OATI | INTO THE FUTURE

OPEN ACCESS TECHNOLOGY INTERNATIONAL, INC.

WEBCARES CERTIFICATION PRACTICE STATEMENT FOR OATI WEBCARES SERVER ROOT CA v2.2

SEPTEMBER 2026

This Certification Practice Statement is made available under the Creative Commons Attribution-No Derivatives 4.0 International (CC BY-ND 4.0) license.

OPEN ACCESS TECHNOLOGY INTERNATIONAL, INC.
7901 Computer Avenue | Bloomington, MN 55435 Phone 763.201.2000 | Fax 763.201.5333 | www.oati.com
©2026 Open Access Technology International, Inc.

Revision History

Version	Date	Comments	Author(s)
0.1	12/19/2025	Created new CPS specific to the OATI webCARES Server Root CA (used the draft version of the master OATI CPS v7.0 to create this CPS from)	OATI
0.2	12/29/2025	Revisions	OATI
1.0	12/31/2025	Approved	OATI
1.1	03/03/2026	Updates throughout, including: Require DNSSEC for CAA and DCV Lookups for Server certificates (SC085, SC094, SC096) Reduced Validity and Data Reuse Periods for Server certificates (SC081)	OATI
2.0	03/17/2026	Approved	OATI
2.1	06/30/2026	Updates to 1.2, 1.5.2.1, 4.3.1.3, 4.9.2, 4.9.13, 4.9.14, 4.9.15, 4.9.16, and 6.1.7	OATI
2.1	07/13/2026	Approved	OATI
2.2	08/07/2026 09/11/2026	SIVP Removals Added Chrome and CCADB Policy adherence Adjusted validity period and data reuse timeframes	OATI

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

Table of Contents

1. Introduction 10

1.1 OATI webCARES Overview 10
1.2 Document Name and Identification 11
1.3 PKI Participants 12
1.3.1 Certification Authorities 12
1.3.2 Registration Authorities 12
1.3.3 Subscribers 12
1.3.4 Relying Parties 13
1.3.5 Other Participants 13
1.4 Certificate Usage 14
1.4.1 Appropriate Certificate Uses 14
1.4.2 Prohibited Certificate Uses 14
1.5 Policy Administration 14
1.5.1 Organization Administering the Document 14
1.5.2 Contact Details 15
1.5.3 Person Determining CPS Suitability for the Policy 15
1.5.4 CPS Approval Procedures 15
1.6 Definitions and Acronyms 16
1.6.1 Acronyms 16
1.6.2 Glossary 18
1.6.3 Conventions 27

2. Publication and Repository Responsibilities 28

2.1 Repositories 28
2.2 Publication of Certification Information 28
2.3 Time or Frequency of Publication 28
2.4 Access Controls on Repositories 28

3. Identification and Authentication 29

3.1 Naming 29
3.1.1 Type of Names 29
3.1.2 Need for Names to be Meaningful 29
3.1.3 Anonymity or Pseudonymity of Subscribers 29
3.1.4 Rules for Interpreting Various Name Forms 29
3.1.5 Uniqueness of Names 29
3.1.6 Recognition, Authentication, and Role of Trademarks 30
3.2 Initial Identity Validation 30
3.2.1 Method to Prove Possession of Private Key 30
3.2.2 Authentication of Organization and Domain Identity 30
3.2.3 Authentication of Individual Identity 37
3.2.4 Non-Verified Subscriber Information 37
3.2.5 Validation of Authority 37
3.2.6 Criteria for Interoperation 37
3.3 Identification and Authentication for Rekey Requests 38
3.3.1 Identification and Authentication for Routine Rekey 38
3.3.2 Identification and Authentication for Rekey After Revocation 38
3.4 Identification and Authentication for Revocation Request 38
3.4.1 Requests Made by Security Officers 38

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

3.4.2 Requests Made by Subscribers 38

4. Certificate Lifecycle Operational Requirements 39

4.1 Certificate Application 39
4.1.1 Who Can Submit a Certificate Application 39
4.1.2 Enrollment Process and Responsibilities 39
4.2 Certificate Application Processing 39
4.2.1 Performing Identification and Authentication Functions 39
4.2.2 Approval or Rejection of Certificate Applications 40
4.2.3 Time to Process Certificate Applications 40
4.2.4 OATI webCARES Digital Certificate Distribution 40
4.2.5 CAA Records 40
4.3 Certificate Issuance 41
4.3.1 CA Actions During Certificate Issuance 41
4.3.2 Notifications to Subscriber by OATI of Issuance of Certificate 42
4.4 Certificate Acceptance 42
4.4.1 Conduct Constituting Certificate Acceptance 42
4.4.2 Publication of the Certificate by OATI 43
4.4.3 Notification of Certificate Issuance by OATI to Other Entities 43
4.5 Key Pair and Certificate Usage 43
4.5.1 Subscriber Private Key and Certificate Usage 43
4.5.2 Relying Party Public Key and Certificate Usage 44
4.6 Certificate Renewal 44
4.6.1 Circumstances for Certificate Renewal 45
4.6.2 Who May Request Renewal 45
4.6.3 Processing Certificate Renewal Requests 45
4.6.4 Notification of New Certificate Issuance to Subscriber 45
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 45
4.6.6 Publication of the Renewal Certificate by OATI 46
4.6.7 Notification of Certificate Issuance by OATI to Other Entities 46
4.7 Certificate Rekey 46
4.7.1 Circumstances for Certificate Rekey 46
4.7.2 Who May Request Certification of a New Public Key 46
4.7.3 Processing Certificate Rekeying Requests 46
4.7.4 Notification of New Certificate Issuance to Subscriber 46
4.7.5 Conduct Constituting Acceptance of a Rekeyed Certificate 46
4.7.6 Publication of the Rekeyed Certificate by OATI 46
4.7.7 Notification of Certificate Issuance by OATI to Other Entities 46
4.8 Certificate Modification 47
4.8.1 Circumstances for Certificate Modification 47
4.8.2 Who May Request Certificate Modification 47
4.8.3 Processing Certificate Modification Requests 47
4.8.4 Notification of New Certificate Issuance to Subscriber 47
4.8.5 Conduct Constituting Acceptance of Modified Certificate 47
4.8.6 Publication of the Modified Certificate by OATI 47
4.8.7 Notification of Certificate Issuance by OATI to Other Entities 47
4.9 Certificate Revocation and Suspension 47
4.9.1 Circumstances for Revocation 48
4.9.2 Who Can Request Revocation 50
4.9.3 Procedure for Revocation Request 52

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

4.9.4 Revocation Request Grace Period 52
4.9.5 Time Within Which CA Must Process the Revocation Request 52
4.9.6 Revocation Checking Requirements for Relying Parties 52
4.9.7 CRL Issuance Frequency 52
4.9.8 Maximum Latency for CRLs 52
4.9.9 Online Revocation/Status Checking Availability 53
4.9.10 Online Revocation Checking Requirements 53
4.9.11 Other Forms of Revocation Advertisements Available 53
4.9.12 Special Requirements re Key Compromise 53
4.9.13 Circumstances for Suspension 53
4.9.14 Who Can Request Suspension 53
4.9.15 Procedure for Suspension Request 54
4.9.16 Limits on Suspension Period 54
4.10 Certificate Status Services 54
4.10.1 Operational Characteristics 54
4.10.2 Service Availability 54
4.10.3 Operational Features 54
4.11 End of Subscription 54
4.12 Key Escrow and Recovery 54
4.12.1 Key Escrow and Recovery Policy and Practices 54
4.12.2 Session Key Encapsulation and Recovery Policy and Practices 54

5. Facility, Management, and Operational Controls 55

5.1 Physical Security Controls 55
5.1.1 Site Location and Construction 55
5.1.2 Physical Access 56
5.1.3 Power and Air Conditioning 57
5.1.4 Water Exposures 58
5.1.5 Fire Prevention and Protection 58
5.1.6 Media Storage 59
5.1.7 Waste Disposal 59
5.1.8 Off-Site Backup 59
5.2 Procedural Controls 59
5.2.1 Trusted Roles 59
5.2.2 Number of Persons Required per Task 60
5.2.3 Identification and Authentication for Each Role 60
5.2.4 Roles Requiring Separation of Duties 61
5.3 Personnel Controls 62
5.3.1 Qualifications, Experience, and Clearance Requirements 62
5.3.2 Background Check Procedures 62
5.3.3 Training Requirements 63
5.3.4 Retraining Frequency and Requirements 63
5.3.5 Job Rotation Frequency and Sequence 63
5.3.6 Sanctions for Unauthorized Actions 63
5.3.7 Independent Contractor Requirements 63
5.3.8 Documentation Supplied to Personnel 63
5.4 Audit Logging Procedures 64
5.4.1 Types of Events Recorded 64
5.4.2 Frequency of Processing Log 65
5.4.3 Retention Period for Audit Log 65

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

5.4.4 Protection of Audit Log 66
5.4.5 Audit Log Backup Procedures 66
5.4.6 Audit Collection System (Internal vs. External) 66
5.4.7 Notification to Event-Causing Subject 66
5.4.8 Vulnerability Assessments 66
5.5 Records Archival 67
5.5.1 Types of Records Archived 67
5.5.2 Retention Period for Archive 67
5.5.3 Protection of Archive 68
5.5.4 Archive Backup Procedures 68
5.5.5 Requirements for Time-Stamping of Records 68
5.5.6 Archive Collection System (Internal or External) 68
5.5.7 Procedures to Obtain and Verify Archive Information 69
5.6 Key Changeover 69
5.7 Compromise and Disaster Recovery 69
5.7.1 Incident and Compromise Handling Procedures 69
5.7.2 Computing Resources, Software, and/or Data Are Corrupted 70
5.7.3 Entity Private Key Compromise Procedures 70
5.7.4 Business Continuity Capabilities After a Disaster 70
5.8 CA or RA Termination 70

6. Technical Security Controls 71

6.1 Key Pair Generation and Installation 71
6.1.1 Key Pair Generation 71
6.1.2 Private Key Delivery to Subscriber 72
6.1.3 Public Key Delivery to Certificate Issuer 73
6.1.4 CA Public Key Delivery to Relying Parties 73
6.1.5 Key Sizes 73
6.1.6 Public Key Parameters Generation and Quality Checking 73
6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field) 73
6.2 Private Key Protection and Cryptographic Module Engineering Controls 73
6.2.1 Cryptographic Module Standards and Controls 73
6.2.2 Private Key (n out of m) Multi-Person Control 74
6.2.3 Private Key Escrow 74
6.2.4 Private Key Backup 74
6.2.5 Private Key Archival 74
6.2.6 Private Key Transfer Into or From a Cryptographic Module 75
6.2.7 Private Key Storage on Cryptographic Module 75
6.2.8 Method of Activating Private Key 76
6.2.9 Method of Deactivating Private Key 76
6.2.10 Method of Destroying Private Key 76
6.2.11 Cryptographic Module Rating 76
6.3 Other Aspects of Key Pair Management 76
6.3.1 Public Key Archival 76
6.3.2 Certificate Operational Periods and Key Pair Usage Periods 77
6.4 Activation Data 77
6.4.1 Activation Data Generation and Installation 77
6.4.2 Activation Data Protection 77
6.4.3 Other Aspects of Activation Data 77
6.5 Computer Security Controls 78

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

6.5.1 Specific Computer Security Technical Requirements 78
6.5.2 Computer Security Rating 78
6.6 Lifecycle Technical Controls 78
6.6.1 System Development Controls 78
6.6.2 Security Management Controls 80
6.6.3 Lifecycle Security Controls 80
6.7 Network Security Controls 80
6.7.1 Anti-Virus 80
6.7.2 Vulnerability Remediation 80
6.8 Time-Stamping 81

7. Certificate and CRL Profiles 82

7.1 Certificate Profile 82
7.1.1 Version Number(s) 82
7.1.2 Certificate Content and Extensions 82
7.1.3 Algorithm Object Identifiers 86
7.1.4 Name Forms 87
7.1.5 Name Constraints 88
7.1.6 Certificate Policy Object Identifier 88
7.1.7 Usage of Policy Constraints Extension 89
7.1.8 Policy Qualifiers Syntax and Semantics 89
7.1.9 Processing Semantics for the Critical Certificate Policies Extension 89
7.2 CRL Profile 89
7.2.1 Version Number(s) 89
7.2.2 CRL and CRL Entry Extensions 89
7.3 OCSP Profile 92
7.3.1 Version Number(s) 92
7.3.2 OCSP Extensions 92

8. Compliance Audit and Other Assessments 93

8.1 Frequency and Circumstances of Assessment 93
8.2 Identity/Qualifications of Assessor 93
8.3 Assessor's Relationship to Assessed Entity 94
8.4 Topics Covered by Assessment 94
8.4.1 Internal Audits 94
8.5 Actions Taken as a Result of Deficiency 94
8.6 Communications of Results 94
8.7 Self-Audits 95

9. Other Business and Legal Matters 96

9.1 Fees 96
9.1.1 Certificate Issuance or Renewal Fees 96
9.1.2 Certificate Access Fees 96
9.1.3 Revocation or Status Information Access Fees 96
9.1.4 Fees for Other Services 96
9.1.5 Refund Policy 96
9.2 Financial Responsibility 96
9.2.1 Insurance Coverage 96
9.2.2 Other Assets 96
9.2.3 Insurance or Warranty Coverage for End-Entities 96

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

9.3 Confidentiality of Business Information 97
9.3.1 Scope of Confidential Information 97
9.3.2 Information Not Within the Scope of Confidential Information 97
9.3.3 Responsibility to Protect Confidential Information 97
9.4 Privacy of Personal Information 97
9.4.1 Privacy Plan 97
9.4.2 Information Treated as Private 97
9.4.3 Information Not Deemed Private 97
9.4.4 Responsibility to Protect Private Information 97
9.4.5 Notice and Consent to Use Private Information 98
9.4.6 Disclosure Pursuant to Judicial or Administrative Process 98
9.4.7 Other Information Disclosure Circumstances 98
9.5 Intellectual Property Rights 98
9.6 Representations and Warranties 98
9.6.1 CA Representations and Warranties 98
9.6.2 RA Representations and Warranties 98
9.6.3 Subscriber Representations and Warranties 98
9.6.4 Relying Party Representations and Warranties 98
9.6.5 Representations and Warranties of Other Participants 99
9.7 Disclaimers of Warranties 99
9.8 Limitations of Liability 99
9.9 Indemnities 99
9.9.1 Indemnification by Subscribers 99
9.9.2 Indemnification by CA 100
9.10 Term and Termination 100
9.10.1 Term 100
9.10.2 Termination 100
9.10.3 Effect of Termination and Survival 100
9.11 Individual Notices and Communications with Participants 100
9.12 Amendments 100
9.12.1 Procedure for Amendment 100
9.12.2 Notification Mechanism and Period 100
9.12.3 Circumstances Under Which OID Must be Changed 100
9.13 Dispute Resolution Procedures 101
9.14 Governing Law 101
9.15 Compliance with Applicable Standards and Laws 101
9.16 Miscellaneous Provisions 101
9.16.1 Entire Agreement 101
9.16.2 Assignment 101
9.16.3 Severability 102
9.16.4 Enforcement (Attorney's Fees and Waiver of Rights) 102
9.16.5 Force Majeure 102
9.17 Other Provisions 102
9.17.1 Legality of Information 102
9.17.2 Subscriber Liability to Relying Parties 102
9.17.3 Use of Agents 102
9.17.4 Conditions of Usage of the OATI webCARES Repository and Website 103
9.17.5 Accuracy of Information 103
9.17.6 Ownership 103
9.17.7 Interpretation 103

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

9.17.8 Copyright Statement..... 103
9.17.9 Other Practice Statements and Agreements 104

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

1. Introduction

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

This CP/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 - TLS 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 CP/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.

This CP/CPS conforms to and incorporates the requirements of the latest applicable versions of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Certificates and the CA/Browser Forum Network and Certificate System Security Requirements, as applicable to the certificate types and services provided by OATI webCARES.

In addition, OATI webCARES attests that it adheres to the latest applicable versions of the following policies and program requirements.

- CCADB Policy – https://www.ccadb.org/policy
- Chrome Root Policy – https://googlechrome.github.io/chromerootprogram/

OATI webCARES monitors revisions to these policies and requirements and implements applicable changes within the applicable effective dates and timelines.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

This CP/CPS applies exclusively to the OATI webCARES Server Root CA and the subordinate CA hierarchy issued beneath that Root CA, including the OATI webCARES Server Issuing CA 2026. This hierarchy is dedicated exclusively to the issuance of publicly trusted TLS server authentication certificates. This CP/CPS does not govern any other OATI webCARES root, subordinate CA, certificate hierarchy, or certificate type unless expressly identified herein.

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.

OATI is a United States based solutions provider that empowers organizations around the world to solve their operational business challenges through advanced technologies. OATI's solutions enable customers to perform trading, perform transaction management, integrate to other solutions, and provide flexibility through configurable applications. OATI's rapid growth globally is a testament to the breadth of solutions provided. OATI intends to provide our customers (and the large amount of potential users) an opportunity to easily and safely utilize OATI offerings through their browsers, phones, or any other form of access.

1.2 Document Name and Identification

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

OATI assigns the following OIDs:

OID	Description
2.23.140.1.2.2	Organization Validated (OV) Certificates Policy OID
1.2.840.114278.11.1	OATI Certificates Policy OID
2.16.840.1.114505.1.12.2.2	NAES Basic Assurance Certificate Policy OID

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

1.3 PKI Participants

This CP/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 - TLS Baseline with Network Security), and in accordance with other applicable industry standards such as NAESB WEQ-012 and the CA/B Forum.

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.
- OATI webCARES Server Root CA does not issue end-entity certificates. The root CA is used solely to issue and sign certificates for subordinate CAs. All publically-trusted TLS certificates are issued exclusively by subordinate CAs.

1.3.2 Registration Authorities

The OATI RA may delegate RA duties to LRAs. 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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

1.3.3.2 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 Organization. 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 organization, 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 Non-Enterprise RA

OATI does not use Non-Enterprise RAs.

1.3.5 Other Participants

OATI does not have any other participants.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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 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).

The OATI webCARES Server Root CA is operated as a publicly-trusted Certification Authority intended for general Internet use and issuance of publicly-trusted TLS server certificates in accordance with the CA/Browser Forum Baseline Requirements.

OATI shall not issue certificates for client authentication, code signing , document signing or any other certificates except TLS server certificate under OATI webCARES Server Root CA.

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 once every 365 days 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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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
7901 Computer Ave
Bloomington, MN 55435
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), the Contact Us form located in the OATI webCARES repository, 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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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 TLS Server 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

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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.

Applicant Representative: A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant:

i. who signs and submits, or approves a certificate request on behalf of the Applicant, and/or
ii. who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or
iii. who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of OATI.

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

Attestation Letter: A letter attesting that Subject Information is correct written by an accountant, lawyer, and government official, or other reliable third party customarily relied upon for such information.

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

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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 within the Organization. See also Security Officer.

Certificate: An electronic document that uses a digital signature to bind a public key and an identity.

Certificate Authority: An organization that is responsible for the creation, issuance, distribution, renewal, rekey, and revocation of Certificates.

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

Certificate Data: Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in OATI's possession or control or to which OATI has access.

Certificate Management Process: Processes, practices, and procedures associated with the use of keys, software, and hardware, by which OATI verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.

Certificate Manufacturing Authority (Issuing Authority): An entity responsible for Signing and Issuing OATI webCARES Digital Certificates.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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

Certificate Profile: A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7 of this CPS or a certificate template file used by CA software.

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

Certification Authority: An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Root CAs and Subordinate CAs.

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."

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

Critical Certificate Authority Operations: Management of the Digital Certificate lifecycle, which includes generation and issuance, distribution, renewal and reissuance, and revocation of OATI'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.

Delegated Third Party: A natural person or Legal Entity that is not OATI but is authorized by OATI, and whose activities are not within the scope of the appropriate CA audits, to assist in

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

the Certificate Management Process by performing or fulfilling one or more of OATI requirements found herein.

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 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).

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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 Relying Parties and Subscribers.

Enterprise RA: An employee or Agent of an organization unaffiliated with OATI 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.

High Risk Certificate Request: A Request that OATI flags for additional scrutiny by reference to internal criteria and databases maintained by OATI, which may include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or the Google Safe Browsing list, or names that OATI identifies using its own risk-mitigation criteria.

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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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."

Legal Entity: An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.

Linting: A process in which the content of digitally signed data such as a Precertificate [RFC 6962], Certificate, Certificate Revocation List, or OCSP response, or data-to-be-signed object such as a tbsCertificate (as described in RFC 5280, Section 4.1.1.1) is checked for conformance with the profiles and requirements defined in this CPS.

Multi-Perspective Issuance Corroboration: A process by which the determinations made during domain validation and CAA checking by the Primary Network Perspective are corroborated by other Network Perspectives before Certificate issuance.

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

Network Perspective: Related to Multi-Perspective Issuance Corroboration. A system (e.g., a cloud-hosted server instance) or collection of network components (e.g., a VPN and corresponding infrastructure) for sending outbound Internet traffic associated with a domain control validation method and/or CAA check. The location of a Network Perspective is determined by the point where unencapsulated outbound Internet traffic is typically first handed off to the network infrastructure providing Internet connectivity to that perspective.

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."

OCSP Responder: An online server operated under the authority of OATI and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

Online Certificate Status Protocol: An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate. See also OCSP Responder.

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.

Primary Network Perspective: The Network Perspective used by the CA to make the determination of 1) the CA's authority to issue a Certificate for the requested domain(s) or IP address(es) and 2) the Applicant's authority and/or domain authorization or control of the requested domain(s) or IP address(es).

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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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

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

Reliable Data Source: An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.

Reliable Method of Communication: A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.

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 OATI, 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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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

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.

Short-lived Subscriber Certificate: For Certificates issued on or after March 15, 2024 and prior to March 15, 2026, a Subscriber Certificate with a Validity Period less than or equal to 10 days (864,000 seconds). For Certificates issued on or after March 15, 2026, a Subscriber Certificate with a Validity Period less than or equal to 7 days (604,800 seconds).

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 or an IP Address 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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

Subscriber Agreement: An agreement between OATI and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.

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.

Validity Period: From RFC 5280 (http://tools.ietf.org/html/rfc5280): "The period of time from notBefore through notAfter, inclusive."

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."

1.6.3 Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this CPS shall be interpreted in accordance with RFC 2119.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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 once every 365 days.

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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

3. Identification and Authentication

3.1 Naming

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

OATI Root Certificates:

- OATI webCARES Server Root CA

OATI Intermediate Certificates:

- OATI webCARES Server Issuing CA 2026

3.1.1 Type of Names

OATI webCARES Certificates with subject DNs (Distinguished Names) are based upon the X.500 naming standards.

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

Distinguished names in OATI webCARES certificates are interpreted using X.500 standards and ASN.1 syntax. See RFC 2253 and RFC 2616 for further information on how X.500 distinguished names in Certificates are interpreted as Uniform Resource Identifiers and HTTP references.

3.1.5 Uniqueness of Names

OATI webCARES Certificates subject attributes must be unique.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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

No stipulation.

3.2.2 Authentication of Organization and Domain 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.

OATI webCARES SHALL not issue certificates containing internal names or Reserved IP addresses, as prohibited by CA/Browser Forum Baseline Requirements.

3.2.2.1 Identity

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 Authentication. The SIVP includes, but is not limited to:

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

- 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.

Prior to using any data source as a Reliable Data Source, OATI shall evaluate the source for its reliability, accuracy, and resistance to alteration or falsification. OATI shall consider the following during its evaluation:

1. The age of the information provided,
2. The frequency of updates to the information source,
3. The data provider and purpose of the data collection,
4. The public accessibility of the data availability, and
5. The relative difficulty in falsifying or altering the data.

OATI uses one primary means to verify organizations/domain Applicants, which is DNS Change – please see section 3.2.2.4.7.

3.2.2.2 DBA/Tradename

In addition to the verification required under 3.2.2.1, the DBA itself would require a letter on company letterhead from the customer and the company they are attempting to do business as. This is then sent to the OATI Contracts team and they would state the DBA relationship.

3.2.2.3 Verification of Country

See section 3.2.2.1.

3.2.2.4 Validation of Domain Authorization or Control

3.2.2.4.1 Validating the Applicant as a Domain Contact

OATI does not use this method of domain validation.

3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact

OATI does not use this method of domain validation.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

3.2.2.4.3 Phone Contact with Domain Contact

OATI does not use this method of domain validation.

3.2.2.4.4 Constructed Email to Domain Contact

OATI does not use this method of domain validation.

3.2.2.4.5 Domain Authorization Document

OATI does not use this method of domain validation.

3.2.2.4.6 Agreed-Upon Change to Website

OATI does not use this method of domain validation.

3.2.2.4.7 DNS Change

OATI shall confirm an Applicant's control over a Fully Qualified Domain Name (FQDN) using a DNS Change validation method in accordance with CA/Browser Forum Baseline Requirements (BR) Section 3.2.2.4.7. OATI shall verify that the Applicant has placed a Random Value or Request Token in the Domain Name System (DNS) as a TXT record at an Authorization Domain Name, as defined in the Baseline Requirements using manual or automated mechanisms using ACME validation (dns-01) method (an Authorization Domain Name prefixed with a Domain Label beginning with an underscore character).

OATI shall support the ACME dns-01 challenge method as defined in RFC 8555, Section 8.4, and as permitted by BR 3.2.2.4.7.

When using ACME dns-01 validation:

1. OATI shall generate a Request Token bound to the corresponding certificate request, in accordance with BR 3.2.2.4.
2. The Applicant shall provision the Request Token as a DNS TXT record at _acme-challenge.
3. OATI shall retrieve the DNS TXT record and verify that the correct Request Token is present prior to certificate issuance.
4. Successful completion of the dns-01 challenge shall constitute confirmation of the Applicant's control over the FQDN.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

If a Random Value is used, the OATI shall provide a Random Value unique to the Certificate request and shall not use the Random Value after

i. 30 days, or
ii. If the Applicant submitted the Certificate request, the time frame permitted for reuse of validated information relevant to the Certificate (such as in Section 4.2.1 of this CPS).

Note: Once the FQDN has been validated using this method, OATI may also issue Certificates for other FQDNs that end with all the Domain Labels of the validated FQDN.

For this method, OATI also utilizes Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.4.7.1. To count as corroborating, a Network Perspective MUST observe the same challenge information (i.e. Random Value Request Token) as the Primary Network Perspective.

Effective March 15, 2026, for TLS Server certificates DNSSEC validation is performed in accordance with CAB Baseline Requirements for TLS section 3.2.2.8.1. DNSSEC validation back to the IANA DNSSEC root trust anchor MUST be performed on all DNS queries associated with the validation of domain authorization or control by the Primary Network Perspective and CAs MUST NOT use local policy to disable DNSSEC validation on any DNS query associated with the validation of domain authorization or control.

3.2.2.4.7.1 Multi-Perspective Issuance Corroboration (MPIC)

OATI has implemented MPIC in conformance with the CA/B Baseline Requirements.

MPIC attempts to corroborate the determinations (i.e., domain validation pass/fail) made by the Primary Network Perspective from multiple remote Network Perspectives before Certificate issuance. This process can improve protection against equally-specific prefix Border Gateway Protocol (BGP) attacks or hijacks.

The set of responses from the relied upon Network Perspectives MUST provide OATI with the necessary information to allow it to affirmatively assess: - a. the presence of the expected 1) Random Value, or 2) Request Token, as required by the relied upon validation method specified in Section 3.2.2.2 and b. OATI’s authority to issue to the requested domain(s), as specified in Section 4.2.5.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

Results or information obtained from one Network Perspective are not reused or cached when performing validation through subsequent Network Perspectives (e.g., different Network Perspectives cannot rely on a shared DNS cache to prevent an adversary with control of traffic from one Network Perspective from poisoning the DNS cache used by other Network Perspectives). The network infrastructure providing Internet connectivity to a Network Perspective MAY be administered by the same organization providing the computational services required to operate the Network Perspective. All communications between a remote Network Perspective and OATI MUST take place over an authenticated and encrypted channel relying on modern protocols (e.g., over HTTPS).

A Network Perspective MAY use a recursive DNS resolver that is NOT co-located with the Network Perspective. However, the DNS resolver used by the Network Perspective MUST fall within the same Regional Internet Registry service region as the Network Perspective relying upon it. Furthermore, for any pair of DNS resolvers used on a Multi-Perspective Issuance Corroboration attempt, the straight-line distance between the two DNS resolvers MUST be at least 500 km. The location of a DNS resolver is determined by the point where unencapsulated outbound DNS queries are typically first handed off to the network infrastructure providing Internet connectivity to that DNS resolver.

If MPIC does not corroborate, OATI may immediately retry MPIC using the same validation method or an alternative method. When retrying, OATI does not rely on corroborations from previous attempts. There is no stipulation regarding the maximum number of validation attempts that may be performed in any period of time.

Network Perspectives are considered distinct when the straight-line distance between them is at least 500 km. Network Perspectives are considered “remote” when they are distinct from the Primary Network Perspective and the other Network Perspectives represented in a quorum.

OATI has implemented MPIC using at least five remote Network Perspectives. OATI does not proceed with certificate issuance if the number of non-corroborations is greater than one and if the remote Network Perspectives that do corroborate the determinations made by the Primary Network Perspective do not fall within the service regions of at least two distinct Regional Internet Registries.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

The Remote Network Perspectives performing MPIC MUST rely upon networks implementing measures to mitigate BGP routing incidents in the global Internet routing system for providing internet connectivity to the Network Perspective.

Beyond the above considerations, computing systems performing MPIC are considered outside of the audit scope described in Section 8.

If any of the above considerations are performed by a Delegated Third Party, OATI MAY obtain reasonable evidence from the Delegated Third Party to ascertain assurance that one or more of the above considerations are followed. As an exception to Section 1.3.2, Delegated Third Parties are not required to be within the audit scope described in Section 8 to satisfy the above considerations.

3.2.2.4.8 IP Address

OATI does not use this method of domain validation.

3.2.2.4.9 Test Certificate

OATI does not use this method of domain validation.

3.2.2.4.10 TLS Using a Random Value

OATI does not use this method of domain validation.

3.2.2.4.11 Any Other Method

OATI does not use any other methods of domain validation that are not detailed in the CPS.

3.2.2.4.12 Validating Applicant as a Domain Contact

OATI does not use this method of domain validation.

3.2.2.4.13 Email to DNS CAA Contact

OATI does not use this method of domain validation.

3.2.2.4.14 Email to DNS TXT Contact

OATI does not use this method of domain validation.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

3.2.2.4.15 Phone Contact with Domain Contact

OATI does not use this method of domain validation.

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact

OATI does not use this method of domain validation.

3.2.2.4.17 Phone Contact with DNS CAA Phone Contact

OATI does not use this method of domain validation.

3.2.2.4.18 Agreed-Upon Change to Website v2

OATI does not use this method of domain validation.

3.2.2.4.19 Agreed-Upon Change to Website - ACME

OATI does not use this method of domain validation.

3.2.2.4.20 TLS Using ALPN

OATI does not use this method of domain validation.

3.2.2.4.21 DNS Labeled with Account ID - ACME

OATI does not use this method of domain validation.

3.2.2.4.22 DNS TXT Record with Persistent Value

OATI does not use this method of domain validation.

3.2.2.5 Authentication for an IP Address

No IP address certificates are issued under this CPS or PKI hierarchy described herein.

3.2.2.6 Wildcard Domain Validation

OATI does not issue wildcard certificates.

3.2.2.7 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, OATI SHALL evaluate the source for its reliability, accuracy, and resistance to alteration or falsification. OATI also considers at least the following during its evaluation:

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

1. The age of the information provided,
2. The frequency of updates to the information source,
3. The data provider and purpose of the data collection,
4. The public accessibility of the data availability, and
5. The relative difficulty in falsifying or altering the data.

3.2.2.8 CAA Records

Please see section 4.2.5.

3.2.2.9 Multi-Perspective Issuance Corroboration

Please see section 3.2.2.4.7.1.

3.2.3 Authentication of Individual Identity

Not Applicable.

OATI webCARES CA does not issue individual validated TLS Server certificates to natural persons.

OATI webCARES CA issues Organization Validated (OV) Server Certificates to legal entities/organizations in accordance with the applicable requirements of Section 3.2.2.

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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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

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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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

OATI maintains a list of safe countries and blocks other connection requests via firewalls. Entities may submit certificate application requests through either Automatic Certificate Management Environment (ACME) protocol or through the webCARES GUI. Issuance of certificates is dependent on successful validation method and compliance with OATI policies.

4.1.2 Enrollment Process and Responsibilities

Certificate enrollment is initiated by an authorized Security Officer (SO) acting as a Local Registration Authority (LRA). All certificate requests MUST include a valid Certificate Signing Request (CSR). The SO submits the CSR through the OATI webCARES system. OATI webCARES validates the CSR and confirms that the Subject and domain information contained in the request is consistent with verified Applicant information. The information contained in the CSR SHALL NOT override verified identity, organization, or domain authorization data.

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 maintains systems and processes to sufficiently authenticate the Applicant's identity in compliance with this CP/CPS.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

Initial identity vetting is performed by the OATI validation team as set forth in Section 3 or by Registration Authorities. All communications sent through as emails are securely stored along with all information presented directly by the Applicant via the OATI web interface or API.

Future requests for certificates are authenticated using multi-factor (Certificate in combination with username/password) authentication techniques.

OATI webCARES may use the documents and data provided in Section 3.2 to verify Organization and Applicant information, or may reuse previous validations themselves, provided that:

1. Subject Identity Information Validation
    - The reuse period is not greater than 398 days;
2. Domain Control Validation
    - The reuse period is not greater than 200 days.
    - For Server Certificates issued on or after March 15, 2027, the reuse period will not be greater than 100 days.
    - For Server Certificates issued on or after March 15, 2029, the reuse period will not be greater than 10 days.

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 may reject applications that fail to meet documented policy, technical, or validation requirements.

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 retrieves and processes CAA records for the URL specified in the commonName field (which is also used in the

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

subjectAltName extension of the server certificate to be issued), following the processing instructions set forth in RFC 8659 and in accordance with section 3.2.2.8 of the Baseline Requirements, for any records found. If this check (and all others) pass, OATI webCARES will issue the server certificate within the Time to Live (TTL) of the CAA record, or 8 hours, whichever is greater.

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.
- Support both Primary CAA and MPIC CAA validation to ensure proper authorization before certificate issuance.
- Support “accounturi” and “validationmethods” parameters extensions to CAA Record per RFC 8657.
- All relevant CAA record processing actions taken, if any, are audited.
- Effective March 15, 2026, for TLS Server certificates, DNSSEC validation is performed in accordance with CAB Baseline Requirements for TLS section 3.2.2.8.1.

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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

4.3.1.1 Manual Authorization of Certificate Issuance for Root CAs

Root certificate issuance by OATI shall require an individual authorized by OATI (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for OATI to perform a certificate signing operation.

4.3.1.2 Linting of To-Be-Signed Certificate Content

OATI has implemented a Linting process to test the technical conformity of each to-be-signed artifact prior to signing it. When a Precertificate has undergone Linting, it is not necessary for the corresponding to-be-signed Certificate to also undergo Linting, provided that OATI has a technical control to verify that the to-be-signed Certificate corresponds to the to-be-signed Precertificate in the manner described by RFC 6962, Section 3.2. Methods used to produce a certificate containing the to-be-signed Certificate content include, but are not limited to:

- Sign the tbsCertificate with a "dummy" Private Key whose Public Key component is not certified by a Certificate that chains to a publicly-trusted CA Certificate; or
- Specify a static value for the signature field of the Certificate ASN.1 SEQUENCE.

OATI uses the Linting tools that have been widely adopted by the industry (see https://cabforum.org/resources/tools/).

4.3.1.3 Linting of Issued Certificates

OATI may use a Linting process to test each issued Certificate.

4.3.2 Notifications to Subscriber by OATI 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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

- 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 OATI

All publically trusted TLS certificates issued by OATI webCARES SHALL be submitted to at least two independent, qualified Certificate Transparency logs prior to issuance, in accordance with CA/Browser Forum Baseline Requirements.

4.4.3 Notification of Certificate Issuance by OATI 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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

- 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. For each renewal request, a BRAF-verified Signing Officer (SO) must confirm, by selecting the designated checkbox that the information contained in the previously issued Certificate remains current, accurate, and valid for the issuance of a new

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

OATI webCARES Digital Certificate. By selecting this checkbox, the SO affirms that they have re-verified the identity and legitimacy of the person, machine, or device to which the OATI webCARES Digital Certificate is being issued, in accordance with the OATI Certification Practice Statement (CPS) and the CA/Browser Forum Baseline Requirements.

No data or documentation shall be accepted for verification purposes beyond the applicable validation reuse period as defined in Section 4.2.1.

Renewed OATI webCARES Digital Certificates are issued with a new validity period, as defined in Section 6.3.2, and contain the same subject information as the previously issued 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.

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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

4.6.6 Publication of the Renewal Certificate by OATI

All publically trusted TLS certificates issued by OATI webCARES SHALL be submitted to at least two independent, qualified Certificate Transparency logs prior to issuance, in accordance with CA/Browser Forum Baseline Requirements.

4.6.7 Notification of Certificate Issuance by OATI 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 OATI

Not applicable.

4.7.7 Notification of Certificate Issuance by OATI to Other Entities

Not applicable.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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 OATI

See Section 4.6.6.

4.8.7 Notification of Certificate Issuance by OATI 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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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.

OATI does not permit certificate suspension.

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 (with the exception of Short-lived Subscriber Certificates) must be immediately revoked within 24 hours and use the corresponding CRLReason (see Section 7.2.2):

1. When requested, in writing, by an SO, without specifying a CRLReason (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL).
2. When OATI 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 OATI 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 OATI that the original certificate request was not authorized and does not retroactively grant authorization (CRLReason #9, privelegeWithdrawn).
5. When OATI obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise (CRLReason #1, keyCompromise).
6. OATI 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, including but not limited to those identified in section 6.1.1.1.1 (CRLReason #1, keyCompromise).
7. OATI obtains evidence that the validation of domain authorization or control for any FQDN or IP address in the Certificate should not be relied upon (CRLReason #4, Superseded).

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

Where the following conditions or circumstances occur, an OATI webCARES Digital Certificate issued by the OATI webCARES system (with the exception of Short-lived Subscriber Certificates) should be revoked within 24 hours, but must be revoked within 5 days and use the corresponding CRLReason:

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 (CRLReason #4, Superseded).
4. OATI obtains evidence that the Certificate was misused (CRLReason #9, privelegeWithdrawn).
5. OATI 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) (CRLReason #5, cessationOfOperation)..
6. OATI is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate FQDN (CRLReason #9, privelegeWithdrawn).
7. OATI is made aware of a material change in the information contained in the Certificate (CRLReason #9, privelegeWithdrawn).
8. OATI is made aware that the Certificate was not issued in accordance with these Requirements or OATI's Certificate Policy or CPS (CRLReason #4, superseded).
9. OATI determines or is made aware that any of the information appearing in the Certificate is inaccurate (CRLReason #9, privelegeWithdrawn).
10. OATI's right to issue Certificates under these Requirements expires or is revoked or terminated, unless OATI has made arrangements to continue maintaining the CRL Repository (CRLReason #unspecified (0)" which results in no reasonCode extension being provided in the CRL).
11. Revocation is required by OATI's Certificate Policy and/or CPS for a reason that is not otherwise required to be specified by this section 4.9.1 (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL).

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

12. OATI 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 (CRLReason #1, keyCompromise).
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. OATI is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use (CRLReason #9, privelegeWithdrawn).
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 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 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 Organization as well. This can be done via the OATI webCARES GUI or via email submittal of a revocation request to OATI Help Desk.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

If the revocation request is sent 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 revocation request, 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 Certificate Problem Reports

A Certificate Problem Report can only be reported to OATI through the OATI webCARES Contact Us form located in the repository. Within 24 hours after receiving the Certificate Problem Report, OATI will begin an investigation. If insufficient information has been provided, OATI may request for additional information. The revocation timeline as stated in Section 4.9.1 will begin once the Certificate Problem Report has been confirmed. OATI will provide a preliminary report on its findings to the entity who filed the report within 24 hours after the Certificate Problem Report has been confirmed.

4.9.2.2 Notifications

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

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

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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

OATI shall process revocation requests in accordance with the CA/Browser Forum Baseline Requirements. 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 shall determine the revocation status of OATI webCARES Digital Certificates by retrieving and processing the applicable Certificate Revocation List (CRL) published by OATI.

OATI does not operate an Online Certificate Status Protocol (OCSP) responder for this hierarchy.

4.9.7 CRL Issuance Frequency

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

CRLs will continue to be issued until one of the following occurs:

- All Subordinate CA Certificates containing the same Subject Public Key are expired or revoked; OR
- The corresponding Subordinate CA Private Key is destroyed.

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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

4.9.9 Online Revocation/Status Checking Availability

OATI webCARES does not support Online Certificate Status Protocol (OCSP) services of this hierarchy.

Revocation status for all OATI webCARES Digital Certificates SHALL be determined exclusively through CRLs published by OATI.

4.9.10 Online Revocation Checking Requirements

See Section 4.9.9.

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 does not permit certificate suspension.

The OATI repository does not include entries that indicate that a Certificate has been suspended.

4.9.14 Who Can Request Suspension

Not applicable - OATI webCARES does not permit certificate suspension.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

4.9.15 Procedure for Suspension Request

Not applicable - OATI webCARES does not permit certificate suspension.

4.9.16 Limits on Suspension Period

Not applicable - OATI webCARES does not permit certificate suspension.

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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

5. Facility, Management, and Operational Controls

5.1 Physical Security 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

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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 at least 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

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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 four 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 seven key types, differentiated by colors Red, Purple, Orange, Blue, Black, Gray, and Green. Each Blue, Black, Gray, 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, one Gray, 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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

5.2.4 Roles Requiring Separation of Duties

The functions performed in these roles form the basis of trust for all uses of OATI. 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, OATI webCARES Development Team, and delegates.
- Auditor – Compliance and delegates.
- Operators – Registration Administrators, Administrators, and delegates.
- Registration Administrator – Help Desk.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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:

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

- 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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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
   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. Records included at a minimum;
      i. the information being validated (e.g., the applied-for FQDN or the organization name);
      ii. the ADN used (if applicable and different from the applied-for FQDN); and
      iii. the validation method used (e.g., the BRs section number or the registered label of an ACME validation method); ;
   C. Approval and rejection of certificate requests;
   D. Issuance of Certificates;
   E. Generation of CRLs; and
   F. MPIC attempts from each Network Perspective, recording at least the following information:

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

- an identifier that uniquely identifies the Network Perspective used;
- the attempted domain name and/or IP address; and
- the result of the attempt (e.g., “domain validation pass/fail”).

G. MPIC quorum results for each attempted domain name or IP address represented in a Certificate request (i.e., “3/4” which should be interpreted as ”Three (3) out of four (4) attempted Network Perspectives corroborated the determinations made by the Primary Network Perspective).

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. Relevant firewall and router activities (as described in Section 5.4.1.1); and
   G. Entries to and exits from the CA facility.

5.4.1.1 Router and Firewall Activities Logs

Logging of router and firewall activities necessary to meet the requirements of Section 5.4.1, Subsection 3.F include at a minimum:

- Successful and unsuccessful login attempts to routers and firewalls; and
- Logging of all administrative actions performed on routers and firewalls, including configuration changes, firmware updates, and access control modifications; and
- Logging of all changes made to firewall rules, including additions, modifications, and deletions; and
- Logging of all system events and errors, including hardware failures, software crashes, and system restarts.

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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

- 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-

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

012 and based upon a risk assessment performed to determine the appropriate length of retention time, which shall be no less than seven years.

OATI 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 validated 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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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 has established Incident Response and Business Continuity Plans that include various industry requirements and best practices. These plans are reviewed, tested and training is provided to staff at least annually. The OATI Incident Response Team is responsible for notifying customers during any security incident that affects customers' use of OATI services and products and will determine when the proper time to send notification will be based on criticality. Multiple methods of notifications will be used: telephone, email, outage announcements from the OATI webSupport™ system, postings on OATI applications, etc.

5.7.1.1 Incident Response and Disaster Recovery Plans

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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

5.7.1.2 Mass Revocation Plans

OATI maintains a comprehensive and actionable plan in the event of mass revocation. Testing of the mass revocation plan is completed annually and lessons learned is incorporated into the plan to improve readiness.

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

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

- Before returning to operation, OATI will ensure the OATI webCARES system integrity has been restored.
- If OATI 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 OATI 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 OATI and destroys all copies of OATI 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 OATI revoking all OATI webCARES Digital Certificates.

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

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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 OATI. 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 OATI 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 OATI'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 OATI'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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

2. There is clear evidence that the specific method used to generate the Private Key was flawed.
3. OATI is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise.
4. OATI has previously been notified that the Applicant's Private Key has suffered a Key Compromise, using OATI's procedure for revocation request as described in Section 4.9.3 and Section 4.9.12.
5. The Public Key corresponds to an industry-demonstrated weak Private Key. At least the following precautions SHALL be implemented:
   A. In the case of Debian weak keys vulnerability (https://wiki.debian.org/SSLkeys), OATI SHALL reject all keys found at https://github.com/cabforum/Debian-weak-keys/ for each key type (e.g. RSA, ECDSA) and size listed in the repository. For all other keys meeting the requirements of Section 6.1.5, with the exception of RSA key sizes greater than 8192 bits, OATI SHALL reject Debian weak keys.
   B. In the case of ROCA vulnerability, OATI SHALL reject keys identified by the tools available at https://github.com/crocs-muni/roca or equivalent.
   C. In the case of Close Primes vulnerability (https://fermatattack.secvuln.info/), OATI SHALL reject weak keys which can be factored within 100 rounds using Fermat's factorization method.

Suggested tools for checking for weak keys can be found at https://cabforum.org/resources/tools/.

OATI does not generate Key Pairs on behalf of a Subscriber, and will not accept a certificate request using a Key Pair previously generated by 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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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 Server Root CA and OATI webCARES Server Issuing CA 2026 issue OATI webCARES Digital Certificates using a 4096 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: Certificate Signing, Off-line CRL Signing, and CRL Signing.

OATI webCARES End Entity Certificates and their associated keys are limited to the following uses: 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 OATI or any of its

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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 validated 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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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 OATI 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 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 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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The Validity Period of an OATI webCARES Server(end-entity) Authentication Certificate SHALL NOT exceed the maximum period permitted by the applicable CA/Browser Forum Baseline Requirements in effect at the time of certificate issuance.

For purposes of calculating the Certificate validity period, OATI measures one day as exactly 86,400 seconds. Any period of time greater than 86,400 seconds, including fractional seconds and/or leap seconds, is considered an additional day.

OATI applies the following maximum validity periods for publicly trusted Server Certificates:

- For Certificates issued on or after March 15, 2026 and before March 15, 2027, the Validity Period SHALL NOT exceed 200 days.
- For Certificates issued on or after March 15, 2027 and before March 15, 2029, the Validity Period SHALL NOT exceed 100 days.
- For Certificates issued on or after March 15, 2029, the Validity Period SHALL NOT exceed 47 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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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

OATI monitors for updated versions of linting software and updates the linting tools used in section 4.3.1.1 and 4.3.1.2 within three (3) months from the release of the update.

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

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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.

OATI has implemented network security controls in conformance with the CA/B Baseline Network and Certificate System Security Requirements.

6.7.1 Anti-Virus

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

6.7.2 Vulnerability Remediation

Based on an OATI assessment of risk, Critical vulnerabilities should be remediated within 15 calendar days of initial detection, High vulnerabilities should be remediated within 30 calendar

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

days of initial detection. Medium/Moderate and Low vulnerabilities are assessed and mitigation plans created within 90 days.

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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

7. Certificate and CRL 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 Content and Extensions

7.1.2.1 Root CA Certificate Profile - OATI webCARES Server Root CA

- version: 3(2)
- serialNumber: non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
- Signature: See Section 7.1.3.2.
- issuer: byte-for-byte identical to the encoded subject.
- validity: 20 years.
- subject: Present, NOT marked as critical, and contains at minimum the following:
  - countryName (OID 2.5.4.6).
  - organizationName (OID 2.5.4.10).
  - commonName.
- subjectPublicKeyInfo: See Section 7.1.3.1.
- issuerUniqueID: Not Present.
- subjectUniqueID: Not Present.
- signatureAlgorithm: byte-for-byte identical to the tbsCertificate.signature.
- Extensions:
  - authorityKeyIdentifier: Not Present.
  - basicConstraints: Present and marked as critical with the cA field set to True. There are no pathLenConstraints.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

- keyUsage: Present and marked as critical with bit positions for keyCertSign and cRLSign set.
- subjectKeyIdentifier: Present, NOT marked as critical.
- extKeyUsage: Not Present.
- certificatePolicies: Not Present.
- Signed Certificate Timestamp List: Not Present.
- No other extensions are present.

7.1.2.2 Issuing CA Certificate (Intermediate CA/TLS Subordinate CA Certificate Profile) – OATI webCARES Server Issuing CA 2026

- version: 3(2)
- serialNumber: non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
- Signature: See Section 7.1.3.2.
- issuer: byte-for-byte identical to the subject field. See Section 7.1.4.1.
- validity: OATI ensures that our Issuing Authority certificates and associated private keys are limited to a maximum of four (4) years for Subscriber certificate signing.
- subject: Present, NOT marked as critical, and contains at minimum the following:
  - countryName (OID 2.5.4.6).
  - organizationName (OID 2.5.4.10).
  - commonName.
- subjectPublicKeyInfo: See Section 7.1.3.1.
- issuerUniqueID: Not Present.
- subjectUniqueID: Not Present.
- signatureAlgorithm: byte-for-byte identical to the tbsCertificate.signature.
- Extensions:
  - authorityKeyIdentifier: Present, NOT marked as critical, and contains at a minimum a keyIdentifier field.
  - basicConstraints: Present and marked as critical with the cA field set to True. There are no pathLenConstraints.
  - certificatePolicies: Present and NOT marked critical.
    - certificatePolicies:policyIdentifier: Present.
    - certificatePolicies:policyQualifiers:policyQualifierId: Present.
    - certificatePolicies:policyQualifiers:qualifier:cPSuri: Present.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

- cRLDistributionPoints: Present, NOT marked as critical, and at minimum contains the HTTP URL of OATI webCARES's CRL service.
- keyUsage: Present and marked as critical with bit positions for DigitalSignature, keyCertSign, and cRLSign set.
- subjectKeyIdentifier: Present and NOT marked as critical.
- extKeyUsage: Present, NOT marked as critical.
  - id-kp-serverAuth: Present.
- authorityInformationAccess: Present, NOT marked as critical, and contains at minimum the HTTP URL of OATI's Issuing CA certificate (accessMethod = 1.3.6.1.5.5.7.48.2).
- nameConstraints: Not Present.

7.1.2.3 Subscriber Certificate (Server Certificate Profile) – From 2026 Server Issuing

- version: 3(2)
- serialNumber: non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
- Signature: See Section 7.1.3.2.
- issuer: byte-for-byte identical to the subject field. See Section 7.1.4.1.
- validity: 396 days. Also see Section 6.3.2.
- subject: Present, NOT marked as critical, and contains at minimum the following:
  - countryName (OID 2.5.4.6).
  - organizationName (OID 2.5.4.10).
  - stateOrProvinceName.
  - localityName.
  - commonName.
- subjectPublicKeyInfo: See Section 7.1.3.1.
- issuerUniqueID: Not Present.
- subjectUniqueID: Not Present.
- signatureAlgorithm: byte-for-byte identical to the tbsCertificate.signature.
- extensions:
  - authorityInformationAccess: Present, NOT marked as critical, and contains at minimum the HTTP URL of OATI's Issuing CA certificate (accessMethod = 1.3.6.1.5.5.7.48.2).
  - authorityKeyIdentifier: Present, NOT marked as critical, and contains a keyIdentifier field.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

  - certificatePolicies: Present and NOT marked critical.
    - certificatePolicies:policyIdentifier: Present. OID: 2.23.140.1.2.2.
    - certificatePolicies:policyQualifiers:policyQualifierId: Present.
    - NAESB Basic Assurance OID 2.16.840.1.114505.1.12.2.2.
- extKeyUsage: Present and NOT marked critical. id-kp-serverAuth present. OID 1.3.6.1.5.5.7.3.1. Does NOT contain the anyExtendedKeyUsage.
- subjectAltName: Present, NOT marked critical. Contains dNSName.
- nameConstraints: Not Present.
- keyUsage: Present and marked as critical with bit positions for digitalSignature and keyEncipherment set.
- basicConstraints: Not Present.
- cRLDistributionPoints: Present, NOT marked as critical, and contains at minimum the HTTP URL of OATI's CRL service.
- Signed Certificate Timestamp List: Present. Contains an OCTET STRING containing the encoded SignedCertificateTimestampList, as specified in RFC 6962, Section 3.3. Each SignedCertificateTimestamp included within the SignedCertificateTimestampList MUST be for a PreCert LogEntryType that corresponds to the current certificate.
- subjectKeyIdentifier: Not Present.
- anyPolicy: Not Present.

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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

7.1.2.5 Precertificates

For purposes of clarification, a Precertificate, 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 the CA/B Forum Baseline Requirements. OATI does not issue precertificates.

7.1.3 Algorithm Object Identifiers

OATI issues certificates using cryptographic algorithms and object identifiers (OIDs) that are permitted by the CA/Browser Forum Baseline Requirements and applicable standards.

7.1.3.1 SubjectPublicKeyInfo (aka Public Key Parameters)

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

No other encodings are permitted for these fields.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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

This section details encoding rules that apply to all Certificates issued by the OATI webCARES CA.

7.1.4.1 Name Encoding/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 – Subscriber Certificates

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. OATI Issuing CAs comply with the name forms detailed in RFC 5280 and the applicable CA/Browser Forum Baseline Requirements.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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. No Name Constraints extension is included in certificates issued by the OATI webCARES Server Root CA and its subordinate CAs.

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 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

See Section 7.1.2.

7.1.6.3 Subordinate CA Certificates

See Section 7.1.2.

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-

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

forum(140) certificate-policies(1)} (2.23.140.1). The Certificate MAY also contain additional policy identifier(s) defined by OATI. See Section 7.1.2.

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.

CRLs published by the OATI webCARES Server Root CA have a validity period of three months. The OATI webCARES Server 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 CRLs published by the OATI webCARES Server Issuing CA 2026 have a validity period of 12 hours. The OATI webCARES Server Issuing CA 2026 publishes new CRLs prior to the expiration of the existing CRL, when a certificate is revoked, and on regular intervals (hourly) to assure availability.

The OATI webCARES Roots 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 X.509 v2 issued in compliance with RFC 5280.

7.2.2 CRL and CRL Entry Extensions

- version: v2.
- Signature: SHA-512.
- issuer: Byte-for-byte identical to the subject field of the CA that issued the CRL.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

- OATI ensures the use of its certificate and associated private key to a maximum of six years for CRL signing.
- thisUpdate: The issue date of the CRL.
- nextUpdate: The date which the next CRL will be issued. OATI Issuer CRLs are three months and Subscribers CRLs are 12 hours.
- The maximum interval (latency) between CRL issuance is 24 hours.
- CRLs are published within four hours of generation.
- revokedCertificates: Present if OATI has issued a Certificate that has been revoked and the corresponding entry has yet to appear on at least one regularly scheduled CRL beyond the revoked Certificate's validity period. OATI removes entries for corresponding Certificates after the Certificate has appeared on at least one regularly scheduled CRL beyond the revoked Certificate's validity period.
- Extensions: Present. See below.
- Signature Algorithm: Byte-for-byte identical to the tbsCertList.signature.
- Any other value: Not present.

CRL Extensions:

- Authority Key Identifier: Present. Not marked as critical. Identical to the subjectKeyIdentifier field of the CA that issued the CRL.
  - keyIdentifier: Present. Identical to the subjectKeyIdentifier field.
  - authorityCertIssuer: Not present.
  - authorityCertSerialNumer: No present.
- CRL Number: Present. Not marked as critical. Consecutively increasing identification number for each CRL.
- issuingDistributionPoint (OID 2.5.29.28): Not Present. OATI CRLs contain entries for all revoked unexpired certificates, so this is not necessary.
- Any other extension: Not present.

revokedCertificates Component:

- serialNumber: Present. Byte-for-byte identical to the serialNumber contained in the revoked Certificate.
- revocationDate: Present. The date and time revocation occurred. **In the instance of a private key compromise prior to the revocation date that is indicated in the CRL entry for that Certificate, OATI is capable of backdating the revocationDate field. This is an

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

exception to the best practices described in RFC 5280; however, industry requirements specify the use of the revocationDate field to support TLS implementations that process the revocationDate field as the date when the Certificate is first considered to be compromised.

- crlEntryExtensions: See below.

crlEntry Extensions Component:

- reasonCode (OID 2.5.29.21): Present and NOT marked as critical. Reason for revocation for the certificate in question.
  - The CRLReason indicated MUST NOT be unspecified (0). If the reason for revocation is unspecified, OATI MUST omit reasonCode entry extension, if allowed by the previous requirements.
  - The CRLReason MUST NOT be certificateHold (6).
  - The CRLReason MUST indicate the most appropriate reason for revocation of the certificate.
  - The CRLReason MUST be included in the reasonCode extension of the CRL entry corresponding to a Subscriber Certificate that is revoked unless the CRLReason is "unspecified (0)".
  - Only the following CRLReasons MAY be present in the CRL reasonCode extension for Subscriber Certificates:
    - **keyCompromise (RFC 5280 CRLReason #1):** Indicates that it is known or suspected that the Subscriber's Private Key has been compromised.
    - **affiliationChanged (RFC 5280 CRLReason #3):** Indicates that the Subject's name or other Subject Identity Information in the Certificate has changed, but there is no cause to suspect that the Certificate's Private Key has been compromised.
    - **superseded (RFC 5280 CRLReason #4):** Indicates that the Certificate is being replaced because: the Subscriber has requested a new Certificate, OATI has reasonable evidence that the validation of domain authorization or control for any fully-qualified domain name or IP address in the Certificate should not be relied upon, or OATI has revoked the Certificate for compliance reasons such as the Certificate does not comply with the CA/B Forum Baseline Requirements or OATI's CPS.
    - **cessationOfOperation (RFC 5280 CRLReason #5):** Indicates that the website with the Certificate is shut down prior to the expiration of the Certificate, or if the

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

Subscriber no longer owns or controls the Domain Name in the Certificate prior to the expiration of the Certificate.

- **privilegeWithdrawn (RFC 5280 CRLReason #9):** Indicates that there has been a subscriber-side infraction that has not resulted in keyCompromise, such as the Certificate Subscriber provided misleading information in their Certificate Request or has not upheld their material obligations under the Subscriber Agreement or Terms of Use.

- Any other value: Not present.

7.3 OCSP Profile

OATI is not issuing OCSP responses for the OATI webCARES Server Root CA and OATI webCARES Server Issuing CA 2026.

7.3.1 Version Number(s)

Not Applicable.

7.3.2 OCSP Extensions

Not Applicable.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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 https://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.

If OATI does not have a currently valid Audit Report indicating compliance with one of the audit schemes listed in Section 8.4, then, before issuing Publicly-Trusted Certificates, OATI shall successfully complete a point-in-time readiness assessment performed in accordance with applicable standards under one of the audit schemes listed in Section 8.4.

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 8.4);
- 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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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 applicable version of the following:

- WebTrust for Certificate Authorities Principles and Criteria version 2.2.2 or newer and either:
  - WebTrust for Certificate Authorities - SSL Baseline with Network Security version 2.7 or newer; OR
  - WebTrust Principles and Criteria for Certification Authorities – SSL Baseline version 2.8 or newer AND WebTrust Principles and Criteria for Certification Authorities – Network Security version 1.7 or newer.
- 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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

8.7 Self-Audits

OATI shall monitor adherence to its CPS and control service quality by performing self-audits on at least a quarterly basis against a randomly selected sample of certificates.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

9.13 Dispute Resolution Procedures

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 Assignment

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

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

9.16.3 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.

9.16.4 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.

9.16.5 Force Majeure

OATI disclaims liability and will not or deemed to be in violation of its obligations hereunder for any delay or failure in performance resulting, directly or indirectly, from acts of God, civil or military authority, acts of the public enemy, war, riots, civil disturbances, insurrections, accidents, fire, explosions, earthquakes, floods, the elements, strikes, labor disputes or any causes beyond its reasonable control; provided that OATI failing to perform in any such event will promptly resume or remedy, as the case may be, the performance of its obligations hereunder as soon as practicable.

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,

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

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

©2002 – 2026 Open Access Technology International, Inc. All rights reserved.

This document and translations of it may be copied and furnished to others; however, it must remain in a complete and unchanged form and not used for commercial purposes. Any other uses of this document requires prior written approval from OATI.

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

9.17.9 Other Practice Statements and Agreements

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

License: This Certification Practice Statement is made available under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.