Joint Interchange Scheduling Working Group

PKI Certificate Standards for Electronic Scheduling and e-Tagging

Draft Electronic Certificate Standards

Revision History

Date	Version	Description	Author
08/19/2005	0.1	Initial Version	Jim Hansen
12/27/2005	0.2	Added scope; added certificate expiration duration; tweaked CRL parameters for validity and publishing periods	ISO New England
01/19/2006	0.3	Incorporated feedback from ITC members	ISO/RTO Council Information Technology Committee
1/23/2006	0.4	Final edits	ISO/RTO Council Information Technology Committee

Table of Contents

1 NAESB PKI PROGRAM OVERVIEW

Insert PKI Standards Overview, Certificate User Checklist, and Certificate Authority Checklist.

PKI Standards

E.g. You must select a certified certificate Authority. You must use a certificate that has been certified. Must execute User Certificate Declaration.

[QUESTION: The above paragraph seems to indicate that "certified" certificates must be used. Why do individual certificates need to be certified? What is the process to have a certificate certified? It should be sufficient to simply acquire a digital certificate from certified CA.]

Certificate User Declaration

Insert section 3 of this document and verbiage describing the company's agreement to be legally bound by transactions involving their certificate. Note: This does not preclude individual companies from establishing mutually agreeable terms to govern legally binding transactions executed using their digital certificates.

CA Checklist

Insert section 2 of this document.

Technical Standards will stand alone.

This document describes the requirements that Certificate Authorities must meet in order to display the NAESB Certification Mark on their web site or to claim that their Certificate meets NAESB standards. This document also describes the minimum characteristics that a Certificate must meet in order to achieve compliance with NAESB standards.

A trusted network of Certificate Authorities is one of the key ingredients needed for secure Internet data transfer. Other capabilities, which are not addressed by this standard, such as reliable message delivery standards, are also needed. NAESB provides assurance to Energy Industry Participants that a Certificate Authority complies with the minimum set of standards described in this document. This is necessary in order to provide for a minimum level of security for the exchange of data across the public Internet. Examples include the exchange of e-Tag data, OASIS data, Electric Industry Data Exchange (EIDE), etc.

These standards are taken, in part, from the NERC e-MARC Certificate Policy for the Energy Market Access and Reliability Certificate Program. Compliance with the e-MARC standard exceeds the requirements described herein. The standards described in this document achieve the level of security commonly used by other industries engaged in commercial activity across the public Internet.

NOTE: The NERC e-MARC proposal was rejected by NERC' PKI Steering Committee due to fatal flaws in the proposed approach and, therefore, failed to achieve standard status. Please remove all references to "standard" when referring to e-MARC. Also, it is recommended that the NERC PKI Steering Committee analysis and decision regarding the e-MARC proposal be included in the appendix of this document for reference.

1.1 Overview

NAESB standards call for the use of Public Key Infrastructure (PKI) using X.509v3 digital certificates to provide for specific security services:

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

NAESB standards ~~PKI~~ require~~s~~ that ~~electronic~~ digital ~~Certificates~~ X.509v3 certificates be ~~provided~~ issued to industry participants after a formal registration process has been completed. These Certificates are provided by Certificate Authorities (CAs). NAESB standards call for these CAs to meet certain minimum criteria as defined in this document and that the Certificate obtained by industry participants meet a certain minimum criteria in order to ensure that the participant's identity is tied to the Certificate and has been verified by the CA. The issuing CA must meet these standards in order for the Certificate to be considered compliant with NAESB standards.

1.2 Certification

Upon achieving NAESB certification, NAESB will update the NERC registry ~~to register the CA along~~ with the appropriate CA object identifiers. The CA will immediately be authorized to display the NAESB certification mark and will be authorized to claim compliance with NAESB Electronic Certificate Standards.

NAESB may rescind a CA's certification for cause at any time by providing 30 days notice in writing to the CA. CA's that receive a rescission notice from NAESB are required to notify all affected certificate holders within 5 days that their NAESB certification has been rescinded and their certificates will no longer be valid.

CA's must be recertified by NAESB upon any of the following events:

- Purchase, Sale of Merger of the CA by another entity
- Every 5 years

1.3 Scope

The standards described in this document are applicable only to the exchange of e-Tag and OASIS data passed between separate legal entities. These standards shall not be used for any other purpose.

1.4 Commitment to Open Standards

The recommendations contained in this document should align with industry best practices for Public Key Infrastructure as prescribed by the National Institute of Standards and Technology in publication NIST 800-32, Internet Engineering Task Force PKI guidelines and standards (e.g. RFC 3280, 2510, 4210, 3647, and any successor standards etc.) and other broadly accepted/adopted standards from internationally recognized standards bodies.

NAESB's long-standing support for open standards has served to create a competitive marketplace of interoperable E-commerce products to serve the Energy industry. As with other NAESB standards initiatives, this standard is being developed to ensure the availability of interoperable PKI products from multiple vendors. NAESB encourages Certificate Authorities to pursue certification under this standard to meet Energy industry needs for PKI.

2 Certificate Authority Certification Requirements

2.1 NAESB/CA Agreement

Prior to NAESB consideration of a CA's request for certification, the CA must enter into a Certification Agreement with NAESB. A copy of this agreement may be obtained at the NAESB web site http://www.naesb.org.

2.2 Certificate Policy and Certification Practice Statement

The CA must document the specific practices and procedures followed to satisfy the requirements of this standard in a set of Certificate Policy and Certification Practice Statement documents. These~~is~~ documents must be posted on the CA's web site.

2.3 Minimum Certification Standards

This section describes the minimum standards that the CA must achieve in order to meet the requirements for NAESB certification.

2.3.1 Repositories and Revocation

The CA shall be responsible for providing repository functions that are available to all Subscribers and Relying Parties. Repositories should contain the most current certificates and certificate revocation lists (CRLs). Upon revocation of a Certificate issued by the CA, the appropriate CRL must be updated as soon as possible but no longer ~~within~~ than 120 minutes from the time certificate revocation was completed. Write access to the repository should be limited to the CA and any other authorized systems or personnel.

2.3.1.1 Circumstances for Revocation ~~(e-MARC 4.4.2)~~

2.3.1.1.1 Permissive Revocation ~~(e-MARC 4.4.2.1)~~

A Subscriber may request revocation of his/her ~~e-MARC~~Certificate at any time for any reason. A Sponsoring Organization may request revocation of a~~n e-MARC~~ Certificate issued to its Business Representative (or device or individual) at any time for any reason.

2.3.1.1.2 Required Revocation ~~(e-MARC 4.4.2.2)~~

An Authorized CA, Subscriber, Sponsoring Organization (where applicable), or Local Registration Authority (LRA) is responsible for promptly requesting revocation of a Certificate under at least the following circumstances:

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

2.3.1.2 CRL Issuance Frequency

The CA must publish their CRL at minimum~~least~~ every twelve hours and, as soon as possible (but no greater than two hours) after a change or modification, including the revocation of a certificate ~~within four hours of modification~~. The validity period of a CRL ~~shall~~ should not exceed ~~24~~ 96 hours. The CA must provide their CRL at multiple locations for access by Relying Parties. Relying Parties must consult the latest version of the CRL prior to establishing connections.

2.3.1.3 Publication of Certificate Information

The CA must publish the Certificates it issues and publish notice of revocation of Certificates in its repository. If available, the CA shall provide OCSP services (Online Certificate Status Protocol). The CRL shall be made available for download to a local CRL server at the relying party's site at the option of the relying party.

The CA must publish its Certificate Policy, Certificate Practice Statement, Subscriber Agreements and Relying Party Agreements on its web site.

2.3.1.4 Access Controls

The repository containing information published by the CA must be restricted to use by parties that have authorized access to the data. The CA must grant relying parties with read only access to the CRLs and Certificate information to companies that have registered with and/or entered into an agreement with the CA. The CA must verify the identity of these companies.

2.3.2 Registration, Verification and Authentication Process

For a Certificate to be considered "NAESB" compliant, the CA or one of its trusted Registration Authorities (RA) must verify and authenticate the identity of the applicant for ~~the~~ a Certificate. This authentication must be based on the personal (physical) presence of the Certificate applicant before an agent of the CA or, before a notary public or other official with comparable authority within the Certificate applicant's jurisdiction. The agent, notary or other official must ~~check~~ validate the identity~~fy~~ of the Certificate applicant against a well-recognized form of government-issued photographic identification such as a passport or driver's license and one other form of identification ~~credential~~.

An applicant for a digital certificate may give authorization to an "agent" entity to acquire a digital certificate on behalf of the applicant. In such cases the agent must present proper authorization from the applicant, as indicated above. Any agent with the proper authority to act on behalf of an applicant shall be viewed as a legal representative of the applicant by the CA.

The CA or one of its trusted RAs must also verify and authenticate the applicant organization and confirm that the applicant is employed by, or a duly authorized agent of, the organization and that the applicant has the permission of the organization to request the Certificate.

The CA or one of its trusted RAs must verify the organization identity as well. The application for a Certificate must include the Organizational (O=) attribute within the Subject name field that must correspond with the legal name of the organization. The application must also include the domain name of the applicant organization in the Common Name (CN=) attribute within the Subject name field. The CA or one of its trusted RAs must confirm that the organization exists by using at least one third party identify proofing service or database. Alternatively, the CA or one of its trusted RAs may use organizational documentation issued by or filed with the applicable government agency or competent authority that confirms the existence of the organization.

The Subscriber must agree to the terms and conditions implemented by the CP and CPS before receiving or utilizing their certificates.

2.3.3 Name Uniqueness

The CA must enforce name uniqueness for a subscriber among the Subject Distinguished Names within the CA's name space. The subscriber may have multiple Certificates that use the same DN.

2.3.4 Private Key Proof of Possession ~~of Private Key~~

The CA must require the Certificate applicant to prove that they rightfully hold the private key corresponding to the public key to be listed in the Certificate. ~~The method to prove possession must be PKCS #10 or another cryptographically equivalent demonstration.~~ When a subscriber generates their own private key they must prove possession of the private key by providing a standard, signed request to the CA or one of its trusted RA's.

2.3.5 Identification and Authentication for Re-key Requests

The CA must verify that the person or organization requesting a re-key (issuance of a new private/public key pair) is the ~~subscriber~~ Subscriber of the Certificate. If the contact information and Certificate information has not changed, then the requirements for authentication for re-key are not as stringent as those required for original Certificate application. At a minimum, the CA must verify an individual's identity through a signed request that binds the request to an existing, valid certificate, a password or some other information that would be known only by the subscriber.

~~At least~~ Minimally once every four years~~,~~ and after revocation or expiration, subscriber information must be re-verified as described in section 2.3.2 above.

2.3.6 Identification and Authentication for Revocation Requests

The CA or one of its trusted RAs must verify that the person or organization requesting a revocation is the ~~s~~Subscriber ~~person~~ or a duly authorized representative of the Sponsoring ~~o~~Organization for that Certificate. If the requestor is the subscriber, then at a minimum, the CA or one of its trusted RAs must verify an individual's identity through a password or some other information that would be known only by the subscriber and the party issuing the password. The CA or one of its trusted RAs may alternatively authenticate the requestor on the basis of a digital signature using the Certificate's associated key pair. Other verifiable means are allowed ~~as well~~ such as in person requests with photo identification, signed and notarized mail, etc.

If the requestor is another individual from the Ssubscriber's organization, then the CA or one of its trusted RAs must authenticate the requestor using methods described in section 2.3.2 above or, by authenticating on the basis of a digital signature using the Certificate's associated key pair. If the requestor is from the Sponsoring Organization, identity validation must be performed in accordance with section 2.3.2 above.

2.3.7 Disaster Recovery

The 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. The CA must have a working, tested, disaster recovery plan. This disaster recovery plan must provide for restoration of service after complete loss of all resources at the CA's primary site. Data stored off-site for disaster recovery and/or backup purposes must be protected from unauthorized access.

2.3.8 Facility, Management, and Operational Controls

2.3.8.1 Physical Controls

The CA 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 2.3.9.

2.3.8.2 Site Location and Construction

CA operations must reside within physically protected environments that deter, prevent, and detect unauthorized use of, access to, destruction of, or disclosure of sensitive information and systems.

2.3.8.3 Physical Access Controls

Physical access to the 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.

2.3.8.4 Audit Logs

Audit logs should be maintained to detail pertinent system and application events that occur on the CA system. These logs should be maintained for a sufficient amount of time such that any discrepancies can be reviewed at a later time. Access to audit logs must be restricted to authorized personnel only.

~~2.3.8.4~~2.3.8.5 Offsite Media Storage

All media containing sensitive information that is taken offsite must be transported and stored in a secure manner. The offsite storage facility must have appropriate physical access controls to grant or restrict access consistent with onsite access controls.

2.3.8.6 Data Retention

All data pertinent to the CA must be retained for a reasonable amount of time, and access should be limited to authorized personnel. All archived information must be validated within a reasonable amount of time.

~~2.3.8.5~~2.3.8.7 Waste Disposal

All media containing sensitive information must be disposed of in a manner that ensures the sensitive information cannot be read. Acceptable methods include shredding documents, overwriting storage devices with all ones or zeros in multiple passes, and rendering storage devices unreadable.

2.3.9 Procedural Controls

2.3.9.1 Trusted Roles

The CA shall identify roles of trusted individuals and identify the level of access appropriate for each role and area of responsibility. The CA shall provide reasonable assurance of the trustworthiness, competence, and integrity of employees filling trusted roles. The CA shall verify the identity and background of these individuals.

2.3.9.2 Training

The CA must provide the trusted individuals with sufficient training to ensure competence and compliance with the CA's security policies and operating procedures.

2.3.9.3 Revocation of Access

The CA must immediately revoke all access granted to a trusted individual when they leave the organization for any reason- or their job duties change in such a way that they no longer function in the trusted role.

2.3.10 Cyber Security Controls

The CA must have a Cyber Security Policy that covers the electronic security perimeter surrounding all Cyber Assets used for CA operations and every Cyber Asset within the perimeter. The CA must take reasonable precautions to secure the electronic security perimeter and to secure access to the cyber assets within the perimeter. The CA must disable all unused ports and services. External access through the security perimeter must require two-factor authentication. The CA must take reasonable precautions to ensure that cyber assets are not vulnerable to viruses, Trojan horse vulnerabilities, spyware, key loggers, or any other malicious software or hardware that could be used to intercept or compromise the sensitive information. The CA should ensure that the Cyber Security Policy is included in any formal or informal audits undertaken by the company.

3 Certificate Requirements

This section describes the requirements that a Certificate must meet in order to be considered as compliant with NAESB standards.

3.1 Certificate Standards

All certificates must comply with international standard X.509v3.

~~3.1~~3.2 Certificate Required Fields

The Certificate must include the NERC Entity Code of the organization or organizational unit represented by the applicant in the "OU" field. The "O" field must contain the Organization's legal name. The CN field must contain the domain name of the organization represented by the applicant.

~~3.2~~3.3 Certificate Duration

The standard expiration period for a certificate shall be no less than 12 months and no greater than 3 years. Certificates must be re-keyed (a new key pair must be generated and a new certificate provided to the subscriber) no less than every 3 years. ~~Certificates must be re-keyed (a new key pair must be generated by the CA and provided to the subscriber) at least every three years.~~

~~3.3~~3.4 Certificate Security

The subscriber organization must take reasonable security measures to protect the private key, passwords and/or challenge phrases, and potential misuse of their Certificate. The subscriber organization should create a Certificate policy that describes protocols and procedures for Certificate security and Certificate revocation. The subscriber organization may wish to re-key or revoke a Certificate when individuals with access to the private key change positions, retire, etc.

Backup and/or Archived copies of the Certificate including the private key should be stored and protected in a manner that ensures only the subscriber can use the backup copy.

~~3.4~~3.5 Key Length

Certificates meeting NAESB standards must contain public keys with a minimum length of ~~be~~ 1024 bitss ~~at minimum~~ (128 bit encryption). (QUESTION: There is no reference to 128 bit encryption in the X.509 standard, ISO/IEC 9594-8, please clarify the parenthetical reference above.) The digest algorithm must be an industry standard algorithm, (e.g. SHA-1 or MD5).

~~3.5~~3.6 Certificate Class

Certificates meeting NAESB standards must be of a class that requires authentication as described in section 2. A Verisign class 3 Certificate meets these criteria for example.

3.7 Authorized Certificate Use

Subscribers are permitted to utilize NAESB compliant certificates in manual and/or automated modes. Manual mode refers to all cases where an individual representing the Subscriber uses a digital certificate to digitally sign e-Tag and/or OASIS related messages. Automated mode refers to all cases where an unmanned machine owned and operated by the Subscriber, or its authorized Agent, uses a digital certificate to sign e-Tag and/or OASIS related messages. The digital certificate may also be used in other operations involving cryptographic functions (e.g. encryption, access control) strictly restricted to e-Tag and/or OASIS functions.