Certificate Policy

for the

Energy Market Access and Reliability Certificate

(e-MARC) Program

Version 4.1.2
Draft

North American Electric Reliability Council
(NERC)

January 2005

TABLE OF CONTENTS

SECTION **PAGE**

SECTION 1

Introduction

1.1 OVERVIEW

In support of deregulated energy markets and system reliability functions, many computer-based systems, applications, and market participants have a significant requirement for the secure operation of these networked computer-based systems, electronic messages, and transactions. One mechanism to fulfill that requirement is the Public Key Infrastructure (PKI), which uses digital certificates to ensure availability of the following security services:

- Confidentiality: The assurance to an entity that no one can read a particular piece of data except the receiver(s) explicitly intended
- Authentication: The assurance to one entity that another entity is who he/she/it claims to be
- Integrity: The assurance to an entity that data has not been altered (intentionally or unintentionally) from sender to recipient and from time of transmission to time of receipt
- Technical Non-Repudiation: A party cannot deny having engaged in the transaction or having sent the electronic message

This PKI mechanism requires public key cryptography, which uses public key certificates to bind a person's or computer system's public key to his/her/its identity and to support symmetric encryption key exchange. In support of this requirement, the North America Electric Reliability Council (NERC) will oversee the administration of this Policy to North American deregulated energy markets and the associated system reliability functions (this certificate is referred to as an "Energy Market Access and Reliability Certificate" or "e-MARC"). NERC will provide this oversight by certifying Registry Domains, Registry Administrations, and service provider(s) to furnish the services presented in this Certificate Policy document (referred to herein as the "Policy").

The e-MARC security services will meet the following requirements for supporting PKI activities:

- Subscriber identification and authentication verification
- Control of computer and cryptographic systems
- Operation of computer and cryptographic systems
- Use of keys and public key certificates by Subscribers and Relying Parties
- Definition of rules to limit liability and provide a high degree of certainty that the stipulations of this Policy are being met

The reliability of the public key cryptography portion of the e-MARCs is a direct result of the secure and trustworthy operation of an established PKI, including equipment, facilities, personnel, and procedures.

This Policy describes the (1) roles, responsibilities, and relationships among the Registry Domains, Registry Administrators, Certification Authorities (CAs), Registration Authorities (RAs), Local Registration Authorities (LRAs), Certificate Manufacturing Authorities (CMAs), Repositories, Subscribers, and Policy Authority (PA) (referred to collectively as "Program Participants" [see sections 1.3.1 – 1.3.9 for definitions]) authorized to participate in the PKI described in this Policy; (2) the primary obligations and operational responsibilities of the Program Participants; and (3) the rules and requirements for the issuance, acquisition, management, and use of an e-MARC.

The Policy also provides a high-level description of the policies and operation of the e-MARC Program and follows *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, Request for Comment (RFC) 2527[1] of the Internet Engineering Task Force (IETF). Specific detailed implementations of this Policy appear in the Certificate Practice Statement (CPS) of any CA certified to issue certificates bound by this Policy.

The Glossary defines key terms used in this Policy. Key words used herein ("must," "must not," "required," "shall," "shall not," "should," "should not," "recommended," "may," and "optional") should be interpreted as described in RFC 2119. This interpretation is listed below.

- **Must:** This word, or the terms "required" or "shall," means that the definition is an absolute requirement of the specification.
- **Must Not:** This phrase, or the words "shall not," means that the definition is an absolute prohibition of the specification.
- **Should:** This word, or the word "recommended," means that there may exist valid reasons in particular circumstances to ignore a specific item, but the full implications must be understood and carefully weighed before choosing a different course.
- **Should Not:** This phrase, or the words "not recommended," means that there may exist valid reasons in particular circumstances when the specific behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
- **May:** This word, or the word "optional," means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation that does not include a particular option must be prepared to interoperate with another implementation, which includes the options, although with reduced functionality. Similarly, an implementation that includes a particular option must be able to interoperate with another implementation that does not include the option (except for the feature that the option provides).

[1] It is understood that RFC 3647 (dated Nov. 2003) has superceded RFC 2527, however, this Policy was developed prior to Nov. 2003 using the prior format and will not change at this time. Future revisions of this Policy may incorporate the new format under RFC 3647.

Additionally, for the purposes of this document the following key words should be interpreted as listed below.

- **Will:** This word should be interpreted the same as "should" and means that there may exist valid reasons in particular circumstances to ignore a specific item, but the full implications must be understood and carefully weighed before choosing a different course.
- **Can:** This word, like "may," means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation that does not include a particular option must be prepared to interoperate with another implementation, which includes the options, although with reduced functionality. Similarly, an implementation that includes a particular option must be able to interoperate with another implementation that does not include the option (except for the feature that the option provides).

1.2 CERTIFICATE POLICY IDENTIFICATION

Upon successfully passing e-MARC Certification & Accreditation (C&A), Authorized CAs shall be required to provide a list of policy Object Identifiers (OIDs) to the PA. Subsequent C&A will be in accordance with Section 2.7.1. The PA shall be responsible for providing the approved OIDs list to all e-MARC subscribers and Relying Parties.

Additionally, all Approved CAs shall provide their full certificate chain to the PA for public disclosure.

1.3 COMMUNITY AND APPLICABILITY

This Policy describes use of a bounded PKI; that is, it describes the rights and obligations of persons and entities authorized under this Policy to fulfill any of the following roles: Registry Domain, Registry Service Provider, Certificate Service Provider, End-Entity, and Policy Authority. Registry Service Provider roles refer to Registry Administrators. Certificate Service Provider roles are the Certification Authority, Registration Authority, Local Registration Authority, Certificate Manufacturing Authority, and Repository. End-Entity roles are Subscriber and Relying Parties. This section describes the requirements for persons and entities authorized to fulfill any of these roles. Section 2 contains general descriptions of these roles and their responsibilities.

1.3.1 Registry Domain

A Registry Domain may support the requirements cited in this Policy only if it is qualified and authorized to do so by the Policy Authority. To qualify as an authorized Registry Domain, the Registry must have the following capabilities:

- Serve as a Registry of organizations participating in an energy market.

- Include an organization's Data Universal Numbering System (DUNS) numbers or other industry-recognized, third-party-assigned business identifiers as one of their attributes.
- Associate a unique alphanumeric code (Entity Code) to each registered individual or organization.
- Identify each CA qualified as an Authorized CA.

1.3.2 Registry Administrator

A Registry Administrator may support this Policy and administer a qualified and authorized Registry Domain only if such Registry Administrator first qualified as an authorized Registry Administrator by performing the following actions:

- Enter into an appropriate e-MARC Contract.
- Document the specific practices and procedures the e-MARC Contractor must implement to satisfy the requirements of this Policy and of the Registry Domain that the Registry Administrator wishes to administer.

1.3.3 Authorized Certification Authority

A Certification Authority may issue certificates (e-MARCs) that identify this Policy only if such CA first qualifies as an "Authorized CA" by performing the following functions:

- Enter into an appropriate e-MARC Contract.
- Document the specific practices and procedures the e-MARC Contractor must implement to satisfy the requirements of this Policy in a Certification Practice Statement (*Certification Practice Statement for the e-MARC Program*) document.
- Pass an e-MARC security certification and accreditation (C&A) in accordance with section 2.7.

1.3.4 Registration Authority

A Registration Authority is responsible for identification and authentication of certificate subjects but does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an Authorized CA). For e-MARCs, the duties of an RA will be carried out locally by an LRA[2].

1.3.5 Local Registration Authority

A Local Registration Authority is a designated local individual that is responsible for identification and authentication of certificate subjects for a local community but does not sign or issue certificates (i.e., an LRA is delegated certain tasks on behalf of an Authorized CA). Each Authorized CA shall perform the role and functions of the LRA or may subcontract LRA

[2] For purposes of clarity, the term LRA will be used from this point forward to refer to the individual responsible for administering the RA duties at the local community level.

functions to third-party LRAs who agree to be bound by this Policy, provided that such arrangements are entered into by the parties in accordance with provisions stated in the CA's e-MARC CPS and are acceptable to the Policy Authority. However, the Authorized CA will remain responsible for the performance of those services in accordance with this Policy and its requirements under the Authorized CA's e-MARC Contract. The only exception would occur when the Policy Authority (see 1.3.9), pursuant to agreement among the Policy Authority and the Authorized CAs, agree to hold the subcontracted LRA responsible for defined portions of the LRA's role and functions.

1.3.6 Certificate Manufacturing Authority

Each Authorized CA shall perform the role and functions of the CMA. An Authorized CA may subcontract CMA functions to third-party CMAs who agree to be bound by this Policy, provided that such arrangements are entered into by the parties in accordance with provisions stated in the CA's e-MARC CPS and are acceptable to the Policy Authority. However, the Authorized CA shall remain responsible for the performance of those services in accordance with this Policy and its requirements under the Authorized CA's e-MARC Contract.

1.3.7 Repository

Each Authorized CA shall perform the role and functions of the Repository. An Authorized CA may subcontract performance of the Repository functions to a third-party Repository provider who agrees to be bound by this Policy, provided that such subcontractor is approved in advance by the NERC. The Authorized CA shall remain responsible for the performance of those services in accordance with this Policy and the requirements of its NERC e-MARC Contract.

1.3.8 End-Entity

An individual or organization (End-Entity) and its agents are Subscribers or Relying Parties as described in Sections 1.3.8.1 and 1.3.8.2 respectively, and may be issued e-MARCs for assignment to devices, groups, organizational roles, or applications provided that responsibility and accountability are attributable to an individual or an organization as defined in Section 7. Note that not all Relying Parties will require an e-MARC.

An e-MARC will only be issued after an Authorized CA receives a request and authorization for issuance from one or more Sponsors. They may be issued to employees, citizens, organizations, and others with whom the Sponsor has a relationship.

Eligibility for a certificate is at the sole discretion of the Authorized CA as specified in the Authorized CA's CPS, and the Authorized CA may administer any number of Subscribers.

1.3.8.1 Subscriber

An Authorized CA may issue an e-MARC to the following classes of Individual Subscribers:

- Individuals authorized to act on behalf of business entities (i.e., Sponsoring Organizations registered in an authorized Registry) recognized by the Authorized CA,

such as employees, officers, and agents of a Sponsoring Organization ("Business Representatives").
- An authorized representative of a Sponsoring Organization responsible for the request, renewal, key generation, and proper storage of a role-based certificate. Role-based certificates are designed to support multiple individuals and a business need, where the actions attributable to that certificate shall be non-repudiable to the Sponsoring Organization.
- Servers, devices, and/or computer applications that may take action on behalf of a business entity (i.e., Sponsoring Organizations registered in an authorized Registry) recognized by the Authorized CA, such as, but not limited to, Web servers, application servers, and custom applications.

1.3.8.2 Relying Parties

A Relying Party is defined as persons and entities who act in reliance on e-MARCs and/or digital signatures verified using e-MARCs. Relying Parties are those eligible energy sector entities that enter into an e-MARC Agreement (i.e., Memorandum of Understanding) to accept e-MARCs and agree to be bound by the terms of this Policy ("Relying Parties"). The Policy Authority has the right to add authorized users in this category at any time during the term of this Policy. Unlike Subscribers, not all Relying Parties will have or need an e-MARC.

1.3.9 Policy Authority

NERC will act as the Policy Authority overseeing the administration of this Policy, contract administration between Authorized Certification Authorities, and the authorization and approval of Registry Domains, Registry Administrators, Certification Authorities, Local Registration Authorities, Certificate Manufacturing Authorities, and Repositories that participate in conformance with this Policy. NERC will appoint a steering committee to assist it in carrying out its Policy Authority responsibilities, as necessary.

1.3.10 Applicability and Applications

There are two classes of certificate assurance within the e-MARC PKI. Each class of certificate assurance provides a different type of operational assurance, which shall be factored into the operational security requirements where e-MARCs are used to support operational missions, as follows:

- e-MARC PKI Software Token –Class 3: This class is the e-MARC PKI baseline for typical applications employed by end-users. This class of certificate assurance can be achieved with implementations that store private key(s) on software tokens (e.g., computer disks) and perform all cryptographic functions in software on the computer.
- e-MARC PKI Hardware Token - Class 4: This class is the e-MARC PKI baseline for all Privileged User operations. This class of assurance differs from the software-based token Class 3 in that storage of private key(s) is on a hardware token (e.g., smart card). All private key operations (e.g., signing, key exchange) are performed on this hardware token

and all cryptographic functions (to include key generation) may be performed on this hardware token.

1.3.10.1 Purpose

Subscribers and Authorized CAs may use e-MARCs to authenticate Subscribers to applications for individual and/or business purposes. Table 9 in section 7.1.6 summarizes key usage of e-MARCs.

1.3.10.2 Suitable Applications

Under the assertion of the Policy OIDs, an e-MARC may be used, but not be limited to being used, in the following suitable applications:

- Energy market transactions
- Energy or transmission scheduling
- Filings with government agencies
- Filings with law enforcement agencies
- Application filing processes, such as applying for or requesting access to physical facilities
- Financial transactions within the energy markets' communities
- Billing, metering, and invoicing
- Conveyance and transfer of operational data
- Conveyance and transfer of system reliability data

1.3.10.3 Restricted and Prohibited Applications

Under the assertion of the Policy OIDs, an e-MARC shall never be used for performing any of the following functions:

- Any transaction or data transfer that may result in imprisonment if compromised or falsified.
- Any transaction or data transfer deemed illegal under federal law
- The bulk encryption (encryption of large contiguous amounts) of data or documents using the certificate's public or private key. (Bulk encryption may be accomplished using symmetric key cipher algorithms with the e-MARC used for secure key exchange only. Public key cryptography is inefficient for encryption of large data files, while symmetric (secret) key cryptography provides a more efficient algorithm. The exchange of the symmetric key or "shared secret" can be securely achieved using a public key cryptographic mechanism to encrypt the "shared secret").

1.4 CONTACT DETAILS

1.4.1 Policy Administration Organization

NERC, as the Policy Authority and Contract Authority, administers this Policy; the address follows:

North American Electric Reliability Council
116-390 Village Boulevard
Princeton, New Jersey 08540-5731

1.4.2 Point of Contact

Attn.: e-MARC Administrator
Phone: (609) 452-8060
e-mail address: emarc.policy@nerc.com

1.4.3 Person Determining e-MARC CPS Suitability for the Policy

Attn.: e-MARC Administrator
Phone: (609) 452-8060
e-mail address: emarc.policy@nerc.com

SECTION 2

GENERAL PROVISIONS

2.1 OBLIGATIONS

This section provides general descriptions of the roles and responsibilities (obligations) of the e-MARC Program Participants operating under this Policy: Registry Domains, Registry Administrators, Authorized CAs, Local Registration Authorities, Certificate Manufacturing Authorities, Repositories, Subscribers, Relying Parties, and the Policy Authority. Additional obligations are set forth in other provisions of this Policy, the Policy Authority's e-MARC Contracts, the e-MARC Agreements with Relying Parties, and the Subscriber Agreements.

2.1.1 Registry Domain Obligations

A Registry Domain is responsible for containing a list of organizations that are eligible to participate under this Policy (see FERC 889). It is the obligation of a Registry Domain to perform the following functions:

- Maintain documented and enforceable requirements for registration.
- Obtain and maintain a registered Internet domain name to uniquely identify the Registry.
- Associate a unique alphanumeric code (Entity Code) with each registered entity.
- Identify each Certification Authority qualified as an "Authorized CA."
- Make all entries electronically and reliably available to all e-MARC Program Participants.

2.1.2 Registry Administrator Obligations

A Registry Administrator is responsible for ensuring that the Registry Domain it has been authorized to administer and maintain by the Policy Authority meets its obligations under this Policy. It is the obligation of the Registry Administrator to perform the following functions:

- Register market participants in the Registry and manage the application/enrollment process.
- Inform LRAs of all changes to the Registry
- Implement an identification and verification process to ensure that market participants are eligible in accordance with the Registry Domain's policies.
- Promptly reflect all registration changes or modifications that affect the status of e-MARCs issued to registered organizations, in accordance with the Certificate Revocation requirements of this Policy (see Section 4.4).

2.1.3 Authorized Certification Authority Obligations

This Policy describes the responsibilities of each Authorized CA that issues e-MARCs (and all of its optional subcontractor LRAs, CMAs, and Repositories) under its e-MARC Contract with the Policy Authority, and governs its performance with respect to all e-MARCs it issues.

An Authorized CA is responsible for all aspects of the issuance and management of e-MARCs, including the disclosure of required terms of use, as required in this Policy, to all End-Entities during the application/enrollment process; the identification verification and authentication process; the certificate manufacturing process; dissemination and activation of the certificate; publication of the certificate (if required); renewal, revocation, and replacement of the certificate; verification of certificate status upon request; and assurance that all aspects of the Authorized CA services and Authorized CA operations and infrastructure related to e-MARCs issued under this Policy are performed in accordance with the requirements, representations, and warranties of this Policy. The only exception shall take place when the Policy Authority, pursuant to agreement among the Policy Authority, Relying Parties, and the Authorized CAs, provides defined portions of the LRA's, CMA's, or Repositories' roles and responsibilities.

Each Authorized CA is responsible for providing an agreement page during End-Entity registration that requires e-MARC users to accept all rules and stipulations set forth in this Policy. Authorized CAs are responsible for overseeing, training, ad appointing LRAs.

2.1.4 Local Registration Authority Obligations

An LRA is responsible for the applicant registration, certificate application, and authentication of identity functions for Business Representatives, Business Representatives authorized to act on behalf of a Sponsoring Organization, Roles, Servers, and, eventually, devices (i.e., Relying Parties**)**. An LRA may also be responsible for handling revocation requests and for aspects of Subscriber education.

2.1.5 Certificate Manufacturing Authority Obligations

A Certificate Manufacturing Authority is responsible for the functions of manufacture, issuance, and revocation of e-MARCs. Authorized Certification Authorities may also serve as Certificate Manufacturing Authorities.

2.1.6 Repository Obligations

A Repository is responsible for maintaining a secure system for storing and retrieving e-MARCs, a current copy of this Policy, other information relevant to the e-MARC Program, and for providing information regarding the status of e-MARCs as valid or invalid (CRL) that can be requested by a Relying Party. This information shall be available no less than 99.95% during each year.

2.1.7 Subscriber Obligations

The responsibilities of each applicant (if approved, this role will be a Subscriber) for an e-MARC are as follows:

- Provide complete and accurate responses to all requests for information made by the Authorized CA or LRA during the applicant registration, certificate application, and authentication of identity processes.
- Generate a key pair using a reasonably trustworthy system and take reasonable precautions to prevent any compromise, modification, loss, disclosure, or unauthorized use of the private key.
- Upon issuance of an e-MARC naming the applicant as the Subscriber, review the e-MARC to ensure that all Subscriber information included in it is accurate and to expressly indicate acceptance or rejection of the e-MARC, consistent with Section 4.3.
- Use the e-MARC and the corresponding private key exclusively for purposes authorized by this Policy and only in a manner consistent with this Policy.
- Employ all reasonable diligence to securely store and protect the certificate's private key from loss, theft, misuse, unauthorized use, misappropriation, or any other circumstance that brings the authenticated use of the certificate into question.
- Instruct the issuing Authorized CA or LRA to revoke the e-MARC promptly upon any actual or suspected loss, disclosure, or other compromise of the private key, or, in the case of a Device or Business Representative's e-MARC, whenever the Subscriber or Device is no longer affiliated with the Sponsoring Organization or the Device is no longer active.
- Instruct the issuing Authorized CA or LRA to revoke the e-MARC immediately upon the Sponsoring Organization's cessation of functions requiring use of the certificate or within 60 days upon change of the Sponsoring Organization's identity (such as merger or acquisition).
- Permit the archive or backup of the private keys of certificates issued in software for Authentication by means of a backup copy made by the Subscriber, approved by the Authorized CA, and/or administered by the Subscriber's Sponsoring Organization. Archive or backup of Authentication certificates issued in hardware shall be in accordance with manufacturer instruction.
- Under no circumstances allow the private key of a certificate issued for Identity/Authentication under this Policy to be backed up or archive except by such means that are under the sole control of the Individual Subscriber.
- Under no circumstances shall the private key of a role based Identity/Authentication certificate stored in a hardware token be held in software back up or archive.

2.1.8 Relying Party Obligations

This agreement governs Relying Party performance with respect to the use of and reliance on e-MARCs, as follows:

- **Acceptance of Certificates.** Each Relying Party will accept e-MARCs issued by all

Authorized CAs. Acceptance does not provide authorization to any service provided by the Relying Party.

- **Certificate Validation.** Each Relying Party will validate every e-MARC it requests and receives with the Authorized CA that issued the certificate.
- **Reliance.** Each Relying Party may rely on a valid e-MARC for verifying the digital signature and symmetric key exchange only if:

  - The e-MARC was used and relied upon to authenticate a subscriber's digital signature for an application bound by this Policy.
  - Prior to reliance, the Relying Party (1) verified the digital signature by reference to the public key in the e-MARC, (2) verified that the status of the e-MARC was valid by checking validity dates, the certificate trust chain, and a current Certificate Revocation List (CRL)[3], (3) verified that an appropriate e-MARC OID (if applicable) is expressed in the certificate, and (4) validate that the CA is currently an Authorized CA as published by the PA.
  - The reliance was reasonable and made in good faith in light of all circumstances known to the Relying Party at the time of reliance.

2.1.9 Policy Authority Obligations

The Policy Authority is responsible for the terms of this Policy, e-MARC Contract administration, and the authorization and approval of Registry Domains, Registry Administrators, Certification Authorities, Local Registration Authorities, Certificate Manufacturing Authorities, and Repositories that participate in conformance with this Policy.

2.2 LIMITATIONS ON LIABILITIES

Nothing in this Policy shall alter or eliminate any other obligation, responsibility, or liability that may be imposed on any Program Participant by virtue of any contract or obligation that is otherwise applicable under relevant law(s).

2.3 RESPONSIBILITIES AND RELATIONSHIPS

2.3.1 Financial Responsibilities

A potential CA must demonstrate sufficient financial viability to be relied upon as an Authorized CA, including having adequate insurance coverage (e.g., Errors and Omissions coverage, liability insurance).

[3] Use of the Online Certificate Status Protocol (OCSP) will not be precluded; however, all vendors are required to support CRLs as a minimum.

2.3.2 Fiduciary Relationships

A subcontracted LRA, CMA, or Repository has a fiduciary relationship with its contracting Authorized CA for all information or data held by that LRA, CMA, or Repository.

2.3.3 Administrative Processes

No stipulation.

2.4 INTERPRETATION AND ENFORCEMENT

2.4.1 Governing Laws

The laws of New Jersey shall govern the enforceability, construction, interpretation, and validity of this Policy.

2.4.2 Severability, Survival, and Merger Notices

Should it be determined pursuant to judicial process that one section of this Policy is invalid or otherwise unenforceable; all other sections shall remain in effect until the Policy is revised. Requirements for revising this Policy and providing notice thereof are described in Section 8. All unchanged responsibilities, requirements, and privileges of this Policy shall be merged into the revised Policy upon release thereof.

2.4.3 Dispute Resolution Procedures

In the event of any dispute or disagreement between or among two or more of the Program Participants ("Disputing Parties") arising out of or relating to this Policy or e-MARC Contracts, CPS, or Agreements, the Disputing Parties shall use their best efforts to settle the dispute or disagreement through negotiations in good faith following notice from one Disputing Party to the other(s). Such negotiations may be mediated or arbitrated at the discretion of the Disputing Parties. If the Disputing Parties cannot reach a mutually agreeable resolution of the dispute or disagreement within sixty (60) days following the date of such notice, then the Disputing Parties may present the dispute to the e-MARC Contract Officer for resolution.

Any contract dispute between Authorized CAs and e-MARC Contract Officers shall be handled under the terms and conditions of the e-MARC Contract.

2.5 FEES

2.5.1 Certificate Issuance, Renewal, and Revocation Fees

The Authorized CA may impose a reasonable fee to issue or renew e-MARCs. The Authorized CA shall not impose a fee to revoke e-MARCs.

2.5.2 Certificate Access Fees

The Authorized CA shall not impose any certificate access fees on Subscribers or Relying Parties with respect to use of their own e-MARCs or the status of such e-MARCs.

2.5.3 Revocation Status Information Access Fees (Certificate Validation Services)

No fees shall be assessed for access to an Authorized CA's published CRL.

2.5.4 Fees for Policy Information

The Authorized CA shall not impose fees for access to Policy information.

2.5.5 Fees for Other Services

Reasonable fees, as set forth in contracts between individual parties, may be charged for other services (e.g., key archive, key replacement).

2.5.6 Refund Policy

There shall be no refunds of any fees from the Policy Authority under any circumstances.

2.6 PUBLICATION AND REPOSITORY

2.6.1 Publication of Authorized CA Information

Each Authorized CA shall operate a secure online Repository available to Subscribers and Relying Parties that must contain (1) all e-MARCs issued by the Authorized CA that have been accepted by the Subscriber, typically available via the Lightweight Directory Access Protocol (LDAP); (2) a CRL ; (3) the Authorized CA's e-MARC for its public key; (4) past and current versions of the Authorized CA's e-MARC CPS; (5) a copy of this Policy; and (6) other relevant information about e-MARCs. Submittal of such information to an Authorized CA's Repository, with the subsequent availability of such information to Subscribers and Relying Parties, constitutes "publication" for purposes of this Policy.

2.6.2 Frequency of Publication

All information to be published in the Repository shall be published promptly after such information is available to the Authorized CA. The Subscriber will publish e-MARCs issued by the Authorized CA promptly upon acceptance of such e-MARCs. Information relating to the status of an e-MARC will be published in accordance with the Authorized CA's e-MARC Contract and Section 4.4.4 of this Policy.

2.6.3 Access Controls

The Authorized CA shall not impose any access controls on this Policy, the Authorized CA's e-MARC for its public key, CRLs, and past and current versions of the Authorized CA's

e-MARC CPS. The Authorized CA may impose access controls on e-MARCs, in accordance with provisions of the Authorized CA's e-MARC Contract, with concurrence of the Policy Authority.

2.6.4 Repository Access and Security

For purposes of this Policy, the requirement of availability will be satisfied if the information can be accessed through or by means of a "site" or "page" via the Internet by means of a "browser" implementing the HyperText Transfer Protocol (HTTP). Such access to Subscribers and Relying Parties must be secure (e.g., HyperText Transfer Protocol with Secure Sockets Layer [HTTPS]) and provided in accordance with all of the security requirements reflected in this Policy and the Authorized CA's CPS.

2.7 QUALITY ASSURANCE INSPECTION AND AUDIT

The Authorized CA shall undergo e-MARC security certification and accreditation (C&A) audits as a condition of obtaining and retaining approval to operate as an Authorized CA under this Policy and the e-MARC Contract. The purpose of the C&A process shall be to verify that the Authorized CA has in place and follows a system that assures that the quality of its Authorized CA services conforms to the requirements of this Policy and the e-MARC Contract.

2.7.1 Frequency of Certification Authority C&A Compliance Audit

Certification Authorities shall undergo C&A under the direction of the Policy Authority, prior to initial approval as Authorized CAs, to demonstrate compliance with (1) this Policy, (2) their e-MARC CPS, and (3) their e-MARC Contracts. Recertification shall be required every 12 months or at any time that a significant change in their operations is made, whichever occurs first, to demonstrate continuing compliance with this Policy.

2.7.2 Identity/Qualifications of C&A Auditor

An independent security auditing firm acceptable to the Policy Authority that is qualified to perform a security audit on a CA shall conduct the C&A process in accordance with the set of procedures approved and published by the PA.

2.7.3 C&A Auditor's Relationship to Audited Party

The C&A auditor shall be an independent, unbiased party that is in no way, beyond the audit itself, associated with the party to be audited.

2.7.4 Topics Covered by C&A Quality Assurance Inspection and Audit

The C&A quality assurance inspection and audit shall be conducted based in part on the guidance provided in the *American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants (AICPA/CICA) WebTrust Principles and Criteria for Certification Authorities* document. The topics covered by the C&A quality assurance inspection and audit

will be sufficient to ensure to the Policy Authority that the prospective CA is capable of issuing certificates under this Policy.

2.7.5 Actions Taken as a Result of Deficiency

When the auditor finds a deficiency in a CA/CMA's operation or the stipulations of its CPS, the following actions must occur:

The auditor shall note the deficiency.

- The auditor shall notify the parties identified in Section 2.7.6 of the deficiency.
- The CA will propose an acceptable remedy within 30 days, including expected time for remediation, to the Policy Authority.
- During the agreed upon remediation period, the PA reserves the right to suspend Authorized CA activity depending upon the severity of the deficiencies noted.
- If an acceptable remedy cannot be agreed to, the PA has the right to decertify the CA upon which time the CA will be suspended and the PA will issue a 60-day notice to the e-MARC community prior to the Authorized CA's certificate being revoked.

The Policy Authority will determine the appropriate remedy, up to and including revocation of the CA's status as an Authorized CA.

The Policy Authority will address any identified deficiencies with the potential or Authorized CA. An Authorized CA whose authority has been revoked may reapply for e-MARC certification, upon correction of the deficiencies. CAs who re-apply for e-MARC Certification are subject to a full and complete C&A process.

2.7.6 Communication of Results

The Certification Authority shall make the results of the security C&A audit available to the Policy Authority for determining the CA's suitability for initial and continued performance as an Authorized CA. The Policy Authority will use the results of the security C&A review, along with any other test evidence the CA offers, for determining the CA's suitability for initial and continued performance as an Authorized CA. At no time will this information provided by a prospective CA be made public or disclosed by the Policy Authority without the prior consent of the subject CA. A pass/fail result will be provided to the public to inform the public of the availability of an Authorized CA. A list of Authorized CAs will be maintained on the NERC Website.

2.8 CONFIDENTIALITY

2.8.1 Types of Information to Be Kept Confidential

The following types of information shall be kept confidential:

- **Subscriber Information.** The Authorized CA shall protect the confidentiality of personal information regarding Subscribers that is collected during the applicant registration, e-MARC application, authentication, and certificate status checking processes in accordance with the *Privacy Act of 1974 and Amendments*[4]. Such information shall be used only for the purpose of providing Authorized CA Services and carrying out the provisions of this Policy and the e-MARC Contract, and shall not be disclosed in any manner to any person without the prior consent of the Subscriber, unless otherwise required by law, except as may be necessary for the performance of the Authorized CA Services in accordance with the e-MARC Contract. In addition, personal information submitted by Subscribers:

  - Must be made available by the Authorized CA to the Subscriber involved following an appropriate request by such Subscriber
  - Must be subject to correction and/or reasonable and appropriate revision by such Subscriber
  - Must be protected by the Authorized CA in a manner designed to ensure the data's integrity and confidentiality
  - Cannot be used or disclosed by the Authorized CA for purposes other than the direct operational support of e-MARCs unless such use is authorized by the Subscriber involved or is required by law, including judicial process

  Under no circumstances shall the Authorized CA (or any authorized LRA, CMA, or Repository) have access to the private keys of any Subscriber to whom it issues an e-MARC to be used solely for generating digital signatures when the non-repudiation bit is expressed. See Section 7 for certificate profile guidelines.

- **Other Subscriber Information.** The Authorized CA shall take reasonable steps to protect the confidentiality of Relying Parties or other Subscriber information provided to the Authorized CA. Such information shall be used only for providing Authorized CA Services and carrying out the provisions of this Policy and the e-MARC Contract, and shall not be disclosed in any manner to any person except as may be necessary for the performance of the Authorized CA Services in accordance with the e-MARC Contract or as otherwise required by law, including judicial process.

2.8.2 Types of Information Not Considered Confidential

Information contained within a single e-MARC or related status information shall not be considered confidential when the information is necessary for providing Authorized CA Services and carrying out the provisions of this Policy and the e-MARC Contract. e-MARCs and their contents published in a Repository shall not be considered confidential for any reason.

[4] *Privacy Act of 1974 and Amendments* (as of January 2, 1991), 5 U.S.C. Sec. 552.a, Title 5, Part 1, Chap. 5, Subchapter II.

2.8.3 Disclosure of Certificate Revocation Information

No stipulation.

2.8.4 Release to Law Enforcement Officials

No stipulation.

2.8.5 Release as Part of Civil Discovery

No stipulation.

2.8.6 Disclosure Upon Owner's Request

No stipulation.

2.8.7 Other Information Release Circumstances

No stipulation.

2.9 INTELLECTUAL PROPERTY RIGHTS

Private keys shall be treated as the sole property of the legitimate holder of the corresponding public key identified in an e-MARC. This Policy and "Energy Market Access and Reliability Certificates," otherwise referred to as "e-MARCs," are the property of the Policy Authority and may be used only by Authorized CAs in accordance with the provisions of this Policy and the Authorized CA's e-MARC Contract. Any other use of the above without the express written permission of the Policy Authority is expressly prohibited.

SECTION 3

IDENTIFICATION AND AUTHENTICATION

3.1 INITIAL REGISTRATION

Subject to the requirements noted below, applications for e-MARCs may be communicated from the applicant to an Authorized CA or an Authorized LRA, and authorizations to issue e-MARCs may be communicated from an Authorized LRA to an Authorized CA, in the following form: (1) electronically, provided that all communication is encrypted and digitally signed, (2) by First Class mail, or (3) in person. The applicant must also specify in his/her application under which Registry Domain he/she is requesting a certificate and include either the applicant's unique "Entity Code" (or "Business Code" for business applicants) assigned to him/her by the Registry and the official company name of the Sponsoring Organization.

3.1.1 Types of Names

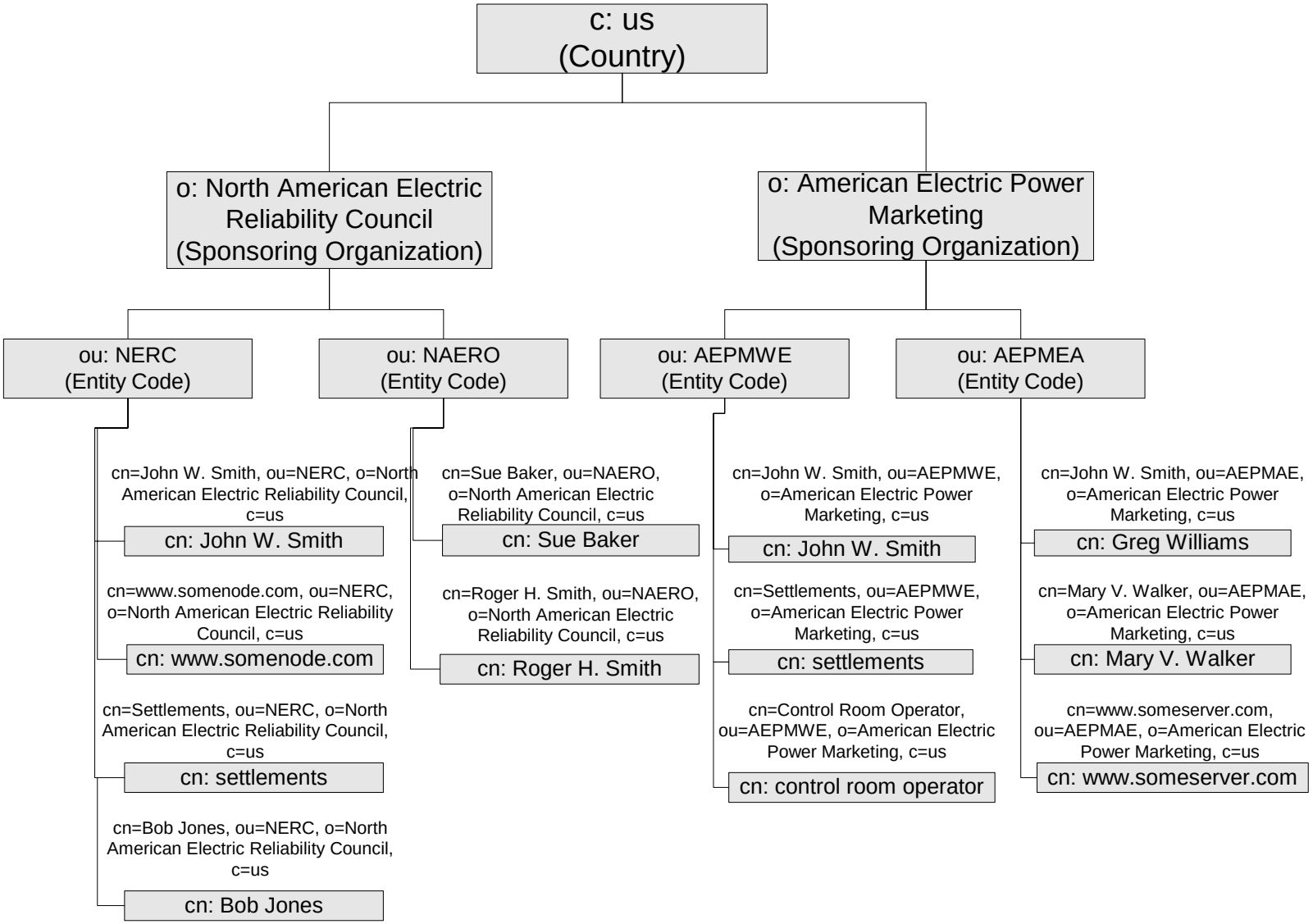
Names in all e-MARC *Subject* field shall contain a unique X.500 Distinguished Name (DN) that must be a printable string, must contain some string of characters (not be blank), and in the case of a Business Representative, must clearly and uniquely identify the official company name of the Sponsoring Organization and the Entity Code of the Sponsoring Organization as they appear in the Registry Domain. Figure 1 illustrates an example DN hierarchy.

3.1.2 Name Meanings

For Business Representatives and Business Representative authorized to act on behalf of a Sponsoring Organization the authenticated Common Name should be the combination of first name, surname, and an optional middle initial. For devices and applications (e.g., Web Servers) the authenticated common name should be the fully qualified domain name of the device/application. Finally, for a role-based certificate the authenticated common name should be the role under which the certificate will be used.

A certificate issued for a device, application, or role must include the point-of-contact's e-mail address and the name of the person who is responsible for that device, application, or role in the *SubjectAltName* field of the certificate.

For Business Representatives, servers**,** and devices, the DN within the certificate's Subject field must also contain the Entity Code of the Sponsoring Organization in the Organizational Unit (OU) field and the official company name of the Sponsoring Organization being represented in the Organization (O) field.



(**NOTE**: C = Country, O = Organization, OU = Organizational Unit, CN = Common Name)

Figure 1. Example DN Hierarchy

Each CA asserting this policy shall only sign certificates with subject names from within a name-space approved by the PA.

When technical means exist for imposing these constraints (such as the name constraints certificate extension), they shall be used. Otherwise, these constraints shall be imposed procedurally or contractually.

3.1.3 Rules for Interpreting Various Name Forms

Rules for interpreting name forms are contained in the applicable certificate profile (see Section 7) and are established by a naming authority if one exists or by the Authorized CA. The naming authority shall be identified contractually or in an Authorized CA's CPS.

3.1.4 Name Uniqueness Across Authorized CAs

Name uniqueness across all e-MARCs must be enforced and each Authorized CA shall enforce name uniqueness within the DNs of the X.500 name space that it has been authorized. When other name forms are used, they too must be allocated such that name uniqueness across all active e-MARCs is ensured. An Authorized CA shall document in its CPS those name forms that will be used and how the Authorized CA will allocate names within the Subscriber community to guarantee name uniqueness among current and past Subscribers (e.g., if "Joe Smith" leaves an Authorized CA's community of Subscribers, and a new, different "Joe Smith" enters the community of Subscribers, these two individuals must be provided unique names). The Entity Codes and Sponsoring Organizations contained in an e-MARC's DN shall be provided and maintained by the Registry Administrator.

3.1.5 Name Claim Dispute Resolution Procedures

The Authorized CA shall investigate and correct if necessary any non-unique names (or "name collisions") brought to its attention. If appropriate, the Authorized CA shall coordinate with and defer to the appropriate naming authority or Registry Administrator any name claim disputes, but the Authorized CA has the right to make all final decisions.

3.1.6 Recognition, Authentication, and Role of Trademarks

The use of trademarks will be reserved to registered trademark holders.

3.1.7 Verification of Possession of Key Pairs

The Authorized CA shall verify that the applicant (to include a role-based certificate applicant acting as an authorized representative of the Sponsoring Organization) possesses the private key corresponding to the public key submitted with the application by using a key transfer protocol or equivalent method, and that these keys form a functioning pair.

3.1.8 Authentication of Sponsoring Organization

If the applicant is requesting a Business Representative, device, application, or role-based e-MARC, in addition to verifying the applicant's individual identity, as outlined in Section 3.1.9, and authorization to represent the Sponsoring Organization, the Authorized CA shall also verify that the entity exists, is registered with a unique Entity Code in an approved Registry Domain, and conducts business at the address listed in the e-MARC application.

In conducting its review and investigation, the Authorized CA shall validate information concerning the entity to establish its authenticity, including legal company or business name, type of entity place of incorporation or principal registration, principal business address (including number and street, city, ZIP code), and principal business telephone number. The Authorized CA may rely on the Registry to verify the business credentials (e.g., Entity Code, Business Code) of the Sponsoring Organization.

If the Sponsoring Organization had previously established the identity of the entity organization using a process that satisfies the Authorized CA and this Policy and there have been no changes in the information presented, then the Authorized CA or LRA and the prospective Subscriber may use private shared information to verify the identity of the Sponsoring Organization.

3.1.9 Authentication of Individual Identity

Authorized Individuals may be authenticated through an electronically submitted application or by personal presence. In accordance with the e-MARC Contract requirements, the Authorized CA shall verify all of the following identification information supplied by the applicant: first name, middle initial, and last name; current address (number and street, city, ZIP code); and principal telephone number.

Subscriber identification must be confirmed via a PA-approved identity-proofing process that incorporates the following factors:

- Submission by the applicant of at least three individual identity items, which must be verified through reference to multiple independent data sources along with crosschecks for consistency. Examples follow:

  - Government-issued identification (ID)
  - United States Alien Registration Number or similar Canadian or Mexican identification
  - Passport number and country
  - Current employer name, address (number and street, city, postal code), and principal telephone number
  - Current valid state-issued driver's license number or state-issued identification card number
  - Social Security Number, or other national identification
  - Date of birth
  - Place of birth

- At least one of the above data sources used must be based on a government-issued ID process or the equivalent identity-verification process.

The use of an alternative notification process that is linked to the requesting individual's physical postal mail address, or equivalent, and verification that the information contained in the certificate application is correct shall be permitted.

In addition, the Authorized CA shall verify the following organizational information:

- The applicant is a duly authorized representative of the Sponsoring Organization as an employee, partner, member, agent, or other association.
- The Sponsoring Organization's identity as specified in Section 3.1.8.

3.2 ROUTINE REKEY (CERTIFICATE RENEWAL)

The longer and more often a key is used, the more susceptible it is to loss or compromise. This weakens the assurance provided to a Relying Party that the unique binding between a key and its named Subscriber is valid. Therefore, it is important that a Subscriber periodically obtain new keys **and** reestablish its identity. Rekeying a certificate means that a new certificate is created that is identical to the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key); a different serial number; and may be assigned a different validity period. Therefore, e-MARCs shall also be rekeyed when they are renewed.

In accordance with the e-MARC Contract, the Authorized CA shall accept e-MARC renewal requests from Subscribers within 90 days from the scheduled end of the operational period (expiration date) of the e-MARC, provided the e-MARC is not currently under revocation or has expired. e-MARCs for subscriber's certificates shall be renewed in accordance with the validity periods contained in Table 6 of Section 7.1.3.

Every third year, the certificate's Subscriber must identify itself in requesting a new request, in accordance with Section 3.1. This process is not designed to place undue burden on the Subscriber or Authorized CA, but rather to verify that the Subscriber still has a valid need for an e-MARC. The Authorized CA shall renew e-MARCs issued to Subscriber(s) only after completing successful identity-proofing verification in accordance with the requirements for individual identity authentication specified in Section 3.1.9.

3.3 REKEY (CERTIFICATE RENEWAL) AFTER REVOCATION

In accordance with the e-MARC Contract, revoked or expired e-MARCs shall not be renewed. Applicants without a valid e-MARC shall be reauthenticated by the Authorized CA or an authorized LRA through a new e-MARC application, just as with an initial applicant's registration, and shall be issued a new e-MARC.

3.4 REVOCATION REQUEST

In accordance with the e-MARC Contract and Section 4.4, an e-MARC revocation request that is submitted electronically may be authenticated on the basis of a digital signature using that e-MARC's associated key pair (i.e., self-revocation) or by a digitally signed request of the PA, associated CA, or LRA using the associated private key of the requestor's certificate. Alternative mechanism may be used for PA, CA, or LRA revocation requests so long as the requestor can be positively authenticated. The identity of the person submitting a revocation request in any other manner shall be authenticated in accordance with Section 3. Revocation requests authenticated on the basis of the e-MARC's associated key pair shall always be accepted as valid. Other revocation request authentication mechanisms may be used as well, including a request in writing signed by the Subscriber and sent via First Class mail or by any means with equivalent assurances of security. These authentication mechanisms must balance the need to prevent unauthorized revocation requests against the need to revoke certificates quickly.

SECTION 4

Operational Requirements

4.1 CERTIFICATE APPLICATION

The following list describes the certificate application process:

- **Application Initiation.** Table 1 lists those persons who may initiate the e-MARC application process

Table 1. Persons Allowed To Initiate the e-MARC Application Process

Applicant or Potential Subscriber	Authorized Initiator
Business Representative, server/device, or application	Sponsoring Organization or potential Subscriber
Relying Party	Relying Party

- **Application Form.** An applicant for an e-MARC shall complete an e-MARC application and provide requested information in a form prescribed by the Authorized CA and this Policy.
- **Applicant Education and Disclosure.** At the time of e-MARC application, the Authorized CA shall inform applicants of the advantages and potential risks associated with using e-MARCs to access nodes (secure servers) electronically and provide information to Subscribers regarding the use of private keys and digital signatures created with such keys, and Subscriber obligations.

4.1.1 Application

It is the intent of this Policy to identify the minimum requirements and procedures that are necessary to support trust in the use of a PKI system for e-MARCs, and to minimize imposition of specific implementation requirements on CMAs, applicants, and all other Relying Parties.

The applicant and/or the CMA must perform the following steps when an applicant applies for a certificate:

- Establish and record identity of an applicant (per Section 3.1).
- Obtain a public/private key pair for each certificate required.
- Establish that the public key forms a functioning key pair with the private key held by the applicant (per Section 3.1.7)
- Provide a point of contact for verification of any roles or authorizations requested.
- Acknowledge the terms and conditions of acceptance and use of the certificate by the applicant.

These steps may be performed in any order that is convenient for the CMA and applicant, and does not defeat security, but all steps must be completed prior to certificate issuance. All communications among CMAs supporting the certificate application and issuance process shall be authenticated and protected from modification. Any electronic transmission of shared secrets shall be protected (e.g., encrypted) using means commensurate with the requirements of the data to be protected by the certificates being issued.

Authorized CAs implementing this Policy shall certify other CAs (to include cross-certification) only as authorized by the Policy Authority and then may only do so within the constraints embodied within such authorizations.

Requests by CAs for Authorized CA certificates shall be submitted to the Policy Authority via the point of contact identified in Section 1.4 and shall be accompanied by a CPS written in the format specified by the *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* document [RFC 2527].

The Policy Authority will evaluate the submitted CPS for acceptability. The Policy Authority may require an initial compliance audit, performed by parties of the Policy Authority's choosing, to ensure that the CMA is prepared to implement all aspects of the submitted CPS, prior to the Policy Authority authorizing the CMA to issue and manage certificates asserting this Policy.

Authorized CAs shall only issue certificates asserting this Policy upon receipt of written authorization signed by a duly authorized representative of the Policy Authority, and then may only do so within the constraints embodied within such authorization.

4.1.2 Delivery of Subscriber's Public Key to Certificate Issuer

Public keys shall be delivered to the certificate issuer in a way that binds the applicant's verified identification to the public key being certified. This binding shall be accomplished using means that are as secure as the security offered by the keys being certified. The binding shall be accomplished using cryptographic, physical, procedural, and other appropriate methods. The methods used for public key delivery shall be stipulated in the CPS.

4.2 CERTIFICATE ISSUANCE

Upon successful completion of the Subscriber identification and authentication process in accordance with the e-MARC Contract, the Authorized CA shall create the requested e-MARC, notify the applicant thereof, and make the e-MARC available to the applicant. The Authorized CA shall use a secondary notification process linked to the e-MARC applicant's physical postal mailing address, or its physical equivalent, to provide notification of the e-MARC issuance only to the Subscriber and the authorized representative of the Sponsor. Authorized e-MARC CAs may use e-mail as a certificate-issuance notification method provided that no sensitive information such as pass phrases, unlock codes, etc., are transmitted in those e-mails.

Upon issuance of an e-MARC, the Authorized CA shall warrant to all Program Participants that:

- The Authorized CA has issued, and will manage, the e-MARC in accordance with the requirements in this Policy.
- The Authorized CA has complied with all requirements in this Policy when identifying the Subscriber and issuing the e-MARC.
- There are no misrepresentations of fact in the e-MARC actually known to or reasonably knowable by the Authorized CA and the Authorized CA has verified the information in the e-MARC pursuant to this Policy.
- Information provided by the Subscriber for inclusion in the e-MARC has been accurately transcribed to the e-MARC.
- The e-MARC meets the material requirements of this Policy.

4.2.1 Delivery of Subscriber's Private Key to Subscriber

Private keys shall be delivered to the Subscriber or authorized representative for server certificates, based on Table 2.

Table 2. Private key Delivery Requirements

Certificate Key Usage	Category	Minimum Private Key Delivery Requirement
CA certificates	Certificate Authorities	FIPS 140 Level 3 hardware device (token)
Authentication Certificates (Web Authentication)	Servers/Devices	Must remain within the cryptographic boundary of the cryptographic module in which it was created or delivered via a secure PKCS #12 file or equivalent.
	Business Representative	Must remain within the cryptographic boundary of the cryptographic module in which it was created or delivered via a secure PKCS #12 file or equivalent.
	Role	FIPS 140 Level 2 hardware device (token)
Identity Certificates (Digital Signing)	Servers/Devices	Must remain within the cryptographic boundary of the cryptographic module in which it was created or delivered via a secure PKCS #12 file or equivalent.
	Business Representative	Must remain within the cryptographic boundary of the cryptographic module in which it was created.
	Role	FIPS 140 Level 2 hardware device (token)

4.2.2 Role-Based Certificates (Tokens)

Certificates shall be issued to persons whenever possible. For cases where there are several persons acting in one capacity (role), a certificate may be issued that corresponds to a private key that is shared by multiple Subscribers. In the case of a shared certificate:

- An authorized representative of the Sponsoring Organization shall be responsible for ensuring control of the private key, including maintaining a list of Subscribers who have access to use of the private key, and accounting for which Subscriber had control of the key at what time.
- The list of those holding the shared private key must be provided to, and retained by, the Authorized CA and/or LRA.

For security reasons, role-based certificates must be issued in Federal Information Processing Standard (FIPS)-140-compliant hardware tokens only. Currently for e-MARCs, hardware tokens must meet the standards for FIPS 140 Level 2. The procedures for issuing tokens for use in shared key applications must comply with all other stipulations of this Policy (e.g., key generation, private key protection, and Subscriber obligations).

Certificates issued to a role-based entity shall be non-repudiable to the organization and not to an individual. The Sponsoring Organization shall be held responsible for all non-repudiable transactions issued by the Sponsoring Organizations role-based certificates.

4.3 CERTIFICATE ACCEPTANCE

As described in the e-MARC Contract and as a condition to issuing the e-MARC, the Subscriber shall indicate acceptance or rejection of the e-MARC to the Authorized CA and acknowledge the Subscriber obligations under Section 2.1.7. During this acceptance process, the Subscriber must indicate, through any mechanism the Authorized CA provides, that he/she has read and agreed to the stipulations of this Policy. By accepting the e-MARC, the Subscriber warrants that all information and representations made by the Subscriber that are included in, and relied upon in issuing, the e-MARC are true and accurate.

4.4 CERTIFICATE REVOCATION

4.4.1 Who Can Request Revocation

The only persons permitted to request revocation of an e-MARC issued pursuant to this Policy are the Subscriber, an authorized representative of the Sponsoring Organization, the LRA, or the issuing Authorized CA.

4.4.2 Circumstances for Revocation

4.4.2.1 Permissive Revocation

As described in the e-MARC Contract, a Subscriber may request revocation of his/her e-MARC at any time for any reason. A Sponsoring Organization may request revocation of an e-MARC issued to its Business Representative (or device or individual) at any time for any reason.

4.4.2.2 Required Revocation

An Authorized CA, Subscriber, Sponsoring Organization (where applicable), or LRA is responsible for promptly requesting revocation of an e-MARC under at least the following circumstances:

- When the private key, or the media holding the private key, associated with the e-MARC (the Subscriber's private key) is, or is suspected of having been, compromised.
- When the individual named as a Business Representative no longer represents, or is no longer affiliated with, the Sponsoring Organization.
- When a device or server is no longer active or no longer affiliated with a Sponsoring Organization.
- If an Authorized CA learns, or reasonably suspects, that the Subscriber's private key has been compromised.
- If the issuing Authorized CA determines that the e-MARC was not properly issued in accordance with this Policy and/or the Authorized CA's e-MARC CPS.
- The Authorized CA or Sponsoring Organization shall revoke the Subscriber's certificate if these entities determine that the certificate has been used in a manner that violates this Policy.

4.4.3 Revocation

4.4.3.1 Procedure for Revocation Request

As described in the e-MARC Contract, an e-MARC revocation request should be promptly communicated to the issuing Authorized CA, either directly or through the LRA authorized to accept such notices on behalf of the Authorized CA. An e-MARC revocation request may be communicated electronically if it is digitally signed with the private key of the requesting entity. Alternatively, the requester may request revocation by contacting the issuing Authorized CA or its LRA in person and providing adequate proof of identification in accordance with this Policy.

4.4.3.2 Revocation Request Grace Period

Revocation is immediate if the certificate has been compromised, lost, or stolen, or if the private key has become unrecoverable. In all other situations, certificates should be revoked as soon as practical; however, a 2-week (10 business days) grace period may be granted at the Authorized CA's discretion.

4.4.4 CRL Issuance Frequency

An Authorized CA must ensure that it issues an up-to-date CRL at least every twelve (12) hours. Additionally, the validity period of a CRL shall not exceed 24 hours. An Authorized CA must ensure that its CRL issuance is synchronized with any directory synchronization to ensure the accessibility of the most recent CRL to e-MARC holders and Relying Parties. It is strongly suggested that Authorized CAs provide multiple locations from which to obtain their CRLs to

avoid possible denial of service to Relying Parties. When a certificate is revoked, an updated CRL must be issued within four (4) hours of the event.

4.4.5 Revocation/Status Checking

4.4.5.1 CRL Checking Requirements

A Relying Party must check the status of all certificates in the certificate validation chain against the current CRL prior to their use. The Relying Party must also verify the authenticity and integrity of CRLs using the digital signature attached to the CRL. The application shall refresh the CRL at least every 12 hours.

4.4.5.2 Online Revocation Checking Requirements

Each Relying Party will validate via the CRL for every e-MARC it receives for every transaction. A transaction includes, but is not limited to, Web-based authentication, digital signature of documents, digital signature of e-mail, and SSL session establishment.

4.4.6 Other Revocation Advertisements

4.4.6.1 Other Forms Available

An Authorized CA may also use other methods to publicize the certificates it has revoked. Any alternative method must meet the following requirements:

- The alternative method must be described in the Authorized CA's approved CPS.
- The alternative method must provide authentication and integrity services commensurate with the assurance class of the certificate being verified.

4.4.6.2 Checking Requirements

A Relying Party may also use other methods to verify the status of certificates. Any alternative method must meet the following requirements:

- The alternative method must be described in the Authorized CA's approved CPS.
- The alternative method must provide authentication and integrity services commensurate with the assurance class of the certificate being revoked.

4.4.7 Special Requirements for Key Compromise

In the event of the compromise, or suspected compromise, of an Authorized CA signing key, the Authorized CA must immediately notify the Policy Authority and all Authorized CAs to whom it has issued cross-certificates.

In the event of the compromise, or suspected compromise, of any other entity's signing key, an entity must notify the issuing Authorized CA immediately.

An Authorized CA must ensure that it's CPS or publicly available documents and appropriate agreements contain provisions outlining the means it will use to provide notice of compromise or suspected compromise.

4.5 COMPUTER SECURITY AUDIT PROCEDURES

All significant security events, including at least those specified in Section 4.6.1, on each Authorized CA's system must be logged. Audit logs for all Authorized CAs should be written in real time to a non-erasable medium or a medium for which erasure, rewrites, and wipes have been fully disabled. These logs shall be maintained in sufficient detail for the Authorized CA to use them as an aid in troubleshooting and as an aid in diagnosing system security breaches. Audit trail files are to be maintained in a secure manner in accordance with section 4.6, and shall not be provided to any entity external to the Authorized CA for any use other than those mentioned in Section 2.7 of this Policy.

4.6 RECORDS ARCHIVAL

4.6.1 Types of Events Recorded

The data and files archived by or on behalf of each Authorized CA must include:

- All e-MARC applications, including all application information
- Certificate issuances and transactions
- System start-up and shutdown actions
- Authorized CA application start-up and shutdown actions
- Attempts to create, remove, or set passwords or change the system privileges of the Security Officer, or Administrator
- Changes to Authorized CA details and/or keys
- Changes to certificate creation policies (e.g., validity period)
- Login and logoff attempts
- Unauthorized attempts at network access to the Authorized CA's system
- Unauthorized attempts to access system files
- Generation of entity keys
- Revocation of certificates
- Attempts to initialize, remove, enable, and disable Subscriber activities, and update or recover their keys
- Failed read-and-write operations on the certificate and CRL directory
- Discrepancy and compromise reports

All logs, whether electronic or manual, should contain the date and time of the event and the identity of the entity that caused the event.

An Authorized CA should also collect and consolidate, either electronically or manually, security information, whether or not system or automatically generated, such as:

- Physical access logs
- System configuration changes and maintenance
- Personnel changes
- Discrepancies and compromise reports
- Record of the destruction of media containing key material, activation data, or personal Subscriber information

An Authorized CA must ensure that all logged events are explained in an audit log summary and that audit logs are actively reviewed either manually or automatically on a regular basis. Any responsive or remedial actions taken following these reviews must be documented.

4.6.2 Retention Period for Archive

Archives of the recorded events listed in Section 4.6.1 shall be retained and protected against modification, loss, or destruction for a period as specified in the Authorized CA's CPS, but in any event not less than seven years without any loss of data. Applications necessary to read these archives must be maintained for the identical period.

4.6.3 Protection of Archive

The archive media must be protected at least at the level required to maintain and protect all Subscriber information and data from disclosure, modification, or destruction. The media on which the archive is stored must be protected from modification and destruction either by physical security alone, or by a combination of both physical security and cryptographic protection, and must also be provided adequate protection from environmental threats such as temperature, humidity, and magnetism.

4.6.4 Archive Backup Procedures

Adequate backup procedures must be in place so that in the event of the loss or destruction of the primary archives, a complete set of backup copies will be readily available within a 48-hour period.

4.6.5 Requirements for Time-Stamping of Records

Archived data, files, and similar records need not be time-stamped as of their creation or modification, but all logs must contain data indicating the time each logged event occurred.

4.6.6 Archive Collection System (Internal or External)

Archive data shall be recorded in any expedient manner.

4.6.7 Procedures to Obtain and Verify Archive Information

Procedures detailing how to create, collect, verify, package, transmit, and store Authorized CA archives shall be published in the Authorized CA's CPS. Only authorized persons shall be permitted to access the archive.

4.7 CA Key Lifetime

The lifetime of a CA certificate (and hence its public/private key pair) is defined as the time under which that CA may issue certificates. The validity period is defined as the time under which that CA certificate is considered valid for validity checking. The maximum lifetime of the self-signed CA issuing End-Entity e-MARCs will be a maximum of 6 years. The validity period of the public/private key pair of each of these CAs will be longer to account for the changeover from the current CA to the new CA.

4.8 COMPROMISE AND DISASTER RECOVERY

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

The Authorized CA must establish business procedures that outline the steps to be taken in the event of the corruption or loss of computing resources, software and/or data. Where a Repository is not under the control of the Authorized CA, an Authorized CA must ensure any agreement with the Repository provides that business continuity procedures be established and documented by the Repository, and must independently verify, or obtain independent verification, that such procedures are followed.

4.8.2 Authorized CA Public Key Is Decommissioned

In the event of a compromised Authorized CA's private key (Section 4.8.3) or the CA is terminated as an Authorized CA, the Authorized CA (or PA in cases where the CA is non-compliant) must provide instruction to its subscribers on the proper removal of the compromised CAs certificate chain from applicable web browsers and applications.

In addition, all subscribers (Individuals, Organizations, and Relying Parties) must remove the compromised certificates from all certificate stores.

After addressing the factors that led to decommissioning, the Authorized CA may:

- Generate a new Authorized CA signing key pair.
- If a new pair is generated, re-issue certificates to all Subscribers and ensure that all CRLs are signed using the new private key (see Section 6.3.3)

4.8.3 Authorized CA Private Key Is Compromised (Key Compromise Plan)

Each Authorized CA must have in place an appropriate *Key Compromise Plan* document that addresses the procedures that will be followed in the event of a compromise of the private signing key used by an Authorized CA to issue e-MARCs. Such plan shall include procedures for revoking all affected e-MARCs and promptly notifying all Subscribers and all Relying Parties, substantially similar to the procedures under Section 4.8.2.

4.8.4 Facility Experiences a Natural or Other Disaster (Disaster Recovery/Business Resumption Plan)

An Authorized CA must have in place an appropriate *Disaster Recovery/Business Resumption Plan* document. Such a plan shall be detailed within the Authorized CA's e-MARC CPS or other appropriate documentation made available to and approved by the Policy Authority.

4.9 AUTHORIZED CA CESSATION OF SERVICES

In the event that an Authorized CA ceases operation or its participation as an Authorized CA in the e-MARC Program is otherwise terminated:

- All Subscribers, Sponsoring Organizations, and Relying Parties must be promptly notified of the cessation.
- All e-MARCs issued by an Authorized CA shall be revoked via CRL no later than the next update time or time of cessation whichever occurs first.
- All current and archived e-MARC identity proofing, certificate validation/revocation/renewal, policy and practices, billing, and audit data shall be transferred to the Policy Authority or arrangements shall be made to provide the information upon request made at any time during a period of not less than 3 years. Transferred data shall not include non-e-MARC data.

If the Authorized CA has arranged for the transfer and retention of the Authorized CA's keys and information to another Authorized CA that meets the requirements of this Policy and the Policy Authority, service may be continued under the new Authorized CA and certificates need not be revoked.

4.10 CUSTOMER SERVICE CENTER

Each Authorized CA shall implement and maintain an e-MARC Customer Service Center to provide assistance and services to Subscribers and Relying Parties, and a system for receiving, recording, responding to, and reporting e-MARC problems within its own organization and for reporting such problems to the Policy Authority.

SECTION 5

Physical, Procedural, and Personnel Security Controls

5.1 PHYSICAL SECURITY CONTROLS

Each Authorized CA, and all associated LRAs, CMAs, and Repositories, shall implement appropriate physical security controls to restrict access to the hardware and software (including the server, workstations, and any external cryptographic hardware modules or tokens) used in connection with providing Authorized CA Services. Access to such hardware and software shall be limited to those personnel performing in a trusted role as described in Section 5.2.1.

5.1.1 Site Location and Construction

Physical security controls shall be implemented that protect the Authorized CA's hardware and software from unauthorized access and damage. Authorized CA cryptographic modules shall be protected against theft, loss, and unauthorized use.

The Authorized CA shall implement appropriate physical security controls to restrict access to and protect the hardware and software used in connection with providing Authorized CA Services. Proper physical barriers shall be in place. For instance, surrounding walls shall extend from real ceiling to real floor, not raised floor or suspended ceiling. The facility will be locked and intruder detection systems will be activated while the facility is unoccupied.

Fire prevention and protection controls will be in place, including a fire extinguisher system. CA facilities must be constructed to prevent exposure of systems to water. All electronic physical security devices will be tested daily.

The Authorized CA equipment shall be dedicated to the e-MARC Authorized CA function; it shall not perform non- Authorized CA-related functions. The Authorized CA's facility shall also store backup and distribution media in a manner sufficient to prevent loss, tampering, or unauthorized use of the stored information.

5.1.2 Asset Classification and Management

Inventory records must be generated and maintained for all equipment used to support Authorized CA operations. Classification of this equipment according to its function and media is required. Assignment of responsibility for each piece of equipment to individuals is also required, thus maintaining a chain of custody.

5.1.3 Physical Access Controls

Physical access to the Authorized CA's systems will be limited to authorized individuals with a valid purpose to enter. Authentication controls will be used to access areas containing the

Authorized CA's systems. Those persons not authorized to enter the facility but who require access for business purposes can enter the facility only if escorted by authorized personnel. All access to the Authorized CA facility must be logged.

5.1.4 Power and Air Conditioning

The Authorized CA facility shall be supplied with power and air conditioning sufficient to create a reliable operating environment. Personnel areas within the facility shall be equipped with sufficient facilities to satisfy operational needs and comply with all applicable health and safety requirements.

5.1.5 Cabling and Network Devices

Cabling and network devices supporting Authorized CA Services shall be protected from interception and damage.

5.1.6 Media Storage, Handling, Destruction, and Reuse

Authorized CA storage media and devices containing storage media shall be checked to ascertain if they contain sensitive data prior to disposal or reuse. Items found to contain sensitive information will be physically destroyed or securely overwritten. All storage media associated with Authorized CA Services shall be protected from environmental threats of temperature, humidity and magnetism.

5.1.7 Physical Security Controls for End-Entities

A Subscriber shall physically protect any password or Personal Identification Number (PIN) that allows entry into the Subscriber's digital certificate. Passwords or PINs should be memorized and not written down. If a password or PIN needs to be written down, it shall be stored in a locked file cabinet or container accessible only to authorized personnel.

5.2 PROCEDURAL SECURITY CONTROLS

5.2.1 Trusted Roles

An Authorized CA must ensure a separation of duties for critical Authorized CA functions to prevent one person from maliciously using the Authorized CA system without detection.

An Authorized CA should provide for a minimum of two distinct PKI personnel roles, distinguishing between day-to-day operation of the Authorized CA system and the management and auditing of those operations. The selection and distinction of trusted roles must provide resistance to insider attack.

5.2.2 Number of Persons Required Per Task

An Authorized CA shall use commercially reasonable practices to ensure that one person acting alone cannot circumvent security safeguards or otherwise compromise the integrity of the e-MARC PKI.

5.2.3 Identification and Authentication for Each Role

All Authorized CA personnel must have their identity and authorization verified under procedures substantially similar to those stipulated in Sections 3.1.9 and 5.3.2 before they are:

- Included in the access list for the Authorized CA site
- Included in the access list for the Authorized CA system
- Given a certificate for the performance of their Authorized CA role
- Given an account on the PKI system

Each of these certificates and accounts must be:

- Directly attributable to a single individual (not shared)
- Securely stored
- Restricted to actions authorized for that role through the use of Authorized CA software, operating system and procedural controls

Authorized CA operations must be secured, using mechanisms such as token-based strong authentication and encryption, when accessed across a shared network.

5.3 PERSONNEL SECURITY CONTROLS

Each Authorized CA and its LRA, CMA, and Repository subcontractors shall formulate and follow personnel and management policies sufficient to provide reasonable assurance of the trustworthiness, and competence of their employees and of the satisfactory performance of their duties in a manner consistent with this Policy.

5.3.1 Personnel Security Controls for Certification Authorities

The individual(s) assuming the role of the Authorized CA Administrator should exhibit loyalty, trustworthiness and integrity, and should demonstrate a high degree of security consciousness.

All Authorized CA personnel shall:

- Not be assigned duties that would interfere with their other responsibilities
- Not knowingly have been previously relieved of a past assignment for reason of negligence or non-performance duties
- Be appointed in writing by an approving authority
- Have received proper training in the performance of their duties

5.3.2 Clearance Procedures

Clearance procedures, such as background checks consistent with all legally binding obligations, are required for personnel filling positions where a high degree of trust is required. Clearance procedures must be an ongoing process.

5.3.3 Training

Authorized CA employees must receive training in the organizational policies and procedures to ensure adherence to the Authorized CA's policies. Training must be an ongoing and documented process.

5.3.4 Sanctions for Unauthorized Actions

In the event of actual or suspected unauthorized action by a person performing duties with respect to the operation of the Authorized CA, his/her access to the system must be revoked or suspended. Breach of this Policy, whether through negligence or with malicious intent, is subject to privilege revocation, administrative discipline, and/or civil and/or criminal prosecution.

5.3.5 Employee Termination Controls

Once an employee holding a position of trust or any level of system access leaves the organization, his/her physical access and system access must be revoked immediately.

5.3.6 Contracting Personnel Controls

Contractor personnel employed to support any Authorized CA are subject to the same clearance procedures specified in Section 5.3.2.

5.3.7 Documentation Supplied to Personnel

This Policy and relevant parts of the e-MARC CPS shall be made available to the Authorized CA personnel and Subscribers. Operations manuals shall be made available to Authorized CA personnel to facilitate the operation and maintenance of the Authorized CA, but must not be copied by them or given to a non-authorized person, and must be returned upon termination of access rights.

5.3.8 End-Entity Controls

Subscribers shall be provided with information on the use and protection of the software used within the e-MARC PKI. The Authorized CA shall provide a support telephone number for all Subscribers.

SECTION 6

Technical Security Controls

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

The following list describes key pair generation:

(a) **General.** Key pairs for all Program Participants must be generated so that the private key is not known by any entity other than the authorized user of the key pair except as noted for key backup and/or archive. LRA keys may be generated either in hardware or software, although hardware-based key generation is preferred. Authorized CA keys must be generated in hardware devices. Key pairs for Subscriber and Relying Party applications can be generated in either hardware or software. Minimum requirements for key pair generation are shown in Table 3.

Table 3. Minimum Key Pair Generation Requirements

Certificate Key Usage	Category	Minimum Key Generation Requirement
CA certificates	Certification Authority	FIPS 140 Level 3 hardware device
CMA certificates	Certificate Manufacturing Authority	FIPS 140 Level 3 hardware device
LRA certificates	Local Registration Authorities	FIPS 140 Level 1 hardware or software
Authentication Certificates (Web Authentication)	Business Representative	FIPS 140 Level 1 hardware or software
	Device	FIPS 140 Level 1 hardware or software
	Role	FIPS 140 Level 1 hardware
Identity Certificates (Digital Signing)	Business Representative	FIPS 140 Level 1 hardware or software
	Device	FIPS 140 Level 1 hardware or software
	Role	FIPS 140 Level 1 hardware

(b) If key pair generation is performed in hardware, the private key must be non-exportable from the hardware device that created it. If key pair generation is performed in software, the application used to generate the key pair must be accessible to the Subscriber and initiated by the authorized user of the key pair.

(c) If key pair generation is performed in a manner inconsistent with the policies described in this section, the public key is not a candidate for signing or certificate issuance by an Authorized CA. If any Program Participants discovers that a certificate was issued in violation of items 6.1.1(a) or 6.1.1(b) above, the certificate must be revoked.

(d) Exact FIPS-level requirements are documented and explained in National Institute of Standards and Technology (NIST) document, FIPS Publication 140-2, *Security Requirements for Cryptographic Modules*, which includes all change documents.

6.1.2 Private Key Delivery to End-Entities

Private keys shall be delivered as specified in Section 4.2.1.

6.1.3 Subscriber Public Key Delivery to Authorized CAs

As part of the e-MARC application process, the Subscriber's public key must be transferred to the LRA or Authorized CA in a way that ensures that (1) it has not been changed during transit, (2) the sender possesses the private key that corresponds to the transferred public key, and (3) the sender of the public key is the legitimate user claimed in the certificate application. If the application process is done on-line, the delivery mechanism should be in accordance with the *Internet X509 Public Key Infrastructure Certificate Management Protocols* (see RFC 2510) or via an equally secure manner.

6.1.4 Authorized CA Public Key Delivery to Users

Authorized CAs must deliver public keys to applicants in accordance with an Authorized CA's CPS.

6.1.5 Key Lengths

Key lengths and algorithms shall be a minimum of 1024 bits and preferably 2048 bits for all e-MARC End-Entities (Subscribers, Business Partners, Devices, and Relying Parties). All Authorized CAs shall use a minimum of 2048 bits for all keys. Table 4 identifies the minimum lengths of all keys.

Table 4. Minimum Key Lengths

Certificate Key Usage	Min. Key Length
CA certificates	2048
Authentication certificates	1024
Digital Signing certificates – Individual	1024

Section 7 contains detailed information describing each certificate.

6.1.6 Public Key Parameter Generation

Public key parameters shall always be generated and checked in accordance with the standard that defines the crypto-algorithm in which the parameters are to be used. For example, public key parameters for use with algorithms defined in the *Digital Signature Standard* [FIPS 186-2] shall be generated and tested in accordance with FIPS 186-2. Public key parameters for use with the RSA algorithm defined in PKCS #1 shall be generated and checked in accordance with PKCS-1, and so on. Whenever a crypto-algorithm is described in accordance with FIPS 186-2, the parameter generation and checking requirements and recommendations of FIPS 186-2 shall

be required of all entities generating key pairs whose public components are to be certified by the e-MARC PKI.

6.1.7 Key Usage Purposes (as per X.509 Version 3 key usage field)

All e-MARC keys shall be certified for use in digital signature. The only exceptions to this separation are server certificates. Since most server applications can only accept a single certificate, multiple usages must be allowed. The use of a specific key is determined by the key usage extension in the X.509 certificate. This restriction is not intended to prohibit use of protocols that provide authenticated connections using key management certificates.

All e-MARC software certificates shall include a single key for use with digital signatures. Such certificates shall be generated and managed in accordance with their respective signature certificate requirements, except where otherwise noted in this Policy. Certificates issued for digital signatures must assert non-repudiation and may be used for authenticating data.

All e-MARC hardware token certificates may include a single key for use by a single individual or multiple individuals (role-based) in support of legacy applications. Such role-based certificates shall be generated and managed in accordance with their respective signature certificate requirements.

6.2 AUTHORIZED CA PRIVATE KEY PROTECTION

Each Authorized CA, LRA, and CMA shall each protect its private key(s) in accordance with the provisions of their e-MARC Contract, this Policy, and best industry practices.

The relevant standard for cryptographic modules is *Security Requirements for Cryptographic Modules* (current version of FIPS 140). The Policy Authority may determine that other comparable validation, certification, or verification standards are sufficient. These standards will be published by the Policy Authority. Cryptographic modules shall be validated to meet or exceed the FIPS 140 level identified in this section, or validated, certified, or verified via one of the standards published by the Policy Authority. A PKI should provide the option of using any acceptable cryptographic module, to facilitate the management of Subscriber certificates.

All cryptographic modules shall be operated such that the private asymmetric cryptographic keys shall never be output in plaintext. No private key shall appear unencrypted outside the Authorized CA equipment.

No one shall have access to a private signing key but the Authorized CA. Any private key management keys held by an Authorized CA shall be stored in a FIPS validated device. Section 6.1.1 stipulates the minimum cryptographic module requirements for key pair generation.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archiving

The issuing Authorized CA must retain all verification public keys. Under no circumstances shall an attempt be made to archive or create a repository for private signing keys except as described for one or more of the following methods:

- **Backup:** The End-Entity named in the certificate's subject makes a duplicate copy of the certificate, including the private key. The duplicate is secured in such a way that only the End Entity can restore the certificate and private key. In the case of a role-based certificate an End-Entity is an authorized agent of the organization.
- **Archive:** The authorized representative of the End-Entity's organization makes a duplicate copy of the certificate including the private key. The duplicate is secured in such a way that only the authorized representative of the End-Entity's organization can restore the certificate and private key (see Section 6.1.1).

Table 5 lists the approved mechanism for each type of e-MARC.

Table 5. Key Backup/Archive Allowances

Certificate Key Usage	Category	Backup Allowed	Archive Allowed
CA certificates	Certificate Authorities	Per FIPS Level 3 requirements	Per FIPS Level 3 requirements
Authentication Certificates (Web Authentication)	Business Representative	Yes	Yes
	Device	Yes	Yes
	Role[5]	Yes	Yes
Identity Certificates (Digital Signing)	Business Representative	Yes	No
	Device	Yes	No
	Role[6].	Yes	No

6.3.2 Usage Periods for the Public and Private Keys (Key Replacement)

Subscriber key pairs must be replaced in accordance with the validity periods specified in the applicable certificate profile (see Section 7.1).

[5] Backups of role based certificate must be maintained securely off-line until such time as they are needed for a recovery effort.

[6] Backups of role based certificate must be maintained securely off-line until such as time they are needed for a recovery effort.

6.3.3 Restrictions on Authorized CA's Private Key Use

The private key used by Authorized CAs for issuing e-MARCs shall be used only for signing such certificates and, optionally CRLs.

6.4 ACTIVATION DATA

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

Each computer that is used to administer or operate within the PKI framework (e.g., CA, RA, LRA, and CMA hardware) must be assessed to have a minimum level of security before accessing the infrastructure. Each machine must be free of viruses, Trojan horse vulnerabilities, spyware, key loggers (except those required by a CA's audit policy and CPS), or any other malicious software or hardware that could be used to intercept or compromise the e-MARC PKI or portions thereof.

6.6 LIFE-CYCLE TECHNICAL CONTROLS

New equipment and software, including patches and updates, must be thoroughly tested on a separate platform prior to implementation on operational systems.

A *Security Policy* document must exist. The *Security Policy* must provide guidance facilitating the secure operation of the Authorized CA and ensuring the integrity of its operating environment.

6.7 NETWORK SECURITY CONTROLS

Access to unused ports and services must be denied. Users shall be provided access only to services that they are specifically authorized to use. Remote access and connections from remote computers must be limited to only those absolutely necessary, and must be properly authenticated. External threats shall be mitigated by controls such as firewalls, network intrusion detection systems, and router access control lists to protect the internal network. The Authorized CA shall document security attributes of all network services.

6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

Sections 6.1.1 and 6.2 state requirements for cryptographic modules.

SECTION 7

Certificate and CRL Profiles

7.1 CERTIFICATE PROFILE

All e-MARCs shall contain public keys used for authenticating the sender of an electronic message and verifying the integrity of such messages (i.e., public keys used for digital signature verification and symmetric key exchange).

The Authorized CA shall create and maintain e-MARCs that conform to the International Telecommunications Union – Telecommunications Sector (ITU-T) Recommendation X.509, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*, October, 2001.

All e-MARCs must include a reference to an OID for this Policy within the appropriate field, and contain the required certificate fields according to the Authorized CA's CPS and the e-MARC Contract.

The Authorized CA certificate shall be issued in the X.509 format, and it will include a reference to the OID for this Policy (or equivalent OID) within the Certificate Policies field. Supported certificate extensions shall be identified in the e-MARC CPS.

This section describes the certificate fields and standard extensions that the e-MARC PKI uses. The e-MARC PKI will provide several standard certificates. Standard certificates have a specific profile and support large communities of users. IETF RFC 3280 provides additional details on the specific format and content of certificates. X.509 Version 3 and RFC 3280 provide guidance that must be supplemented with choices identified in this profile. Each Authorized CA will provide Certificate profiles for all certificates it intends to issue under this Policy. Documentation of these profiles must be provided in the Authorized CA's CPS in a format similar to that in Appendix A. Interoperability testing with the Authorized CAs is designed to help ensure compatibility with the profiles defined under this Policy.

The e-MARC Authorized CAs issue separate certificates to e-MARC End-Entities, (which include Subscribers, Relying Parties, Business Representatives, and Roles) for Authentication Certificates (Web Authentication) and Identity Certificates (Digital Signing). Servers, devices, and applications will receive a single certificate that will support both Identity and Authentication. Many servers, devices, and applications do not currently support separate signing and key exchange keys, therefore use of the same key for both is being permitted.

The e-MARC server, device, and application certificates primarily support secure Web applications using SSL. SSL relies on the initiator's key to exchange a symmetric session key. Servers, devices, and applications initiating SSL sessions with other servers may also need to

authenticate using a digital signature key. The e-MARC server, device, and application certificates are required to contain the appropriate e-mail point of contact (POC) within the certificate profile. The POC's e-mail address shall be contained in the subject alternative name extension.

The End-Entity Identity/Authentication certificate is the electronic equivalent of an ID card. This certificate should contain limited, relatively static information. Although not necessary, it may include more dynamic information such as detailed organizational affiliation and e-mail address. If an email address is included, it must be contained in the subject alternative name (subAltName) extension of the associated certificate. The subject name in an End-Entity certificate is the DN for a corresponding entry in a directory.

The following sections provide a minimal set of required fields within an e-MARC certificate. Details on the exact contents of an e-MARC will be provided within an Authorized CA's CPS.

7.1.1 Version Numbers

All certificates shall be X.509 Version 3 certificates.

7.1.2 Signature Algorithms

All certificates shall use Secure Hash Algorithm 1 (SHA-1) with the Rivest, Shamir, and Adleman (RSA) algorithm or the Digital Signature Algorithm (DSA) with SHA-1.

7.1.3 Certificate Validity Periods

Table 6 lists the certificate validity periods.

Table 6. Certificate Validity Periods

Certificate Key Usage	Validity Period
e-MARC CA certificates	3 years minimum
Server and Device certificates	3 years
Authentication (Web Authentication) certificates	1 year
Identity (Digital Signing) certificates	1 year

7.1.4 Public Algorithm Identifiers

Certificates under this Policy will use the OIDs listed in Table 7 for signatures.

Table 7. OIDS for Signatures

Signature Algorithm	OID
id-dsa-with-sha1	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 3}
sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
ecdsa-with-SHA1	{iso(1) member-body(2) us(840) ansi-x9-62 (10045) signatures (4) 1 }

7.1.5 Public Key Lengths

All certificates will conform to the minimum public key lengths stated in Table 8.

Table 8. Public Key Lengths

Certificate Key Usage	Min. Public Key Length
e-MARC CA certificates	2048
Server and Device certificates	1024
Authentication certificates (Web Authentication)	1024
Identity Certificates (Digital Signing)	1024

7.1.6 Key Usage Extension

All certificates will have the key usage (marked as Critical) extension. This extension will be used to determine the allowed use of the certificate (i.e., the Certificate Key Usage).

All certificates will display the key usage extension and use one or more of these available values:

Digital Signature (0)
Non Repudiation (1)
Key Encipherment (2)
Data Encipherment (3)
Key Agreement (4)
Certificate Signing (5)
CRL Signing (6)
Encipher Only (7)
Decipher Only (8)

Table 9 lists mandatory key usage requirements.

Table 9. Mandatory Key Usage

Certificate Type	**Category**	**Key Usage**	**Description**
Authorized CA Certificates	Certification Authorities	Digital Signature (0), Non Repudiation (1), Certificate Signing (5), CRL Signing (6)	To enable CAs to issue, end-entity certificates, and CRLs
Authentication Certificates (Web Authentication)	Business Representative	Digital Signature (0) Key Encipherment (2) Key Agreement (4)	To enable a Business Representative to authenticate itself to Relying Parties.
	Device	Digital Signature (0), Key Encipherment (2) Key Agreement (4)	To enable a device to authenticate itself to other devices for the purpose of secure electronic transactions.
	Role	Digital Signature (0) Key Encipherment (2) Key Agreement (4)	To enable a role-based user or group of users to authenticate itself to Relying Parties**.**
Identity Certificates (Digital Signing)	Business Representative	Digital Signature (0), Non Repudiation (1) Key Encipherment (2) Key Agreement (4)	To enable a Business Representative to verify digitally signed documents and transactions, and participate in non-repudiable transactions. This certificate may also be used to authenticate to Relying Parties while supporting non-repudiation.

	Device	Digital Signature (0), Non Repudiation (1), Key Encipherment (2) Key Agreement (4)	To enable a device to authenticate itself to other devices for the purpose of secure electronic transactions, establish secure symmetric key exchanges, and verify digitally signed transactions.
	Role	Digital Signature (0), Non Repudiation (1) Key Encipherment (2) Key Agreement (4)	To enable a role-based user or group of users to establish secure symmetric key exchanges, verify digitally signed documents and transactions, and participate in non-repudiable transactions. This certificate may also be used to authenticate to Relying Parties while supporting non-repudiation.

7.1.7 Basic Constraints

This extension must be present in all Certificate Authority certificates (marked as critical) with Subject Type = CA. It is recommended, but not required, to set the Path Length Constraint.

7.1.8 Subject Key Identifier

The subject key identifier extension must be present in all certificates as it facilitates certification path construction. For Certificate Authority certificates, the value of the subject key identifier must be the same as the authority key identifier extension of certificates issued by the subject of this certificate.

7.1.9 Authority Key Identifier

The authority key identifier extension must be present in all certificates as it facilitates certificate path construction in instances where a Certificate Authority has multiple signing keys (either due to multiple concurrent key pairs or due to changeover). The identification must be based on the key identifier (the subject key identifier in the issuer's certificate) but in addition may also use the issuer's name and/or serial number.

7.1.10 Subject Alternative Name

This is an optional extension based on RFC 822 [RFC 822], which may be used to further clarify the owner of the certificate or to strengthen name uniqueness. When the Subject Alternative name (subjectAltName) extension contains an Internet mail address, the address must be included as an rfc822Name. The format of an rfc822Name is an "addr-spec" as defined in RFC 822. An addr-spec has the form "local-part@domain".

7.1.11 Name Forms

In a certificate, the issuer's DN and subject's DN fields shall contain the full X.500 Distinguished Name of the Authorized CA and the subject to which the certificate was issued, respectively.

7.1.12 Name Constraints

No stipulation.

7.1.13 Certificate Policy Object Identifier

All certificates must include a Certificate Policy Identifier equal to the Authorized CA Policy Object ID and must include a Policy Qualifier which points to the Certificate Authority's CPS. Other Policy Qualifiers may be used to point to legal, privacy, or restricted use notices.

7.1.14 Authority Information Access

All certificates may include at least one authority information access extension. The authority information access extension as outlined in RFC 3280 indicates how to access CA information and services for the issuer of the certificate in which the extension appears. Information and services may include on-line validation services and CA policy data. The location of CRLs is not specified in this extension; that information is provided by the CRLDistributionPoints extension. This extension may be included in subject or CA certificates, and it must be non-critical.

7.1.15 CRL Distribution Point

All certificates must include at least one CRL Distribution Point and may use any of the currently available protocols, including HTTP, File Transfer Protocol (FTP), or LDAP.

7.1.16 Usage of Policy Constraints Extension

No stipulation.

7.1.17 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.18 Processing Semantics for the Critical Certificate Policy Extension

No stipulation.

7.1.19 Certificate Profile and Certificate Profile Extensions

Any variance from the above profile recommendations shall be documented in the Authorized CA CPS and approved by the Policy Authority.

7.2 CRL PROFILE

7.2.1 Version Numbers

CRLs issued under this Policy shall assert a version number as described in the X.509 standard [ISO 9594-8]. CRLs shall assert X.509 Version 2.

7.2.2 CRL and CRL Entry Extensions

Any variance from the above profile recommendations shall be documented in the Authorized CA CPS and approved by the Policy Authority.

SECTION 8

POLICY ADMINISTRATION

8.1 POLICY CHANGE PROCEDURES

8.1.1 Policy Change Notice

Notice of all proposed changes to this Policy under consideration by the Policy Authority that may materially affect users of this Policy (other than editorial or typographical corrections, minor changes to the contact details, or other minor changes) will be provided to Authorized CAs, and Subscribers, and will be posted on the PA's Website. The Authorized CA shall publish notice of such proposed changes to the appropriate Repository and shall advise their Subscribers of such proposed changes by means of a specific e-mail or postal notice.

8.1.2 Comment Period

Any interested person may submit written comments to the Policy Authority within 45 days of the original change notice. If the proposed change is modified as a result of such comments, a new notice of the modified, proposed change shall be given.

8.1.3 Process for Policy Adoption

Proposed changes to this Policy will be brought to the PKI Steering Committee members. The proposed changes will be reviewed by committee members, who will vote on whether to accept or reject them. If accepted, the Policy changes will be published on the Policy Authority's Website. Subscribers are responsible for periodically checking this Website to ensure that no Policy changes have been issued. End-Entities relying on the e-MARCs will be given a reasonable amount of time to transition to use of the updated Policy.

8.2 PUBLICATION AND NOTIFICATION PROCEDURES

A copy of this Policy shall be made available in electronic form on the Policy Authority's Website, and may also be obtained via e-mail upon request from the Policy Authority. The Authorized CA shall also make available copies of this Policy both online and in writing.

8.3 CPS APPROVAL PROCEDURES

The Policy Authority, or its duly authorized agent, must approve an Authorized CA's e-MARC CPS prior to its incorporation into the Authorized CA's operational procedures. The approval process will include a subset of the following criteria:

- Compliance with RFC 2527
- Compliance with the e-MARC Policy (this document)
- Completion of the C&A process
- Compliance with the *e-MARC Requirements* document.

Glossary

Administrator. One who administers daily operations; one who directs, or executes processes associated with the e-MARC PKI.

Agency. A term used to identify all federal agencies, authorized federal contractors, agency-sponsored universities and laboratories, and, when authorized by law or regulation, state, local, and tribal governments.

AICPA/CICA. American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants.

Applicant. An individual or authorized representative who is beginning or is in the process of obtaining an e-MARC. Once an e-MARC has been issued, the applicant becomes a Subscriber.

Authenticate. One party has presented an identity and claims to be that identity. Authentication enables another party to gain confidence that the identity claim is legitimate.

Authorized CA. A Certification Authority that has been authorized by the Policy Authority to issue e-MARCs and provide Authorized CA Services under this Policy.

Authorized CA Services. The services, relating to e-MARCs, to be provided by Authorized CAs under this Policy.

Authorized Individual. An individual who has been authorized to perform sensitive tasks within the e-MARC PKI.

C. Country.

CA. See "Certification Authority."

C&A. Certification and Accreditation

Certificate. A data record that, at a minimum, (1) identifies the Authorized CA issuing it, (2) names or otherwise identifies its Subscriber, (3) contains a public key that corresponds to a private key under the control of the Subscriber, (4) identifies its operational period, and (5) contains an e-MARC serial number and is digitally signed by the Authorized CA issuing it. As used in this Policy, the term of "certificate" refers to certificates that expressly reference the OID of this Policy in the Certificate Policies field of an X.509 Version 3 certificate.

Certificate Key User. A participant in the e-MARC PKI that utilizes an e-MARC for electronic energy market transactions.

Certificate Issuer. A person or device that issues e-MARCs that abide by the stipulations set forth in this Policy.

Certificate Manufacturing Authority (CMA). An entity that is responsible for the manufacturing and delivery of e-MARCs signed by an Authorized CA, but is not responsible for identification and authentication of certificate subjects (i.e., a CMA is an entity that is delegated or outsourced the task of manufacturing the certificate on behalf of an Authorized CA).

Certificate Profile. The technical contents of an e-MARC issued under the corresponding OID.

Certification Authority. An entity (a person or software) that is responsible for authorizing and causing the issuance of a certificate. See "Authorized CA."

Certification Practice Statement. A statement of the practices that a Certification Authority employs in issuing, providing access to, suspending, revoking, and renewing certificates in accordance with specific requirements (i.e., requirements specified in this Policy, requirements specified in a contract for services).

CMA. See "Certificate Manufacturing Authority."

CN. Common Name

COMSEC. Communications Security

Contract Authority. A person or organization that is responsible for overseeing the legal aspects of the e-MARC PKI.

CPS. See "Certification Practice Statement."

CRL. Certificate Revocation List

Crypto-algorithm. A mathematical process that creates a computational procedure solving a problem in a finite number of steps.

DER. Distinguished Encoding Rules

Digital Signature. A string of bits associated with a collection of data (e.g., file, document, message, transaction). This string of bits can only be generated by the holder of a private key, but it can be verified by anyone with access to the corresponding public key. Some algorithms include additional steps (e.g., one-way hashes, timestamps) in the basic process.

Digital Signature Certificate. A certificate used for the sole purpose of digitally signing a document or transaction that enforces technical non-repudiation.

Digital Signature Key. An electronic key that asserts the digital signature key usage parameter.

DSA. Digital Signature Algorithm

DSS. Digital Signature Standard

DUNS. Data Universal Numbering System

e-MARC. Energy Market Access and Reliability Certificate. An e-MARC is a certificate that provides commercial public key certificate services to those participating in energy markets and identified in authorized Registry Domains. An e-MARC is issued by an Authorized CA in accordance with this Policy and as identified in the e-MARC OID.

e-MARC CPS. A Certification Practice Statement (a document) of the procedures that an Authorized CA employs in issuing, providing access to, suspending, and revoking e-MARCs.

Encryption Certificate. An e-MARC that asserts the encryption key usage parameter.

End-Entity. Subscribers that rely upon the use of an e-MARC for energy transactions.

Entity Code. A unique alphanumeric code assigned to a registered organization in a Registry Domain by the Registry Administrator.

FAR. Federal Acquisition Regulation

FED-STD. Federal Standard

FIPS. Federal Information Processing Standard. These Federal standards prescribe specific performance requirements, practices, formats, communications protocols, etc., for hardware, software, data, telecommunications operation, etc. Federal agencies are expected to apply these standards as specified unless a waiver has been granted in accordance with agency waiver procedures.

FIPS PUB. Federal Information Processing Standard Publication

FPKI. Federal Public Key Infrastructure

FTP. File Transfer Protocol

Government. Federal Government and authorized agencies and entities.

HTTP. HyperText Transfer Protocol

HTTPS. HyperText Transfer Protocol with Secure Sockets Layer

IANA. Internet Assigned Numbers Authority

ID. Identification

IETF. See "Internet Engineering Task Force."

Internet Engineering Task Force (IETF). A large, open, international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

ISO. International Standards Organization

ITU. International Telecommunications Union

ITU-T. International Telecommunications Union – Telecommunications Sector

ITU-TSS. International Telecommunications Union – Telecommunications Systems Sector

Key Changeover (CA). The procedure used by an Authority to replace its own private key (e.g., due to compromise) and replace current valid certificates issued with old key.

Key pair. Two mathematically related keys, having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (2) even knowing one key, it is computationally infeasible to discover the other key.

LDAP. Lightweight Directory Access Protocol

Local Registration Authority. An application that resides locally at an organization that is responsible for identification and authentication of certificate subjects but does not sign or issue certificates. Communicates solely with its central Registration Authority.

LRA. See "Local Registration Authority."

Mutual Authentication. Parties at both ends of a communications activity that authenticate each other (see "Authenticate").

NERC. North American Electric Reliability Council

NIST. National Institute of Standards and Technology

Non-repudiation. The inability to deny actions. Non-repudiation of delivery prevents a recipient from denying receipt of a message.

O. Organization.

Object Identifier. A specially formatted number that is registered with an internationally recognized standards organization.

OCSP. Online Certificate Status Protocol.

OID. See "Object Identifier."

Operating Rules. See "e-MARC Operating Rules."

Operational Period of an e-MARC. The period of validity of an e-MARC. This period would typically begin on the date the e-MARC was issued (or such later date as specified in the particular e-MARC) and end on the date and time it expired (as specified in the e-MARC) or was earlier revoked or suspended.

OU. Organizational Unit

Out-of-band. A communication among parties using a means or method that differs from the current method of communication (e.g., one party uses U.S. Post Office mail service to communicate with another party when the other party is communicating online).

PA. See "Policy Authority."

PKCS. Public Key Certificate Standard

PKI. Public Key Infrastructure

PKIX. Public Key Infrastructure (X.509)

PIN. Personal Identification Number

PKI Steering Committee. Members within the Energy industry who are responsible for the overall direction of the e-MARC architecture and technical capabilities.

Policy. This document.

Policy Authority. The entity responsible for organizing and administering the e-MARC Policy and e-MARC Contract (s).

Potential Subscriber.

Private Key. One key of a key pair used to create a digital signature. The private key must be kept a secret.

Program Participants. Collectively, the Registry Administrators, Authorized CAs, Registration Authorities, Certificate Manufacturing Authorities, Repositories, Subscribers,

Authorized Users, and Policy Authority authorized to participate in the e-MARC PKI as defined in this Policy.

Public Key. One key of a key pair used to verify a digital signature. The public key is made freely available to anyone who will receive digitally signed messages from the holder of the key pair. The public key is usually provided via an e-MARC issued by an Authorized CA and is often obtained by accessing a Repository. A public key is used to verify the digital signature of a message purportedly sent by the holder of the corresponding private key.

RA. See "Registration Authority."

RDN. Relative Distinguished Name

Registration Authority. An entity that is responsible for identification and authentication of certificate subjects but does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an Authorized CA).

Registry. An entity or device that is responsible for accepting, processing and distributing information to e-MARC Subscribers.

Registry Administrator. An entity or organization authorized to administer a Registry Domain in accordance with this Policy.

Registry Domain. A registry of market participants. Within the context of this Policy, a Registry Domain is typically a bounded set of market participants within a particular energy segment, such as gas or electricity. The Registry and Registry Domain must comply with this Policy and have a unique registered Internet domain name.

Repository. A database containing information relating to certificates and an Authorized CA as specified in this Policy.

Responsible Individual. A trustworthy person designated by a Sponsoring Organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.

Revoke a Certificate. To end prematurely the operational period of a certificate from a specified time forward.

RFC. Request for Comment

RSA. Rivest, Shamir, and Adleman (a proprietary asymmetric cryptographic algorithm)

Security Officer. A person who is responsible for maintaining the appropriate security classifications and authorizing end user identities.

SHA. Secure Hash Algorithm

SHA-1. Secure Hash Algorithm 1

S/MIME. Secure Multipurpose Internet Mail Extension

Sponsoring Organization. A business entity, government agency, or other organization with which a Business Representative is affiliated (e.g., employee, agent, member, user of a service, Business Partner, customer).

Spyware. A malicious application running on a machine that is intended to compromise communications and data integrity.

SSL. Secure Sockets Layer

Subject. A person whose public key is certified in an e-MARC. Also referred to as a "Subscriber."

Subscriber. A person who (1) is the subject named or identified in an e-MARC issued to such person, and (2) holds a private key that corresponds to a public key listed in that e-MARC, and (3) is the person to whom digitally signed messages verified by reference to that e-MARC are to be attributed. See "Subject."

Suspend a Certificate. To halt temporarily the operational period of a certificate for a specified time or from a specified time forward.

Token. A physical device that is used as the initial authenticator to grant access to private keys.

Transaction. Any financially binding action, as defined by the software application or process being secured (protected) or implemented.

Trustworthy System. Computer hardware, software, and procedures that (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.

URI. Uniform Resource Identifier

U.S.C. United States Code

UTF. Unicode Transformation Format

Valid Certificate. An e-MARC that (1) an Authorized CA has issued, (2) the Subscriber listed in it has accepted, (3) has not expired, and (4) has not been revoked. An e-MARC is not valid until it has been both issued by an Authorized CA and accepted by the Subscriber.

Written. Any type of material that conveys information, such as via a written record, or any writing, including e-mail or other electronic communication, that is legally binding in the jurisdiction in which it was created or received.

Web. An abbreviation for the World Wide Web. The Web is a popular subset of the Internet that affords reader-friendly access to information via HyperText Markup Language (HTML), and Extended Markup Language (XML), and other commands embedded in text displayed as "(Web)pages" on "(Web)sites."

X.509 Certificate. Digital information signed by a certificate authority, an X.509 certificate contains subject-related information that links a specific user to his or her public key.

Bibliography

The following documents were used in part to develop this Policy:

ABA DSG	*American Bar Association (ABA)Digital Signature Guidelines*, August 1, 1996. http://www.abanet.org/scitech/ec/isc/dsgfree.html
AICPA C&A	*American Institute of CPAs/Canadian Institute of Chartered Accountants WebTrust Principles and Criteria for Certification Authorities*, *http://www.webtrust.org/CertAuth_fin.htm*
CIMC	*Certificate Issuing and Management Components Family of Protection Profiles*, Version 1.0, 31 October 2001.
DoDCP	*X.509 Certificate Policy for the United States Department of Defense*, Version 6.0, May 31, 2002.
FERC 889	*Open Access Same-Time Information System (Formerly Real-Time Information Networks) and Standards of Conduct*, Federal Energy Regulatory Commission (FERC) Order No. 889, 61 FR 21,737, May 10, 1996.
FIPS 112	*Password Usage*, May 30, 1985. http://www.itl.nist.gov/fipspubs/
FIPS 140-1	*Security Requirements for Cryptographic Modules*, January 1994. http://csrc.nist.gov/cryptval/
FIPS 140-2	*Security Requirements for Cryptographic Modules*, May 2001. http://csrc.nist.gov/cryptval/
FIPS 186	*Digital Signature Standard*, May 19, 1994. http://csrc.nist.gov/cryptval/
FOI ACT	*Freedom of Information Act*, 5 U.S.C. 551. http://www4.law.cornell.edu/uscode/5/552.html
FPKI-Prof	*Federal PKI X.509 Certificate and CRL Extensions Profile*, 15 February, 2002 (http://csrc.nist.gov/pki/twg/y2002/papers/twg-02-04.xls)
ISO 9594-8	Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, ITU-T Recommendation X.509 (2000), October 2001 *http://www.itu.int/dms_pub/itu-t/rec/x/T-REC-X.509-200110-I!Cor1!PDF-E.pdf*
ITMRA	*Information Technology Management Reform Act of 1996*, 40 U.S.C 1452. http://www4.law.cornell.edu/uscode/40/1452.html
NS 4009	*National Information Systems Security Glossary*, NSTISSI 4009, January 1999. http://www.nstissc.gov/Assets/pdf/4009.pdf
PKCS #1	*RSA Cryptography Standard*, *http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/*
PKCS #12	*Personal Information Exchange Syntax Standard*, April 1997. http://www.rsasecurity.com/rsalabs/pkcs/pkcs-12/
PKIX	*Public-Key Infrastructure (X.509).* *http://www.ietf.org/html.charters/pkix-charter.html*
Privacy Act	*The Privacy Act of 1974, http://www.usdoj.gov/foia/privstat.htm*

of 1974

RFC 822 *Standard for the format of ARPA Internet text messages*, David H. Crocker, August 1982.
http://www.ietf.org/rfc/rfc0822.txt?number=822

RFC 2119 *Key Words in RFCs to Indicate Requirement Levels*, S. Bradner, March 1997.
http://www.ietf.org/rfc/rfc2119.txt?number=2119

RFC 2256 *A Summary of the X.500(96) User Schema for use with LDAPv3*, M. Wahl, December 1997.
http://www.ietf.org/rfc/rfc2256.txt?number=2256

RFC 2459 *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, R. Housley, W. Ford, W. Polk, D Solo, January 1999.
http://www.ietf.org/rfc/rfc2459.txt?number=2459

RFC 2510 *Internet X509 Public Key Infrastructure Certificate Management Protocols*, Adams and Farrell, March 1999.
http://www.ietf.org/rfc/rfc2510.txt?number=2510

RFC 2527 *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, Santosh Chokhani and Ford, March 1999.
http://www.ietf.org/rfc/rfc2527.txt?number=2527

RFC 3280 *Certificate and Certificate Revocation List (CRL) Profile* (obsoletes RFC 2459), April 2002.
http://www.ietf.org/rfc/rfc3280.txt?number=3280

RFC 3629 *UTF-8, a transformation format of ISO 10646*, F. Yergeau, November 2003.
http://www.ietf.org/rfc/rfc3629.txt?number=3629

RFC 3647 *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* (obsoletes RFC 2527), Santosh Chokhani, W. Ford, R. Sabett, C. Merrill, and S. Wu, November 2003.
http://www.ietf.org/rfc/rfc3647.txt?number=3647

Appendix A

The following table provides a sample template for Authorized CAs to detail intended Certificate Profiles within their Certification Practice Statements.

Field	Certificate Type
Basic Certificate	
Version	
Serial Number	
Issuer Signature Algorithm	
Issuer Distinguished Name	
Validity Period	
Subject Distinguished Name	
Subject Public Key Information	
Issuer Unique Identifier	
Subject Unique Identifier	
Issuer's Signature	
Standard Extensions	
authority key identifier	
subject key identifier	
key usage	
Extended key usage	
Private key usage period	
Certificate policies	
Policy Mapping	
subject Alternative Name	
Issuer Alternative Name	
Subject Directory Attributes	
Basic Constraints	
Name Constraints	
Policy Constraints	
CRL Distribution Points	
Private Internet Extensions	
Authority Information Access	