclosed to an unauthorized person or an unauthorized person has had access to it.

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

LDH Label: From RFC 5890 (http://tools.ietf.org/html/rfc5890): "A string consisting of ASCII letters, digits, and the hyphen with the further restriction that the hyphen cannot appear at the beginning or end of the string. Like all DNS labels, its total length must not exceed 63 octets."

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

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.

Non-Reserved LDH Label: From RFC 5890 (http://tools.ietf.org/html/rfc5890): "The set of valid LDH labels that do not have '-' in the third and fourth positions."

P-Label: A XN-Label that contains valid output of the Punycode algorithm (as defined in RFC 3492, Section 6.3) from the fifth and subsequent positions.

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.

Qualified Auditor: A natural person or Legal Entity that meets the requirements of Section 8.2.

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 an OATI webCARES Digital Certificate and/or any other information in the OATI webCARES Repository to verify the OATI 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 created. 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 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.

Root CA: The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

Root Certificate: The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

Security Officer: A person contractually responsible for issuing and managing OATI webCARES Digital Certificates within an OU or an Unaffiliated Individual with access to the OATI webCARES solution. Each individual designated as an 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 LRA and Enterprise RA.

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

Subject: The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.

Subject Identity Information: Information that identifies the Certificate Subject. Subject Identity Information does not include a Domain Name listed in the subjectAltName extension or the Subject commonName field.

Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

Subscribers: An organization, person, or device that has been issued an OATI 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.

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 an LRA.

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

WHOIS: A query and response protocol based on RFC3912, RFC7482, or an HTTPS website 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.

XN-Label: From RFC 5890 (http://tools.ietf.org/html/rfc5890): “The class of labels that begin with the prefix "xn--" (case independent), but otherwise conform to the rules for LDH labels.”

2. Publication and Repository Responsibilities

2.1 Repositories

OATI operates its own Repository located at www.oaticerts.com/repository.

2.2 Publication of Certification Information

The OATI CPS, Certificate Chain, CRLs, contact information, and links to the current publicly available audit reports are published within the Repository.

2.3 Time or Frequency of Publication

Updates to the Repository are made periodically as determined by OATI staff.

The CRLs are updated hourly as well as anytime a certificate is revoked.

This CPS shall be reviewed and updated by OATI as needed, but at least annually.

2.4 Access Controls on Repositories

Documentation posted within the OATI Repository is considered publicly available. All OATI webCARES CA PKI Participants (as described above) have read access to the Repository.

Only OATI employees in certain roles may be granted write access to the Repository. This access is granted according to OATI access control policies.

3. Identification and Authentication

3.1 Naming

The names of the certificates covered by this CPS are as follows.

OATI Root Certificates:

- OATI WebCARES Root CA
- webCARES Root CA 2018

OATI Intermediate Certificates:

- webCARES Issuing CA 2017
- webCARES Issuing CA 2020
- webCARES Issuing CA 2021

3.1.1 Type of Names

OATI webCARES Certificates are based upon the X.509 v3 structure and extensions. The X.509, Amendment 1 to ISO/IEC 9594-8:2017 provides for a number of extensions. These extensions allow various management and administrative controls that are useful for OATI webCARES purposes.

3.1.2 Need for Names to be Meaningful

OATI webCARES Certificate names must be meaningful.

3.1.3 Anonymity or Pseudonymity of Subscribers

3.1.3.1 Anonymous Digital Certificates

OATI webCARES will not issue anonymous Digital Certificates.

3.1.3.2 Pseudonymous and Role-Based 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.

3.1.4 Rules for Interpreting Various Name Forms

OATI webCARES Certificate Names are interpreted using the X.509 standard.

The OATI NA coordinates the creation and issuance of DNs 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 email 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.

3.1.5 Uniqueness of Names

OATI webCARES Certificate names must be unique.

3.1.6 Recognition, Authentication, and Role of Trademarks

Certificate requests SHALL NOT contain any information that infringes upon the rights of a third party related to trademarks, names, or intellectual property rights. Use of trademarked information by an Applicant is not required to be verified. Applicants are responsible for ensuring the legality of information they present within the certificate application. OATI has the right to reject any certificate applications that violate this section (3.1.6) of the OATI CPS.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

OATI proves Private Key possession by generating Key Pairs on behalf of Subscribers (please see Section 6.2.1).

3.2.2 Authentication of Organization Identity

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

OATI webCARES personnel follow an extensive SIVP prior to issuing OATI webCARES 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). This application process, including the various verification and identity proofing processes, applies to all applications received for OATI 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 email addresses that will be included in certificates by sending an email 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.

3.2.3 Authentication of Individual Identity

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. SOs 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 a secure online process where notification is sent via the distribution channels normally used for sensitive, personal communications. The corporate issued picture ID or secure online process must originate with a government issued photo ID.

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.

3.2.4 Non-Verified Subscriber Information

No stipulation.

3.2.5 Validation of Authority

Please see Sections 1.3.4 and 3.2.2.

3.2.6 Criteria for Interoperation

Not applicable to OATI.

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

3.3 Identification and Authentication for Rekey Requests

3.3.1 Identification and Authentication for Routine Rekey

OATI does not perform Certificate Rekey activities; instead a certificate would be revoked and a new certificate will be issued.

3.3.2 Identification and Authentication for Rekey After Revocation

OATI does not perform Certificate Rekey activities; instead a certificate would be revoked and a new certificate will be issued. 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.

3.4 Identification and Authentication for Revocation Request

3.4.1 Requests Made by Security Officers

SOs may request revocation of certificates through the OATI webCARES GUI. SOs are authenticated and identified via an OATI webCARES Digital Certificate, username, and password upon logging in to OATI webCARES.

3.4.2 Requests Made by Subscribers (End-Users)

Subscribers or their SOs may request certificate revocation by emailing webCARESSupport@oati.net. Revocation requests received via any method other than that noted in 3.4.1 will be subject to further identification and authentication.

4. Certificate Lifecycle Operational Requirements

Digital Certificate Lifecycle 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

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

SOs are authorized to request certificates for their Subscribers. OATI Help Desk staff are able to request certificates for SOs via the BRAF process described within this CPS.

4.1.2 Enrollment Process and Responsibilities

SOs will enter the email, commonName, and OU (if applicable) into OATI webCARES. OATI webCARES will then use the organization, location, and other information from the BRAF to create a certificate request. This is submitted to OATI webCARES for processing and, if approved, a link will be provided to the SO for generation/download of the certificate.

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

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

OATI webCARES ensures that the commonName is not a duplicate for that OU and verifies that the email format is correct. The SO verifies that the commonName is appropriate for that user and that the email address is their correct email address. Other certificate fields are validated as part of the BRAF process. Please see Section 3 for initial identity verification.

4.2.2 Approval or Rejection of Certificate Applications

If the information being submitted to OATI webCARES is determined to be inaccurate, the application is rejected. OATI also reserves the right to reject a certificate application at its discretion.

4.2.3 Time to Process Certificate Applications

Certificate applications are either accepted or rejected immediately upon submittal within OATI webCARES.

4.2.4 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.

4.2.5 CAA Records

As part of the issuance process for server certificates, OATI webCARES checks for a CAA record for the URL specified in the commonName field (which is also used in the subjectAltName extension of the server certificate to be issued), following the processing instructions set forth in RFC 8659, for any records found. If this check (and all others) pass, OATI webCARES will issue a server certificate for this URL within the next five 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 server 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.

4.3 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.

4.3.1 CA Actions During Certificate Issuance

OATI webCARES validates that the SO has performed the necessary steps to validate the Subscriber's identity, employment, email address, and authorization to use the certificate prior to issuing the certificate.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

Notification of certificate issuance is provided by OATI webCARES to the SO that requested the certificate. The SO is then responsible for providing the certificate to the Subscriber.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

By accepting an OATI webCARES Server 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 Server Certificate for accuracy.
- Subscriber has installed the OATI webCARES Server Certificate only on servers that are accessible at the subjectAltName(s) listed in the OATI webCARES Digital Certificate.
- An OATI webCARES Digital Signature created using the Private Key corresponding to the Public Key included in the OATI webCARES Server Certificate is the Digital Signature of the Subscriber and the OATI webCARES Server 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 OATI webCARES regarding the information contained in the OATI webCARES Server Certificate are accurate and true.
- The OATI webCARES Server Certificate is used consistent with this CPS and exclusively for authorized and legal purposes.

4.4.2 Publication of the Certificate by the CA

The certificate shall be published to the SO that requested the certificate, who shall then provide the certificate to the Subscriber. In addition, the certificate is posted to Certificate Transparency logs, and may be posted to a public LDAP Repository or published to other entities as required.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Notification of certificate issuance is provided by OATI webCARES to the SO that requested the certificate. Other entities are not notified of the certificate issuance.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

OATI webCARES Subscribers shall be responsible for obligations as required by the CA/B 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 OATI 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.

4.5.2 Relying Party Public Key and Certificate Usage

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 OATI 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.

4.6 Certificate Renewal

OATI does not perform certificate renewals as defined in WebTrust for CA standards. Instead a new certificate is issued with a new Public Key, this is how OATI refers to renewals.

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 395 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 OATI webCARES 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.

4.6.1 Circumstances for Certificate Renewal

No stipulation for active webCARES Digital Certificates.

4.6.1.1 Notice Prior to Expiration

OATI webCARES RAs shall make reasonable efforts to notify Subscribers via email 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.

4.6.2 Who May Request Renewal

SOs may request certificate renewals within the OATI webCARES GUI.

SOs may enable a certificate to be end user renewable. In which case, an end user may request certificate renewal prior to expiration.

4.6.3 Processing Certificate Renewal Requests

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.

4.6.4 Notification of New Certificate Issuance to Subscriber

SOs are notified of the successful certificate issuance.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

The act of downloading/installing the OATI webCARES Digital Certificate constitutes the acceptance of the certificate renewal.

4.6.6 Publication of the Renewal Certificate by the CA

The certificate shall be published to the SO that requested the certificate, who shall then provide the certificate to the Subscriber. In the case where a certificate is end user renewable, the certificate is only published to the Subscriber that requested it. In addition, the certificate is posted to Certificate Transparency logs, and may be posted to a public LDAP Repository or published to other entities as required.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Notification of certificate issuance is provided by OATI webCARES to the SO that requested the certificate. Other entities are not notified of the certificate issuance.

4.7 Certificate Rekey

OATI does not perform Certificate Rekey activities; instead a certificate would be revoked and a new certificate will be issued which contains a new Key Pair.

4.7.1 Circumstances for Certificate Rekey

Not applicable.

4.7.2 Who May Request Certification of a New Public Key

Not applicable.

4.7.3 Processing Certificate Rekeying Requests

Not applicable.

4.7.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.7.5 Conduct Constituting Acceptance of a Rekeyed Certificate

Not applicable.

4.7.6 Publication of the Rekeyed Certificate by the CA

Not applicable.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

Certificate modification is not permitted by OATI. In circumstances that require modifying certificate information such as name change, role change, or reorganization of DN, the SO or OATI would issue a new certificate as described above.

4.8.2 Who May Request Certificate Modification

No stipulation.

4.8.3 Processing Certificate Modification Requests

OATI would issue a new certificate as described above.

4.8.4 Notification of New Certificate Issuance to Subscriber

See Section 4.4.3.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

See Section 4.6.5.

4.8.6 Publication of the Modified Certificate by the CA

See Section 4.6.6.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.6.7.

4.9 Certificate Revocation and Suspension

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 at any time.

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

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 10 minutes of revocation and the serial number will remain in the CRL until after the end of the OATI webCARES Digital Certificate's validity period.

4.9.1 Circumstances for Revocation

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.

Where the following conditions or circumstances occur, an OATI webCARES Digital Certificate issued by the OATI webCARES system must be immediately revoked within 24 hours:

1. When requested, in writing, by an SO.
2. When the CA 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.
3. When the CA 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.
4. When the SO or Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization.
5. When the CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise.
6. The CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys).
7. The CA obtains evidence that the validation of domain authorization or control for any FQDN or IP address in the Certificate should not be relied upon.

Where the following conditions or circumstances occur, an OATI webCARES Digital Certificate issued by the OATI webCARES system should be revoked within 24 hours, but must be revoked within 5 days:

1. When OATI is notified that a device, server, or application is no longer active or no longer affiliated with the Subscriber's organization.
2. When a contract is terminated with OATI webCARES.
3. When the Certificate no longer complies with the requirements of this CPS.
4. The CA obtains evidence that the Certificate was misused.
5. The CA is made aware of any circumstance indicating that use of an FQDN 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).
6. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate FQDN.

7. The CA is made aware of a material change in the information contained in the Certificate.
8. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or CPS.
9. The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate.
10. 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.
11. Revocation is required by the CA's Certificate Policy and/or CPS.
12. The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed.
13. 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 business days from the date the request was received.
14. 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.
15. 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).
16. For SO certificates: When OATI is notified that a party listed as the SO no longer represents a Business Organization.

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 or ongoing disputes. 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.

Subscribers must promptly notify their OATI webCARES SO, or OATI Help Desk, upon suspicion of loss or compromise of their Private Keys. 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.

The reason for revocation shall be included within the webCARES system for audit trail purposes.

4.9.2 Who Can Request Revocation

An End Entity may request revocation of his/her/its OATI webCARES Digital Certificate at any time for any reason. The request may be made to the End Entity's SO or to the OATI Help Desk. SOs may request revocation of a certificate within their OU as well. This can be done via the OATI webCARES GUI or via email submittal of a Certificate Problem Report to OATI Help Desk. If the revocation request is to the OATI Help Desk, the request must be submitted to OATI via the webCARESSupport@oati.net email address. Within 24 hours after receiving the Certificate Problem Report, the OATI Help Desk will begin an investigation request for revocation, 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 consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties).
3. The number of reports received about a particular Certificate or Subscriber.
4. 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).
5. Relevant legislation.

The OATI Help Desk will provide a preliminary report on its findings to both the Subscriber and the entity who filed the report within 24 hours after receipt of the request.

4.9.2.1 Notifications

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

- Reasonably suspected or detected compromise of the CA Private Key(s).
- Successful physical or electronic penetration of the CA system(s).
- Successful denial of service attack on CA components.

- An incident prevents the CA from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL.

4.9.3 Procedure for Revocation Request

See Section 4.9.2.

4.9.4 Revocation Request Grace Period

No stipulation, but OATI will take action to revoke the certificate if it has not been completed within the timeframes noted above.

4.9.5 Time Within Which CA Must Process the Revocation Request

If it is determined that revocation is necessary, the revocation request shall be processed in accordance with Section 4.9.1. If deemed necessary, the report will be forwarded to law enforcement authorities.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying Parties may check the status of certificates via the CRL or OCSP.

4.9.7 CRL Issuance Frequency

OATI CRLs containing entries for all revoked certificates are scheduled to publish at least once every hour for each of its Issuers. CRLs expire 12 hours from when they are issued.

4.9.8 Maximum Latency for CRLs

OATI does not impose a maximum latency for its CRLs. Generally, CRLs are published to the Repository within a few minutes of being generated.

4.9.9 Online Revocation/Status Checking Availability

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

These serial numbers are also available for verification through an Online Certificate Status server using the OCSP protocol. This is available 24x7 at the following URL: ocsp.oaticerts.com/ocsp.

OATI maintains OATI webCARES CRL and OCSP capability with resources sufficient to provide a response time of 10 seconds or less under normal operating conditions.

4.9.10 Online Revocation Checking Requirements

OATI webCARES OCSP responses conform to RFC 6960 and/or RFC 5019, 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 RFC 6960. 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.

4.9.10.1 Subscriber OCSP Validity Period

OCSP responses have a validity interval between 11 and 12 hours. OATI updates the information provided via an OCSP on an hourly basis.

4.9.10.2 Subordinate OCSP Validity Period

OATI shall update information provided via an Online Certificate Status Protocol (i) at least every twelve months; and (ii) within 24 hours after revoking a Subordinate CA Certificate.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements re Key Compromise

Please see Section 4.9.1.

Subscribers must notify OATI immediately in the event of a key compromise. Subscribers are responsible for investigating any suspected key compromise. OATI will notify Subscribers in the event OATI suspects that a Subscriber's key has been compromised. If it has been determined that there is a key compromise, OATI will take action to revoke the certificate as noted in Section 4.9.1. Methods that parties may use to demonstrate a private key compromise include:

- Submitting the private key.
- Providing verifiable information regarding a vulnerability or security incident.
- Other methods may be considered by OATI.

4.9.13 Circumstances for Suspension

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

4.9.14 Who Can Request Suspension

SOs or the Subscriber of the certificate may request a certificate suspension.

4.9.15 Procedure for Suspension Request

Certificates may be requested for suspension via the OATI webCARES GUI, or phone call or email to OATI Help Desk with appropriate verification.

4.9.16 Limits on Suspension Period

Certificates may be suspended until the certificate expires.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

See Section 4.9.9.

4.10.2 Service Availability

See Section 4.9.9.

4.10.3 Operational Features

See Section 4.9.9.

4.11 End of Subscription

SOs can revoke their own certificates from OATI webCARES.

Upon validity date expiration, the OATI webCARES digital certificate will no longer be usable.

If services are terminated, OATI will take action to revoke the certificates applicable to the terminating services.

4.12 Key Escrow and Recovery

OATI does not conduct key escrow with a third party. This section is not applicable to OATI.

4.12.1 Key Escrow and Recovery Policy and Practices

Not applicable.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. Facility, Management, and Operational Controls

5.1 Physical Controls

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

5.1.1 Site Location and Construction

The OATI North Campus Data Center is located in Minneapolis, Minnesota and the OATI South Campus Data Center is located in Bloomington, Minnesota. Through the use of geographically diverse Data Centers, coupled with Active/Active replication contained within the highest tier of physical infrastructure, OATI has redefined expectations for the energy industry. At the structural level, OATI Data Centers and all supporting electrical and mechanical rooms are self-contained in six-sided cement block walls. By compartmentalizing each critical area, any fire, leak, weather event, or other disaster will be contained, preventing it from affecting the other critical areas of the facility.

5.1.1.1 OATI Private Cloud Active/Active Architecture

The OATI Private Cloud infrastructure provides application availability from two separate Data Centers in an Active/Active configuration. Backend data processing is performed by a four-node active/passive cluster. Two cluster members are at each site, and the database can run at either site. Two separate storage systems are configured, one at each site, with continuous synchronous data replication between the two systems. Multiple applications and web servers are configured at both sites and are active at all times, allowing customer requests to be handled at either site. Both sites feature full monitoring systems, network and systems redundancy.

This Active/Active configuration provides outstanding availability and reliability. Planned maintenance can be performed on any server or network device without affecting uptime of the application.

By linking two locations into one virtual Data Center through multiple redundant fiber links, infrastructure functions are dispersed to optimize best use of equipment. In an Active/Active configuration, two production level Data Centers at geographically dispersed locations are available for prompt shifting between sites to optimize the highest available hardware and network assets. All database, application, and web servers are configured as four-node clusters. This configuration results in no data loss in the event of a site failure. Server load

balancing is done via an intelligent appliance that uses health probes to determine the load and health of a server and perform concurrent connections calculations. Using these metrics, the appliance directs traffic to the server that will handle the request most efficiently and in the shortest time.

5.1.1.2 OATI Server Virtualization

Building upon the OATI Private Cloud, yet another layer of redundancy is found in the OATI virtualized server and storage infrastructure. OATI Server Virtualization features advanced blade servers and state-of-the-art storage drive arrays. Each server instance that is part of a customer deployment is carefully sized and configured to provide outstanding application performance and meet all documented performance requirements. OATI Server Virtualization allows OATI to dynamically scale horizontally and vertically, as needed, in order to meet evolving system needs. Further, OATI Server Virtualization minimizes the impact of hardware failure; if a hardware component within the blade server farm fails, the virtual servers running on that farm continue to run on the remaining equipment. In this way, OATI Server Virtualization removes single points of failure by separating the server instance from the underlying hardware.

5.1.2 Physical Access

The computer hardware, software, servers, and procedures used by OATI webCARES CA provide a reasonable level of availability and reliability while maintaining a secure environment in enforcement of the OATI security policies and procedures.

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

Gaining physical access to the cryptographic module requires a minimum of two OATI Trusted Employees in order to open the Faraday Cage. These enclosures protect from High Altitude Electromagnetic Pulse as well as Intentional Electromagnetic Interference attacks.

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

5.1.3 Power and Air Conditioning

All OATI facilities are designed and implemented with power system redundancy appropriate to the functional level of the facility. Generators are used for backup power. UPS units are used to guarantee power availability during generator spin-up and also to condition power.

5.1.3.1 Redundant Electrical Systems

The OATI North Campus Data Center features a tri-redundant electrical system (three separate utility feeds) built to Tier IV standards. Each feed provides power to one “power rail.” Should one of these feeds be interrupted, the other two feeds will provide uninterrupted power to every computer component and every critical component supporting the Data Center.

Each power rail is backed up by a dedicated UPS device and by a dedicated 1500 kilowatt generator, which will automatically provide power in the event of a power loss, for as long as necessary for restoration of utility power.

The OATI South Campus Data Center facility features a sophisticated electrical system comprised of 600 KW on-site natural gas micro turbine generation as the primary source of electrical power, operating in co-generation with utility grid power interconnection. A 1500 KW diesel generator provides emergency backup power if utility and micro turbine should be unavailable. These power sources are supplemented by 100 KW of renewable solar PV generation installed on the roof. All electrical sources and facility loads are managed by a pair

of fully redundant hot-standby Programmable Logic Controllers to regulate electrical source and load parameters dynamically to maintain critical electrical system availability.

Electrical power is supplied to the Data Center by 2N redundant dedicated Uninterruptible Power Supply (UPS) devices located in physically isolated rooms. The UPS units receive power from any combination of the generation sources under control of the PLC. Each UPS feed provides power to one Data Center "power rail." Under normal operating conditions each rail supplies 50% of Data Center power. Should one of these feeds be interrupted, the other feed will seamlessly assume the entire electrical load, powering every computer and every critical component supporting the Data Center.

5.1.3.2 2-N Mechanical Systems

The OATI North Campus Data Center features a 2-N cooling system, meaning two entirely redundant cooling loops serve the Data Center. Each cooling loop consists of its own chiller, cooling tower, pump system, chilled water storage tank, and cooling unit system. Under the 2-N design, the Data Center will remain fully cooled and operational during any planned or unplanned cooling system outage.

The OATI South Campus Data Center features a 2-N cooling system to provide cooling, which is based on fully redundant chillers, cooling towers and pumps. The cooling system design leverages Minnesota's cool climate with the addition of a free cooling heat exchanger, which acts as a third chiller when outdoor temperatures are below 35 degrees. This provides not only increased redundancy but much higher efficiency for several months each year. Under the 2-N design, the Data Center will remain fully cooled and operational during any planned or unplanned cooling system outage.

5.1.4 Water Exposures

Although no water piping is located within or above Data Center floor space; interstitial sloped roofs within the Data Center space captures any water that may somehow migrate over the Data Center space.

5.1.5 Fire Prevention and Protection

The OATI Campus Data Center features the most robust technology in fire detection and protection. All compartments feature VESDA systems that continuously sample the air to provide the earliest possible warning of an impending fire hazard, and then initiate an

appropriate response to enable OATI intervention prior to a fire event to prevent injury, property damage, or business disruption. Additionally, in the event of a fire situation, the OATI Campus Data Center is protected by two independent fire suppression systems.

5.1.6 Media Storage

5.1.6.1 Offline Backup Media

In some cases, data backups may be stored long-term using offline recovery media [Tape, external disk, etc. (together and separately, "Long-Term Media")] within the OATI webCARES enclosures. When offline backup media is used, the data will be copied to two Long-Term Media before it is deleted from the online system.

5.1.6.2 Online Backup Media

In some cases, data backups may be stored long term on an online backup location (employing Long-Term Media) within the OATI webCARES enclosures.

5.1.7 Waste Disposal

In the event sensitive media and/or documentation are no longer needed for operations, those media and/or documentation shall be destroyed in a secure manner.

5.1.8 Off-Site Backup

Active data are immediately and synchronously replicated from Data Center to Data Center over the two dedicated (redundant) fiber channel links. These links are entirely separate from the dual (redundant) Ethernet data links, adding additional separation for added security. Replicated data are available for use instantaneously, allowing OATI to recover from disasters quickly and without data loss.

5.2 Procedural Controls

5.2.1 Trusted Roles

OATI webCARES operations are handled by multiple PKI personnel in Trusted Roles. A Trusted Role is one whose incumbent performs functions on the OATI webCARES system that can introduce security problems if not carried out properly, whether accidentally or maliciously.

5.2.2 Number of Persons Required per Task

The OATI implementation of the HSM requires multiple OATI employees to take certain actions on the OATI webCARES system. The HSM allows OATI to establish an "M of N"[1] access security structure for access to the Private Keys that it is securely storing. As any significant action[2] or maintenance to the OATI webCARES system requires access to the Root, Intermediate, and/or IA Private Keys, the "M of N" access required by the HSM ensures that the OATI webCARES system cannot be compromised by a single OATI employee.

OATI implementation of the HSM requires three OATI employees to initialize[3] (or re-initialize after operation has commenced) the OATI webCARES system and two OATI employees to perform day-to-day operations and/or maintenance[4] on the OATI webCARES system. Through the use of the HSM, access to the OATI webCARES system requires the use of multiple keys that are provided to strategic and trusted OATI employees. The structure and use of the HSM keys is as follows. The HSM includes six key types, differentiated by colors Red, Purple, Orange, Blue, Black, and Green. Each Blue, Black, and Green key has an associated PIN that must be entered when used to access the OATI webCARES CA. Red, Purple, and Orange keys do not have a PIN. For initialization (or re-initialization after operation has commenced) of the OATI webCARES CA, one Red, one Purple, one Orange, one Blue, one Black, and one Green key are required for access. For operation of the remote PED, one Red key and one Orange key are required for access. For day-to-day operations and/or maintenance of the OATI webCARES CA, one Black key and one Green key, or one Blue key and one Green key are required for access.

5.2.3 Identification and Authentication for Each Role

All persons filling Trusted Roles shall be selected on the basis of loyalty, trustworthiness, and integrity, in addition to all background checks and other security measures required by applicable standards and regulations.

---

[1] "M of N" authentication provides the capability to enforce multi-person integrity over CA operations. The mechanism requires a group of "N" keys to be setup, and using sophisticated algorithms, you must produce "M" of the group to conduct operations.

[2] Significant Action is defined as one that, if done improperly, could compromise or allows access to the webCARES CA Private Keys (Root, Intermediate, and/or IA keys).

[3] Initialization, re-initialization, and setup include one-time token initialization and one time token cloning.

[4] Day-to-day operations and maintenance includes, but is not limited to, maintenance activities such as backups, hardware support, one-time setup of security domains and users as well as the webCARES CA key generation procedure.

5.2.4 Roles Requiring Separation of Duties

The functions performed in these roles form the basis of trust for all uses of the CA. Two approaches are taken to increase the likelihood that these roles can be successfully carried out; role separation and restricted access.

- Administrator
  - Authorized to install, configure, and maintain the CA.
  - Establish and maintain user accounts.
  - Configure profiles and audit parameters.
  - Management of CA Private Key life cycle.
  - View and maintain CA system archives and audit logs
- Auditor
  - Authorized to maintain audit logs.
  - Perform or oversee internal compliance audits to ensure that the CA is operating in accordance with its CPS.
  - Perform the duties of an AO as defined in the OATI webCARES CPS.
- Operator
  - Authorized to perform system backup and recovery.
  - Other routine operation of CA equipment.
- Registration Administrator
  - Authorized to request or approve certificates or certificate revocations.
  - Verify the identity of Subscribers and accuracy of information included in Certificates.
  - Maintains records and other documentation acquired during identity proofing/validation of Subscribers.

Members of the following departments of OATI are eligible to be assigned to the respective Trusted Role.

- Administrator – IT, Executives, and OATI webCARES Development Team.
- Auditor – Compliance and Delegates.
- Operators – Registration Administrators and Administrators.
- Registration Administrator – Help Desk.

5.3 Personnel Controls

OATI screens all employees working with or having access to the OATI 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 OATI 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 PKI knowledge, authentication, and vetting policies and procedures (including this CPS), common threats to the information verification process (including phishing and other social engineering tactics), and necessary 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.

5.3.1 Qualifications, Experience, and Clearance Requirements

Only trained personnel are given authority to access Production Systems. Upon employment, a background check is conducted and access to Production Systems is only provided following completion of a training course and a successful background check. All access to Production Systems requires two approvals — one by a project manager and another by an IT Director. In addition, all Production access activity is recorded for audit purposes.

Staff must have proper training, clean background checks, a demonstrated functional need for the access, and undergo a corporate authorization process, called a PAR, in order to receive physical access to any OATI webCARES equipment. The PAR system requires manager, President, and Security System Administrator approval prior to access being granted.

5.3.2 Background Check Procedures

All employees and contract employees have a background screening investigation conducted as a condition of employment as well as five year recurring background checks for employees granted more privileged accesses. OATI follows both NERC CIP and NIST SP 800-53 background check requirements. The background screening investigation includes at a minimum:

- Identity verification (e.g., Social Security Number verification in the U.S.).
- Seven-year criminal check.
- Motor vehicle operator's license information (as applicable).

OATI utilizes a Background Screening Investigation Decision Tree for determining whether or not an employee or potential employee is acceptable for the position.

5.3.3 Training Requirements

Personnel serving in a Trusted Role shall undergo training appropriate to their duty and function. At a minimum, Trusted Role applicants must complete a training program prior to becoming approved to hold a Trusted Role.

5.3.4 Retraining Frequency and Requirements

Trusted Role personnel undergo at least annual re-certification training. Training would also be required upon any signification changes to OATI webCARES operations or functionality.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

An OATI employee found to be in violation of the OATI webCARES processes and procedures is subject to disciplinary actions deemed appropriate by Personnel Services and Management which may include termination of employment, probation, removal of Trusted Role status, retraining, and more.

5.3.7 Independent Contractor Requirements

OATI does not employ independent contractors in Trusted Role positions. In the event OATI did employ an independent contractor in a Trusted Role position, they would be subject to the same requirements as an OATI employee.

5.3.8 Documentation Supplied to Personnel

Documentation given to Trusted Role personnel consists of (at a minimum) the OATI webCARES Trusted Role Process and Procedure and the Trusted Role Training document.

5.4 Audit Logging Procedures

The following process outlines OATI's logging process for auditing purposes.

5.4.1 Types of Events Recorded

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 certificate and key lifecycle events, including:
   A. Key generation, backup, storage, recovery, archival and destruction;
   B. Certificate requests, renewal, and re-key requests, and revocation;
   C. Approval and rejection of certificate requests;
   D. Cryptographic device lifecycle management events;
   E. Generation of Certificate Revocation Lists and OCSP entries; and
   F. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.
2. Subscriber Certificate lifecycle management events, including:
   A. Certificate requests, renewal and re-key requests, and revocation;
   B. All verification activities stipulated in the CA/B Forum Baseline Requirements and this CPS;
   C. Approval and rejection of certificate requests;
   D. Issuance of Certificates; and
   E. Generation of CRLs 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. Installation, update and removal of software on a Certificate System;
   E. System crashes, hardware failures, and other anomalies;
   F. Firewall and router activities; and

G. Entries to and exits from the CA facility.

5.4.2 Frequency of Processing Log

The audit logs are automatically compiled daily for predefined events relating to the security of the OATI webCARES CA. OATI will review the audit logs as required for cause.

5.4.3 Retention Period for Audit Log

Audit logs are kept indefinitely.

5.4.4 Protection of Audit Log

OATI webCARES audit logs are compiled and archived in a confidential manner that maintains integrity and prevents their modification, substitution, or unauthorized destruction. Only parties with access privileges to the relevant audit records are able to view them digitally. Media containing the audit logs is accessible only to privileged OATI staff.

5.4.5 Audit Log Backup Procedures

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

5.4.6 Audit Collection System (Internal vs. External)

OATI webCARES maintains audit logs that are visible to customers (external) via the application interface. Users are only able to view audit log certificate information for certificates that are under their control.

Internal OATI webCARES audit logs are only available to specific OATI staff with a specific job need and necessary privileges to view them.

5.4.7 Notification to Event-Causing Subject

Auditable events are not immediately distributed to users or their SOs. SOs receive a monthly activity report via email which contains any certificate actions they have taken on their user's certificates. Company AOs also receive this monthly report.

5.4.8 Vulnerability Assessments

OATI performs monthly internal and external network penetration testing against Production and Development Systems. Application penetration testing is incorporated into the SDLC and is performed prior to Production releases.

Additionally, the OATI Risk Assessment and Management (ORAM) Team performs an annual risk assessment of threats and vulnerabilities. The assessment includes:

- Identifying foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes.
    - Assessing the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes.
    - Assessing the sufficiency of the policies, procedures, information systems, technology, and other arrangements that OATI has in place to counter such threats.

5.5 Records Archival

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 for CAs, CA/B Forum BRs, and NAESB WEQ-012.

5.5.1 Types of Records Archived

Data to be archived include (at a minimum):

- 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
- And others as specified in WebTrust for CAs, CA/B Forum BRs, NAESB WEQ-012 or other applicable requirements

5.5.2 Retention Period for Archive

Data will be archived for time periods required by applicable standards and regulatory stipulations including, but not limited to, WebTrust for CAs, CA/B Forum BRs, and NAESB WEQ-012 and based upon a risk assessment performed to determine the appropriate length of retention time, which shall be no less than seven years.

The CA SHALL retain all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, for at least seven years after any Certificate based on that documentation ceases to be valid.

5.5.3 Protection of Archive

The OATI webCARES system 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. Only OATI webCARES Administrators have access to view the OATI webCARES archives.

OATI does not archive Subscriber Private Keys.

5.5.4 Archive Backup Procedures

OATI webCARES archives are backed up using a mechanism specific to the HSMs that OATI owns. This process ensures that these archives never leave a FIPs certified HSM, and is done so using a FIPs certified backup/transfer process. These backups occur in two different ways:

1. OATI uses multiple active HSM devices. These devices are all online at any time. These devices use an internal synchronization method to ensure that all Private Keys are present

in every device. These devices are stored within the OATI webCARES enclosures in the OATI Data Centers.

2. OATI uses multiple "HSM Backup" devices. These devices are offline at all times (except when backups are being done). These devices are stored within the OATI webCARES enclosures in the OATI Data Centers.

5.5.5 Requirements for Time-Stamping of Records

OATI webCARES archives are automatically time-stamped as they are created. Please see Section 6.8.

5.5.6 Archive Collection System (Internal or External)

OATI utilizes internal systems to collect OATI webCARES archives.

5.5.7 Procedures to Obtain and Verify Archive Information

Only OATI webCARES Administrators have access to view the OATI webCARES archives. Archived keys SHOULD only be accessed when requested by an internal or external auditor.

5.6 Key Changeover

Not applicable.

5.7 Compromise and Disaster Recovery

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, OATI webCARES operations would continue at another other site with minimal disruption.

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.

5.7.1 Incident and Compromise Handling Procedures

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

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

When computing resources, software, and/or data are corrupted, the CA shall respond as follows:

- Before returning to operation, OATI will ensure the OATI 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 Key Pair.

5.7.3 Entity Private Key Compromise Procedures

Please see Sections 4.9 and 5.7.1.

5.7.4 Business Continuity Capabilities After a Disaster

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

5.8 CA or RA Termination

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

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

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Subscriber keys are generated by the company SO. This key generation is done in the Subscriber's browser software.

CA keys are generated by the CA. This key generation is done within an HSM. A Key Generation Script shall be prepared and followed.

6.1.1.1 Witnesses

OATI will videotape the key generation ceremony and may engage a Qualified Auditor to witness and validate the ceremony as well. For Root key generation, OATI will engage a Qualified Auditor to issue a report opining that the CA followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair.

For both Root and Issuer key pair generation, OATI SHALL:

1. Generate the Key Pair in a physically secured environment as described in the CA's Certificate Policy and/or Certification Practice Statement.
2. Generate the Key Pair using personnel in Trusted Roles under the principles of multiple person control and split knowledge.
3. Generate the Key Pair within cryptographic modules meeting the applicable technical and business requirements as disclosed in the CA's Certificate Policy and/or Certification Practice Statement.
4. Log its Key Pair generation activities.
5. Maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in its Certificate Policy and/or Certification Practice Statement and (if applicable) its Key Generation Script.

6.1.1.1.1 Subscriber Key Pair Generation

OATI shall reject a certificate request if any of the following conditions are met:

1. The Key Pair does not meet the requirements set forth in Section 6.1.5 and/or Section 6.1.6.

2. There is clear evidence that the specific method used to generate the Private Key was flawed.
3. The CA is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise.
4. The CA has previously been made aware that the Applicant's Private Key has suffered a Key Compromise, such as through the provisions of Section 4.9.1.1.
5. The CA is aware of a demonstrated or proven method to easily compute the Applicant's Private Key based on the Public Key (such as a Debian weak key, see https://wiki.debian.org/SSLkeys).

OATI does not generate Key Pairs on behalf of a Subscriber, and will not accept a certificate request using a Key Pair previously generated OATI. OATI subscriber certificates do not contain the anyExtendedKeyUsage value.

6.1.2 Private Key Delivery to Subscriber

As Subscriber Private Keys are not provided to the SOs, but generated in their own browser, this is not applicable.

Parties other than the Subscriber or SO SHALL NOT archive the Subscriber Private Key without authorization by the Subscriber or SO.

If OATI 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 shall revoke all certificates that include the Public Key corresponding to the communicated Private Key.

6.1.3 Public Key Delivery to Certificate Issuer

All subscriber-CA communications are delivered over a secure online TLS connection (session).

6.1.4 CA Public Key Delivery to Relying Parties

CA Certificates, including Public Keys, are available for download from the Repository.

6.1.5 Key Sizes

OATI WebCARES Root CA issues OATI webCARES Digital Certificates using a 4096 bit RSA key with Secure Hash Algorithm 1 (SHA-1).

OATI webCARES Root CA 2018 issues OATI webCARES Digital Certificates using a 4096 bit RSA key with Secure Hash Algorithm 2 (SHA-512).

OATI webCARES Issuing CA 2017 issues OATI webCARES Digital Certificates using a 2048 bit RSA key with Secure Hash Algorithm 2 (SHA-256).

OATI webCARES Issuing CA 2020 issues OATI webCARES Digital Certificates using a 2048 bit RSA key with Secure Hash Algorithm 2 (SHA-512).

OATI webCARES Issuing CA 2021 issues OATI webCARES Digital Certificates using a 2048 bit RSA key with Secure Hash Algorithm 2 (SHA-512).

6.1.6 Public Key Parameters Generation and Quality Checking

Public Key parameters are generated in combination by the SO and the OATI webCARES system. These are partially based on values entered during the BRAF process. Any parameters generated by the SO are verified by the OATI webCARES system for accuracy and against all restrictions placed on them by this CPS, as well as by any other applicable governing document or standard. BRAF parameters are verified by the OATI webCARES Administrator during the BRAF process.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

OATI webCARES CA certificates and their associated keys are limited to the following uses: Non-Repudiation, Certificate Signing, Off-line CRL Signing, CRL Signing.

OATI webCARES End Entity Certificates and their associated keys are limited to the following uses: Client Authentication and Server Authentication.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and 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. 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 (see Section 4.9). 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 (see Section 4.9).

6.2.2 Private Key (n out of m) Multi-Person Control

Please see Section 5.2.2.

6.2.3 Private Key Escrow

OATI does not conduct key escrow with a third party. This section is not applicable to OATI.

6.2.4 Private Key Backup

OATI CA Private Keys are backed up using a mechanism specific to the HSMs that OATI owns. This process ensures that these Private Keys never leave a FIPs certified HSM, and is done so using a FIPs certified backup/transfer process. These backups occur in two different ways:

1. OATI uses multiple active HSMs devices. These devices are all online at any time. These devices use an internal synchronization method to ensure that all Private Keys are present in every device. These devices are stored within the OATI webCARES enclosures in the OATI Data Centers.
2. OATI uses multiple "HSM Backup" devices. These devices are offline at all times (except when backups are being done). These devices are stored within the OATI webCARES enclosures in the OATI Data Centers.

OATI webCARES does not conduct Private Key backup services for Subscribers.

6.2.5 Private Key Archival

OATI webCARES does not conduct Private Key archival services for Subscribers.

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.

Subordinate CA Private Keys SHALL NOT be archived by parties other than the Subordinate CA.

Archived CA keys MUST be subject to the same or greater level of security controls as keys currently in use. Archived keys SHOULD only be accessed when requested by an internal or external auditor.

If it becomes necessary to put archived CA keys back online, OATI will only put them online for the minimum amount of time to complete the required task and then move the CA keys back offline.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

Subscribers must protect their Private Keys in accordance with the applicable guidelines on Private Key protection.

CA Private Keys are not allowed to be transferred out of cryptographic modules under any circumstances.

CA Private Keys are not allowed to be generated outside of cryptographic modules under any circumstances. CA Private Keys are allowed to be transferred between cryptographic modules assuming both modules comply with the requirements of this CPS and the transfer mechanism complies with FIP standards.

6.2.7 Private Key Storage on Cryptographic Module

Subscribers must protect their Private Keys in accordance with the applicable guidelines on Private Key protection. Subscribers must promptly notify their OATI webCARES SO, or OATI Help Desk, upon suspicion of loss or compromise of their Private Keys (see Section 4.9). 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 (see Section 4.9).

For CA Private Keys, see Section 6.2.6. Private Keys are encrypted in storage on the cryptographic module.

6.2.8 Method of Activating Private Key

CA Private Key activation requires two Trusted Role members, from different groups, to both provide a physical key issued to them. In addition, one of the two must provide a PIN number for activation.

6.2.9 Method of Deactivating Private Key

OATI webCARES CA Private Keys are securely and confidentially stored. Once a Key Pair is retired it should never be put back into Production.

When a CA Private Key is no longer wished to be made available to Subscribers, the OATI webCARES Administrator disables the use of the Private Key in the OATI webCARES management interface. This is done within the standard OATI webCARES change management and approval process.

OATI 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.

6.2.10 Method of Destroying Private Key

OATI has never destroyed a webCARES key pair before, and has no current plans to do so at this time. 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 such as dual control and ensuring that all activation data is destroyed.

6.2.11 Cryptographic Module Rating

OATI webCARES cryptographic modules for its CA Private Keys are validated to FIPS 140-2 Level 3 standards.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

No stipulation.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

OATI webCARES End-User (Client) Digital Certificates issued to Subscribers have a certificate lifetime of two years.

OATI webCARES Server Certificates have a certificate lifetime of 397 days.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

OATI HSM PIN codes are generated by the OATI webCARES Administrator Trusted Role, and distributed to key holders as part of the HSM key holder distribution process.

6.4.2 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.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

All OATI webCARES systems must meet the following criteria:

- Configured based on OATI approved configuration template
- Limited to OATI approved third party software
- Regularly scanned by currently updated AV software
- Run configured HIDS and Network Firewall software
- Maintain current security patch versions of all security patches following the standard OATI system patching process
- Be segregated behind a dedicated OATI webCARES firewall, and physically located behind a dedicated physical boundary

- Be protected by a Multi-Factor Authentication system
- Be subject to strong password policies
- Be subject to strong configuration management policies
- Prohibit object re-use
- Requires encryption for all external communications
- Be subject to both separation of duties and Trusted Role regulations
- Provide significant auditing capabilities
- And others as specified in WebTrust for CAs, CA/B Forum BRs, NAESB WEQ-012 or other applicable requirements

6.5.2 Computer Security Rating

No stipulation.

6.6 Lifecycle Technical Controls

6.6.1 System Development Controls

6.6.1.1 Access

In order for an OATI employee to have access to a Development System, they must first have an acceptable and current background check as well as complete the Development Environment training program. Once these requirements are met, the employee requests access to specific Development Systems that they have been assigned to; this is approved by their Manager as well as an IT Staff Member. This access is granted per project as the employee has been assigned. Employee access to Production Systems requires the same current background check, as well as completion of the Development Environment training program as mentioned above. In addition, the employee must also complete the Production Environment training program and receive Director or higher approval in order to be eligible. Upon completing the aforementioned requirements, the employee then requests access to specific Production Systems that they have been assigned to as well as the access level; this is approved by their Manager as well as a member of IT Management. Access to Development and Production Systems is removed upon termination of employment. Access to Development and Production Systems is reviewed at least quarterly as well as when an employee changes job roles.

6.6.1.2 Change Management

OATI's SDLC describes the procedures in place for the request and designing of new applications, enhancements, emergency changes, integration, development, deployment, integration, documentation, and testing of applications. The OATI SDLC also describes the specific roles and job functions throughout each step of the process. OATI has controls in place to address these items, and is audited against these controls.

OATI Change Control and Configuration Management Procedures provide instructions governing methods in the Development non-Production and operational environment. OATI employs, at a minimum, two Environments per project (Development and Production). Changes are not made on Production Systems until they have been properly installed and tested on the Development System. OATI's SDLC describes the procedures in place for the request and designing of new applications, enhancements, emergency changes, integration, development, deployment, documentation, and testing of applications. The OATI SDLC also describes the specific roles and functions throughout each step of the process. OATI has controls in place to address these items, and is audited against these controls.

OATI's Production Environment Authentication System is used for tracking code changes and manual data changes. In addition, all OATI applications include an audit trail which tracks the data changes.

OATI enforces multi-factor authentication for all accounts capable of directly causing certificate issuance. OATI webCARES CA key(s) are securely generated using 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 OATI webCARES system which includes a unique username, strong password, and client authentication certificate.

6.6.1.3 Training

Training is provided to Development teams on coding practices to be avoided, they are given techniques on how to implement selected functionality in a secure way. OATI also requires all personnel to undergo periodic Cyber Security training.

6.6.2 Security Management Controls

See Section 6.6.1.

6.6.3 Lifecycle Security Controls

No stipulation.

6.7 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.

6.7.1 Anti-Virus

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

6.8 Time-Stamping

The OATI webCARES system will time stamp and record 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 actions taken on OATI webCARES Digital Certificates, the OATI webCARES system will time stamp CRLs. The OATI webCARES system will operate on CST.

OATI webCARES will synchronize with at least one hardware NTP time source.

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 OIDs, are populated according to RFC 5280 and in cases where stipulations of RFC 5280 and the applicable CA/B Forum BRs differ, the CA/B Forum BRs notion will be adhered to. Only fields 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 Certificate Extensions

7.1.2.1 Root CA Certificate

- certificatePolicies: Not Present.
- basicConstraints: Present and marked as critical with the cA field set to True. There are no pathLenConstraints.
- keyUsage:
  - OATI WebCARES Root CA: Present, NOT marked as critical with bit positions for keyCertSign and cRLSign set.
  - OATI webCARES Root CA 2018: Present and marked as critical with bit positions for keyCertSign and cRLSign set.
- extKeyUsage: 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).

7.1.2.2 Issuing CA Certificate

- certificatePolicies: Present and NOT marked critical.
  - certificatePolicies:policyIdentifier: Present.
  - certificatePolicies:policyQualifiers:policyQualifierId: Present.
  - certificatePolicies:policyQualifiers:qualifier:cPSuri: Present.

- basicConstraints:
  - webCARES Issuing CA 2021: Not Present.
  - webCARES Issuing CA 2017: Not Present.
  - webCARES Issuing CA 2020: Present and marked as critical with the cA field set to True. There are no pathLenConstraints.
- 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).
- keyUsage:
  - webCARES Issuing CA 2021: Not Present.
  - webCARES Issuing CA 2017: Not Present.
  - webCARES Issuing CA 2020: Present and marked critical with bit positions for keyCertSign and cRLSign set.
- extKeyUsage: Present, NOT marked as critical.
  - webCARES Issuing CA 2021:
    - id-kp-clientAuth: Present.
  - webCARES Issuing CA 2017:
    - id-kp-clientAuth: Present.
  - webCARES Issuing CA 2020:
    - id-kp-serverAuth: Present.
    - id-kp-clientAuth: Present.
    - OCSP: Present.
    - MUST NOT include the anyExtendedKeyUsage KeyPurposeId.
- authorityKeyIdentifier:
  - webCARES Issuing CA 2021: Present, NOT marked as critical, and contains at a minimum a keyIdentifier field, authorityCertIssuer, or authorityCertSerialNumber field.
  - webCARES Issuing CA 2017: Present, NOT marked as critical, and contains at a minimum a keyIdentifier field, authorityCertIssuer, or authorityCertSerialNumber field.
  - webCARES Issuing CA 2020: Present, NOT marked as critical, and contains at a minimum a keyIdentifier field. Does NOT contain authorityCertIssuer or authorityCertSerialNumber field.

- 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).

7.1.2.3 Subscriber Certificate

- certificatePolicies: Present and NOT marked critical.
  - certificatePolicies:policyIdentifier: Present.
  - certificatePolicies:policyQualifiers:policyQualifierId: Present.
- basicConstraints: Not 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.
- extKeyUsage: Present and NOT marked critical. Either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present. MUST NOT contain the anyExtendedKeyUsage.
- authorityKeyIdentifier:
  - webCARES Issuing CA 2021: Present, NOT marked as critical, and contains at a minimum a keyIdentifier, authorityCertIssuer or authorityCertSerialNumber fields.
  - webCARES Issuing CA 2017: Present, NOT marked as critical, and contains at a minimum a keyIdentifier, authorityCertIssuer or authorityCertSerialNumber fields.
  - webCARES Issuing CA 2020: Present, NOT marked as critical, and contains at a minimum a keyIdentifier field. MUST NOT contain an authorityCertIssuer or authorityCertSerialNumber field.
- 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).

7.1.2.4 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 extKeyUsage 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, or
- Serial Numbers are generated with non-sequential numbers greater than zero containing at least 64 bits of output from a CSPRNG.

7.1.2.5 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.

7.1.3 Algorithm Object Identifiers

OATI does not issue any new Subscriber certificates, Subordinate CA certificates, or certificates to verify OCSP responses using the SHA-1 hash algorithm.

7.1.3.1 SubjectPublicKeyInfo

The following requirements apply to the subjectPublicKeyInfo field within a Certificate. No other encodings are permitted.

7.1.3.1.1 RSA

OATI indicates an RSA key using the rsaEncryption (OID: 1.2.840.113549.1.1.1) algorithm identifier.

The encoding for AlgorithmIdentifier for RSA keys is byte-for-byte identical with the following hex-encoded bytes: 300d06092a864886f70d0101010500.

7.1.3.2 Signature AlgorithmIdentifier

All objects signed by a CA Private Key will conform to these requirements on the use of the AlgorithmIdentifier or AlgorithmIdentifier-derived type in the context of signatures.

In particular, it applies to all of the following objects and fields:

- The signatureAlgorithm field of a Certificate.
- The signature field of a TBSCertificate (for example, as used by either a Certificate.
- The signatureAlgorithm field of a CertificateList
- The signature field of a TBSCertList
- The signatureAlgorithm field of a BasicOCSPResponse.

No other encodings are permitted for these fields.

7.1.3.2.1 RSA

The encoding for AlgorithmIdentifier for RSA keys is byte-for-byte identical with the following hex-encoded bytes: 300d06092a864886f70d0101010500.

7.1.4 Name Forms

7.1.4.1 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.

For every valid Certification Path (as defined by RFC 5280, Section 6):

- For each Certificate in the Certification Path, the encoded content of the Issuer Distinguished Name field of a Certificate is byte-for-byte identical with the encoded form of the Subject Distinguished Name field of the Issuing CA certificate.
- For each CA Certificate in the Certification Path, the encoded content of the Subject Distinguished Name field of a Certificate is byte-for-byte identical among all Certificates whose Subject Distinguished Names can be compared as equal according to RFC 5280, Section 7.1, and including expired and revoked Certificates.

7.1.4.2 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. Subject attributes MUST NOT contain **only** metadata such as '.', '-', and ' ' (i.e.

space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

7.1.4.2.1 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. The FQDN MUST consist solely of Domain Labels that are P-Labels or Non-Reserved LDH Labels. OATI confirms that the Applicant controls the FQDN or has been granted the right to use it by the Domain Name Registrant, as appropriate. Underscore characters are not permitted in server certificate dnSNames. The entry MUST NOT contain an Internal Name.

  For client certificates this extension will contain at minimum an email address which conforms to RFC 822 "Standard for the format of ARPA Internet Text Messages."

7.1.4.2.2 Subject Distinguished Name Fields

- **Certificate Field**: subject:commonName (OID 2.5.4.3)
  Required/Optional: Required.
  Contents: If present, for server certificates this field will contain a single FQDN. The value will be encoded as a character-for-character copy of the dNSName entry value from the subjectAltName extension. Specifically, all Domain Labels of the FQDN will be encoded as LDH Labels, and P-Labels MUST NOT be converted to their Unicode representation.

- **Certificate Field**: subject:organizationName (OID 2.5.4.10)
  Required/Optional: Required.
  Contents: The subject:organizationName field will contain either the Subject's Organization's name or DBA as verified under Section 3.2.2.2. 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:localityName (OID: 2.5.4.7)
  Required/Optional: Required

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

- **Certificate Field**: subject:stateOrProvinceName (OID: 2.5.4.8)
  Required/Optional: Required
  Contents: The subject:stateOrProvinceName field will contain the Subject's state or province information as verified under Section 3.2.2.1.

- **Certificate Field**: subject:postalCode (OID: 2.5.4.17)
  Required/Optional: Optional
  Contents: If present, the subject:postalCode field will contain the Subject's zip or postal information as verified under Section 3.2.2.1.

- **Certificate Field**: subject:countryName (OID: 2.5.4.6)
  Required/Optional: Required
  Contents: The subject:countryName will contain the two-letter ISO 3166-1 country code associated with the location of the Subject verified under Section 3.2.2.1.

- **Certificate Field**: subject:organizationalUnitName (OID: 2.5.4.11)
  Required/Optional: Optional.
  Prohibited if the subject:organizationName is absent or the certificate is issued on or after September 1, 2022.
  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.

- **Certificate Field**: 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.

- **Other Subject Attributes**

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

7.1.4.3 Subject Information – Root and 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.

7.1.4.3.1 Subject Distinguished Name Fields

- **Certificate Field**: subject:commonName (OID 2.5.4.3)
  Required/Optional: Required.
  Contents: This field MUST be present and the contents SHOULD be an identifier for the certificate such that the certificate's Name is unique across all certificates issued by the issuing certificate.

- **Certificate Field:** subject:organizationName (OID 2.5.4.10)
  Required/Optional: Required.
  Contents: This field MUST be present and the contents MUST contain either the Subject CA's name or DBA as verified under Section 3.2.2.2. The CA may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that the CA documents the difference and any abbreviations used are locally accepted abbreviations; e.g., if the official record shows "Company Name Incorporated", the CA MAY use "Company Name Inc." or "Company Name".

- **Certificate Field:** subject:countryName (OID: 2.5.4.6)
  Required/Optional: Required.
  Contents: This field MUST contain the two-letter ISO 3166-1 country code for the country in which the CA's place of business is located.

7.1.5 Name Constraints

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

7.1.6 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).

7.1.6.1 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

7.1.6.2 Root CA Certificates

webCARES Root CA 2018: The OATI Root CA Certificate does NOT contain the certificatePolicies extension.

OATI WebCARES Root CA: No stipulation.

7.1.6.3 Subordinate CA Certificates

No stipulation.

7.1.6.4 Subscriber Certificates

A Certificate issued to a Subscriber MUST contain, within the Certificate's certificatePolicies extension, one or more policy identifier(s) that are specified beneath the CA/Browser Forum's reserved policy OID arc of {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1)} (2.23.140.1). The Certificate MAY also contain additional policy identifier(s) defined by OATI.

OATI server certificates include the following Reserved Certificate Policy Identifier:

- **Certificate Policy Identifier:** 2.23.140.1.2.2
  - The Certificate complies with these Requirements and includes Subject Identity Information that is verified in accordance with Section 3.2.2.1. Such Certificates will also include organizationName, localityName (to the extent such field is required under

Section 7.1.4.2.2), stateOrProvinceName (to the extent such field is required under Section 7.1.4.2.2), and countryName in the Subject field.

7.1.7 Usage of Policy Constraints Extension

The Policy Constraints extension shall be empty.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profile

CRLs issued by OATI conform to RFC 5280 standards.

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 12 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.

7.2.1 Version Number(s)

All OATI webCARES CRLs are version 2 CRLs issued in compliance with RFC 5280.

7.2.2 CRL and CRL Entry Extensions

CRL Number: Consecutively increasing identification number for each CRL.

Authority Key Identifier: The Authority Key Identifier of the CA that issued the CRL.

CRL Reason Code: Reason for revocation for the certificate in question.

- reasonCode (OID 2.5.29.21): Present and NOT marked as critical.
  - The CRLReason indicated MUST NOT be unspecified (0).
  - The CRLReason MUST NOT be certificateHold (6).
  - The CRLReason MUST indicate the most appropriate reason for revocation of the certificate, as defined within this CPS.

7.3 OCSP Profile

If an OCSP response is for a Root CA or Subordinate CA Certificate, and that certificate has been revoked, then the revocationReason field within the RevokedInfo of the CertStatus will be present.

The CRLReason indicated will contain a value permitted for CRLs, as specified in Section 7.2.2.

7.3.1 Version Number(s)

OATI supports OCSP and its responders conform to the RFC 6960 standard.

7.3.2 OCSP Extensions

OATI identifies the OCSP responder within the AIA extension via an OCSP responder URL. The responder does not respond with a “good” status on certificates which have not been issued.

The singleExtensions of an OCSP response will NOT contain the reasonCode (OID 2.5.29.21) CRL entry extension.

8. Compliance Audit and Other Assessments

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 WebTrust Program for Certification Authorities (WebTrust for CAs). 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.

8.1 Frequency and Circumstances of Assessment

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

8.2 Identity/Qualifications of Assessor

The OATI webCARES annual examinations shall be conducted by an independent third-party Qualified Auditor. Qualified Auditors are able to demonstrate:

- Independence from the subject of the audit;
- The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme (see Section 8.0);
- Employment of individuals who have proficiency in examining PKI technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
- Licensure by WebTrust;
- Binding by law, government regulation, or professional code of ethics; and
- Except in the case of an Internal Government Auditing Agency, maintaining Professional Liability/Errors and Omissions insurance with policy limits of at least one million US dollars in coverage.

8.3 Assessor's Relationship to Assessed Entity

The Qualified Auditor selected shall be independent from OATI.

8.4 Topics Covered by Assessment

The external assessments shall conform to the current version of the following:

- WebTrust for Certificate Authorities Principles and Criteria
- WebTrust for Certificate Authorities - SSL Baseline with Network Security
- NAESB WEQ-012 Business Practice Standards
- CA/Browser Forum Baseline Requirements

8.4.1 Internal Audits

OATI also monitors adherence to its CPS, CA/B Forum BRs, NAESB WEQ-012, and WebTrust for CA 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 OATI webCARES Digital Certificates issued by OATI during the period commencing immediately after the previous self-audit sample was taken.

8.5 Actions Taken as a Result of Deficiency

If any deficiency is deemed to exist that causes OATI be non-compliant with applicable law, this CPS, or any standard listed in Section 8.4, an appropriate mitigation plan shall be developed and submitted to OATI management and then subsequently implemented. Disclosure of the deficiency shall be made to the external Qualified Auditor described in Section 8.2 during the annual examination timeframe.

8.6 Communications of Results

Results of the external audits noted in Section 8 are publicly available in the OATI webCARES Repository (www.oaticerts.com/repository). The audit reports may also be made available to applicable root browser programs and others as appropriate.

9. Other Business and Legal Matters

9.1 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.

9.1.1 Certificate Issuance or Renewal Fees

See Section 9.1 above.

9.1.2 Certificate Access Fees

See Section 9.1 above.

9.1.3 Revocation or Status Information Access Fees

See Section 9.1 above.

9.1.4 Fees for Other Services

See Section 9.1 above.

9.1.5 Refund Policy

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

9.2 Financial Responsibility

9.2.1 Insurance Coverage

OATI maintains insurance coverage in line with industry best practices for liabilities to other participants.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

OATI webCARES customers may reference the warranty provision within their OATI webCARES Customer Agreement.

9.3 Confidentiality of Business Information

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

9.3.1 Scope of Confidential Information

OATI webCARES customers may reference the nondisclosure section of their OATI webCARES Customer Agreement.

9.3.2 Information Not Within the Scope of Confidential Information

OATI webCARES customers may reference the nondisclosure section of their OATI webCARES Customer Agreement.

9.3.3 Responsibility to Protect Confidential Information

OATI webCARES customers may reference the nondisclosure section of their OATI webCARES Customer Agreement.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

OATI webCARES customers may reference the nondisclosure section of their OATI webCARES Customer Agreement.

9.4.2 Information Treated as Private

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

9.4.3 Information Not Deemed Private

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

9.4.4 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 noted in this CPS.

9.4.5 Notice and Consent to Use Private Information

OATI webCARES customers may reference the nondisclosure section of their OATI webCARES Customer Agreement.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

OATI webCARES customers may reference the nondisclosure section of their OATI webCARES Customer Agreement.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

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

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

OATI warrants that it has the authority to enter into OATI webCARES Agreements and provide the services specified in such agreements.

9.6.2 RA Representations and Warranties

No stipulation.

9.6.3 Subscriber Representations and Warranties

No stipulation.

9.6.4 Relying Party Representations and Warranties

No stipulation.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

OATI, 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.

Except as otherwise provided in Section 9.6 herein and as provided in the CA/B Forum BRs, OATI makes no other warranties of any kind.

9.8 Limitations of Liability

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 OATI webCARES, even if advised of the possibility of such damages.

Except as otherwise provided herein, under no circumstances will OATI or OATI 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.

9.9 Indemnities

9.9.1 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 OATI 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 OATI 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.

9.9.2 Indemnification by CA

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

9.10 Term and Termination

9.10.1 Term

This OATI CPS will remain in force until termination is communicated via the OATI webCARES Repository.

9.10.2 Termination

This OATI CPS will remain in force until termination is communicated via the OATI webCARES Repository.

9.10.3 Effect of Termination and Survival

OATI will communicate to customers via the OATI webCARES Repository in the event of termination of this CPS.

9.11 Individual Notices and Communications with Participants

OATI webCARES customers may reference the Notice section of their OATI webCARES Customer Agreement.

9.12 Amendments

9.12.1 Procedure for Amendment

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.

9.12.2 Notification Mechanism and Period

All changes to this CPS will be published appropriately in the OATI webCARES Repository.

9.12.3 Circumstances Under Which OID Must be Changed

No stipulation.

9.13 Dispute Resolution Provisions

No stipulation.

9.14 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.

9.15 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 CPA Canada 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.

9.16 Miscellaneous Provisions

OATI webCARES customers may reference the OATI webCARES Customer Agreement.

9.16.1 Entire 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 OATI 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.

9.16.2 Other Practice Statements and Agreements

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

9.16.3 Assignment

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

9.16.4 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.

9.16.5 Enforcement (Attorney's Fees and Waiver of Rights)

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.

9.17 Other Provisions

9.17.1 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.

9.17.2 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.

9.17.3 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.

9.17.4 Conditions of Usage of the OATI webCARES Repository and Website

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

9.17.5 Accuracy of Information

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

9.17.6 Ownership

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

9.17.7 Interpretation

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

9.17.8 Copyright Statement