

OATI

Open Access Technology International, Inc.

OATI webCARES



Certification Practice Statement

April 25, 2002

TRADE SECRET

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

Table of Contents

1. Introduction.....	6
1.1. Certification Practice Statement	6
1.2. Digital Signature Technology	6
1.3. Digital Certificates.....	7
1.4. Customer Service and Education.....	7
1.5. Reference Documents	8
1.5.1. Technical Information	8
1.5.2. Legal Information	8
2. OATI webCARES Public Key Infrastructure	9
2.1. OATI's PKI Hierarchy	9
2.1.1. OATI Naming Authority	9
2.1.1.1. OATI e-MARC Certificate Profile	10
2.1.1.2. Enhanced Naming and Extensions	10
2.1.1.3. Guarantee of Name Uniqueness Between Current and Past Subscribers	10
2.1.2. OATI Repository	10
2.1.3. OATI Registration Authority.....	10
2.1.4. OATI Root.....	11
2.1.5. OATI Intermediate Certification Authority (ICA)	11
2.1.6. OATI Issuing Authorities (IAs).....	11
3. OATI Certification Authority Framework.....	12
3.1. OATI webCARES System	12
3.2. Eligible Entities.....	12
3.3. Security Officer.....	12
3.4. Backup Security Officer.....	12
3.5. Audit Officer	13
3.6. Security Officer Conformance to this CPS	13
3.7. OATI Representations	13
3.8. Time Stamping.....	14
3.9. Record Retention Policy.....	14
3.10. OATI webCARES Disaster Recovery Plan	14
3.11. Availability of OATI Issuing Authority Certificates	14
3.12. OATI webCARES Personnel	14
3.13. Confidential Information	14
3.14. OATI Data Center Security	15

4. OATI SIVP	16
4.1. Application Procedures	16
4.1.1. Business Representative Application	16
4.1.2. Unaffiliated Individual Application	16
4.1.3. Machine, Server, or Application	17
4.1.4. Qualified Relying Party	17
4.2. Identification and Verification Procedure	17
4.2.1. Unsuccessful Identification and Verification Procedure	17
4.2.2. Successful Identification and Verification Procedure	18
5. OATI webCARES e-MARC Certificate Issuance	19
5.1. Certificate Issuance Support	19
5.2. Subscriber's Obligation to Review and Correct e-MARC Certificate	19
5.3. Subscriber's Acceptance of e-MARC Certificate	19
5.4. Certificate Operational Period	19
5.5. Publication within the OATI Repository	19
5.6. SO's Duty to Protect Private Key(s)	19
6. e-MARC Certificate Usage	21
6.1. Use of OATI e-MARC Certificates	21
6.1.1. Acceptable Uses of e-MARC Certificates	21
6.1.2. Unacceptable Uses of e-MARC Certificates	21
6.2. Digital Signature Validity	21
6.3. Failure of Digital Signature Confirmation	21
6.4. Security Measures	21
7. e-MARC Certificate Revocation	22
7.1. Conditions Requiring e-MARC Certificate Revocation	22
7.2. e-MARC Certificate Revocation Procedure	22
7.3. Notice of e-MARC Certificate Revocation	22
7.4. OATI webCARES Certificate Revocation List (CRL)	23
7.5. Qualified Relying Party CRL Checking	23
7.6. Effect of Revocation	23
8. e-MARC Certificate Renewal	24
8.1. e-MARC Certificate Renewal Procedure	24
8.2. e-MARC Certificate Renewal Fee	24
9. e-MARC Certificate Expiration	25
10. General Provisions Concerning the OATI Root, Intermediate, and Issuing Authorities	26

10.1.	OATI Root	26
10.2.	OATI Intermediate Authority	26
10.3.	OATI Issuing Authorities.....	26
10.4.	OATI webCARES Backup System.....	26
10.5.	OATI Root and Intermediate Authority CRL Publishing	26
11.	<i>Acronyms</i>.....	27
12.	<i>Glossary</i>.....	28

OATI webCARES Certification Practice Statement

Version 1.0

1. Introduction

The NERC draft Certificate Policy for Energy Market Access and Reliability Certificates (e-MARC) identifies that the secure and trusted transfer of electronic information is necessary for the deregulated energy markets and system reliability function. The NERC e-MARC Policy outlines the implementation of a Public Key Infrastructure (PKI) to achieve this goal. The envisioned PKI will incorporate Digital Certificates using Public Key Cryptography to securely transfer energy market and system reliability electronic information between identifiable parties.

OATI will act as a Certification Authority (CA) as defined in the NERC e-MARC Policy. The OATI CA and webCARES System will conform to the NERC e-MARC Policy statement. As a NERC e-MARC conformant CA, OATI will undertake the roles of Naming Authority, Registration Authority, Certificate Manufacturing Authority, and e-MARC Certificate Repository. To accomplish these tasks, OATI has developed the webCARES (web Certificate Administration, Renewal, and Enrollment Services) System. The webCARES System will allow authenticated Subscribers to actively manage certificates within their specified organizational unit. This OATI Certification Practice Statement defines and discusses each of the roles that OATI will undertake as a NERC e-MARC conformant CA and how these roles are integrated into the webCARES System.

1.1. Certification Practice Statement

The NERC e-MARC Policy Statement requires that all entities choosing to provide Certification Authority Services compose and publish a Certification Practice Statement (CPS). To conform to the NERC e-MARC Policy Statement, OATI developed this CPS. The purpose of this CPS is to: 1) document the procedures and practices that the OATI CA will follow to create, sign, issue, validate, revoke, renew, and generally manage Digital Certificates; 2) inform Subscribers of the OATI CA Service of their rights and responsibilities; 3) outline the rights and responsibilities of the OATI CA; and 4) instill public confidence in the OATI CA through the disclosure of all industry accepted policies, practices, and procedures that ensure the creation of a secure and trusted PKI.

Every e-MARC certificate issued and signed by the OATI webCARES System will incorporate by reference the OATI CPS. It is very important for anyone who uses or relies on an OATI e-MARC certificate to read this CPS carefully. This CPS provides the user with important information regarding rights and responsibilities as an e-MARC user or Qualified Relying Party. In addition, this CPS will reference the reader to more detailed information regarding legal and technical matters relating to the overall functioning of a PKI.

OATI will publish this CPS in a publicly accessible site for any interested party to access and view. Any subsequent revisions or changes to this CPS will also be posted in a timely manner along with the past versions to be used for historical purposes.

1.2. Digital Signature Technology

Digital Signatures are created using Public Key Cryptography. Public Key Cryptography uses a pair of mathematically related keys to encrypt and decrypt data. The first key in the pair is called the Public Key. This key is generally known to the public and is typically used to encrypt the data being transferred. The other key in the pair is the Private Key. The Private Key must only be known by the "owner" of the key pair. The Private Key is the only key that can decrypt data or information that was initially encrypted using its corresponding Public Key. While a Public Key is typically used to encrypt data and the corresponding Private Key is used to decrypt the data,

the process can work in both directions. Either key may be used to encrypt data and the corresponding key will be the only key able to decrypt it. Typically, the Public Key encrypts data because only the associated Private Key will be able to decrypt the data. If the Private Key were used to encrypt data, then any other person that knows the corresponding Public Key would be able to decrypt and access the data being sent. A certificate's Private Key is typically only used for digitally signing data packets. When data packets are digitally signed using a certificate pair's Private Key, then anyone using the corresponding Public Key to decrypt the data knows it could only have come from the owner of the Private Key as that person is the only one that knows or has access to the Private Key.

Another fundamental tool used for creating and verifying a digital signature's authenticity is a hash function. A hash function is a mathematical algorithm that uses the data to be transferred as input, and outputs a unique digital representation of the data in a standard length, typically much shorter than the original data. Each set of data that is input into a hash function will create a unique hash result. Even changing a set of data by one character will return a completely unique hash result. Thus, to verify that data have not been altered or tampered with in transit, the sender will create a digital hash of the data and include that along with the actual data. When the data packets are received, the recipient uses the same hash function to create a hash result. If the hash result created by the recipient matches the one sent by the sender, then the recipient can rely on the fact that the data sent have not been altered or tampered with during transit.

1.3. Digital Certificates

While data can be digitally signed and authenticated using a combination of Public Key Cryptography and a hashing function, there still must be infrastructure in place to link a digital signature to a person's physical identity. To solve the problem of linking a digital signature to a person's identity, a trusted third party is required to associate a digital signature to an identity. Within a PKI, a Certification Authority (CA) is a trusted third party that verifies a digital signature associated with a person's physical identity. The CA is responsible for verifying a Subscriber's physical identity before issuing the applicant a digital certificate. A digital certificate is analogous to a driver's license. A digital certificate provides identifying information relating to the holder of the certificate. In addition, the certificate includes the Subscriber's Public Key, the hash function used to sign the certificate, and other relevant information such as the effective time (issuance date and expiration date) of the certificate. Before issuing the certificate to the Subscriber, the CA will use all of the information contained in the certificate and apply a hash function to create a hash result of the information. The hash result will then be encrypted using the CA's Private Key. The hashing of the Subscriber's information along with encrypting the hash result with the CA's Private Key creates a digital signature that is then associated with the digital certificate. Therefore, when OATI digitally signs a Subscriber's certificate, the recipient of the digital certificate can rely on the fact that the person listed in the certificate is actually the person represented.

1.4. Customer Service and Education

OATI's CPS assumes that the reader is familiar with Digital Signatures, PKIs, and the OATI webCARES system. If you are not familiar with this technology, or you would like to learn more, please browse the material listed in the "Reference Document" section of this CPS. If you would like further training or education regarding this topic, OATI advises that the reader attend a training course or seminar on the topic of PKI and Digital Signatures.

If you have specific questions regarding the OATI webCARES system or this CPS, please contact an OATI webCARES Customer Assistance representative at webCARES@oatiinc.com.

1.5. Reference Documents

1.5.1. Technical Information

- Information Security Primer – Helping the Energy Industry Adapt to the Internet Age, without Compromising Operational Security or Operating Flexibility – Prepared for EPRI (<http://www.nerc.com/~filez/cip.html>).
- The PKI Page – A website with numerous links to PKI information (<http://www.pki-page.org/>).

1.5.2. Legal Information

- The Digital Signature Guidelines – American Bar Association (ABA) Information Security Committee (http://www.abanet.org/scitech/ec/isc/digital_signature.html).
- The Uniform Electronic Transactions Act (UETA) 1999 – National Conference of Commissioners on Uniform State Laws (<http://www.nccusl.org/>).
- Federal Public Key Infrastructure (FPKI) Steering Committee Website (<http://www.cio.gov/fpkisc/>).

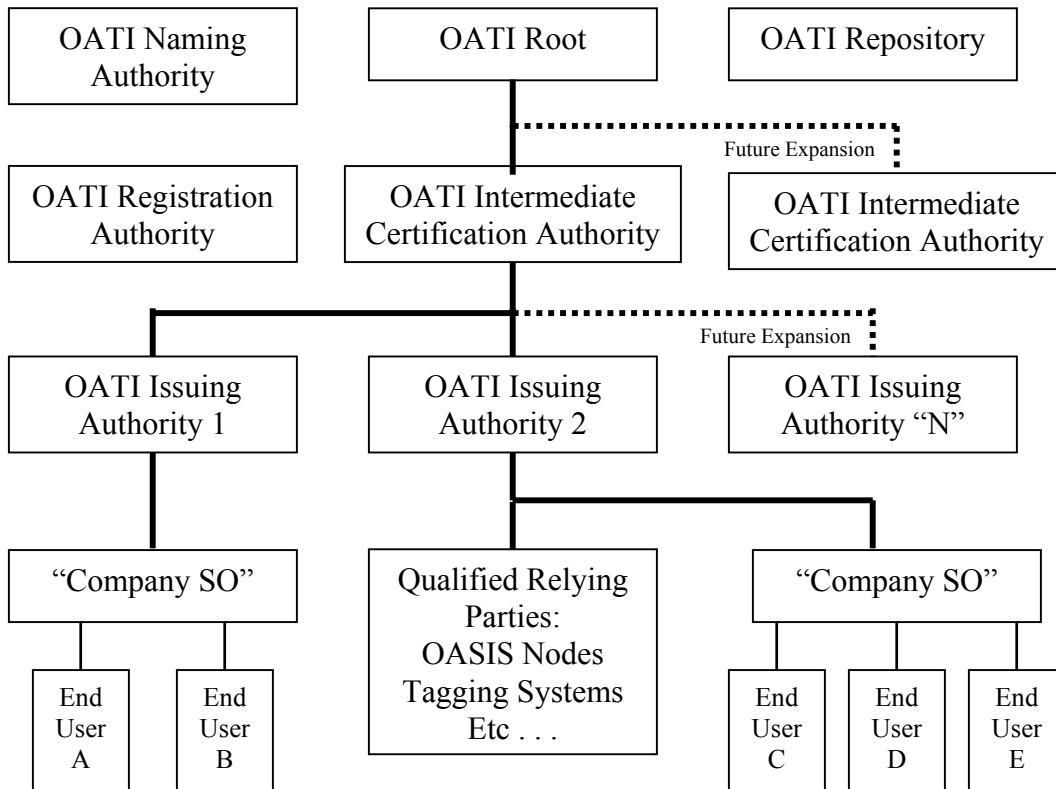
2. OATI webCARES Public Key Infrastructure

2.1. OATI's PKI Hierarchy

OATI's webCARES PKI is implemented with the following hierarchical structure:

1. OATI Root
2. OATI Intermediate Certification Authority (ICA)
3. OATI Issuing Authority (IA)
4. Company Security Officers (SO)
5. End Users

Additionally, the OATI CA will operate an e-MARC Repository and OATI will initially act as a Naming Authority for webCARES system users.



2.1.1. OATI Naming Authority

The OATI Naming Authority (NA) coordinates the creation and issuance of Distinguished Names (DN) for all certificates issued to Security Officers and End Users. Certificates issued within the OATI PKI will contain a unique X.509 DN. The DN assigned by the OATI NA will clearly identify the official Company Name, the Company's entity code, the name of the End User, and the e-mail address or machine ID of the End User. By combining all of these elements into the DN, OATI will assure that every DN assigned will be unique and clearly identify the party using the certificate.

OATI will undertake Naming Authority responsibilities until such time as a Regulatory Body within the De-Regulated Electric Utility Industry accepts this role.

2.1.1.1. OATI e-MARC Certificate Profile

All OATI e-MARC certificates, from the OATI Root certificate to the End User certificates issued through the OATI webCARES System, will conform to the ITU-T Recommendation X.509, "The Directory: Authentication Framework", June 1997. All OATI e-MARC certificates include a reference to the OATI Object Identifier (OID) issued to OATI by the American National Standards Institute (ANSI).

- OATI's OID 1.2.840.114278
- OID for OATI's CPS 1.2.840.114278.11.1

2.1.1.2. Enhanced Naming and Extensions

OATI webCARES certificates are based upon the X.509 v1, v2, and v3 structure and extensions. The X.509, Amendment 1 to ISO/IEC 9594-8:1995 provides for a number of extensions. These extensions allow various management and administrative controls that are useful for OATI's webCARES purposes.

2.1.1.3. Guarantee of Name Uniqueness Between Current and Past Subscribers

OATI will guarantee name uniqueness among all e-MARC certificates issued by the OATI webCARES System through the inclusion of an End User's e-mail address within the Distinguished Name assigned.

2.1.2. OATI Repository

OATI will operate an on-line Repository for the purposes of publishing information necessary to maintain a PKI. The OATI Repository will publish information to Subscribers and Qualifying Relying Parties using two methods. The first method will be an unsecured website that will be accessible by the public. This site will contain the NERC draft e-MARC Policy statement, a copy of the current OATI CPS, all past versions of the OATI CPS, the most recent OATI Certificate Revocation List (CRL), the OATI CA's e-MARC Certificate for its signing key, and all other relevant information relating to the OATI PKI and its functions.

The second method of information posting in the OATI Repository will be through secure access to the OATI webCARES System. All verified users with access to the OATI webCARES System may view all e-MARC Certificates issued by the OATI CA that have been accepted by the user. A Company's SO will be able to view all Certificates issued to the company's End Users.

All information published in the OATI repository will be published promptly, upon availability to the OATI CA, according to generally accepted industry practices.

2.1.3. OATI Registration Authority

The OATI Registration Authority (RA) is responsible for performing the OATI webCARES Subscriber Identification and Verification Procedure (SIVP). The SIVP is the OATI process to ensure that OATI does not issue a certificate to an entity that cannot be verified using commercially reasonable industry practices and procedures. The actual SIVP will be discussed later within this CPS.

2.1.4. OATI Root

The OATI Root will only be used to sign and issue a certificate for the OATI Intermediate Certification Authority (ICA). If, for any reason, the ICA is lost, then the OATI Root will be the backup until such time as the existing ICA can be repaired or replaced with a new ICA.

As an extra layer of security, once the OATI Root signs and issues a certificate for the OATI ICA, then the OATI Root will be physically taken off the network. In addition, the OATI Root will be securely stored. The OATI Root will only be removed from secure storage and placed on the network to renew its own key pair, sign and issue new certificates for the ICA, or to sign and issue new certificates for the OATI Issuing Authorities if absolutely necessary.

2.1.5. OATI Intermediate Certification Authority (ICA)

The OATI ICA will only be used to sign and issue Certificates for the OATI Issuing Authorities (IA). As with the OATI Root, once the ICA has signed and issued certificates for the IAs, then the ICA will be taken off the network and stored securely along with the OATI Root.

2.1.6. OATI Issuing Authorities (IAs)

The OATI IAs will actually sign and issue certificates to SOs, Qualified Relying Parties, and other entities that are verified by the OATI RA. The OATI IA will also sign and issue new End User certificates when a request is made by a SO using the OATI webCARES User Interfaces.

3. OATI Certification Authority Framework

3.1. OATI webCARES System

The OATI webCARES System is a secure web based application that allows a Subscriber to actively manage and audit the e-MARC certificates that have been issued by the OATI Issuing Authority. All Subscribers that have been issued a certificate directly from the OATI Issuing Authority will also be given login access to the OATI webCARES system. A Subscriber with access to the OATI webCARES System will be termed a “Security Officer (SO)”. A SO will not only have the ability to manage his or her own certificates, but also to issue and manage certificates for all users within the SO’s organizational unit.

3.2. Eligible Entities

While the term Security Officer is applied to the actual person who applied for and manages an OATI webCARES System issued certificate, the OATI webCARES System will issue certificates to the following distinct entities:

- Business Representative – Individual authorized to act on the behalf of a business entity. An example is an Energy Trader at a Publicly Owned Utility.
- Unaffiliated Individual – A member of the general public.
- Machine, Server, or Applications – Systems authorized to take action on behalf of a business entity. Examples are web servers, applications servers, and custom client applications.
- Qualified Relying Party – Person or entity authorized to accept and rely upon e-MARC certificates for purposes of authentication, integrity, and non-repudiation. Examples of Qualified Relying Parties are Energy Trading Systems (OATI ETS) and OASIS Nodes.

For all entities that desire, not only may a Security Officer be designated, but also a Backup Security Officer and Audit Officer. **Each of the roles and responsibilities beyond that of the Primary SO are optional and are to be further defined by each Organization on an individual basis.**

3.3. Security Officer

The role of Security Officer is mandatory for every Organization or entity subscribing to the OATI webCARES System. A Security Officer (SO) will be responsible for managing the certificates within his or her Organizational Unit. A SO will use the OATI webCARES System to perform the duties and responsibilities described in this CPS. A SO may issue, revoke, renew, and track certificates for his or her End Users. A SO will be provided with personal access to the OATI webCARES System to perform his or her role.

3.4. Backup Security Officer

The role of Backup Security Officer is not mandatory, but is strongly recommended by OATI. The purpose of the Backup SO is to support the Organization if the primary SO is unavailable. The Backup SO will have the same duties and responsibilities as the Primary SO, as defined in this CPS and the OATI webCARES User Agreement executed by the Company. The Backup SO will be provided with personal access to the OATI webCARES System.

3.5. Audit Officer

Designation of an Organization Audit Officer, while optional, is recommended by OATI. An Audit Officer will have personal access to the OATI webCARES System for the purposes of monitoring audit logs and oversight of the SO and Backup SO. Each month, an Organization's Audit Officer will be sent a detailed report, via e-mail, documenting necessary certificate information within his or her Organizational Unit. The monthly Audit Report will contain all certificate activity that occurred during the month and will include a log of the Security Officer who took the certificate action along with a time and date stamp for each action.

3.6. Security Officer Conformance to this CPS

All Company Security Officers who use the OATI webCARES system to Issue, Renew, Revoke, and Audit certificates shall conform to the OATI CPS while performing these duties. Every Security Officer shall conform to the following guidelines that include, but are not limited to:

1. No Security Officer shall Issue a certificate to an End User without first verifying the identity of the End User;
2. If a Security Officer inappropriately issues a certificate, it is the duty and responsibility of the Security Officer to revoke the inappropriately issued certificate as soon as reasonably possible;
3. Every Security Officer will follow all reasonable practices and take reasonable precautions to protect his or her private key;
4. Every Security Office must inform each End User of all practices and precautions for protecting their own private key;
5. In the event that an End User's private key is compromised, the Security Officer must revoke the compromised certificate within a reasonable time;
6. If the Security Officer's private key is compromised, the Security Officer must revoke his or her own certificate within a reasonable time; If a definite date and time of compromise can be determined, then OATI recommends that all certificates issued by the Security Officer after the date and time of compromise must be revoked. If a definite time and date of compromise cannot be determined, then OATI recommends that the Security Officer revoke all End User certificates issued using the Security Officer's compromised Key Pair.

3.7. OATI Representations

OATI represents that an OATI e-MARC Certificate is issued only after OATI has followed its authentication procedures outlined in this CPS, and when maintained and used in the prescribed manner during the applicable time period, will prevent "Secure Transaction" compromises. A "Secure Transaction" is a successful SSL session in which no errors are reported, both parties are authenticated, and keys exchanged. Additionally, OATI represents that the OATI server issuing e-MARC certificates will be maintained and operated in a secure manner and will not be compromised. In the event of either such compromise, OATI agrees to reimburse the customer the cost of their e-MARC certificate application fee. Additionally, OATI offers customized compensation packages at competitive rates to accommodate OATI e-MARC certificate customers' needs. Rates will be quoted upon request. The terms and conditions of this CPS are intended to benefit only those OATI customers directly engaged in one of the designated e-MARC Certificate transactions provided for in this CPS, and not for any third parties who may be incidentally affected.

3.8. Time Stamping

The OATI webCARES System will time stamp and record all actions taken on a certificate. OATI will time stamp certificate issuance, renewal, revocation, and expiration. In addition to time stamping all actions taken on certificates, the webCARES System will time stamp all Certificate Revocation Lists. All time stamp information will be available via access to the OATI webCARES System. The OATI webCARES System will operate on Central Standard Time (CST), the industry standard within the deregulated energy industry.

3.9. Record Retention Policy

OATI will retain, according to generally accepted industry practices, all records associated with OATI e-MARC certificates for at least five (5) years after a certificate is revoked or expires. Records will be retained in electronic format where applicable, all other retained records will be in a physical medium.

3.10. OATI webCARES Disaster Recovery Plan

OATI personnel have developed and documented a disaster recovery plan for the webCARES system for internal use by OATI webCARES staff. The OATI webCARES disaster recovery plan will be periodically tested and refined as necessary to conform to the current industry standards for disaster recovery.

3.11. Availability of OATI Issuing Authority Certificates

OATI will maintain copies of its own certificates and any revocation data applicable to these certificates. These certificates and the associated data will be made available for the purposes of audits and verification of digital signatures created using OATI CA certificates. OATI's certificates and revocation information can be viewed at the following URL: <http://www.oaticerts.com/repository>.

3.12. OATI webCARES Personnel

OATI shall screen all employees working with or having access to the webCARES System. In addition, OATI shall employ a system of "separation of powers" by assigning webCARES personnel to no more than one critical position each, thus ensuring that no single employee has the opportunity to compromise the entire system. Each employee assigned to a critical position will have appropriate personnel assigned for backup purposes. No OATI webCARES personnel will be assigned to more than one critical position in the webCARES System.

3.13. Confidential Information

The basis of any PKI is the association of a user's identifying information with a digital certificate. While certain information must be made public for this purpose, OATI will protect the following information as confidential:

- OATI webCARES Application Records (successful and unsuccessful)
- Application Information not Required for Certificate Identification Purposes
- OATI webCARES User Agreements
- Complete OATI webCARES System Audit Records
- Security Measures such as OATI webCARES Disaster Recovery Plan, the full OATI SIVP process, and other information relating to operation of the OATI PKI.

3.14. OATI Data Center Security

The OATI Data Center utilizes proximity card access; both to the building itself as well as to the secured server room, thus limiting access to authorized OATI employees only. This security system is integrated into the OATI Data Center alarm system, which provides notification both to OATI employees as well as to the proper authorities in the event of unauthorized access. In addition to the alarm system and proximity card access, all OATI employees must sign in when entering the facility and sign out when leaving. This policy is strictly adhered to. All visitors to the OATI Data Center must sign in at the front desk when arriving, be issued an identification badge, be escorted by an appropriate OATI employee, and sign out with the front desk when leaving. These measures ensure that OATI personnel always have complete knowledge of who is in the OATI facility. The visitor policy is also strictly enforced.

Additional security for the OATI webCARES system requires that only OATI employees holding critical positions within the OATI webCARES project team access the System itself. Only employees holding critical positions know the correct access credentials for the webCARES System and are allowed to access it. All maintenance and system updates are pre-scheduled events that are strictly overseen by appropriate OATI webCARES personnel.

4. OATI SIVP

The OATI Subscriber Identification and Verification Procedure (SIVP) shall be completed for all applicants before obtaining an OATI e-MARC certificate. Once an appropriate User Agreement has been signed with OATI, then the OATI SIVP process requires that an applicant acquire and complete an appropriate OATI webCARES application form. OATI personnell will send a Subscriber the applicable application form upon execution of the appropriate User Agreement. OATI shall provide an appropriate Subscriber application form for each type of entity that may apply for an e-MARC certificate (Business Representative, Unaffiliated Individual, Machine/Server/Applications, and Qualified Relying Parties.).

4.1. Application Procedures

The following application procedures apply to all applicants for an OATI webCARES System e-MARC certificate.

4.1.1. Business Representative Application

To verify a Business Representative, both the Sponsoring Organization's identity and the Security Officer's identity must be verified. To verify the Sponsoring Organization, the Applicant must submit the following Information for the Organization:

- Organization Legal Name
- Organization Mailing Address
- Organization Telephone Number
- Federal Employer Identification Number (EIN)
- DUNS Number

To verify the Organization's Security Officer's identity, the Security Officer must submit the following information:

- Full Name (First, Last, MI)
- Department and Job Title
- Work Address
- Work Telephone Number and Fax Number
- Work E-Mail Address
- Supervisor's Name (within Organization) and supervisor's Work Phone Number
- Authorized Party and contact information (an authorized party is defined as an Organization's employee with authority to bind the Organization by contract)

Each Subscriber's Organization will also be allowed to designate a Backup SO and an Audit Officer. For each of these entities specified, the same information as that of the Primary SO must be submitted and verified.

4.1.2. Unaffiliated Individual Application

An Unaffiliated Individual may apply for an OATI e-MARC certificate for his or her own personal use. An Unaffiliated Individual, by definition, will not be applying for an OATI e-MARC certificate as the Agent of an Organization. Therefore, unlike a Business Representative, the Unaffiliated Individual must be Identified and Verified solely using his or her own personal information. An Unaffiliated Individual applying for an e-MARC certificate and access to the OATI webCARES System must submit the following identification information:

- Full Name (First, Last, MI)
- Home Mailing Address
- Home Phone Number
- E-Mail Address
- Social Security Number
- Place and Date of Birth

- Currently Valid Credit Card Number and
- Driver's License Number (and State of issuance), Passport Number, Alien Registration Number, or State Issued Identification Card Number (and State of Issuance)

OATI will maintain unpublished information in a secure, confidential manner. OATI will only use personal identification information submitted to complete the OATI SIVP process.

An Unaffiliated Individual will not be allowed to submit the name of a Backup SO or Audit Officer. An Unaffiliated Individual, as a SO will be solely responsible for his or her own certificate(s) at all times.

4.1.3. Machine, Server, or Application

In the case of a Machine, Server, or Application, the individual responsible for the entity will be verified as the SO. Therefore, the SO who will manage the certificate(s) for the Machine, Server, or Application must submit both the Organization and Personal information to be Identified and Verified. The Organization and SO information to be submitted is the same as listed above for a Business Representative in section 4.1.1. Additionally, the SO for a Machine, Server, or Application must submit the following information identifying the entity itself:

- Machine, Server, or Application Name
- Location on the Network (i.e. IP Address)
- System URL (if applicable)

As with a Business Representative, a Backup SO and Audit Officer may be specified for the Machine, Server, or Application certificate request.

4.1.4. Qualified Relying Party

A qualified Relying Party must submit the same information as a Machine, Server, or Application.

4.2. Identification and Verification Procedure

Once an e-MARC certificate application has been submitted, OATI personnel will undertake specific procedures to Identify and Verify that a Subscriber is actually the person being represented. For security reasons, OATI cannot disclose the exact Identification and Verification Procedures in this CPS.

As an example of the Identification and Verification Procedures followed for a Business Representative, OATI will access Dunn & Bradstreet's service to verify that the DUNS Number submitted matches the information in the actual Dunn & Bradstreet database. OATI will also contact the appropriate Federal Agency to confirm that the Federal Employer Identification Number (EIN) submitted exists and is linked to the Organization submitted in the form.

The OATI SIVP is internally documented and will be completed for every application submitted. No exceptions will be made for any Subscriber for any reason. All Subscribers must complete the entire SIVP process to ensure that their Identity is Verified to commercially reasonable industry standards.

4.2.1. Unsuccessful Identification and Verification Procedure

If any application for an OATI e-MARC certificate fails for any reason, the applicant will be notified in a commercially reasonable manner as soon as practicable. An unsuccessful applicant may reapply for an OATI e-MARC certificate. OATI will not inform an unsuccessful applicant regarding which piece(s) of information failed to verify. The responsibility of ensuring that complete and accurate data have been submitted to OATI is the sole responsibility of the applicant.

For security purposes, an application submitted by an applicant that has previously failed the OATI SIVP will undergo strict scrutinization. The previously failed applicant must provide OATI with any additional information or documentation required for the verification procedure.

At any time, OATI may refuse to approve an application for an e-MARC certificate for any reason at its sole discretion. Upon refusal to accept an application, OATI will notify the applicant within a commercially reasonable time. In addition, OATI reserves the right to provide information to U.S. Federal Agencies for security purposes.

4.2.2. Successful Identification and Verification Procedure

Upon completion of a successful OATI SIVP, the applicant will be informed in writing by Electronic Mail. The Electronic mail will include instructions for accessing the OATI webCARES System and acquiring OATI certificates. Contemporaneously, OATI shall contact a verified OATI webCARES Security Officer to provide that entity with a username and temporary password for the system. The Electronic mail is sent to the Security Officer e-mail address listed in the appropriate application form. The additional contact for supplying a username and temporary password will be by telephone to the number listed on the application form for the entity.

5. OATI webCARES e-MARC Certificate Issuance

Upon signing an OATI webCARES User Agreement, a Subscriber will be eligible to receive an OATI e-MARC certificate. OATI personnel will contact a Subscriber using the e-mail address listed in their application form. The e-mail contact will contain information describing the OATI webCARES System. In addition, the e-mail will contain the URL for the OATI webCARES System along with instructions for initially using the webCARES System to download and install a SO certificate. Concurrent to an email being sent to the Subscriber, OATI will also contact the Subscriber using an out-of-band communication method to transfer the Subscriber a username and temporary password that will allow access to the OATI webCARES System.

5.1. Certificate Issuance Support

OATI shall provide all necessary user instructions, guides, and support to aid a Subscriber in downloading and installing an OATI e-MARC certificate issued by the OATI webCARES System. These resources are only available to a verified and trusted Subscriber of the OATI webCARES System.

5.2. Subscriber's Obligation to Review and Correct e-MARC Certificate

Upon accessing the OATI webCARES System for the first time to download a certificate, the Subscriber must review and verify that all information represented in the e-MARC certificate is correct and accurate. If the certificate information is found to be incorrect, the Subscriber shall not download and install the e-MARC certificate. In addition, the Subscriber must inform OATI webCARES personnel as soon as practical to allow corrections to be made to the certificate. Once corrections are completed, OATI personnel will contact the Subscriber to inform him or her that the certificate is now correct and ready to be utilized.

5.3. Subscriber's Acceptance of e-MARC Certificate

By downloading and installing an OATI webCARES System issued e-MARC certificate, a Subscriber affirmatively accepts the Subscriber Obligations stipulated within this CPS. In addition, by accepting the certificate, the Subscriber warrants that all information and representations made by the Subscriber, that are included in the e-MARC certificate, are true and accurate.

5.4. Certificate Operational Period

By downloading an e-MARC certificate from the OATI webCARES System, the Subscriber automatically commences the operational period of the e-MARC certificate. All e-MARC certificates issued by the OATI webCARES System Issuing Authority have a validity period of one (1) year from the time they are downloaded by a Subscribing SO.

5.5. Publication within the OATI Repository

Immediately upon download of an e-MARC certificate from the OATI webCARES System, the OATI Repository is automatically updated with the certificate's information.

5.6. SO's Duty to Protect Private Key(s)

By accepting and issuing e-MARC certificates using the OATI webCARES System, a Security Officer assumes the duty to control and protect the Private Keys of the e-MARC certificates. A Security Officer has a duty to inform all

End Users that the Security Officer has issued an e-MARC certificate to regarding the applicability and requirements of this CPS.

6. e-MARC Certificate Usage

6.1. Use of OATI e-MARC Certificates

6.1.1. Acceptable Uses of e-MARC Certificates

e-MARC certificates issued by the OATI webCARES System are suitable for the following applications and uses:

- Energy Market Transactions
- Energy or Transmission Scheduling
- Filings with Government Agencies
- Filings with Law Enforcement Agencies
- Application Processes
- Financial Transactions within the Energy Markets Community
- Billing, Metering, and Invoicing
- Conveyance and Transfer of Operational Data
- Conveyance and Transfer of System Reliability Data

6.1.2. Unacceptable Uses of e-MARC Certificates

e-MARC certificates issued by the OATI webCARES System are unsuitable for the following applications or uses:

- Transactions or Data Transfers that, if compromised or falsified, may cause physical injury or loss of life
- Transactions or Data Transfers, that if compromised or falsified, may result in imprisonment
- Transactions or Data Transfers deemed illegal under federal law

6.2. Digital Signature Validity

A digital signature created during the operational period of a valid e-MARC certificate whose certificate chain can be successfully confirmed is binding against and non-reputable by the holder of the key pair listed in the e-MARC certificate.

6.3. Failure of Digital Signature Confirmation

If an e-MARC certificate issued from the OATI webCARES System cannot be properly confirmed, then the party relying on the e-MARC certificate assumes all risks associated with relying on a non-confirmable certificate.

6.4. Security Measures

Any party signing with or relying upon an e-MARC certificate issued by the OATI webCARES System that is associated with any data transfer shall apply reasonable security measures to assure that the data and digital signature are authentic and that confidentiality and integrity are assured.

7. e-MARC Certificate Revocation

An e-MARC certificate issued by the OATI webCARES System shall only be revoked by the Security Officer with responsibility for the certificate or by the OATI Certification Authority Administrator. e-MARC certificate revocation will take place using the appropriate tools available to the Security Officer within the OATI webCARES System.

7.1. Conditions Requiring e-MARC Certificate Revocation

Where the following conditions or circumstances occur, an e-MARC certificate issued by the OATI webCARES System must be immediately revoked by the appropriate Security Officer or the OATI webCARES Administrator:

- When any of the information on the e-MARC certificate changes or becomes obsolete.
- When a Private Key, or the media holding the Private Key, is suspected to be compromised or actually is compromised.
- When the parties listed as the Security Officer and Backup Security Officer no longer represent a Business Organization (certificates may not be revoked if the Backup Security Officer assumes the responsibility the departed Security Officer).
- When a device, server, or application is no longer active or no longer affiliated with the sponsoring Organization.
- Upon a change of an Unaffiliated Individual or Business Representative's Company's registration information.
- If the OATI CA learns, or reasonably suspects, that a Subscriber's Private Key has been compromised, or
- If the OATI CA determines that an e-MARC certificate was not properly issued in accordance with the NERC e-MARC Policy or the OATI e-MARC CPS.

OATI specifically reserves the right to revoke any e-MARC certificate issued by the OATI webCARES System for any issue relating to security or other national interest. Additionally, OATI reserves the right to provide U.S. federal agencies information relating to the application for, use of, and misconduct associated with any e-MARC certificate issued through the OATI webCARES System.

7.2. e-MARC Certificate Revocation Procedure

All e-MARC certificates issued through the OATI webCARES System will be revoked using the webCARES System User Interface. e-MARC certificates may be revoked by either an appropriate Security Officer or an OATI webCARES System Administrator.

If the situation occurs where a certificate's Private Key has been compromised, the certificate shall be revoked as soon as reasonably practicable.

7.3. Notice of e-MARC Certificate Revocation

Upon revocation of an e-MARC certificate issued by the OATI webCARES System, the OATI CA will publish notice of the revocation within the OATI Repository via the OATI webCARES Certificate Revocation List (CRL). In addition, the appropriate Security Officer can view the current certificate status using the OATI webCARES System User Interface. The details of the revocation, such as the revoking party and the time stamp of the action, will become part of the webCARES Audit Log that is accessible by the appropriate parties.

7.4. OATI webCARES Certificate Revocation List (CRL)

The OATI Repository will post a new OATI Issuing Authority CRL every hour or when a revocation event occurs. Each CRL issued will have a twelve (12) hour validity period. The OATI CRL will be accessible from the OATI Repository page at the following URL: <http://www.oaticerts.com/repository/>.

7.5. Qualified Relying Party CRL Checking

Any Qualified Relying Party relying on e-MARC certificates issued by the OATI webCARES System must verify the status of all certificates listed in a certificate's validation chain. The check must be done against the latest CRL posted in the OATI Repository. The Qualified Relying Party must also verify the validity of the CRL posted in the OATI Repository to ensure that its validity period has not expired.

7.6. Effect of Revocation

Upon revocation of an e-MARC certificate, the e-MARC certificate's operational period shall be considered immediately terminated for all purposes. **A party relying on a revoked e-MARC certificate does so at their own risk.**

If an OATI Issuing Authority certificate is revoked, then all SO certificates issued by the Issuing Authority prior to the revocation are still valid. If applicable, only certificates issued by the Issuing Authority after revocation are invalid and must be immediately revoked.

Revocation of an e-MARC certificate shall not affect any contractual obligations between the Subscriber and OATI. In addition, the policies and duties set forth in this CPS shall remain in effect even after revocation occurs.

8. e-MARC Certificate Renewal

The OATI webCARES System will allow renewal of all e-MARC certificates issued by the system as long as they have not been previously revoked. The renewal process can be accomplished using the webCARES User Interface for certificate renewal.

8.1. e-MARC Certificate Renewal Procedure

At the time any e-MARC certificate issued by the OATI webCARES System is renewed, all Subscriber information will automatically populate the renewed certificate. When renewed, the certificate's Public and Private Keys will be regenerated for security purposes.

At the time of renewal, it is the duty of the Security Officer performing the renewal to verify that all user information associated with the certificate is correct and still applicable to the End User. If any of the information has changed, the Security Officer must inform the OATI webCARES Administrator immediately to allow for the correction of the user information before the certificate renewal actually occurs.

Procedures and requirements for e-MARC certificate renewal are subject to change at OATI's discretion without prior notice.

8.2. e-MARC Certificate Renewal Fee

OATI e-MARC certificate renewal fees are covered under the applicable User Agreement executed by the parties or by amendment to an existing User Agreement if the User is an existing OATI Customer.

9. e-MARC Certificate Expiration

The OATI webCARES System will distinguish and highlight certificates that are expiring within ninety (90) days via the Certificate Management User Interface. Notice to the Security Officer will be accomplished by a specific color code in the appropriate certificate row. This service will allow a Security Officer to timely and efficiently manage certificate renewals and avoid certificate expiration.

If an e-MARC certificate is allowed to expire, the underlying contractual obligations between the Subscriber and OATI remain valid. In addition, the policies and duties set forth in this CPS shall remain in affect even after expiration occurs.

Subscribers cannot renew an e-MARC certificate once its expiration date passes. The Subscriber must follow the procedures to re-issue the e-MARC End User certificate if another certificate is desired. The re-issuance of a new certificate will be accompanied by all appropriate fees as set out in the OATI webCARES User Agreement.

Procedures and requirements for e-MARC certificate expiration are subject to change at OATI's discretion without prior notice.

10. General Provisions Concerning the OATI Root, Intermediate, and Issuing Authorities

10.1. OATI Root

The OATI Root certificate utilizes a 4096 bit Key Size for security purposes. The OATI Root certificate is valid for eight (8) years from initial creation. Every four (4) years the Root certificate will be renewed. At the time of renewal, the Root certificate will undergo a standard re-key procedure to ensure the security of the Root certificate.

10.2. OATI Intermediate Authority

The OATI Intermediate certificate utilizes a 2048 bit Key Size for security purposes. The OATI Intermediate certificate is valid four (4) years from initial creation. Every two (2) years the Intermediate certificate will be renewed. At the time of renewal, the Intermediate certificate will undergo a standard re-key procedure to ensure the security of the Intermediate certificate.

10.3. OATI Issuing Authorities

The OATI Issuing Authority certificates utilizes a 2048 bit Key Size for security purposes. The OATI Issuing Authority certificates is valid two (2) years from initial creation. Every year the Issuing Authority certificates will be renewed. At the time of renewal, the Issuing Authority certificates will undergo a standard re-key procedure to ensure the security of the Issuing Authority certificates.

10.4. OATI webCARES Backup System

The OATI webCARES System includes a completely functioning backup system housed offsite in a secure location. The OATI webCARES Backup System shall be operational within a reasonable time after the loss of the primary webCARES System. The backup system has the same functionality as the primary system, including CRL creation and publishing every hour or upon revocation action.

10.5. OATI Root and Intermediate Authority CRL Publishing

The OATI Root and Intermediate Authority publish a separate CRL (independent of the OATI Issuing Authority CRL published every hour) every six (6) months. This CRL has a validity period of one (1) year. The OATI Root and Intermediate Authority have the capability to generate and publish a new CRL on demand if necessary. The OATI Root and Intermediate Authority CRL are published in the OATI Repository at the following URL: <http://www.oaticerts.com/repository/>.

11. Acronyms

- ANSI – American National Standards Institute
- AO – Audit Officer
- BSO – Backup Security Officer
- CA – Certification Authority
- CPS – Certification Practice Statement
- CRL – Certificate Revocation List
- CST – Central Standard Time
- DN – Distinguished Name
- EIN – (Federal) Employer Identification Number – aka Tax Identification Number
- e-MARC – Energy Market Access and Reliability Certificates
- IA – (Certificate) Issuing Authority
- ICA – Intermediate Certification Authority
- NA – Naming Authority
- NERC – North American Electric Reliability Council
- OATI – Open Access Technology International
- OID – Object Identifier
- PKI – Public Key Infrastructure
- RA – Registration Authority
- SIVP – Subscriber Identification and Verification Procedure
- SO – Security Officer
- SSL – Secure Socket Layer
- TLS – Transport Socket Layer
- URL – Uniform Resource Locator
- webCARES – web-based Certificate Administration, Renewal, and Enrollment System

12. Glossary

- **Audit Officer:** A person designated within an Organization to oversee and audit the actions of the Security Officer and Backup Security Officer as they pertain to issuing and managing OATI e-MARC certificates.
- **Backup Security Officer:** A person designated within an Organization to take on the duties and responsibilities of Security Officer in the absence of the Primary Security Officer.
- **Business Representative:** An agent of an Organization who applies for access to the OATI webCARES System for the purpose of issuing and managing OATI e-MARC certificates for End Users within the Organization.
- **Certificate Manufacturing Authority** (aka Issuing Authority): An entity responsible for Signing and Issuing Digital Certificates to Security Officers and End Users.
- **Certification Practice Statement:** A statement outlining the practices and procedures that a Certification Authority employs in issuing and signing Digital Certificates.
- **Digital Certificate:** An electronic record that lists a Public Key and confirms that the prospective signer identified in the certificate holds the corresponding Private Key.
- **Digital Signatures:** The transformation of a message using asymmetric cryptography such that the recipient of the message can use the sender's Public Key to accurately determine whether the message was created using the Sender's corresponding Private Key. A Digital Signature allows a recipient to determine if the message has been altered or changed after the Digital Signature was created.
- **Distinguished Name:** The set of information that identifies a person or entity in the real world. The format of an OATI e-MARC Distinguished Name is as follows: Country/State (or Province)/City/Organization/Organizational Unit/End User's Name/End User's E-Mail or IP Address.
- **End User** (aka End Entity): The recipient of an OATI e-MARC certificate. The End User is designated in the Distinguished Name assigned to the certificate.
- **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.
- **Key Pair:** A pair of mathematically derived keys made up of both a Public and Private Key.
- **Naming Authority:** An entity responsible for assigning and managing Distinguished Names within a Public Key Infrastructure. The Naming Authority is also responsible to ensure that all Distinguished Names assigned within the PKI are unique.
- **Private Key:** A mathematical key that is kept secret by the holder, which is used to create Digital Signatures. A Private Key may also be used to decrypt data or communications encrypted using its corresponding Public Key.
- **Public Key:** A mathematical key that can be made public and is used to verify digital signatures created with its corresponding Private Key. A Public Key may also be used to encrypt data or communications that can then be decrypted only using the corresponding Private Key. The Public Key of a key pair is typically made public by including the Public Key on the holder's Digital Certificate.

- **Public Key Infrastructure:** The term describing a managed infrastructure for the distribution and management of Public Keys and Digital Certificates. This includes the architecture, organization, techniques, practices, and procedures that are integrated to support the operation of a PKI.
- **Qualifying Relying Party:** A server or application that requires valid certificates from those entities or persons requesting access to the server or application. A Qualifying Relying Party will utilize an OATI e-MARC certificate to establish the necessary SSL or TLS session with the entity or person requesting access.
- **Registration Authority:** An entity responsible for Identifying and Verifying Subscribers for Digital Certificates within a Public Key Infrastructure.
- **Repository:** A database containing documentation and information relevant to the operation of a Public Key Infrastructure. This includes all copies of the relevant Policy Statement, Certification Practice Statement, Certificate Revocation Lists, Certification Authority Certificates, and other appropriate information.
- **Security Officer:** A person responsible for issuing and managing OATI e-MARC certificates within an Organizational Unit or an Unaffiliated Individual with access to the OATI webCARES System. Each individual, designated as a Security Officer, must have their identity verified using the OATI SIVP before they may access the OATI webCARES System or receive an OATI e-MARC certificate.
- **Unaffiliated Individual:** A person applying for access to the OATI webCARES System for the purpose of issuing and managing OATI e-MARC 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 a Security Officer.
- **OATI webCARES System:** OATI's web based certificate management system that will allow a Subscribed user to issue, revoke, renew, and audit certificates for an Organization.