**1. RECOMMENDED ACTION: EFFECT OF EC VOTE TO ACCEPT RECOMMENDED ACTION:**

|  |  |  |  |
| --- | --- | --- | --- |
| X | Accept as requested | X | Change to Existing Practice |
|  | Accept as modified below |  | Status Quo |
|  | Decline |  |  |

**2. TYPE OF DEVELOPMENT/MAINTENANCE**

|  |  |  |  |
| --- | --- | --- | --- |
| **Per Request:** | | **Per Recommendation:** | |
|  | Initiation |  | Initiation |
| X | Modification | X | Modification |
|  | Interpretation |  | Interpretation |
|  | Withdrawal |  | Withdrawal |
|  |  |  |  |
|  | Principle |  | Principle |
|  | Definition |  | Definition |
| X | Business Practice Standard | X | Business Practice Standard |
|  | Document |  | Document |
|  | Data Element |  | Data Element |
|  | Code Value |  | Code Value |
|  | X12 Implementation Guide |  | X12 Implementation Guide |
|  | Business Process Documentation |  | Business Process Documentation |

**3. RECOMMENDATION**

**SUMMARY:**

This document provides the technology review and proposed upgrade for the NAESB WEQ PKI Standard (WEQ-012). This standard is intended to support and enable the NAESB Accreditation Requirements for Certification Authorities that was posted for formal comment on June 25, 2012

**Recommended Standards:**

**Public Key Infrastructure (PKI)**

**Introduction**

The NAESB WEQ has developed these Business Practice Standards WEQ-012 and the NAESB Accreditation Requirements for Certification Authorities to establish a secure PKI. Nothing in these Business Practice Standards WEQ-012 would preclude it from being adopted by other energy industry quadrants as appropriate. These Business Practice Standards WEQ-012 describe the requirements that Certification Authorities and End Entities must meet in order to claim the electronic Certificates issued by that certificate authority meets the NAESB Business Practice Standards WEQ-012. This document also describes the minimum requirements that an End Entity must meet in order to achieve compliance with the NAESB Business Practice Standards WEQ-012.

A trusted network of Certification Authorities is one of the key ingredients needed for secure Internet data transfers. NAESB WEQ provides assurance to energy industry participants that an Authorized Certification Authority complies with the minimum set of requirements described in the NAESB Business Practice Standards and Models Relating To Public Key Infrastructure (PKI) recommendation through the NAESB Certification Program. 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, EIDE, etc. Certification Authorities that comply with all provisions of the NAESB Business Practice Standards and Models Relating To Public Key Infrastructure (PKI) are termed Authorized Certification Authorities. Other capabilities, which are not addressed by these Business Practice Standards and Models Relating To Public Key Infrastructure (PKI), such as reliable message delivery standards, may also be needed and will be specified in separate Business Practice Standard(s).

In addition to the certification authority and Certificate provisions of the NAESB Business Practice Standards and Models Relating To Public Key Infrastructure (PKI), End Entities that wish to use the PKI established by this Business Practice Standards WEQ-012 must attest to their understanding of and compliance with their Authorized Certification Authority’s CP or Certification Practice Statements, and agree to be bound to electronic transactions entered into by the End Entity using a valid Certificate issued in the name of the End Entity.

The NAESB Business Practice Standards and Models Relating To Public Key Infrastructure (PKI) described in this document achieve the level of security commonly used by other industries engaged in commercial activity across the public Internet.

Within this document the words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, “OPTIONAL” are to be interpreted as in RFC 2119.

## Scope

The NAESB Business Practice Standards and Models Relating To Public Key Infrastructure (PKI) facilitate an infrastructure to secure electronic communications. The NAESB Business Practice Standards and Models Relating To Public Key Infrastructure (PKI) establish the obligations of both Authorized Certification Authorities and End Entities under these standards . These Business Practice Standards WEQ-012 do not specify how Certificates issued by Authorized Certification Authorities are to be used to secure specific software applications or electronic transactions. Those standards will be developed under separate NAESB Business Practice Standards.

This standard is comprised of two related documents, “The NAESB Business Practice Standards and Models Relating To Public Key Infrastructure (PKI)” **(“WEQ-012 Business Practice Standards”**) and “NAESB Accreditation Requirements for Certification Authorities”, **(“Accreditation Document”)**. Collectively these two documents are referred to as the “**PKI Requirements**”. The WEQ-012 Business Practice Standards document contains the WEQ-012 standards. The second document, the Accreditation Document, contains technical specifications that may be revisedto address changes in technology, the identification of new security threats or any other purpose which NAESB finds necessary. The WEQ-012 Business Practice Standards should be interpreted and applied consistent with the terms of the Accreditation Document.

## Commitment to Open Business Practice Standards

The Business Practice Standards contained in this document are intended to align with industry best practices for PKI as prescribed by the NIST in publication NIST SP 800-32, Internet Engineering Task Force PKI guidelines and standards (e.g. RFC 3280, 3647, 4210, and any successor standards etc.) and other broadly accepted/adopted standards from internationally recognized standards bodies.

To assist End Entities evaluating/comparing particular Certification Authorities in determining compliance with the provisions in these Business Practice Standards WEQ-012, cross references to the Set of Provisions outlined in RFC 3647 for CPs and/or Certification Practice Statements are provided in parenthesis for each major section.  These RFC cross references are for reference only; they are not to be considered as part of the NAESB Business Practice Standards WEQ-012.

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 Business Practice Standards initiatives, Business Practice Standard WEQ-012 is intended to facilitate the availability of interoperable PKI products from multiple vendors.

For NAESB Business Practice Standards requiring certificates, it is recommended that End Entities (?) entities acquire certificates through NAESB approved Authorized Certificate Authority.

**Definition of Terms**

**012-0** RESERVED. All previously designated definition of terms are considered reserved (Business Practice Standards WEQ-012-0.1 through WEQ-012-0.15), and are included in Business Practice Standards WEQ-000 (Abbreviations, Acronyms, and Definition of Terms).

**Business Practice Standards**

## 012-1 Introduction (RFC 3647 Section 1) [[1]](#footnote-1)

The NAESB Business Practice Standards and Models Relating To Public Key Infrastructure (PKI) and Accreditation Document define the minimum requirements for Certification Authorities, the electronic Certificates issued by those Certification Authorities and End Entities that use those Certificates. The Business Practice Standards are cross referenced with RFC 3647 for Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, but do not in themselves represent a CP and/or a Certification Practices Statement.

## 012-1.1 Overview (RFC 3647 Section 1.1)

## The Business Practice Standards WEQ-012 require the use of a PKI using X.509 v3 digital Certificates to provide for the following 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.

The NAESB Business Practice Standards and Models Relating To Public Key Infrastructure (PKI) requires that prior to the issuance of a digital X.509 v3 certificate industry participants shall complete the applicable registration process. These Certificates are provided by Authorized Certification Authorities.

## 012-1.2 IDENTIFICATION standards are SPECIFIED in the Accreditation DocuMENT

### 012-1.2.1 CERTIFICATE CLASS IDENTIFICATION standards are SPECIFIED in the Accreditation DocuMENT

### 012-1.2.2 Certificate Class Hierarchy standards are SPECIFIED in the Accreditation DocuMENT

## 012-1.3 Community and Applicability standards are SPECIFIED in the Accreditation DocuMENT

### 012-1.3.1 CERTIFICATION AUTHORITIES standards are SPECIFIED in the Accreditation DocuMENT

### 012-1.3.2 RAs standards are SPECIFIED in the Accreditation DocuMENT

### 012-1.3.3 End Entities (RFC 3647 Section 1.3.3)

End Entities participating in the Business Practice Standards WEQ-012 shall be required to be registered in the NAESB EIR and furnish proof that they are an entity authorized to engage in the wholesale electricity market. Entities or organizations that may require access to applications secured under the NAESB Business Practice Standards WEQ-012, but do not qualify as a wholesale electricity market participant (e.g., regulatory agencies, universities, consulting firms, etc.) must register under the sponsorship of an End Entity as an un-Affiliate Entity.

Registered End Entities and the user community they represent shall be required to meet to all End Entity obligations in Business Practice Standards WEQ-012.

### 012-1.3.4 Applicability

Certificates issued under the NAESB Business Practice Standards WEQ-012

may be used in, but not be limited to, the following suitable applications:

 Energy market transactions

 Energy or transmission scheduling

 Filings with government agencies

 Filings with law enforcement agencies

 Application filing processes, such as applying for or requesting access to

physical facilities

 Financial transactions within the energy markets’ communities

 Billing, metering, and invoicing

 Conveyance and transfer of operational data

 Conveyance and transfer of system reliability data

**Certificates issued under the Business Practice Standards WEQ-012 shall never**

**be used for performing any of the following functions:**

** Any transaction or data transfer that may result in imprisonment if**

**compromised or falsified.**

** Any transaction or data transfer deemed illegal under federal law**

## 012-1.4 Obligations standards are SPECIFIED in the Accreditation DocuMENT

### 012-1.4.1 Certificate Authority Obligations standards are SPECIFIED in the Accreditation DocuMENT

### 012-1.4.2 RA OBLIGATIONS standards are SPECIFIED in the Accreditation DocuMENT

### 012-1.4.3 End Entity Obligations (RFC 3647 Section 9.6.3)

Each End Entity organization shall certify to their certification entity that they have reviewed and acknowledge the following Business Practice Standards WEQ-012.

1. End Entity acknowledges the electric industry’s need for secure private electronic communications that facilitate the following purposes:
   * 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.
2. End Entity acknowledges the industry’s endorsement of public key cryptography, which utilizes public key Certificates to bind a person’s or computer system’s public key to its entity and to support symmetric encryption key exchange.
3. .
4. End Entity has evaluated each of its selected certification authority’s Certification Practices Statement in light of those industry standards as identified by the certification authority.

End Entities shall be obligated to register their legal business identification and secure an “Entity Code” that will be published in the NAESB EIR and used in all Subscriber applications submitted by, and Certificates issued to, that End Entity.

End Entities shall also be required to comply with the following requirements:

* Identify, through the NAESB EIR, the specific entity hey have selected to use as their certification authority(ies);:
* Execute all agreements and contracts with the registered Authorized Certification Authority(ies) as required by the Certificate Authority’s(ies) Certification Practices Statement necessary for the certificate authority(ies) to issue Certificates to the End Entity for use in securing electronic communications.
* Comply with all obligations required and stipulated by the Authorized Certification Authority in their certification practices agreement, e.g., certificate application procedures, Applicant identity proofing/verification, and certificate management practices.
* Confirm that it has a PKI certificate management program, has trained all affected employees in that program, and has established controls to ensure compliance with that program. This program shall include, but is not limited to:
  + Certificate private key security and handling policy(ies)
  + Certificate revocation policy(ies)
* Identify the type of Subscriber (I.e., individual, role, device or application) and provide complete and accurate information for each Certificate request.

### 012-1.4.4 Relying Party Obligations

Relying Party obligations shall be specified within the context of each NAESB standard that employs these Business Practice Standards WEQ-012.

### 012-1.4.5 REPOSITORY OBLIGATIONS standards are SPECIFIED in the Accreditation DocuMENT

## 012-1.5 RESERVED

## 012-1.6 RESERVED

### 012-1.6.1 RESERVED

## 012-1.7 Confidentiality (RFC 3647 Section 9.3, 9.4)

The following types of information shall be kept confidential:

* **Subscriber Information.** The End Entities shall protect the confidentiality of personal information regarding Subscribers that is collected during the Applicant registration, application, authentication, and Certificate status checking processes in accordance with the *Privacy Act of 1974 and Amendments****[[2]](#footnote-2)***. Such information shall be used only for the purpose of providing Authorized Certification Authority services 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 Certification services. In addition, personal information submitted by Subscribers:
  + Must be made available to the Subscriber involved following an appropriate request by such Subscriber
  + Must be subject to revision by such Subscriber to update information as necessary;
  + Cannot be used or disclosed for purposes other than the direct support of Business Practice Standards WEQ-012 unless such use is authorized by the Subscriber or is required by law,

## 012-1.8 Intellectual Property Rights

Private keys for Certificates shall be treated as the property of the End Entity identified in the Certificate. All other intellectual property rights as specified in the Accreditation Document.

## 012-1.9 Initial Registration

Certificates may be applied for and issued under Business Practice Standards WEQ-012 for the following types of Subscribers:

* Individual Subscriber – Certificates issued and used by a single named individual
* Role - Certificates issued in the name of a “role” performed by the End Entity organization, typically at a fixed physical location, but whose use is shared by multiple individuals, e.g., system control center shift personnel
* Device – Certificate issued and used in the operation of a physical computer system(s), e.g., web server(s)
* Application – Certificates issued and used by a software application

### 012-1.9.1 Types of names

The nomenclature, syntax and contents of Name fields in a digital certificate should be specified by any NAESB standard that employs the Business Practice Standards WEQ-012. They must clearly and uniquely identify the official company name of the Subscriber’s organization and the Entity Code of the Subscriber’s organization as they appear in the NAESB EIR.

### 012-1.9.2 RESERVED

### 012-1.9.3 Method to prove possession of private key standards are SPECIFIED in the Accreditation DocuMENT

### 012-1.9.4 Authentication of organization identity standards are SPECIFIED in the Accreditation DocuMENT

### 012-1.9.5 Authentication of individual identity standards are SPECIFIED in the Accreditation DocuMENT

## 012-1.10 Routine Rekey standards are SPECIFIED in the Accreditation DocuMENT

## 012-1.11 Certificate Application standards are SPECIFIED in the Accreditation DocuMENT

## 012-1.12 Certificate Issuance standards are SPECIFIED in the Accreditation DocuMENT

## 012-1.13 Certificate Acceptance standards are SPECIFIED in the Accreditation DocuMENT

## 012-1.14 Certificate Suspension and Revocation standards are SPECIFIED in the Accreditation DocuMENT

## 012-1.15 CRL Issuance Frequency and Validity PERIOD standards are SPECIFIED in the Accreditation DocuMENT

## 012-1.16 CRL Checking REQUIREMENTS standards are SPECIFIED in the Accreditation DocuMENT

## 012-1.17 Special Requirements for key compromise standards are SPECIFIED in the Accreditation DocuMENT

## 012-1.18 Security Audit Procedures standards are SPECIFIED in the Accreditation DocuMENT

### 012-1.18.1 Types of events recorded standards are SPECIFIED in the Accreditation DocuMENT

### 012-1.18.2 Frequency of Log Processing standards are SPECIFIED in the Accreditation DocuMENT

### 012-1.18.3 Audit Log Retention standards are SPECIFIED in the Accreditation DocuMENT

## 012-1.19 Records Archival standards are SPECIFIED in the Accreditation DocuMENT

### 012-1.19.1 Types of events recorded standards are SPECIFIED in the Accreditation DocuMENT

### 012-1.19.2 Retention period for archive standards are SPECIFIED in the Accreditation DocuMENT

### 012-1.19.3 Protection of archive standards are SPECIFIED in the Accreditation DocuMENT

### 012-1.19.4 Archive backup procedures standards are SPECIFIED in the Accreditation DocuMENT

### 012-1.19.5 Requirements for time-stamping of records standards are SPECIFIED in the Accreditation DocuMENT

### 012-1.19.6 Procedures to obtain and verify archive information standards are SPECIFIED in the Accreditation DocuMENT

### 012-1.19.7 Key Changeover standards are SPECIFIED in the Accreditation DocuMENT

### 012-1.19.8 Certificate Authority Termination standards are SPECIFIED in the Accreditation DocuMENT

## 012-1.20 Physical, Procedural, and Personnel Security Controls standards are SPECIFIED in the Accreditation DocuMENT

## 012-1.21 Physical Controls standards are SPECIFIED in the Accreditation DocuMENT

### 012-1.21.1 Site location and construction

### 012-1.21.2 Physical access standards are SPECIFIED in the Accreditation DocuMENT

### 012-1.21.3 Power and air conditioning standards are SPECIFIED in the Accreditation DocuMENT

### 012-1.21.4 Cabling and Network Devices standards are SPECIFIED in the Accreditation DocuMENT

## 012-1.22 Procedural Controls standards are SPECIFIED in the Accreditation DocuMENT

### 012-1.22.1 Trusted roles standards are SPECIFIED in the Accreditation DocuMENT

### 012-1.22.2 Number of persons required per task standards are SPECIFIED in the Accreditation DocuMENT

### 012-1.22.3 Identification and authentication for each role standards are SPECIFIED in the Accreditation DocuMENT

## 012-1.23 Key Pair Generation, Installation, and managementstandards are SPECIFIED in the Accreditation DocuMENT

### 012-1.23.1 Certification Authority Key pair generation standards are SPECIFIED in the Accreditation DocuMENT

### 012-1.23.2 key delivery to Certificate issuer standards are SPECIFIED in the Accreditation DocuMENT

### 012-1.23.3 Key sizes standards are SPECIFIED in the Accreditation DocuMENT

### 012-1.23.4 Private Key Protection standards are SPECIFIED in the Accreditation DocuMENT

### 012-1.23.5 Usage Periods for Public and Private Keys standards are SPECIFIED in the Accreditation DocuMENT

## 012-1.24 Computer Security Controls standards are SPECIFIED in the Accreditation DocuMENT

## 012-1.25 Network Security Controls standards are SPECIFIED in the Accreditation DocuMENT

## 012-1.26 Certificate PROFILE standards are SPECIFIED in the Accreditation DocuMENT

### 012-1.26.1 Version Numbers standards are SPECIFIED in the Accreditation DocuMENT and the Core WEQ-012 document

### 012-1.26.2 Certificate Extensions standards are SPECIFIED in the Accreditation DocuMENT

### 012-1.26.3 CP Object Identifier standards are SPECIFIED in the Accreditation DocuMENT

### 012-1.26.4 Subject Alternative Name

Subject alternative name standards are specified in the Accreditation Document and may be specified in any NAESB standard employing the Business Practice Standards WEQ-012.

### 012-1.26.5 CRL Distribution Point standards are SPECIFIED in the Accreditation DocuMENT

This PKI Requirements references published works of the Internet Engineering Task Force of The Internet Society.

Copyright (C) The Internet Society (2003).  All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works.  However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English. The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assignees.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

**4. SUPPORTING DOCUMENTATION**

**a. Description of Request:**

2012 WEQ Annual Plan Item 4.c: Develop modifications for WEQ-012 as needed to reflect current market conditions:

i) Authorized Certification Authority Standard and Credentialing Practice ([R11014](http://www.naesb.org/pdf4/r11014.docx))

ii) Technology Review and Upgrade for NAESB Public Key Infrastructure Standard WEQ-012 ([R11015](http://www.naesb.org/pdf4/r11015.doc)).

**b. Description of Recommendation:**

Technology Review and Upgrade for NAESB PKI WEQ-012 Standard

**c. Business Purpose:**

1. **Commentary/Rationale of Subcommittee(s)/Task Force(s):**

[September 22, 2011 PKI Subcommittee Meeting Minutes](http://www.naesb.org/pdf4/weq_pki_092211dm.doc)

[October 20, 2011 PKI Subcommittee Meeting Minutes](http://www.naesb.org/pdf4/weq_pki_102011dm.doc)

[November 10, 2011 PKI Subcommittee Meeting Minutes](http://www.naesb.org/pdf4/weq_pki_111011dm.doc)

[December 8, 2011 PKI Subcommittee Meeting Minutes](http://www.naesb.org/pdf4/weq_pki_120811dm.doc)

[January 4, 2012 PKI Subcommittee Meeting Minutes](http://www.naesb.org/pdf4/weq_pki_010412dm.doc)

[January 26, 2012 PKI Subcommittee Meeting Minutes](http://www.naesb.org/pdf4/weq_pki_012612dm.doc)

[February 16, 2012 PKI Subcommittee Meeting Minutes](http://www.naesb.org/pdf4/weq_pki_021612dm.doc)

[March 8, 2012 PKI Subcommittee Meeting Minutes](http://www.naesb.org/pdf4/weq_pki_030812dm.doc)

[March 22, 2012 PKI Subcommittee Meeting Minutes](http://www.naesb.org/pdf4/weq_pki_032212dm.doc)

[April 26, 2012 PKI Subcommittee Meeting Minutes](http://www.naesb.org/pdf4/weq_pki_042612dm.doc)

[May 31, 2012 PKI Subcommittee Meeting Minutes](http://www.naesb.org/pdf4/weq_pki_053112dm.doc)

June 14, 2012 PKI Subcommittee Meeting Minutes (pending)

July 3, 2012 PKI Subcommittee Meeting Minutes (pending)

July 9, 2012 PKI Subcommittee Meeting Minutes (pending)

1. RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Chokhani, S.; Ford, W.; Sabett, R.; Merrill, C.; and Wu, S., RFC Editor, November 2003.  (<http://www.ietf.org/rfc/rfc3647.txt>) [↑](#footnote-ref-1)
2. *Privacy Act of 1974 and Amendments* (as of January 2, 1991), 5 U.S.C. Sec. 552.a, Title 5, Part 1, Chap. 5, Subchapter II. [↑](#footnote-ref-2)