R03007 North American Energy Standards Board

Request for Initiation of a NAESB Standard for Electronic Business Transactions
or
Enhancement of an Existing NAESB Standard for Electronic Business Transactions

Instructions:

1. Please fill out as much of the requested information as possible. It is mandatory to provide a contact name, phone number and fax number to which questions can be directed. If you have an electronic mailing address, please make that available as well.

2. Attach any information you believe is related to the request. The more complete your request is, the less time is required to review it.

3. Once completed, send your request to:

   Rae McQuade
   NAESB, Executive Director
   1100 Louisiana, Suite 3625
   Houston, TX 77002
   Phone: 713-356-0060
   Fax: 713-356-0067

by either mail, fax, or to NAESB's email address, naesb@aol.com.

Once received, the request will be routed to the appropriate subcommittees for review.

North American Energy Standards Board

Request for Initiation of a NAESB Standard for Electronic Business Transactions
or
Enhancement of an Existing NAESB Standard for Electronic Business Transactions

Date of Request: May 23, 2003

1. Submitting Entity & Address:

OASIS Standards Collaborative
NERC
116-390 Village Boulevard
Princeton, New Jersey 08540-5731

2. Contact Person, Phone #, Fax #, Electronic Mailing Address:

Name: Monroe Landrum
Title: Manager, Operating Systems
Phone: (205) 257-6936
Fax: (205) 257-6663
Email: MJLANDRU@southernco.com

3. Description of Proposed Standard or Enhancement:

Enhance the current OASIS Standards and Communications Protocols (S&CP) to ensure compliance with the Energy Market Access and Reliability Certificates (e-MARC) Security Initiative, currently being developed and implemented by the North American Electric Reliability Council. E-MARC is the certificate policy that will implement a Public Key Infrastructure (PKI) for securing digital communications in all standardized wholesale electricity data exchanges.

4. Use of Proposed Standard or Enhancement (include how the standard will be used, documentation on the description of the proposed standard, any existing documentation of the proposed standard, and required communication protocols):

The standard will require that OASIS nodes be secured through the use of e-MARC digital certificates. Requirements for securing explicit portions of the OASIS will be defined through modification of the OASIS Standards and Communications Protocols document.

5. Description of Any Tangible or Intangible Benefits to the Use of the Proposed Standard or Enhancement:

Tangible benefits include:

- **Providing a common log-in and authentication standard for OASIS**
- **Eliminating the maintenance overheads associated with client-side management of multiple usernames and passwords for different OASIS sites**
- **Providing server-side management of password resets**

Intangible benefits include:

- **Privacy**
- **Authentication**
- **Integrity**
- **Non-repudiation**

6. Estimate of Incremental Specific Costs to Implement Proposed Standard or Enhancement:

PKI User Certificates

PKI users will be responsible for costs charged by the trusted certificate authority service providers associated with issuance and management of e-MARC certificates. Recurring costs may be on the order of $50-$250 per user certificate.

These costs are associated with:

- **Application/enrollment process**
- **Identification, verification, and authentication process**
- **Certificate manufacturing process**
- **Dissemination and activation of the certificate**
- **Publication of the certificate (if required)**
- **Renewal, suspension, revocation, and replacement of the certificate**
- **Verification of certificate status upon request**
- **Compliance with trusted certificate policy**

PKI Server Certificates

Entities requiring PKI server certificates will be responsible for the initial registration costs charged by the trusted certificate authority service providers. There non-recurring costs for enhancement of server application software, to recognize and implement PKI based user authentication, may be on the order of $10,000-$100,000.

Entities requiring PKI server certificates will be responsible for the costs charged by the trusted certificate authority service providers associated with issuance and management of e-MARC certificates. These recurring costs may be on the order of $1,000-$10,000 per application/server certificate.

These costs are associated with:

- **Application/enrollment process**

- **Identification, verification, and authentication process**
- **Certificate manufacturing process**
- **Dissemination and activation of the certificate**
- **Publication of the certificate (if required)**
- **Renewal, suspension, revocation, and replacement of the certificate**
- **Verification of certificate status upon request**
- **Compliance with trusted certificate policy**

7. Description of Any Specific Legal or Other Considerations:

The e-MARC certificate policy contains contractual obligations required of entities using the certificate. Additional legal and liability requirements, associated with the certificate authority service providers, are specified in the e-MARC certificate policy.

8. If This Proposed Standard or Enhancement Is Not Tested Yet, List Trading Partners Willing to Test Standard or Enhancement (Corporations and contacts):

Those parties responsible for implementing the standards will be responsible for testing.

9. If This Proposed Standard or Enhancement Is In Use, Who are the Trading Partners:

PKI and application security, similar in nature to that proposed in this standards request, are currently used in a number of existing applications. These applications include OASIS, ISO-NE market, NYISO market, and the IMO market. This standards request will establish a consistent method of securing diverse applications, as well as providing reliability certificates, used to seamlessly access systems subject to these standards.

10. Attachments (such as: further detailed proposals, transaction data descriptions, information flows, implementation guides, business process descriptions, examples of ASC ANSI X12 mapped transactions):

The following two documents will be submitted as electronic attachments to this standards request:

- **Certificate Policy for Energy Market Access and Reliability Certificates**
- **OASIS Security Requirements**

Certificate Policy

for

Energy Market Access and Reliability Certificates

(e-MARC)

Draft Version 1.4
Accepting changes per PKISC conference call/webcast
(25.April.'03 and 29.April.'03)

North American Electric Regulatory Council
(NERC)

May 2003

TABLE OF CONTENTS

SECTION **PAGE**

SECTION 1

Introduction

1.1 OVERVIEW

In support of deregulated energy markets and system reliability function, many computer-based systems, applications, and market participants have a significant requirement for the secure operations of these networked computer-based systems, electronic messages, and transactions. One mechanism to fulfill that requirement uses digital signatures to ensure:

- Privacy: 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) between "there" and "here," or between "then" and "now"; and,
- Non-Repudiation: A party cannot deny having engaged in the transaction or having sent the electronic message.

This mechanism chosen requires the use of public key cryptography which utilizes 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 goal, the North America Electric Reliability Council (NERC) will provide for commercial public key certificate services to the deregulated energy markets and system reliability function (referred to as "Energy Market Access and Reliability Certificates" or "e-MARC"). NERC will do this by certifying Registry Domains, Registry Administrations, and service provider(s) to provide the services presented in this policy.

The security of these services is ensured be defining requirements on Public Key Infrastructure (PKI) activities, including the following:

- 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 to 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 security solution is a direct result of the secure and trustworthy operations of an established PKI, including equipment, facilities, personnel, and procedures.

This CP describes (1) roles, responsibilities, and relationships among the Registry Domains, Registry Administrators, Certification Authorities (CAs), Registration Authorities (RAs), Certificate Manufacturing Authorities (CMAs), Repositories, Subscribers, Qualified Relying Parties, and Policy Authority (referred to collectively as “Program Participants”) authorized to participate in the public key infrastructure described by 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 to verify digital signatures.

This Certificate Policy (CP) provides a high level description of the policies and operation of the e-MARC Program and follows the *X.509 Public Key Infrastructure Certificate Policy and Certificate Practices Framework* as detailed in RFC 2527 of the Internet Engineering Task Force (IETF). Specific detailed implementations of this policy will be found in the Certificate Practice Statement (CPS) of any Certification Authority (CA) certified to issue certificates bound by this policy.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119. This interpretation is shown below.

MUST: This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.

MUST NOT: This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.

SHOULD: This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

SHOULD NOT: This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular 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 adjective "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 which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

1.2 POLICY IDENTIFICATION

This Policy is registered with the _______________ and has been assigned the following object identifiers (OIDs) for the e-MARC Certificates defined in this Policy.

Identity e-MARC Certificates: { _____________________ }
Business Representative e-MARC Certificates: { _____________________ }

Server e-MARC Certificates: { _____________________ }
Qualified Relying Party Application e-MARC Certificates: { ___________________ }

All e-MARC certificates issued under this Policy shall reference this Policy by including the appropriate OID for this Policy in the *Certificate Policies* field of the e-MARC Certificate. The foregoing OIDs may not be used except as specifically authorized by this Policy.

1.3 COMMUNITY AND APPLICABILITY

This Policy describes a bounded public key infrastructure. It describes the rights and obligations of persons and entities authorized under this Policy to fulfill any of the following roles: Registry Service Provider roles, Certificate Service Provider roles, End Entity roles, and Policy Authority role. Registry Service Provider role are Registry Administrators. Certificate Service Provider roles are Certification Authority, Registration Authority, Certificate Manufacturing Authority, and Repository. End Entity roles are Subscriber and Relying Party. Requirements for persons and entities authorized to fulfill any of these roles are in this Section. A general description of each of these roles and their responsibilities is set forth in Section 2 of this Policy.

1.3.1 Registry Domains

A Registry Domain may participate in this Policy only if qualified and authorized to do so by the Policy Authority. In order to qualify as an authorized Registry Domain, the Registry must:

(a) Be a registry of organizations participating in an energy market;

(b) Include organizations’ DUNS numbers or other industry recognized, third-party assigned business identifier as one of their attributes;

(c) Associate a unique alphanumeric code (Entity Code) to each registered organization,” and,

(d) Identify each Certification Authority qualified as an “Authorized CA.

1.3.2 Registry Administrators

A Registry Administrator may participate in this Policy and administer a qualified and authorized Registry Domain only if such Registry Administrator first qualified as an authorized Registry Administrator by:

(a) Entering into an appropriate e-MARC Contract; and

(b) Documenting the specific practices and procedures that it will implement to satisfy the requirements of this Policy and of the Registry Domain they wish to administer.

1.3.3 Authorized Certification Authorities (CAs)

A CA may issue certificates that identify this Policy (“e-MARC certificates”) only if such CA first qualifies as an “Authorized CA” by:

(a) Entering into an appropriate e-MARC contract;

(b) Documenting the specific practices and procedures it will implement to satisfy the requirements of this Policy in a certificate practice statement (“e-MARC CPS”); and,

(c) Successfully completing e-MARC Security Certification and Accreditation.

For the purposes of this document, a “**certification authority”** is an entity that is responsible for authorizing and causing the issuance of a Certificate. The term “**Authorized CA”** refers to a certification authority that has been authorized by the Policy Authority to issue e-MARC certificates and provide Authorized CA services under the Policy.

1.3.4 Registration Authorities (RAs)/Local Registration Authorities (LRAs)

Each Authorized CA shall perform the role and functions of the Registration Authority (RA). An Authorized CA may subcontract RA functions to third party RAs or 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 remains responsible for the performance of those services in accordance with this Policy and its requirements under the Policy Authority's e-MARC Contract. The only exception is when the Policy Authority, pursuant to agreement between the Policy Authority, Qualified Relying Parties, and the Authorized CAs provides defined portions of the RA role and function.

1.3.5 Certificate Manufacturing Authorities (CMAs)

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 remains responsible for the performance of those services in accordance with this Policy and its requirements under the Policy Authority's e-MARC Contract.

1.3.6 Repositories

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 who agrees to be bound by this Policy, provided that such subcontractor is approved in advance by NERC, but the Authorized CA remains responsible for the performance of those services in accordance with this Policy and the requirements of its NERC e-MARC Contract.

1.3.7 End Entities

An Individual or organization and their agents may be Subscribers or Qualified Relying Parties. As described in Sections 1.3.7.1 Subscribers~~1.3.7.1 Subscribers 1.3.7.1 Subscribers~~ and 1.3.7.2 Qualified Relying Parties, Subscribers may be issued e-MARC certificates for assignment to devices, groups, organizational roles or applications provided that responsibility and accountability is attributable to an individual or an organization as defined in Section 7.

e-MARC certificates will only be issued after receiving requests or 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 and the Authorized CA may administer any number of Subscribers.

1.3.7.1 Subscribers

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

(a) Members of the general public ("Unaffiliated Individuals");

(b) 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");

(c) 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 client applications ("Devices").

(d) Qualified Relying Parties ("Qualified Relying Party Applications") that choose to use e-MARC.

1.3.7.2 Qualified Relying Parties (QRP)

Persons and entities authorized to accept and rely upon e-MARC certificates for purposes of privacy, authentication, integrity, and non-repudiation of electronic records and messages are those eligible entities that enter into an e-MARC Agreement (i.e., Memorandum of Understanding) to accept e-MARC certificates and agree to be bound by the terms of this Policy ("Qualified Relying Parties"). Eligible entities include all recognized energy market participants registered in an authorized Registry, Canadian, Mexican, and U.S. Federal agencies, Provincial, State and local agencies, authorized contractors and sponsored universities and laboratories of the Policy Authority, and other organizations as deemed appropriate under this policy and by the Policy Authority. The Policy Authority has the right to add authorized users in these categories at any time during the term of this Policy.

1.3.8 Policy Authority (PA)

NERC serves as the PA and is responsible for organizing and administering the e-MARC Policy and e-MARC Contract (s).

1.3.9 Applicability and Applications

1.3.9.1Purpose

Subscribers and Authorized CAs may use e-MARC certificates to authenticate Subscribers to Qualified Relying Party applications for individual and/or business purposes, and for authentication of Qualified Relying Party applications. The following table summarizes the functional uses of e-MARC certificates:

Certificate Type	Subscriber Class	Description of Use of Certificate
Unaffiliated Individual	Unaffiliated Individual	To enable an Unaffiliated Individual to authenticate itself to Qualified Relying Parties, establish secure symmetrical key exchanges, verify digitally signed documents and transactions, and participate in non-reputable transactions.
Business Representative	Business Representative authorized to act on behalf of a Sponsoring Organization	To authenticate itself to Qualified Relying Parties, establish secure symmetrical key exchanges, verify digitally signed documents and transactions, and participate in non-reputable transactions.
Device	Servers, devices, and/or computer applications authorized to act on behalf of a Sponsoring Organization	To authenticate itself to Qualified Relying Parties, establish secure symmetrical key exchanges, verify digitally signed documents and transactions, and participate in non-reputable transactions.
Qualified Relying Party Application	Qualified Relying Party	To enable a Qualified Relying Party to authenticate itself to Unaffiliated Individuals, Business Representatives, and Authorized CAs and to verify digitally signed documents/transactions

1.3.9.2 Suitable Applications

e-MARC certificates, under the assertion of the e-MARC Policy OID, may be, but are not limited to, use in the following suitable applications:

(a) Energy Market transactions;

(b) Energy or Transmission Scheduling;

(c) Filings with government agencies;

(d) Filings with law enforcement agencies;

(e) Application processes, such as applying for or requesting access to physical facilities;

(f) Financial transactions within the energy markets community;

(g) Billing, Metering, and Invoicing;

(h) Conveyance and transfer or operational data; and

(i) Conveyance and transfer or system reliability data.

1.3.9.3 Restricted and Prohibited Applications

e-MARC certificates, under the assertion of the e-MARC Policy OID, shall NEVER be used for:

(a) Any transaction or data transfer that if compromised or falsified may directly cause physical injury or loss of life.

(b) Any transaction or data transfer that if compromised or falsified may result in imprisonment.

(c) Any transaction or data transfer deemed illegal under federal law.

(d) The bulk encryption 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 certificate used for secure key exchange use only).

1.4 CONTACT DETAILS

1.4.1 Policy Administration Organization

NERC, as the Policy Authority and Contract Authority, administers this Policy:

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

1.4.2 Contact Person

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 a general description of the roles and responsibilities of the e-MARC Program Participants operating under this Policy: Authorized Registration Domains, Registry Administrators, Authorized CAs, Registration Authorities, Certificate Manufacturing Authorities, Repositories, Subscribers, Qualified 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 Qualified Relying Parties, and the Subscriber Agreements.

2.1.1 Registry Domains Obligations

A Registry Domain is responsible for containing a list of organizations that are authorized to participate in a particular energy market or reliability function and recognized by other participants in that market. It is the obligation of a Registry Domain to:

(a) have documented and enforceable requirements for market participants;

(b) obtain and maintain a registered Internet domain name to uniquely identify the registry;

(c) include organizations' DUNS numbers or other industry recognized, third-party assigned business identifier as one of their attributes;

(d) associate a unique alphanumeric code (Entity Code) to each registered organization;

(e) identify each Certification Authority qualified as an "Authorized CA"; and

(f) make all entries electronically and reliably available to all e-MARC Program Participants.

2.1.2 Registry Administrator Obligations

It is the responsibility and obligation of a Registry Administrator to ensure that the Registry Domain that it has been authorized to administer and maintain by the Policy Authority meets its obligations under this policy and:

(a) Registering market participants in the registry and managing the application/enrollment process;

(b) Implementing an identification and verification process to ensure that market participants are eligible in accordance with the Registry Domain's policies;

(c) Promptly reflecting all registration changes or modifications that affect the status of e-MARC certificates issued to registered organizations, in accordance with the Certificate Revocation requirements of this Policy.

2.1.3 Authorized CA Obligations

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

Each Authorized CA is responsible for all aspects of the issuance and management of e-MARC certificates, including the disclosure of required terms of uses as required in this Policy to all end entities, 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, suspension, revocation, and replacement of the certificate; verification of certificate status upon request; and ensuring that all aspects of the Authorized CA Services and Authorized CA operations and infrastructure related to e-MARC Certificates issued under this Policy are performed in accordance with the requirements, representations, and warranties of this Policy. The only exception is when the Policy Authority, pursuant to agreement between the Policy Authority, Qualified Relying Parties, and the Authorized CAs provides defined portions of the RA role and function.

Each Authorized CA is responsible for providing a disclaimer page during end-entity registration that requires e-MARC users to accept all rules and stipulations set forth in the e-MARC CP.

2.1.4 RA Obligations

A Registration Authority (RA) is responsible for the applicant registration, certificate application, and authentication of identity functions for Unaffiliated Individuals, Business Representatives, Devices, and Qualified Relying Parties. An RA may also be responsible for handling suspension and revocation requests, and for aspects of Subscriber education.

2.1.5 CMA Obligations

A Certificate Manufacturing Authority (CMA) is responsible for the functions of manufacture, issuance, suspension, and revocation of e-MARC certificates.

2.1.6 Repository Obligations

A Repository is responsible for maintaining a secure system for storing and retrieving e-MARC certificates, a current copy of this Policy, and other information relevant to e-MARC certificates, and for providing information regarding the status of e-MARC certificates as valid or invalid that can be determined by a Qualified Relying Party.

2.1.7 Subscriber Obligations

The responsibilities of each applicant for an e-MARC certificate are to:

- Provide complete and accurate responses to all requests for information made by the Authorized CA or RA 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 Certificate naming the applicant as the Subscriber, review the e-MARC Certificate to ensure that all Subscriber information included in it is accurate, and to expressly indicate acceptance or rejection of the e-MARC Certificate, consistent with Section 4.3.

- Use the e-MARC Certificate 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 RA to revoke the e-MARC Certificate 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 e-MARC Certificate, 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 RA to revoke the e-MARC Certificate immediately upon

Sponsoring organization’s cessation of functions requiring use of the certificate or within 60 days upon change of Sponsoring organization’s identity (such as merger or acquisition).

- Permit the backup of the private keys of certificates issued for authentication or encryption only by means of 1) a backup copy under the sole control of the Subscriber, or 2) a key backup program approved by the Authorized CA and administered by the Subscriber’s Sponsoring Organization.

- Under no circumstances allow the private key of a certificate issued for the sole purpose of digitally signing documents under this Policy to be backed up or escrowed except by such means that is under the sole control of the Subscriber.

2.1.8 Qualified Relying Party Obligations

This Policy is binding on each Qualified Relying Party by virtue of its e-MARC Agreement, and governs its performance with respect to its application for, use of, and reliance on e-MARC certificates.

(a) Acceptance of Certificates. Each Qualified Relying Party will validate e-MARC certificates issued by all Authorized CAs.

(b) Certificate Validation. Each Qualified Relying Party will validate every e-MARC certificate it requests and receives with the Authorized CA that issued the certificate.

(c) Reliance. A Qualified Relying Party may rely on a valid e-MARC Certificate for purposes of verifying the digital signature and symmetric key exchange only if:

- The e-MARC Certificate was used and relied upon to authenticate a Subscriber’s digital signature for an application bound by this Policy;

- Prior to reliance, the Qualified Relying Party (1) verified the digital signature by reference to the public key in the e-MARC certificate, and (2) verified that the status of the e-MARC Certificate was valid by checking a current Certificate Revocation List (CRL);

- The reliance was reasonable and in good faith in light of all the circumstances known to the

Qualified Relying Party at the time of reliance; and,

- For the purpose of non-repudiation, the Qualified Relying Party shall only rely on digital signatures created using an e-MARC certificate with the non-repudiation bit set in the key usage extension.

2.1.9 Policy Authority Obligations

The Policy Authority is responsible for the terms of this Policy, contract administration, and the authorization and approval of Registry Domains, Registry Administrators, Certification Authorities, Registration Authorities, Certificate Manufacturing Authorities, and Repositories to participate in 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.

Issues of liability must be expressly set forth in contracts between individual parties.

[NOTE: To be addressed by NERC.]

2.3 RESPONSIBILITIES AND RELATIONSHIPS

2.3.1 Financial Responsibilities

A potential CA must demonstrate adequate financial strength to become an Authorized CA, including having adequate insurance coverage (e.g., Errors and Omissions coverage, liability insurance, etc.).

2.3.2 Fiduciary Relationships

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

2.3.3 Administrative Processes

No stipulation.

2.4 INTERPRETATION AND ENFORCEMENT

2.4.1 Governing Law

The law of [*THE STATE WHERE NERC IS INCORPORATED, OR SOME ONE PARTICULAR STATE*] shall govern the enforceability, construction, interpretation, and validity of this Policy. [**For review by NERC.]**

2.4.2 Severability, Survival, Merger, Notice

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 are 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, Suspension, and Revocation Fees

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

2.5.2 Certificate Access Fees

The Authorized CA shall not impose any certificate access fees on Subscribers with respect to use of their own e-MARC Certificate(s) or the status of such e-MARC Certificate(s).

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 escrow, key replacement,e tc).

2.5.6 Refund Policy

There shall be no refunds of any fees 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 Qualified Relying Parties that shall contain: (1) all e-MARC certificates issued by the Authorized CA that have been accepted by the Subscriber, typically available via Lightweight Directory Access Protocol (LDAP); (2) a CRL ; (3) the Authorized CA's e-MARC Certificate for its signing 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-MARC certificates. Submittal of such information to said Repository, with the subsequent availability of such information to Subscribers and Qualified 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-MARC certificates issued by the Authorized CA promptly upon acceptance of such e-MARC certificates. Information relating to the status of an e-MARC Certificate will be published in accordance with the Policy Authority's e-MARC Contract, if applicable.

2.6.3 Access Controls

The Authorized CA shall not impose any access controls on this Policy, the Authorized CA's e-MARC Certificate for its signing key, CRLs, and past and current versions of the Authorized CA's e-MARC CPS. The Authorized CA may impose access controls on e-MARC certificates, in accordance with provisions of the Authorized CA's e-MARC Contract, if applicable.

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 HTML protocol. Such access to Subscribers and Qualified Relying Parties must be secure – provided in accordance with all of the security requirements reflected in this Policy and the CA Requirements document..

2.7 QUALITY ASSURANCE INSPECTION AND REVIEW

The Authorized CA, shall undergo e-MARC Security Certification and Accreditation (C&A) reviews as a condition of obtaining and retaining approval to operate as an Authorized CA under this Policy and 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 Review

Certification authorities shall undergo C&A under the direction of the Policy Authority prior to initial approval as Authorized CA, to demonstrate 1) compliance with this Policy, 2) their e-MARC CPS, and 3) their e-MARC contracts. Re-certification 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.

2.7.2 Identity/Qualifications of C&A Reviewer

An independent security audit firm acceptable to the Policy Authority that is qualified to perform a security audit on a CA shall conduct the C&A process.

2.7.3 C&A Auditor's Relationship to Audited Party

The auditor shall be an independent, unbiased party that is in no way affiliated with the party to be audited.

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

The C&A quality assurance inspection shall be conducted pursuant to the guidance provided in the American Institute of Certified Public Accountants' / Canadian Institute of Chartered Accountants (AICPA/CICA's) WebTrust Principles and Criteria for Certification Authorities.

2.7.5 Actions Taken as a Result of Deficiency

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

(a) The compliance auditor shall note the deficiency;

(b) The compliance auditor shall notify the parties identified in Section 2.7.6 of the deficiency;

(c) The CA will propose a remedy, including expected time for remediation, to the Policy Authority.

The Policy Authority will determine the appropriate remedy, up to and including revocation and non-recognition of the Authorized CA certificate. Upon correction of the deficiency, the Policy Authority may reinstate a previously Authorized CA.

The Policy Authority will address any identified deficiencies with the potential or Authorized CA.

2.7.6 Communication of Results

The Certification Authority shall make the results of the C&A review available to the Policy Authority for determining the CA's suitability for initial and continued performance as an Authorized CA.

2.8 CONFIDENTIALITY

2.8.1 Types of Information to 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 Certificate application, authentication, and certificate status checking processes in accordance with the *Privacy Act of 1974 and*

Amendments[1]. 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:

(a) must be made available by the Authorized CA to the Subscriber involved following an appropriate request by such Subscriber;

(b) must be subject to correction and/or reasonable and appropriate revision by such Subscriber;

(c) must be protected by the Authorized CA in a manner designed to ensure the data's integrity and confidentiality; and

(d) cannot be used or disclosed by the Authorized CA for purposes other than the direct operational support of e-MARC 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 RA, CMA, or Repository) have access to the private keys of any Subscriber to whom it issues an e-MARC Certificate to be used solely for the purpose of generating digital signatures when the non-repudiation bit is expressed. Subscriber private key backup or key escrow programs are permitted for the purposes of recovering the private keys of e-MARC certificates issued for encryption. See Section 7, for a complete certificate profile..

<u>Other Subscriber Information</u>. The Authorized CA shall take reasonable steps to protect the confidentiality of Qualified Relying Party or other Subscriber information provided to the Authorized CA. 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 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.

[1] Privacy Act of 1974 and Amendments (as of Jan 2, 1991), 5 USC Sec. 552.a, Title 5, Part 1, Chap. 5, Subchapter II.

2.8.2 Types of Information Not Considered Confidential

Information contained within a single e-MARC Certificate 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.

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 Certificate. This Policy is the property of the Policy Authority. "Energy Market Access and Reliability Certificates," otherwise referred to as "e-MARCs" or "e-MARC certificates," and the e-MARC OIDs 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

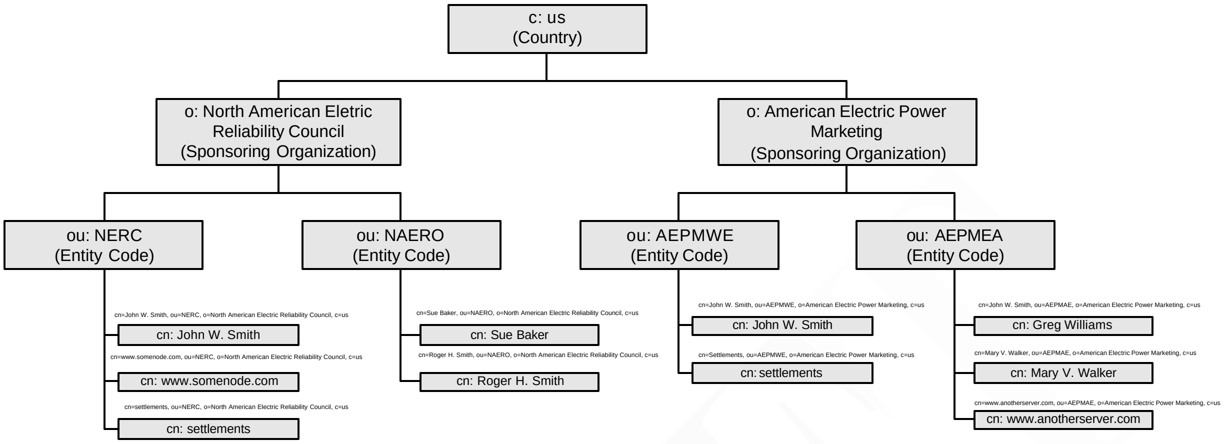
IDENTIFICATION AND AUTHENTICATION

3.1 INITIAL REGISTRATION

Subject to the requirements noted below, applications for e-MARC certificates may be communicated from the applicant to an Authorized CA or an authorized RA, and authorizations to issue e-MARC certificates may be communicated from an authorized RA to an Authorized CA, (1) electronically, provided that all communication is encrypted and/or digitally signed, (2) by first class mail, or (3) in person. The applicant must also specify in their application, which Registry Domain they are requesting a certificate under and include both their unique "Entity Code" assigned to them by the Registry and the official company name of the sponsoring organization. Unaffiliated individuals, however, do not have to provide an "Entity Code" or the company name of a sponsoring organization

3.1.1 Types of Names

All e-MARC certificates subjects 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 Qualified Relying Party, Business Representative or Device certificate, 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. Unaffiliated individuals must go through a verification process prior to obtaining an e-MARC certificate. Shown below is an ***example*** DN hierarchy:


c: us
(Country)
o: North American Eletric Reliability Council
(Sponsoring Organization)
o: American Electric Power Marketing
(Sponsoring Organization)
ou: NERC
(Entity Code)
ou: NAERO
(Entity Code)
ou: AEPMWE
(Entity Code)
ou: AEPMEA
(Entity Code)
cn=John W. Smith, ou=NERC, o=North American Electric Reliability Council, c=us
cn: John W. Smith
cn=www.somenode.com, ou=NERC, o=North American Electric Reliability Council, c=us
cn: www.somenode.com
cn=settlements, ou=NERC, o=North American Electric Reliability Council, c=us
cn: settlements
cn=Sue Baker, ou=NAERO, o=North American Electric Reliability Council, c=us
cn: Sue Baker
cn=Roger H. Smith, ou=NAERO, o=North American Electric Reliability Council, c=us
cn: Roger H. Smith
cn=John W. Smith, ou=AEPMWE, o=American Electric Power Marketing, c=us
cn: John W. Smith
cn=Settlements, ou=AEPMWE, o=American Electric Power Marketing, c=us
cn: settlements
cn=John W. Smith, ou=AEPMAE, o=American Electric Power Marketing, c=us
cn: Greg Williams
cn=Mary V. Walker, ou=AEPMAE, o=American Electric Power Marketing, c=us
cn: Mary V. Walker
cn=www.anotherserver.com, ou=AEPMAE, o=American Electric Power Marketing, c=us
cn: www.anotherserver.com

(**NOTE**: C = country, O = Organization, OU = Organizational Unit, cn = common name)

3.1.2 Name Meanings

In the case of Unaffiliated Individuals, the authenticated common name (labeled “cn” in the above diagram) should be a combination of first name, surname and an optional middle initial. In the case of Business Representatives, the authenticated common name should be the combination of first name, surname and an optional middle initial. In the case of Qualified Relying Parties, the authenticated common name should be the combination of first name, surname and an optional middle initial unless the Qualified Relying Party represents a device or application (e.g., web servers) in which case the common name should be the fully qualified domain name of the device/application.

A certificate issued for a device or application must include the Point-of-Contact email address or person who is responsible for that device or application in the SubjectAltName field of the certificate.

For Business Representatives, Qualified Relying Parties, and Devices, the DN within the certificate subject must also contain the Entity Code of the sponsoring organization in the OU field and the official company name of the sponsoring organization being represented in the O field.

3.1.3 Rules for Interpreting Various Name Forms

Rules for interpreting name forms are contained in the applicable certificate profile (see Section 7.1.2), and are established by a naming authority if one exists, or by the Authorized CA itself. The naming authority shall be identified contractually or in a CPS.

3.1.4 Name Uniqueness

Name uniqueness across all e-MARC certificates must be enforced and each Authorized CA shall enforce name uniqueness within 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-MARC certificates is ensured. An Authorized CA shall document in its CPS what name forms will be used and how they 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 with an e-MARC Certificate 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 but the Authorized CA reserves 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 Pair

The Authorized CA shall verify that the applicant possesses the private key corresponding to the public key submitted with the application by utilizing a key transfer protocol or equivalent method, and that these keys form a functioning pair.

3.1.8 Authentication of Sponsoring Organization or Qualified Relying Party Identity

If the applicant is requesting a Business Representative e-MARC or Qualified Relying Party Certificate, 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 Certificate 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 principle registration, , principle business address (including number and street, city, postal code), and principle business telephone number. The Authorized CA may rely on the Registry to verify the business credentials (e.g., entity code, business code, etc.) of the Sponsoring Organization.

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

3.1.9 Authentication of Individual Identity

3.1.9.1 Unaffiliated Individual e-MARC Certificates

Unaffiliated 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 principle telephone number. Subscriber identification must be confirmed via a Policy Authority-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 cross-checks for consistency, for example:

- Currently-valid credit card number;
- 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 principle telephone number;
- Currently valid state-issued driver’s license number or state-issued identification card number;
- Social Security Number, or similar Canadian or other national identification;
- Date of birth; and
- Place of birth.

At least one of the above data sources must be based on an antecedent in-person, 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.

3.1.9.2 Business Representative and Device e-MARC Certificates

If the applicant is requesting a certificate for a Business Representative, device, or application certificate, the authorized CA shall verify:

(a) that the applicant is a duly authorized representative of the Sponsoring Organization as an employee, partner, member, agent, or other association; and

(b) the Sponsoring Organization's identity as specified in section 3.1.8.

3.1.9.3 Qualified Relying Party e-MARC Certificates

If the applicant is requesting a Qualified Relying Party e-MARC Certificate, the Authorized CA shall verify:

(a) that the applicant is authorized to act on behalf of the Qualified Relying Party;

(b) the affiliation of the e-MARC Certificate applicant with the Qualified Relying Party; and

(c) 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 discovery. 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 <u>and</u> re-establish its identity. Re-keying 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-MARC certificates shall also be rekeyed when they are renewed.

In accordance with the e-MARC contract the Authorized CA shall accept e-MARC Certificate renewal requests from their Subscribers within 90 days from the scheduled end of the operational period (expiration date) of the e-MARC Certificate, provided the e-MARC Certificate is not currently under revocation or suspension or expired. e-MARC certificates shall be renewed in 1-year increments.

Since the key pair is required to change, the Authorized CA shall require the Subscriber to request a new e-MARC Certificate with an associated new public/private key pair each year. For the first two years a renewal request may take place based on the presentation of the existing valid certificate. Every third year the certificate Subscriber must identify itself as for a new request, in accordance with section 3.1. The Authorized CA shall renew e-MARC certificates issued to Qualified Relying Parties 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, suspended, revoked, or expired e-MARC certificates shall not be renewed. Applicants without a valid e-MARC Certificate shall be re-authenticated by the Authorized CA or an authorized RA through a new e-MARC Certificate application, just as with an initial applicant registration, and shall be issued a new e-MARC Certificate.

3.4 REVOCATION REQUEST

In accordance with the e-MARC contract and section 4.4.1, an e-MARC Certificate revocation request that is submitted electronically may be authenticated on the basis of a digital signature using the e-MARC Certificate's associated key pair. 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 Certificate'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 quickly revoke certificates.

SECTION 4

Operational Requirements

4.1 CERTIFICATE APPLICATION

Application Initiation. The following persons may initiate the e-MARC Certificate application process:

Potential Subscriber	Authorized Initiator
Unaffiliated Individual	Potential Subscriber only
Business Representative, device, or application	Sponsoring Organization; or potential Subscriber
Qualified Relying Party	Duly authorized representative of the Qualified Relying Party

(a) Application Form. An applicant for an e-MARC Certificate shall complete an e-MARC Certificate application and provide requested information in a form prescribed by the Authorized CA and this Policy.

(b) Applicant Education and Disclosure. At the time of e-MARC Certificate application, the Authorized CA shall inform applicants of the advantages and potential risks associated with using e-MARC certificates to access Qualified Relying Parties 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 use of a PKI system for e-MARC certificates, and to minimize imposition of specific implementation requirements on CMAs, Subscribers, 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 Subscriber (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 Subscriber (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 Subscribers, and that does not defeat security; but all 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 CP 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 said authorizations.

Requests by CAs for Authorized CA certificates shall be submitted to the Policy Authority using the contact provided in Section 1.4, and shall be accompanied by a CPS written to the format of the *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* [RFC2527].

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 the e-MARC CP.

Authorized CAs shall only issue certificates asserting the e-MARC CP 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 said 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 Certificate, notify the applicant thereof, and make the e-MARC Certificate available to the applicant. The Authorized CA shall use a secondary notification process linked to the e-MARC Certificate applicant's physical postal mail address, or equivalent to provide notification of the e-MARC Certificate issuance only to the Subscriber or the authorized representative of the Sponsor.

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

(a) the Authorized CA has issued, and will manage, the e-MARC Certificate in accordance with the requirements in this Policy;
(b) the Authorized CA has complied with all requirements in this Policy when identifying the Subscriber and issuing the e-MARC Certificate;
(c) there are no misrepresentations of fact in the e-MARC Certificate actually known to or reasonably knowable by the Authorized CA and the Authorized CA has verified the information in the e-MARC Certificate pursuant to this policy;
(d) information provided by the Subscriber for inclusion in the e-MARC Certificate has been accurately transcribed to the e-MARC Certificate; and
(e) the e-MARC Certificate meets the material requirements of this Policy.

4.2.1 Delivery of Subscriber's Private key to Subscriber

The private key shall be generated and remain within the cryptographic boundary of a cryptographic module, and as such there is no need to deliver the subscriber's private key. Private keys associated with certificates may be generated and stored in software cryptographic modules.

4.2.2 Control Room 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. Certificates corresponding to private keys held by multiple Subscribers shall not be used for contracting or e-commerce applications. 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;
- That list of those holding the shared private key must be provided to, and retained by, the Authorized CA and/or LRA/RA; and

For reasons of security, control room certificates must be issued in FIPS-140 compliant hardware tokens only. 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, etc.).

4.3 CERTIFICATE ACCEPTANCE

As described in the e-MARC contract, as a condition to issuing the e-MARC Certificate, the Subscriber shall indicate acceptance or rejection of the e-MARC Certificate to the Authorized CA and acknowledge the Subscriber obligations under Section 2.1.7. By accepting the e-MARC Certificate, the Subscriber is warranting that all information and representations made by the Subscriber that are included in, and relied upon in issuing, the e-MARC certificate are true and accurate.

4.4 CERTIFICATE SUSPENSION AND REVOCATION

4.4.1 Who Can Request Revocation

The only persons permitted to request revocation of an e-MARC Certificate issued pursuant to this Policy are the Subscriber, an authorized representative of the Sponsoring Organization, the RA, 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 their own e-MARC Certificate at any time for any reason. A Sponsoring Organization may request revocation of an e-MARC Certificate issued to its Business Representative (device or individual) at any time for any reason.

4.4.2.2 Required Revocation

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

(a) When any of the identifying information on the e-MARC Certificate changes or otherwise becomes obsolete.

(b) When the private key, or the media holding the private key, associated with the e-MARC Certificate (the Subscriber's private key) is, or is suspected of having been, compromised.

(c) When the individual named as a Business Representative no longer represents, or is no longer affiliated with, the Sponsoring Organization.

(d) When a device or server is no longer active or no longer affiliated with a Sponsoring Organization.

(e) Upon a change of an Individual or Sponsoring Organization's registration in the Registry Domain (where applicable). Changes in registration information, including DUNS number or Entity Code or any other attribute that the appropriate Registry Administrator deems to warrant revocation within the intent of this Policy. During the transition to e-MARC certificates, exiting Subcriber certificates will be accepted, by Qualified Relying Parties up to one year.

(f) If an Authorized CA learns, or reasonably suspects, that the Subscriber's private key has been compromised; or

(g) If the issuing Authorized CA determines that the e-MARC Certificate was not properly issued in accordance with this Policy and/or the Authorized CA's e-MARC CPS.

Failure to do so shall subject the subscriber to assume liabilities under this Policy.

4.4.3 Revocation

4.4.3.1 Procedure for Revocation Request

As described in the e-MARC Contract an e-MARC Certificate revocation request should be promptly communicated to the issuing Authorized CA, either directly or through the RA authorized to accept such notices on behalf of the Authorized CA. An e-MARC Certificate 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 RA 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. In all other situations, certificates should be revoked as soon as practicable; however, a 2-week (10 business days) grace period may be given at the Authorized CA's discretion.

4.4.4 Suspension

4.4.4.1 Who Can Request Suspension

The only persons permitted to request suspension of an e-MARC Certificate issued pursuant to this Policy are the Subscriber, the Sponsoring Organization (where applicable), the RA, and the issuing Authorized CA. Although not required, a certificate **may** be placed in suspended status following an unsigned request for certificate revocation, pending authentication of the revocation request.

4.4.4.2 Procedure for Suspension Request

As described in the e-MARC Contract an e-MARC Certificate suspension request should be promptly communicated to the issuing Authorized CA, either directly or through the RA authorized to accept such notices on behalf of the Authorized CA. An e-MARC Certificate suspension request may be communicated electronically if it is digitally signed with the private key of the Subscriber' identity certificate, or the Sponsoring Organization (where applicable). Alternatively, the Subscriber, or Sponsoring Organization (where applicable) may request suspension by contacting the issuing Authorized CA or its RA in person and providing adequate proof of identification in accordance with this Policy.

4.4.4.3 Limits on Suspension Period

A certificate may maintain a suspended state up to 2 weeks (10 business days). After that time, if no action has been taken, the Authorized CA shall change the certificate status to a revoked and inform the Subscriber of the action taken.

4.4.5 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 12 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 certificate holders and Qualified Relying Parties. When a certificate is revoked an updated CRL must be issued within four (4) hours of the event.

4.4.6 Revocation/Status Checking

4.4.6.1 CRL Checking Requirements

A Qualified Relying Party must check the status of all certificates in the certificate validation chain against the current CRL prior to their use. The Qualified 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.

4.4.6.2 Online Revocation Checking Requirements

Each Qualified Relying Party will validate via CRL every e-MARC Certificate it receives for every transaction.

4.4.7 Other Revocation Advertisements

4.4.7.1 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; and
- The alternative method must provide authentication and integrity services commensurate with the assurance level of the certificate being verified.

4.4.7.2 Checking Requirements

A Qualified Relying Party may also use other methods to verify the status of 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 level of the certificate being revoked.

4.4.8 Special Requirements for Key Compromise

In the event of the compromise, or suspected compromise, of a 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 its' 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. 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:

- e-MARC certificate applications, including all application information;
- Certificate issuances and transactions;
- System start-up and shutdown;
- Authorized CA application start-up and shutdown;
- attempts to create, remove, set passwords or change the system privileges of the PKI Master Office, PKI Office, or PKI 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 system;
- unauthorized attempts to access system files;
- generation of own and subordinate Entity keys;
- revocation of certificates;
- attempts to initialize, remove, enable, and disable Subscribers, and update and recover their keys;

- failed read-and-write operations on the certificate and CRL directory; and
- 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 which 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 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 that the archive is stored on 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 time 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 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 the purposes of validity checking. The maximum lifetime of the Root CA certificate will be 50 years. The maximum lifetime of any intermediary CAs will be 10 years, while the lifetime of CA issuing end-entity e-MARC certificates will be a maximum of 5 years. The validity period of each of these CAs will be longer to account.

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, a 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 Revoked

In the even of the need for revocation of an Authorized CA's Digital Signature certificate, the Authorized CA must immediately notify:

- The Policy Authority;
- All Authorized CAs to whom it has issued cross-certificates;
- All of its RAs;
- All Subscribers; and
- All individuals or organizations who are responsible for a certificate used by a device or application.

The Authorized CA must also:

- Publish the certificate serial number on an appropriate CRL; and
- Revoke all cross-certificates signed with the revoked Digital Signature certificate.

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

- Generate a new Authorized CA signing key pair; and/or
- 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*)

As required by the e-MARC contract each Authorized CA must have in place an appropriate key compromise plan 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-MARC certificates. Such plan shall include procedures for revoking all affected e-MARC certificates and promptly notifying all Subscribers and all Qualified Relying Parties substantially similar to the procedures under Section 4.8.2.

4.8.4 Secure Facility after a Natural or Other Disaster (*Disaster Recovery Plan*)

An Authorized CA must have in place an appropriate disaster recovery/business resumption plan. Such 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 e-MARC or is otherwise terminated:

(a) All Subscribers, sponsoring organizations, and Qualified Relying Parties must be promptly notified of the cessation.

(b) All e-MARC certificates issued by an Authorized CA shall be revoked no later than the time of cessation.

(c) All current and archived e-MARC identity proofing, certificate, validation, revocation/suspension, 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

As described in the e-MARC contract each Authorized CA shall implement and maintain an e-MARC Customer Service Center to provide assistance and services to Subscribers and Qualified 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 RAs, 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 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 so as to prevent exposure of systems to water. All electronic physical security devices will be tested daily.

The Authorized CA equipment shall consist of equipment 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, 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 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 audit 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 utilize commercially reasonable practices to ensure that one person acting alone cannot circumvent security safeguards or otherwise compromise the integrity of the e-MARC system.

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 physical access to 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; and
- 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 RA, 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 on-going process.

5.3.3 Training

Authorized CA employees must receive training in the organizational policies and procedures to ensure the Authorized CA's policies are adhered to. 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, their access to the system must be revoked or suspended. Breach of this CP 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, their physical access and system access must be revoked immediately.

5.3.6 Contracting Personnel

Contractor personnel employed to operate any part of the Authorized CA are subject to the same clearance procedures specified in section 5.3.2.

5.3.7 Documentation Supplied to Personnel

The CP and relevant parts of the CPS shall be made available to the Authorized CA personnel and subscribers. Operation 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 suspension or termination of access rights.

5.3.8 Personnel Security Controls for End Entities

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

SECTION 6

Technical Security Controls

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

(a) General. Key pairs for all Program Participants must be generated in such a way that the private key is not known by other than the authorized user of the key pair except as noted for key backup and/or escrow. Authorized CA, RA, and CMA keys may be generated in either hardware or software, although hardware based key generations is preferred. Key pairs for Subscribers and Qualified Relying Party application can be generated in either hardware or software.

(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 system used to generate the key-pair must be accessible to the Program Participant and initiated by the authorized user of key pair (subscriber and/or Program Participant).

(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 it is discovered by any Program Participants that a certificate was issued in violation of 6.1.1a or 6.1.1b, the certificate must be revoked.

6.1.2 Private Key Delivery to Entity

Private keys shall be delivered pursuant to Section 4.2.1

6.1.3 Subscriber Public Key Delivery to Authorized CA

As part of the e-MARC Certificate application process, the Subscriber's public key must be transferred to the Registration Authority 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 done on-line, the delivery mechanism should be in accordance with the Public Key Infrastructure X.509V3 (PKIX-3) Certificate Management Protocol (See RFC 2510), or via an equally secure manner.

6.1.4 Authorized CA Public Key Delivery to Users

No stipulation.

6.1.5 Key Sizes

Key sizes and algorithms shall be a minimum of 1024 bits and preferably 2048 bits for all e-MARC end-entities (Subscribers, Business Partners, Devices, and Qualified Relying Parties). All Authorized CAs in the e-MARC trust hierarchy shall use a minimum of 2048 bits for all keys.

6.1.6 Public key parameters 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 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 v3 key usage field)

Public keys that are bound into certificates which assert the e-MARC assurance policies for creation of digital signatures shall be certified for use solely in signing and authentication, but not encryption. 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 (like the Secure Sockets Layer) that provide authenticated connections using key management certificates.

6.2 AUTHORIZED CA PRIVATE KEY PROTECTION

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

The relevant standard for cryptographic modules is *Security Requirements for Cryptographic Modules* [current version of FIPS140]. 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 held in strictest confidence.

Note that Section 6.1.1 stipulates minimum cryptographic module requirements for key generation.

	Subscriber	Authorized **RA**	Authorized **CA**
FIPS 140 validation	Level 1 or 2	Level 2	Level 3
Operational requirement	Shall not output private asymmetric key in plaintext		

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

The issuing Authorized CA must retain all verification public keys. In no circumstances shall an attempt be made to archive or create a repository for private signing keys (see section 6.1.1 Key Pair Generation).

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

Subscriber key pair must be replaced in accordance with the validity periods specified in the applicable certificate profile. (see Section 7.1 Certificate and CRL Profiles).

6.3.3 RESTRICTIONS ON AUTHORIZED CA'S PRIVATE KEY USE

The private key used by Authorized CAs for issuing e-MARC certificates shall be used only for signing such Certificates and, optionally, CRLs or other validation services responses pursuant to Section 4.8.2.

A private key held by a CMA, if any, and used for purposes of manufacturing e-MARC certificates, is considered the Authorized CA's signing key, is held by the CMA as a fiduciary, and shall not be used by the CMA for any other purposes, except as agreed to by the Policy Authority and the Authorized CA. Any other private key used by a CMA for purposes associated with its CMA function shall not be used for any other purpose without the express permission of the Authorized CA.

The private key used by each RA employed by an Authorized CA in connection with the issuance of e-MARC certificates shall be used only for communications relating to the approval or revocation of such certificates.

6.4 ACTIVATION DATA

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

No stipulation.

6.6 Life Cycle Technical Controls

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

A security policy document must exist. This document 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 those who 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

Requirements for cryptographic modules are as stated above in Sections 6.1.1 and 6.2.

SECTION 7

Certificate and CRL Profiles

7.1 CERTIFICATE PROFILE

e-MARC certificates 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-MARC certificates that conform to the International Telecommunications Union – Telecommunications Sector (ITU-T) Recommendation X.509, “The Directory: Authentication Framework,” June 1997.

All e-MARC certificates 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 will include a reference to the OID for this Certificate policy (or equivalent OID) within the Certificate Policies field. Supported Certificate extensions shall be identified in the e-MARC CPS.

7.1.1 Version Number

The Authorized CA shall issue X.509 “Version 3” certificates.

7.1.2 Certificate Extensions

Certificate extensions shall include the extensions specified in the Minimum Interoperability Specification for PKI Components, Version ~~1~~, Sept. 3, 1997. MITRE will check.

7.1.3 Algorithm Identifiers

Certificates under this Policy will use the following OIDs for signatures:

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 }

Certificates under this Policy will use the following OIDs for identifying the algorithm for which the subject key was generated:

id-dsa	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1}
Id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-x9-62(10045) public-key-type (2) 1}
rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}

The e-MARC PKI shall certify only public keys associated with the crypto-algorithms identified above, and shall only use the signature crypto-algorithms described above to sign certificates, certificate revocation lists and any other PKI product.

7.1.4 Name Forms

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

7.1.5 Name Constraints

Subject and Issuer DNs must comply with Policy Authority standards and be present in all certificates.

7.1.6 Certificate Policy Object Identifier

The Authorized CA must ensure that the e-MARC Certificate Policy OID is contained within the certificates.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

The Authorized CA must populate the policyQualifiers extension with the URI of its CP.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

No stipulation.**7.1.10 Certificate Profile and Certificate Profile Extensions**

Certificates issued by an Authorized CA may conform to the profile recommendations in the Federal PKI X.509 Certificate and CRL Extensions Profile (http://csrc.nist.gov/pki/twg/y2000/papers/twg-00-18.xls). Any variance from the above profile recommendations shall be approved by the Policy Authority, and documented in the Authorized CA CPS

7.2 CRL PROFILE

7.2.1 Version Number(s)

CRLs issued under this Policy shall assert a version number as described in the X509 standard [ISO9594-8]. CRLs may assert X.509 "Version 1" or "Version 2" certificates.

7.2.2 CRL and CRL Entry Extensions

Certificates issued by an Authorized CA may conform to the profile recommendations in the Federal PKI X.509 Certificate and CRL Extensions Profile (http://csrc.nist.gov/pki/twg/y2000/papers/twg-00-18.xls), or may issue CRLs asserting no extensions. Any variance from the above profile recommendations shall be approved by the Policy Authority, and documented in the Authorized CA CPS.

SECTION 8

POLICY ADMINISTRATION

8.1 POLICY CHANGE PROCEDURES

8.1.1 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, subscribers, and Qualified Relying Parties, and will be posted on the Policy Authority's WWW 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 email or postal notice.

8.1.2 Comment Period

Any interested person may submit written comments with the Policy Authority dispatched within 45 days of the original 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 Adoption

Proposed changes to this policy will be brought forth to the Senior Steering Committee members. The proposed change(s) will be reviewed and members of the committee will vote whether to accept or reject it. If accepted, the policy change will be published on the Policy Authority's WWW website. Subscribers are responsible for periodically checking to ensure no policy changes have been issued. Entities relying on the e-MARC certificates will be given a reasonable amount of time to transition to 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 WWW 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 below criteria:

(1) Compliance with RFC 2527

(2) Compliance with the e-MARC Certificate Policy

(3) Completion of the C & A process

(4) Fulfilling the e-MARC Requirement's document.

Glossary

e-MARC. Energy Market Access and Reliability Certificates. Aimed at providing commercial public key certificate services to the those participating in energy markets and identified in authorized Registry Domains.

e-MARC certificates. Certificates issued by an Authorized CA in accordance with this Policy, which certificates reference, this Policy by inclusion of the e-MARC OID.

e-MARC CPS. An e-MARC CPS is a certification practice statement of the practices that an Authorized CA employs in issuing, suspending, and revoking e-MARC certificates and providing access to the same.

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.

Agency Applications. See "Qualified Relying Party."

Authenticate. Relates to a situation where one party has presented an identity and claims to be that identity. Authentication enables another party to gain confidence that the claim is legitimate.

Authorized CA. A certification authority that has been authorized by the Policy Authority to issue e-MARC certificates and provide Authorized CA Services under the Policy.

Authorized CA Services. The services relating to e-MARC certificates to be provided by Authorized CAs under this Policy (See section 2.1.1).

CA. See "Certification Authority."

Certificate. A data record that, at a minimum: (a) identifies the Authorized CA issuing it; (b) names or otherwise identifies its Subscriber; (c) contains a public key that corresponds to a private key under the control of the Subscriber; (d) identifies its operational period; and (e) contains an e-MARC Certificate 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 "*CertificatePolicies*" field of an X.509 v.3 certificate.

Certificate Manufacturing Authority (CMA). An entity that is responsible for the manufacturing and delivery of e-MARC certificates 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 actually manufacturing the Certificate on behalf of an Authorized CA).

Certification Authority. A certification authority is an entity that is responsible for authorizing and causing the issuance of a Certificate. See "Authorized CA."

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

CMA. See "Certificate Manufacturing Authority".

CPS. See "Certification Practice Statement".

CRL. Certificate Revocation List

CSOR. Computer Security Objects Register operated by the National Institute of Standards and Technology (NIST).

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

DSA. Digital Signature Algorithm

DSS. Digital Signature Standard

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 Standards. These are Federal standards that 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 to agency waiver procedures.

FIPS PUB. Federal Information Processing Standards Publication

Government. Federal Government and authorized agencies and entities.

NERC. North America Electric Reliability Council

e-MARC Contract.

e-MARC Operating Agreement.

IETF. See “Internet Engineering Task Force.”

Internet Engineering Task Force (IETF). The Internet Engineering Task Force is a large open international community of network designers, operators, vendors, and researches 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 a Authorities to replace its own private key (e.g., due to compromise) and replace current valid certificates issued with old key.

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

Mutual Authentication. Parties at both ends of a communication activity authenticate each other (see authentication).

NIST. National Institute of Standards and Technology.

Object Identifier. An object identifier is a specially formatted number that is registered with an internationally-recognized standards organization.

OID. See "Object Identifier".

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

Operational Period of an e-MARC Certificate. The operational period of an e-MARC Certificate is the period of its validity. It would typically begin on the date the certificate is issued (or such later date as specified in the certificate), and ends on the date and time it expires as noted in the certificate or is earlier revoked or suspended.

Out-of-band. Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party using U.S. Postal mail to communicate with another party where current communication is online communication).

PKI. Public Key Infrastructure

PKIX. Public Key Infrastructure (X.509)

PIN. Personal Identification Number

Policy. Means this Certificate Policy.

Policy Authority. The entity specified in Section 1.4

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

Program Participants. Collectively, the Registry Administrators, Authorized CAs, Registration Authorities, Certificate Manufacturing Authorities, Repositories, Subscribers, Qualified Relying Parties, and Policy Authority authorized to participate in the public key infrastructure defined by this Policy.

Public Key. The 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 Certificate 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.

Qualified Relying Party. A recipient of a communication event protected by a certificate-based security service that is authorized by this Policy to rely on an e-MARC Certificate to verify the digital signature on the message, including the revocation status of any presented certificate.

RA. See "Registration Authority."

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

Registry Domain. A registry of market participant. A Registry Domain typically describes a bounded set of market participants within a particular energy segment, such as gas or electricity. The Registry and Registry Domain must comply with the policies set forth in this document and have a unique registered Internet domain name.

Registry Administrator. An entity or organization authorized to administer a Registry Domain in accordance with the policies set forth in this document.

Repository. A database containing information and data 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. Means to prematurely end the operational period of a Certificate from a specified time forward.

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

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

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

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

Transaction. Any financially binding action. As defined by the software application or process being secured or implemented.

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

URI. Universal Resource Identifier**.**

U.S.C. United States Code

Valid Certificate. Means an e-MARC Certificate 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. Thus, an e-MARC Certificate is not "valid" until it is both issued by an Authorized CA and has been accepted by the Subscriber.

Written. A written record, or any writing, includes email or other electronic communication legally binding in the jurisdiction where created or received.

WWW. World Wide Web, a popular subset of the Internet; affords reader-friendly access to information by means of Hyper-Text Markup Language (HTML) and Extended Markup Language (XML) and other commands embedded in text displayed as "(web)pages" on/at "(web)sites."

Bibliography

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

ABADSG Digital Signature Guidelines, 1996-08-01.
http://www.abanet.org/scitech/ec/isc/dsgfree.html.

FIPS 112 Password Usage, 1985-05-30
http://csrs.nist.gov/fips/

FIPS 140-1 Security Requirements for Cryptographic Modules, 1994-01
http://csrs.nist.gov/fips/fips1401.htm

FIPS 140-2 Security Requirements for Cryptographic Modules, 2001-05
http://csrs.nist.gov/fips/fips1402.htm

FIPS 186 Digital Signature Standard, 1994-05-19 http://csrs.nist.gov/fips/fips186.pdf

FOIACT 5 U.S.C. 552, Freedom of Information Act.
Http://www4.law.cornell.edu/uscode/5/552.html

FPKI-Prof Federal PKI X.509 Certificate and CRL Extensions Profile
http://csrc.nist.gov/pki/twg/y2000/papers/twg-00-18.xls

ISO9594-8 Information Technology-Open Systems Interconnection-The Directory: Authentication Framework, 1997.
ftp://ftp.bull.com/pub/OSIdirectory/ITU/97x509final.doc

ITMRA 40 U.S.C. 1452, Information Technology Management Reform Act of 1996.
Http://www4.law.cornell.edu/uscode/40/1452.html

NAG69C Information System Security Policy and Certification Practice Statement for Certification Authorities, rev C, November 1999.

NS4005 NSTISSI 4005, Safeguarding COMSEC Facilities and Material, August 1997.

NS4009 NSTISSI 4009, National Information Systems Security Glossary, January 1999.

PKCS#12 Personal Information Exchange Syntax Standard, April 1997.
Http://www.rsa.com/rsalabs/pubs/PKCS/html/pkcs-12.html

RFC 2510 Certificate Management Protocol, Adams and Farrell, March 1999.

RFC 2527 Certificate Policy and Certificate Practices Framework, Chokhani and Ford, March 1999.

Security Requirements for Certificate Issuing and Management Components, 3 November 1999, Draft

United States Department of Defense X.509 Certificate Policy, Version 6.0, 31 May 2002

OASIS Security Requirements

Developed by: OASIS Standards Collaborative (OSC)

Version 1.0

INTENTIONALLY
BLANK

Table of Contents

1 Introduction

1.1 Scope

This document describes the security requirements for OASIS Phase 2, Electronic Tagging, and for any other industry systems that require strong security and authentication.

1.2 Overview

No formal method of securing communications among OASIS nodes, E-Tag nodes, or authenticating market participants has been available. The general consensus among OASIS administrators, market participants, and E-Tag participants is that if these systems were to be compromised, it would have a significant impact of system reliability and energy markets. The following security services were identified as the most critical:

1. Privacy: Messages are private among communicating parties.
2. Authentication: Determining whom you are communicating with.
3. Message Integrity: Ensuring that messages are not tampered with during transit.

Since both OASIS and E-Tag use HTTP 1.0/1.1, a technology capable of securing HTTP or the message content is necessary. Additionally, the technology chosen must be easily implemented and cost effective while still achieving the stated objectives (see section 2). The following security architecture is believed to meet these requirements and objectives:

1. Secure Sockets Layer, version 3.0.
2. Mutual Authentication (both Client and Server must have certificates and be authenticated)
3. 1024 bit X.509V3 certificates from approved commercial Certificate Authorities capable of supporting 128-bit SSLv3.0 encryption.

Additional details will be provided in the remainder of this document. **If unfamiliar with cryptographic concept or SSL, it is highly recommended that section 4 be reviewed first.**

1.3 Notation Convention

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119.

A “CLIENT” shall be considered to be any system that initiates an SSL or HTTP connection/session. A “SERVER” shall be considered to be any system that accepts an SSL or HTTP connection/session and/or processes E-Tag methods.

2 Requirements

The requirements for OASIS security expand on the SSL/TLS security options provided under SMXP1.0, section 7.0. Review the SMXP1.0 specification for additional information regarding SSLv3.0 as it applies to the SMXP1.0.

2.1 SSLv3.0

ETag1.7 nodes (clients and servers) must use SSLv3.0 on IP port 443. Both client and server authentication (mutual) must be enabled. TLS1.0 may optionally be supported but must not be required by servers or clients.

2.1.1 Encryption

Secure Sockets Layer employs symmetric cryptography for the bulk encryption of session messages sent between the client and server. The session key for the bulk encryption of data shall be 128-bits long and the X.509v3 certificate used by a server must be capable of supporting a 128-bit key exchange. Conversely, the SSLv3.0 implementations (i.e., toolkits, operating system and libraries) utilized by both the client and server must be capable of supporting 128-bit encryption.

2.1.2 Performance

Depending on the cryptographic protocols being used and SSL parameters chosen, SSL connections can be anywhere between 2 and 100 times slower than ordinary TCP connections. To minimize the impact this may have on systems, there are several basic SSL performance rules that should be observed by clients and servers:

Asymetric Algorithm of choice: RSA

Symmetric Algorithm of choice: RC4 (128-bit). 3DES is more secure but has a significant performance penalty associated with it.

Digest Algorithm of choice: SHA-1. MD5 is slightly faster, but SHA-1 is more secure and MD5 is being phased out.

Session Resumption: Clients should always attempt to use session resumption. Servers should allow it if clients tend to reconnect within 5 to 10 minutes.

Record Size: Send data in the largest chunks possible.

Not all SSL/TLS toolkits and implementations may allow direct control over cryptographic settings and operating parameters. However, to the extent a client or server does have control over these operating parameters they should be set accordingly. The use of hardware or inline SSL accelerators may also be used to improve performance (see section 3.3). **See section 4 for more information on cryptography and SSL.**

2.1.3 Non-repudiation

SSL and TLS are not able to provide non-repudiation of data. While SSL/TLS ensures that communicating parties are certain of who they are talking to and provides for the highly secure and tamper proof transfer of data, the data itself is not signed with either of the communicating parties private keys. Consequently, outside of an SSL/TLS session, the data cannot stand-alone as non-repudiatable. Sufficient logging and vigilance on the part of both sender and receiver are necessary to adequately defend against possible claims repudiating data.

2.2 Certificates

Standard 1024-bit X.509v3 certificates (RFC 2459) shall be used by clients and servers.

2.2.1 Server Certificates

A server's certificate subject (i.e., distinguished name) shall have:

1. The "CN" field (Common Name) set to the fully qualified host name of the server.
2. The "OU" field (Organizational Unit) of the certificate's subject shall be set to the NERC registered code of the PSE/CA/TP associated with the server or that of a service provider acting on behalf of the PSE/CA/TP.
3. The "O" field (Organization) of the certificate's subject shall be the legal name of the entity represented by the NERC code located in the certificate's "OU" field.

The "CN", "OU" and "O" fields MUST be consistent with the NERC registry.

2.2.2 Client Certificates

A client certificate must be associated with a NERC registered PSE/CA/TP via the certificate's subject "OU" and "O" fields. The "CN" field of the certificate may either be the fully qualified host name of the client system communicating with the server or the name of an employee/individual authorized as a business representative by the NERC registered PSE/CA/TP.

2.2.3 Certificate Authorities

Client and server certificates may be acquired from any NERC approved Certificate Authority (see section 4.6 for description). The currently approved Certificate Authorities include [note: bogus list – need to evaluate several CA's yet]:

Certificate Authority	Product Name	Client	Server
ABC Certificates	ABC	Yes	No
Certificates "R" Us	DEF	Yes	No

Certificates “R” Us	GHI	No	Yes
Secure IT	JKL	No	Yes

2.3 Client Authentication

Servers must authenticate a client using the clients X.509v3 certificate. When establishing an SSLv3.0 session, the server shall request the clients certificate by issuing an SSLv3.0 `CertificateRequest` message to the client, per the SSLv3.0 specification (see Appendix B). In the event that a client attempts to establish a non-secure (i.e., port 80) HTTP session with the server (accept for “server.htm” file – section 2.6), the server must respond with an HTTP 403.4 error indicating that SSL is required.

The server must also perform the following certificate validation:

1. The certificate provided by the client must have had its subject and issuing Certificate Authority registered in the NERC Registry as detailed in section 2.8
2. In the event the client’s certificate subject “CN” field is an IP address or host name, the server must verify that the client has initiated communications from the specified IP address or host.
3. The server must validate all certificates it receives by verifying the Certificate Authorities signature within them.
4. The server must check the validity period for all certificate, including the “not before” and “not after” times.

If any of these checks fail, the client shall not be permitted access and the server must return an HTTP 403 Forbidden.

The server shall also make a reasonable effort to check the current revocation status of any certificates before accepting them. This may be accomplished using a published Certificate Revocation List (CRL) and/or the Online Certificate Status Protocol (OCSP), provided by the Certificate Authority that signed the client certificate. If the certificate is determined to be revoked, suspended, or invalid, the server must cease communications with the client and return an HTTP 403 Forbidden. If a valid CRL cannot be obtained or an OCSP server contacted for more than 36 hours, the server must also cease communications with the client and return an HTTP 403 Forbidden, unless officially directed otherwise by NERC.

Until the authentication failure is resolved, If the client attempts to continue to establish SSLv3.0 sessions, the server shall block the client from attempting further connections and notify NERC and the associated Security Officer (SO) of the PSE/CA/TP, via the phone number(s) or e-mail address contained in the NERC registry (see section 2.8).

2.4 Server Authentication

Clients shall only attempt to establish SSLv3.0 sessions and exchange production data with servers identified in the NERC Registry (see section2.8). Clients may establish SSLv3.0 sessions for testing purposes with other servers provided that only non-sensitive data is excha nged and the intent is made clear. The client must also perform the following certificate validation:

1. The host that communications has been established with must match the IP address or host name identified in the “CN” field of the certificate’s subject.
2. The client must validate Certificate Authorities signature within the server’s certificate.
3. The client must check the validity period of the server’s certificate, including the “not before” and “not after” times.

Failing any of these checks, the client must cease communications and notify NERC.

The client shall also make a reasonable effort to check the current revocation status of the server’s certificate. This may be accomplished using a published Certificate Revocation List (CRL) and/or the Online Certificate Status Protocol (OCSP), provided by the Certificate Authority that signed the client certificate. If the certificate is determined to be revoked, suspended or invalid, the client must cease communications. If a valid CRL cannot be obtained or an OCSP server contacted for more than 36 hours, the client must also cease communications with the server, unless officially directed otherwise by NERC.

2.5 Authorization

Assuming a client has been authenticated as described in section 2.3, the server shall authorize the client to perform only those operations allowed by the type of entity (PSE/CA/TP) they have been authenticated as and the security categories that the Security Officer (SO) has authorized the certificate to perform (see section 2.8). The type of client shall be determined by cross-referencing the client’s certificate subject with the NERC Registry. See the appropriate application specification (OASIS, E-Tag, etc.) for further information.

It is still reasonable and acceptable, depending on the application and environment, that the client’s company may not be recognized as a customer or valid entity by an organization. If so, the client may not be authorized to perform certain functions. Which companies and organizations a market participant chooses to recognize as a customer is under their control and discretion.

2.6 Firewalls, IP Security, and Server.htm

All Servers shall be placed behind a firewall. The firewall shall allow clients to access the server on port 443, the standard SSLv3.0 port. Client access to the server on IP ports other than 443 shall be restricted, except for a single HTML file on port 80. This HTML file shall be located at the root of the server and have a file name of "server.htm." This file shall allow anonymous access and contain the following information:

1. Server's host name
2. One or more administrative contacts including a 24 hour administrative contact (phone, fax, e-mail, pager)
3. Date/Time of the NERC Registry currently loaded.

Any unsecured links from "server.htm" shall only reference other sections of the file (server.htm) or files/resources on other servers. If images (gif and/or jpg) are included in this file, they should be served from a different server. Other html files and resources may be served from the server, and consequently reference in the "server.htm" file, as long as they are accessed via IP port 443 using SSLv3.0 and the client is authenticated using their certificate.

Since the firewall shall allow only IP ports 443 and 80, ICMP messages shall not be supported inbound, such as ping and trace-route. Outbound ICMP messages may still be performed. The html file located at "http://hostname:80/server.htm" , where "hostname" is the host name of the server in the NERC Registry, may be used to verify connectivity. As a substitute for ping, an HTTP TRACE on port 80 may also be performed to verify connectivity. Attempts to access the server on ports other than 443 and 80 shall be logged and include the date/time and IP address of the system attempting access. Firewall logs shall be kept for a minimum of 30 days after which they may be purged.

2.7 Logging

In addition to logs generated by the Firewall, the server shall log the following information for all messages/requests exchanged between the client and server (server may log additional information at its discretion):

1. Date and time to the millisecond that the server received the message/request.
2. Client's certificate full subject.
3. IP address of the client.
4. Success/Failure of the operation (http status codes)
5. Target URL of the client's message/request.
6. Content of the client's message/request for any action that involves the creation of modification of data on the server. This is not necessary for query only operations.

This data must be maintained for a minimum of three (3) months and available upon request by NERC.

2.8 NERC Registry and Access Control

Each valid and NERC authenticated market participant (PSE/CA/TP/Vendor) must establish a primary and backup Security Office (SO). Each SO must provide one or more phone numbers, one of which must be reachable 24x7, and at least one e-mail address. The SO shall be responsible for all modifications to data contained in the NERC registry for their company, including which client certificates and servers are authorized to perform specific market functions.

2.8.1 Physical, Procedural, and Personnel Security Controls

Given the critical nature of the registry and access control information that it contains, NERC must ensure a high degree of physical, procedural, and personnel security controls are in place for all systems and individuals involved in the maintenance and operations of the registry. In order for the industry to trust and rely the validity and accuracy of the registry, these types of control are necessary.

It is expected that NERC or a separate Registry Task Force will formalize and finalize the requirements and implementation details of the registry and that it will comply with the general set of requirements defined in this document.

2.8.1.1 Physical

NERC shall implement appropriate physical security controls to restrict access to the hardware and software (including servers, workstations, databases and any external cryptographic hardware modules, certificates, and tokens) used in conjunctions with the registry and access control information. Access to such hardware and software shall be limited to those personnel performing in a Trusted Role as described in Section 2.8.1.2.

2.8.1.2 Procedural and Personnel

NERC must ensure the following procedural and personnel controls are implemented and followed:

1. A separation of duties for critical registry functions to prevent one person from maliciously using the system without detection
2. Reasonable procedures and practices are in place to ensure that one person acting alone cannot circumvent safeguards.
3. All personnel involved in the maintenance or operation of the registry have their identity verified.
4. When accessing the system across a shared network, communications must be secured and authenticated.

5. 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.

These procedure and personnel controls shall apply to NERC employees and all contractors and subcontracts that may be involved in the maintenance or operation of the registry.

2.8.2 Access Control Modifications

Requests by a Security Officer (SO) to modify the registry shall ONLY be communicated to NERC by an authorized SO via out-of-band methods or by submittal of an authenticated message (secure e -mail or SSL). Acceptable out-of-band methods include:

1. Phone. NERC must call the SO back at their registered phone number and challenge the SO with a previously established pass-phrase.
2. In person. SO must provide two authenticating credentials such as a valid drivers license and a company ID.

2.8.3 Access Control List

The registry shall contain the following security categories for each market participant:

1. **Tag:** Produce, process, or approve tags.
2. **Schedule:** Produce, process, or approve schedules for energy or transmission.
3. **Transmission**: Reserve Transmission Capacity and participate in secondary markets.
4. **Energy**: Participation in other energy markets.
5. **Admin**: Administer other non-security and access control related attributes within the NERC Registry, such as POR/POD registrations and the like.
6. **Other:** As required or defined by NERC

In addition to other data currently required in the NERC Registry, all market participants and nodes, via their Security Officer, must register with NERC the following information:

1. For each server function being performed in the security categories above, one or more fully qualified server host names and the CA providing the server's certificate. If a service provider is being used, it must also be identified.
2. One or more client certificate subjects, their associated Certificate Authorities, and for which security categories they are authorized for (Tag,

Schedule, Transmission, etc.). This is only appropriate or necessary when acting as a client. The certificate subject's "OU" and "O" fields must also match those of the market participant.

For any single certificate, the Security Officer (SO) must also be able to globally perform the following functions:

1. Enable and disable it across all security categories and roles - as in the case when an employee is transferred, takes vacation, leaves the organization, or a certificate has been compromised - by setting an EXECUTE attribute to either "Y" or "N".
2. Provide an effective period during which the certificate may be used by supplying an effective from and to date.

Both a client certificate and a server may be associated with more than one security category or server function. In the case of a service provider, it is acceptable for the same server to provide services for more than one PSE/CA/TP or market participant. In this case, the same fully qualified host name and the CA providing the server's certificate will be provided by each PSE/CA/TP and the server may utilize the same server certificate.

In combination with the type of market participant the company or organization happens to be (TP, CA, PSE, etc.), which is also contained in the registry, certain functions and roles may be unavailable.

2.8.4 Publication

NERC shall publish the full registry as a coordinated set of three files:

1. The registry itself - preferably formatted as an XML document.
2. An SHA-1/RSA digital signature (see section 4) of the registry, signed using a valid client certificate obtained by NERC from one of the approved Certificate Authorities.
3. The NERC certificate used to create the SHA-1/RSA digital signature.

The registry, signature, and signing certificate shall be published in an SSL secured HTTP or LDAP server. Before relying on the registry obtained from NERC, both clients and servers must verify the signature on the signed registry file and the validity of the certificate used to sign the registry. In the case of an SSL secured LDAP or HTTP server, the same checks as described in section 2.4 shall be used.

In the event the signature on the file or the certificate is found to be invalid or the authentication check of the LDAP or HTTP server fails, NERC shall be notified immediately and the last known valid registry shall continue to be used.

3 Appendix A: Resources

3.1 Specifications and RFC

Secure Sockets Layer (version 3.0)	http://www.netscape.com/eng/ssl3/
Transport Layer Security (RFC 2246)	http://www.ietf.org/rfc/rfc2246.txt
Key words use (RFC 2119)	http://www.ietf.org/rfc/rfc2119.txt
X.509v3 Certificate and CRL Profile (RFC 2459)	http://www.ietf.org/rfc/rfc2459.txt

3.2 SSL/TLS Toolkits

COMPANY	DESCRIPTION	URL
RSA Security	SSL/TLS/PKI toolkits - Java and C++	http://www.rsasecurity.com/products/bsafe/index.html
Baltimore	SSL/TLS/PKI toolkits - Java and C++	http://keytools.baltimore.com/ssl/index.html
DART	SSL/TLS toolkit – ActiveX/COM	http://www.dart.com/powertcp/
PHAOS Technology	SSL/TLS toolkit – Java	http://www.phaos.com/e_security/prod_ssl.html
Sun Microsystems	SSL/TLS toolkit – Java	http://java.sun.com/products/jsse/
OpenSSL	Open Source SSL/TLS toolkit – C++	http://www.openssl.org/
PureTLS	Open Source SSL/TLS toolkit – Java	http://www.rtfm.com/puretls/
Certicom	SSL/TLS tookit – Java and C	http://www.certicom.com/
IBM	PKIX Reference Implementation	http://www-3.ibm.com/security/library/wp_pkix.shtml
Mozilla.org	Cryptographic libraries	http://www.mozilla.org/projects/security/pki/psm/

3.3 Hardware and Inline Accelerators

COMPANY	DESCRIPTION	URL
Rainbow	CryptoSwift: PCI and Inline Accelerators	http://www.rainbow.com/
nCipher	nFast: PCI Accelerator	http://www.ncipher.com/

Intel	NetStructure: Inline Accelerator	http://www.intel.com/netstructure/ecommerce_equipment.htm
F5	E-Commerce Controller: Inline Accelerator	http://www.f5.com/

3.4 General Links and Books

LINKS	
PKI related links and resources	http://www.pki-page.org/
Encryption and Security-related Resources	http://www.cs.auckland.ac.nz/~pgut001/links.html
Introduction to SSL	http://developer.netscape.com/docs/manuals/security/sslin/contents.htm
PKI Forum	http://www.pkiforum.org/
PKI Guru	http://www.pkiguru.com/

BOOKS		
Title	Author	ISBN
SSL and TLS Essentials	Stephen Thomas	0-471-38354-6
SSL and TLS, Designing and Building Secure Systems	Eric Rescorla	0-201-61598-3
Internet Cryptography	Richard E. Smith	0-201-92480-3
Digital Certificates, Applied Internet Security	Jalal Feghhi, Jalil Feghhi, Peter Williams	0-201-30980-7

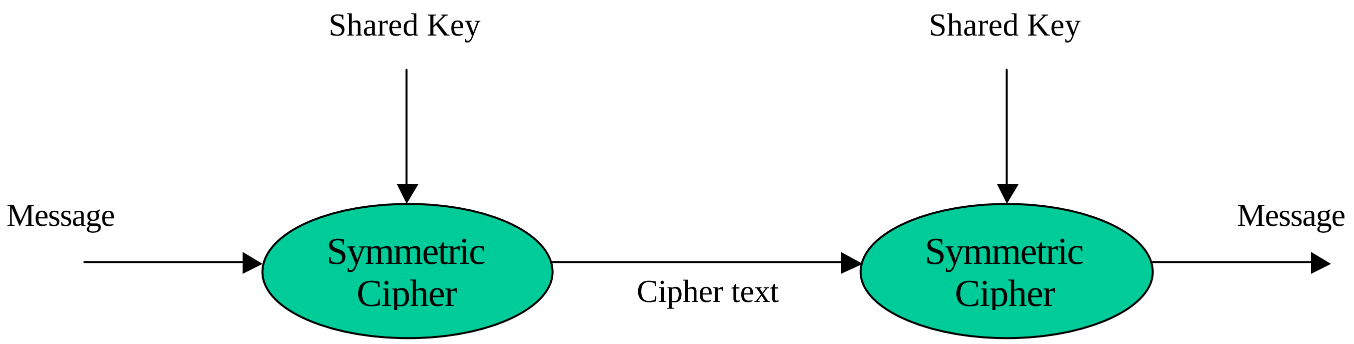
4 Appendix B: Cryptography and SSLv3.0 Overview

The books referenced in section 3 provide a complete description of public key infrastructures and the implementation of SSL and TLS. Below is a quick overview of how cryptographic algorithms, X.509v3 certificates and SSL/TLS work together.

4.1 Cryptographic Algorithms

4.1.1 Symetric Encryption

Secret Key Cryptography is commonly referred to as "**symmetric encryption.**" When utilizing symmetric cipher, both sender and receiver have the "shared key" and it is used for both encryption and decryption.



Common symmetric key ciphers:

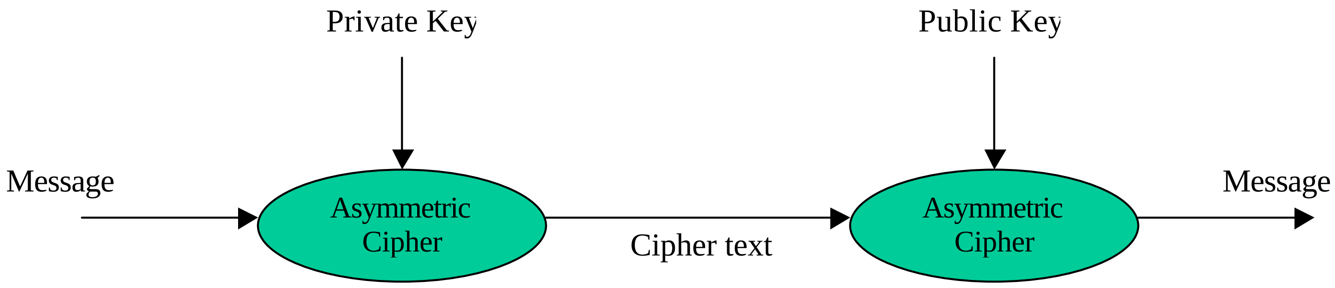
•**DES**: Data Encryption Standard (56 bit block cipher)
•**3DES**: Triple-Strengths Data Encryption Standard (112 bit block cipher)
•**RC2**: Rivest Cipher 2 (variable key length block cipher)
•**RC4**: Rivest Cipher 4 (variable key length stream cipher)

Note1: **RC4** is extremely fast; a Pentium II/400 can achieve speeds on the order of 45 MB/s. **RC2** and **3DES**, however, are many times slower.

Note2: The US National Institute of Standards and Technology (NIST) has selected the Advanced Encryption Standard (AES) to replace DES as the US government's standard encryption algorithm.

4.1.2 Asymetric Encryption

Public Key Cryptography is commonly referred to as "**asymmetric cryptography**." The two primary uses of public key cryptography are **key establishment** (section 4.4) and **digital signatures** (section 4.3). When utilizing an asymmetric cipher, messages are encrypted by one of the key pairs and decrypted with the other.



In the example above, the private key is closely guarded by the sender and never shared. The receiver only knows the public key that corresponds to the private key used to encrypt the message. Alternatively, a message may be encrypted using a public key and may then only be decrypted by the private key.

Common Asymmetric key ciphers/algorithms:

•**DSA/DSS**: Digital Signature Algorithm (type: Digital Signature)
•**El Gamal**: (type: Digital Signature)
•**RSA**: Rivest, Shamir, Adleman (type: Signature, encryptions, key exchange)
•**Diffie-Hellman**: (type: Key exchange)

4.2 Hashing and Digesting

A **Message-digest algorithm** take a variable-length message as input and produces a fixed-length digest as output. The fixed length output is called the "**message-digest**", "the **digest**" or a "**hash**." The algorithms are also referred to as a "**one-way hash algorithm**" or simply a "**hash algorithm**." A message digest algorithm must satisfy four properties:

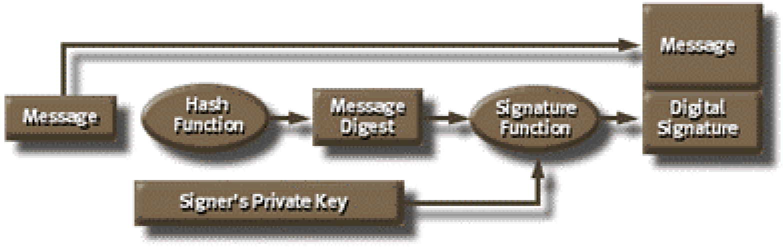
1. In must not be feasible to determine the input message based on its digest.
2. In must not be possible to find an arbitrary message that has a particular, desired digest.
3. Should be computationally infeasible to find two messages that have the same digest.
4. Mappings from a message to a digest should appear random and flipping even one bit of the message results in an entirely new and uncorrelated digest.

Message -Digest Algorithm	Digest Length (bits)
MD2	128
MD4	128
MD5	128
SHA	160
SHA-1	160

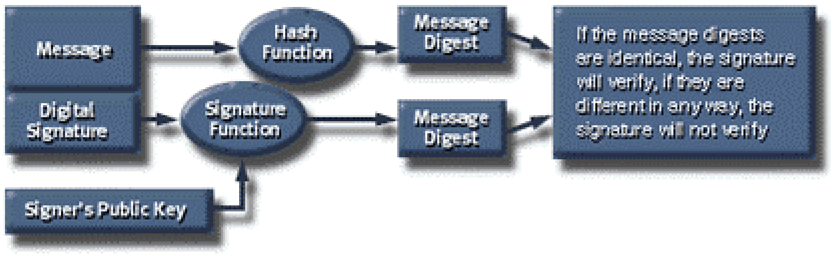
Note: MD5 and SHA-1 are newer algorithms and generally used by SSL and TLS. MD5 has an approximate 2 to 1 speed advantage over SHA-1, but MD5 is slowly being phased out.

4.3 Digital Signatures

In order to sign a message, the message originator creates a message digest and signs (encrypts) the digest with their private key. The original message and the signed hash are then sent to the recipient(s).



Recipient(s) uses the same hash function on the message as the signer. Recipient(s) then uses the signer's public key to decrypt the message digest the originator signed. If the message digests are identical, the signature will verify and one can safely assume the message came from the signer and has not been altered or counterfeited.



If the message digests are identical, the signature will verify, if they are different in any way, the signature will not verify

Note: Currently **RSA** and **DSS** are commonly used to create digital signatures. DSS was invented by the NSA (FIPS-186) and uses the SHA-1 digest algorithm. RSA, however, may use any digest, such as MD5.

4.4 Key Establishment

Two types of key establishment exist, *key exchange (*also known as a *key transport)* and *key agreement*. In the case of key exchange, one side generates a symmetric key, encrypts it using a public key of the other side, and then sends it to the other side. In *key agreement*, both sides cooperate to generate a shared key.

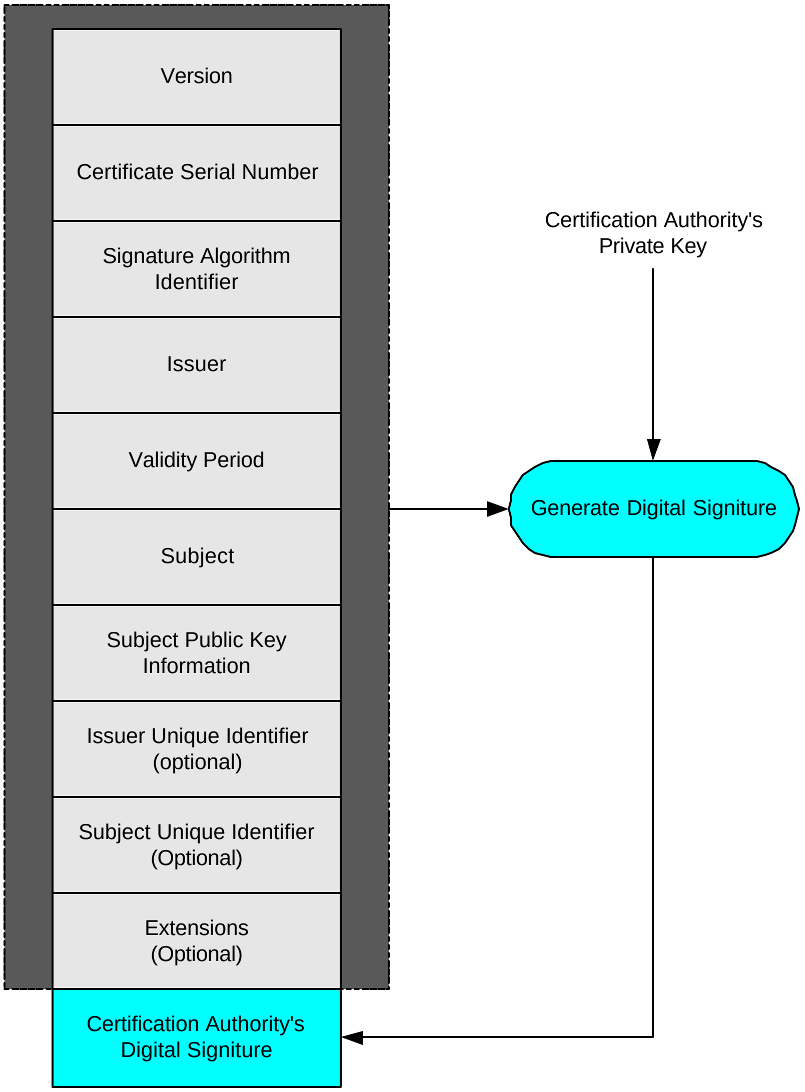
Cryptographic Algorithms supporting Key Establishment:

- **RSA**: (Rivest, Shamir, Adelman) Supports *key exchange*.
- **DH**: (Diffie-Hellman) Supports *key agreement*.

4.5 Digital Certificates

Certificates are electronic documents that correlate (called binding) a public key with a specific entity. Commonly this entity is a person but may be a computer, software, document, etc. Certificates may be used to authenticate persons in a SSL session, to encrypt messages or digitally sign messages. Digital Certificates contain, among other things, the following information:

- **Version:** Contains the version number of the encoded certificate (currently 1, 2, or 3).
- **Serial Number:** A unique number assigned by the CA
- **Signature Algorithm:** Algorithm used by the CA to digitally sign the certificate (RSA or DSA)
- **Issuer Name:** The CA who has signed the certificate
- **Validity Period:** Time interval during which the certificate is valid.
- **Subject Name:** This is the identity of the entity whose public key is certified in the public key. Sometime called a Distinguished Name (DN).
- **Subject Public Key Information:** Contains public key and parameters.
- **Issuer unique identifier:** Optional field to allow the reuse of issuer names over time.
- **Subject unique identifier:** Optional field to allow the reuse of the subject name over time.
- **Extensions:** Way to associate additional information for subjects, public keys, etc.


Version
Certificate Serial Number
Signature Algorithm Identifier
Issuer
Validity Period
Subject
Subject Public Key Information
Issuer Unique Identifier (optional)
Subject Unique Identifier (Optional)
Extensions (Optional)
Certification Authority's Digital Signiture
Certification Authority's Private Key
Generate Digital Signiture

X.509 v3 Certificate Format

By signing a certificate, a Certificate Authority if acting as a trusted third-party and certifying that the contents of the certificate are verifiably correct.

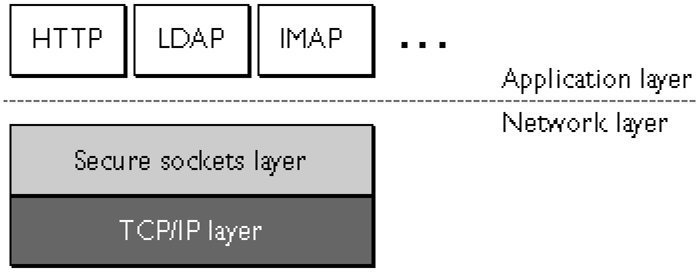
4.6 Certificate Authorities (CA)

Typically a CA verifies the credentials of entities seeking certificates, issue them, and then make these certificates available in some common database (usually a directory.) CAs must be trusted in order for their certificates to be meaningful. A very large PKI may also include an RA, or Registration Authority, or even a LRA or Local Registration Authority that does actual physical verification.

A CRL is a Certificate Revocation List. CRLs are regularly created, signed, and published by CAs in order to list certificates that have been compromised or revoked prior to the certificates expiration date. A CA may also provide a server or system that may be queried using the Online Certificate Status Protocol (OCSP). This type of service provides for real-time certificate status checking. Most CRLs are published only once or twice a day.

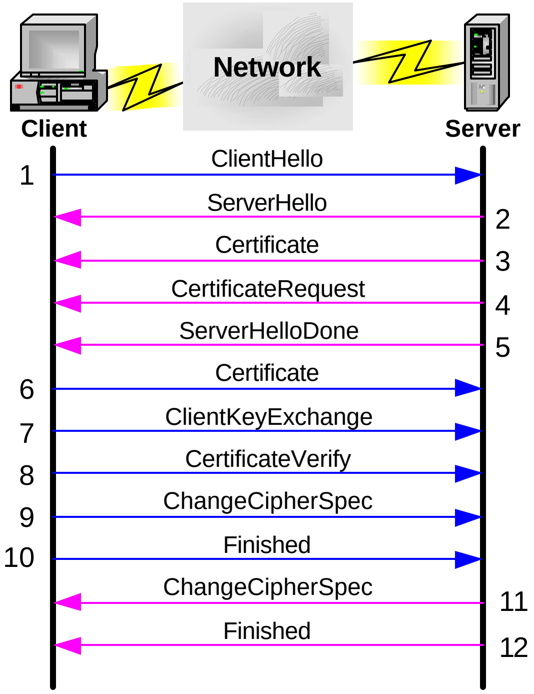
4.7 Secure Sockets Layer (SSL/TLS)

SSLv3 (version 3) is functionally a security protocol that fits between the application layer and TCP. As such, it can secure many different application layer protocols such as HTTP, FTP, Telnet, etc.



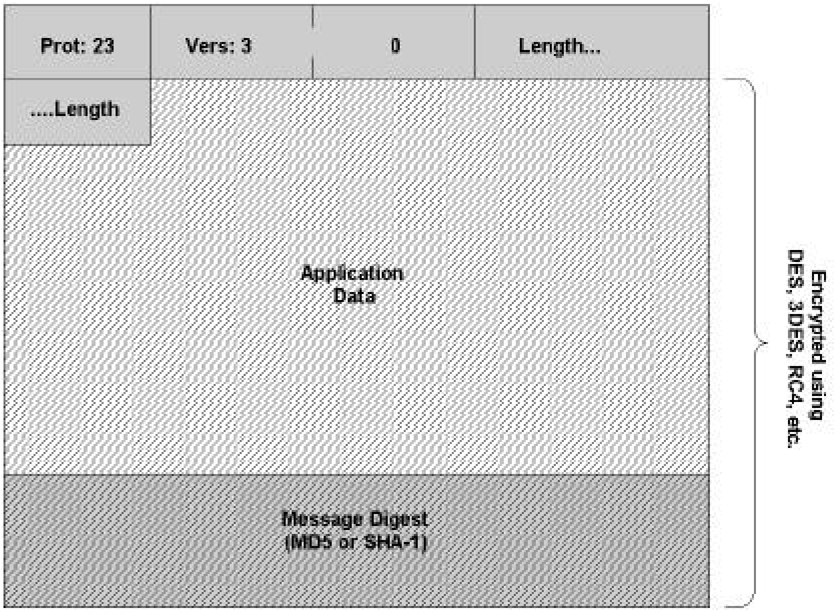
Originally developed by Netscape, the protocol was eventually turned over to the Internet Engineering Task Force (IETF). In January 1999, the Transport Layer Security (TLS) protocol was published by the IETF (RFC 2246). The Transport Layer Security protocol (TLS) is the successor to SSLv3. It should be considered the next version of SSL and is currently at version 1.0. Inside the TLS/SSL hello message, an SSLv3 session is identified as version 3.0 and a TLS session is identified as version 3.1.

In SSL and TLS, there is always a "client" role and a "server" role. The message protocol when both client and server authentication are enforced is as follows:



- **Step 1**: Client sends **ClientHello** message proposing SSL options such as version and cipher algorithms supported.
- **Step 2**: Server responds with a **ServerHello** message selecting the SSL options to use.
- **Step 3**: Server sends its public key certificate in the **Certificate** Message
- **Step 4**: Server sends a **CertificateRequest** message to indicate that it wants to authenticate the client.
- **Step 5**: Server concludes its part of the negotiation with a **ServerHelloDone** message.
- **Step 6**: Client sends its public key certificate in a **Certificate** message.
- **Step 7**: Client sends session key information (encrypted with the servers public key) in a **ClientKeyExchange** message.
- **Step 8**: Client sends **CertificateVerify** message, which signs important information about the session using the client's private key; the server uses the public key from the client's certificate to verify the client's identity.
- **Step 9**: Client sends a **ChangeCipherSpec** message to activate the negotiated options for all future message it (the client) will send.
- **Step 10**: Client sends a **Finished** message to let the server check the newly activated options.
- **Step 11**: Server sends a **ChangeCipherSpec** message to activate the negotiated options for all future messages it (the server) will send.
- **Step 12**: Server sends a **Finished** message to let the client check the newly activated options.
- SSL is now ready for the application to use as an authenticated, high integrity, secure and private communications channel.

An SSL message:


Prot: 23
Vers: 3
0
Length...
....Length
Application Data
Message Digest (MD5 or SHA-1)
Encrypted using DES, 3DES, RC4, etc.