RECOMMENDATION TO NAESB EXECUTIVE COMMITTEE

For Quadrant: **Wholesale Electric Quadrant**
Requesters: **WEQ PKI Subcommittee**
Request No.: **2012 WEQ AP Item 4.c.i-ii/R11014/R11015**
Request Title: Develop modifications for WEQ-012 as needed to reflect current market conditions (Authorized Certification Authority Standard and Credentialing Practice (R11014). Technology Review and Upgrade for NAESB Public Key Infrastructure Standard WEQ-012 (R11015))

1. RECOMMENDED ACTION:

X	Accept as requested
	Accept as modified below
	Decline

EFFECT OF EC VOTE TO ACCEPT RECOMMENDED ACTION:

X	Change to Existing Practice
	Status Quo

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

RECOMMENDATION TO NAESB EXECUTIVE COMMITTEE

For Quadrant: **Wholesale Electric Quadrant**
Requesters: **WEQ PKI Subcommittee**
Request No.: **2012 WEQ AP Item 4.c.i-ii/R11014/R11015**
Request Title: Develop modifications for WEQ-012 as needed to reflect current market conditions (Authorized Certification Authority Standard and Credentialing Practice (R11014). Technology Review and Upgrade for NAESB Public Key Infrastructure Standard WEQ-012 (R11015))

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. This standard is comprised of two complimentary and interdependent documents, "The NAESB Business Practice Standards and Models Relating To Public Key Infrastructure (PKI)" **("Core WEQ-012")** and "NAESB Accreditation Requirements for Certification Authorities", **("Accreditation Document")**. Collectively these two documents are referred to as the **"Business Practice Standards WEQ-012"**. The first is the Core WEQ-012 document (this document), which contains the formal set of WEQ-012 standards that are expected to remain in force until being replaced or retired through the normal course of evolution within NAESB. The second document, the Accreditation Document, contains technical specifications that may be revised, as needed, to address changes in technology, the identification of new security threats or any other purpose which NAESB finds necessary. In the event of a conflict between the two documents the Accreditation document shall take precedence.

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~~ authenticating Internet data transfers. NAESB Business Practice Standards WEQ-012~~WEQ~~ provide~~s~~ 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~~ authentication in support ~~offer~~ 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

Comment [DH1]: OATI: Recommend deleting this text because according to definitions below the Accreditation Requirements are part of the Business Practice Standards WEQ-012. Please see additional comment 4 below.

Comment [DH2]: OATI: Relocated this paragraph to beginning of document because it contains definitions that are applicable to the paragraphs below. This is non-substantive change.

Comment [DH3]: Three definitions are created here:

•"Core WEQ-012" = NAESB Business Practice Standards and Models Relating To Public Key Infrastructure (PKI)
•"Accreditation Document" = NAESB Accreditation Requirements for Certification Authorities
•"Business Practice Standards WEQ-012" = Core WEQ-012 and Accreditation Document

These definitions are not used consistently throughout the document. Specifically, in many cases the term "Business Practice Standards and Models Relating To Public Key Infrastructure (PKI)" is used. Use of a previously defined term in this manner creates confusion. OATI suggests consistent use of these definitions throughout the document, and careful choice of the correct defined term in each instance.

Comment [PS4]: OATI: Clarification is needed whether the Accreditation document is or is not part of the WEQ-012 standard. If it is, any revision to it must be performed pursuant to the NAESB Standards process.

Comment [PS5]: OATI: Suggest removal of End Entities as they are called out in next sentence.

Comment [PS6]: OATI: The WEQ does not provide assurance; these standards provide assurance.

Comment [MB7]: OATI: PKI Digital Certificates are used for authentication purposes. Required physical and cyber security provisions (even as those may relate to PKI technology re: CEII/Critical Assets) remain subject to NERC CIP requirements.

Comment [MB8]: OATI: Prior to the identification of specific examples, each should be studied/reviewed to identify the application of other industry standards (such as NERC CIP) that may also apply. In that case, NERC/NAESB/the industry must consider the impact of such security pr... [1]

RECOMMENDATION TO NAESB EXECUTIVE COMMITTEE

For Quadrant: **Wholesale Electric Quadrant**
Requesters: **WEQ PKI Subcommittee**
Request No.: **2012 WEQ AP Item 4.c.i-ii/R11014/R11015**
Request Title: Develop modifications for WEQ-012 as needed to reflect current market conditions (Authorized Certification Authority Standard and Credentialing Practice (R11014). Technology Review and Upgrade for NAESB Public Key Infrastructure Standard WEQ-012 (R11015))

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~~ trusted authentication~~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.

Comment [MB9]: OATI: Again, PKI technology addresses the issue of authentication—and security (physical and cyber) is guided under NERC CIP standards. Additionally, PKI technology client (End-User) certificates are not commonly used by other industries. In contrast, Server (hardware) certificates are commonly used by other industries. This distinction is salient and should be noted and retained throughout these standards.

Certification

Certification Authorities must comply with the provisions of the NAESB Business Practice Standards and Models Relating To Public Key Infrastructure (PKI), ~~and~~ conform to the NAESB Certification Program, and provide an attestation to NAESB from the chief executive officer of the respective Certification Authority to be considered an Authorized Certification Authority. The attestation must include certification that the Certification Authority is knowledgeable and understands the requirements specified in Business Practice Standards WEQ-012, and attests that the Certification Authority meets all applicable provisions contained therein. Upon achieving NAESB certification, NAESB will provide the North American Electric Reliability Corporation (NERC) with the names of Authorized Certification Authorities. The Authorized Certification Authority~~certificate authority~~ will immediately be authorized to display the NAESB certification mark and will be authorized to claim compliance with NAESB Business Practice Standards WEQ-012. ~~All i~~Industry applications or business processes within the guidance of NAESB (e.g., OASIS) required to be secured under these Business Practice Standards WEQ-012 must permit access to any legitimate user that presents a valid electronic Certificate issued by an Authorized Certification Authority.

Comment [MB10]: OATI: OATI agrees with the audit requirements specified in WEQ-012, and recommends such an attestation to bind the organization to the requirements. This will enhance the trust of NAESB and other CAs who will be able to rely on this attestation .

Comment [DH11]: OATI: Change to Authorized Certificate Authority. There is another comment about this issue below as well regarding consistent usage of terms for CA.

Comment [MB12]: OATI: Recommended rewording. There are many other applications that do not fall within the guidance of NAESB. Additionally, OATI again recommends a review of each NAESB guided application or business process to identify whether there are other industry standards (NERC CIP) that apply. Please see Note 8 above.

Comment [PS13]: OATI: Suggested change to be more clear that the applications will dictate whether they do or do not require use of certs in conformance with these standards.

NAESB may rescind an Authorized Certification Authority's certification, for cause, at any time by providing 30 days notice in writing to the Authorized Certification Authority. Authorized Certification Authority's that receive a rescission notice from NAESB are required to notify all affected Certificate holders within 5 days that their NAESB Business Practice Standards and

RECOMMENDATION TO NAESB EXECUTIVE COMMITTEE

For Quadrant: **Wholesale Electric Quadrant**
Requesters: **WEQ PKI Subcommittee**
Request No.: **2012 WEQ AP Item 4.c.i-ii/R11014/R11015**
Request Title: Develop modifications for WEQ-012 as needed to reflect current market conditions (Authorized Certification Authority Standard and Credentialing Practice (R11014). Technology Review and Upgrade for NAESB Public Key Infrastructure Standard WEQ-012 (R11015))

Models Relating To Public Key Infrastructure (PKI) certification has been rescinded. ~~and their Certificates will no longer be valid.~~

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

- Purchase, sale or merger of the Authorized Certification Authority by/with another entity
- Renewal as required by the NAESB Certification Program

Scope

The NAESB Business Practice Standards and Models Relating To Public Key Infrastructure (PKI) provide for an infrastructure to secure electronic communications. The NAESB Business Practice Standards and Models Relating To Public Key Infrastructure (PKI) dictate the obligations of both Authorized Certification Authorities and End Entities that will rely on this infrastructure. These Business Practice Standards WEQ-012 do not specify how Certificates issued by Authorized Certification Authorities ~~are to~~may be used to add additional authentication requirements to~~secure~~ specific software applications or electronic transactions within the guidance of NAESB. Those standards will be developed under separate NAESB Business Practice Standards.

~~This standard is comprised of two complimentary and interdependent documents, "The NAESB Business Practice Standards and Models Relating To Public Key Infrastructure (PKI)" **("Core WEQ-012")** and "NAESB Accreditation Requirements for Certification Authorities", **("Accreditation Document")**. Collectively these two documents are referred to as the "**Business Practice Standards WEQ-012**". The first is the Core WEQ-012 document (this document), which contains the formal set of WEQ-012 standards that are expected to remain in force until being replaced or retired through the normal course of evolution within NAESB. The second document, the Accreditation Document, contains technical specifications that may be revised, as needed, to address changes in technology, the identification of new security threats or any other purpose which NAESB finds necessary. In the event of a conflict between the two documents the Accreditation document shall take precedence.~~

Commitment to Open Business Practice Standards

The recommendations contained in this document should align with industry best practices for PKI as prescribed by the NIST and Technology 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.

Comment [MB14]: OATI: Rescission of NAESB certification will not result in revocation of validity of underlying certificates. Rather, such revocation only affects acceptance of such certificates in certain specified applications/business processes.

Comment [MB15]: OATI: Again, PKI technology is used for authentication purposes, and security is under the purview of NERC CIP standards.

Comment [MB16]: OATI: NAESB has guidance related to specific industry applications/business processes. Many industry applications do not fall within this area.

RECOMMENDATION TO NAESB EXECUTIVE COMMITTEE

For Quadrant: **Wholesale Electric Quadrant**
Requesters: **WEQ PKI Subcommittee**
Request No.: **2012 WEQ AP Item 4.c.i-ii/R11014/R11015**
Request Title: Develop modifications for WEQ-012 as needed to reflect current market conditions (Authorized Certification Authority Standard and Credentialing Practice (R11014). Technology Review and Upgrade for NAESB Public Key Infrastructure Standard WEQ-012 (R11015))

~~To assist Certification Authorities and 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.~~

Comment [PT17]: OATI: For the most part RFC cross references were removed from this document and the Accreditation Document; any remaining references are suggested to be removed.

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, these Business Practice Standards WEQ-012 are~~is~~ being developed to ensure the availability of interoperable PKI products from multiple vendors while maintaining a high level of security as that may otherwise be required under industry standards, such as NERC CIP standards. NAESB encourages ~~Certification~~ certification ~~Authorities~~ authorities to pursue certification under the NAESB Business Practice Standards and Models Relating To Public Key Infrastructure (PKI) to meet the energy industry's needs for PKI.

Comment [TW18]: OATI: Use of Certification Authority and certificate authority both with and without capital letters are mixed within the standards and should be 1) added to the WEQ-000 Glossary as a defined term(s) and capitalized, or 2) used without the capitalization. Suggest the latter. Whatever decision is made should be carried throughout this document.

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]

The NAESB Business Practice Standards and Models Relating To Public Key Infrastructure (PKI) define the minimum requirements that must be met by Certification Authorities, the electronic Certificates issued by those Certification Authorities and End Entities that use those Certificates. Additional requirements may be specified by industry participants for their applications in order to comply with their security requirements or those required by other industry organizations such as NERC. ~~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.~~

Comment [PT19]: OATI: RFC cross references were removed from this document.

[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)

RECOMMENDATION TO NAESB EXECUTIVE COMMITTEE

For Quadrant: **Wholesale Electric Quadrant**
Requesters: **WEQ PKI Subcommittee**
Request No.: **2012 WEQ AP Item 4.c.i-ii/R11014/R11015**
Request Title: Develop modifications for WEQ-012 as needed to reflect current market conditions (Authorized Certification Authority Standard and Credentialing Practice (R11014). Technology Review and Upgrade for NAESB Public Key Infrastructure Standard WEQ-012 (R11015))

012-1.1 OVERVIEW ~~(RFC 3647 Section 1.1)~~

The Business Practice Standards WEQ-012 call for the use of a PKI using X.509 v3 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.

The NAESB Business Practice Standards and Models Relating To Public Key Infrastructure (PKI) requires that digital X.509 v3 certificates be issued to industry participants ~~after a formal registration process has been completed~~ as part of a formal registration process. These Certificates are provided by Authorized Certification Authorities. The NAESB Business Practice Standards and Models Relating To Public Key Infrastructure (PKI) call for these Authorized Certification Authorities to meet certain minimum criteria and that the Certificates issued to 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 certificate authority. The Issuing Certification Authority must meet the provisions in the NAESB Business Practice Standards and Models Relating To Public Key Infrastructure (PKI) in order for the Certificate to be considered compliant with NAESB Business Practice Standards.

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**

Comment [PT20]: OATI: All other RFC cross references were removed.

Comment [TW21]: OATI: This requirement was true in the original WEQ-012 with NERC managing the Registry; registration in TSIN was prerequisite to issuing a certificate due to the inclusion of a registered entity code in the OU field of the Subject. This requirement on what must be included in the Subject is being revised. Perhaps it is best to change this phrase to be "as part of a formal registration process." This way it does not stipulate the order of steps required in the registration process.

Comment [TW22]: OATI: Since the standard calls out that each sub-standard of 1.2 is specified in the Accreditation document, do not think it is necessary to include that statement here.

Comment [TW23]: OATI: These requirements are not properly addressed in the Accreditation document at present. Is it the intent to require use of uniform set of OIDs associated with each assurance level across all ACAs? Or, will ACA be required to identify the OID used for each level (in the registry)? WEQ-012 allowed for the certification path to be used in place of stipulated OID provided that certification path is unique to the assurance level of certs issued under that path, or is identified as meeting only the lowest assurance level of all certificates if multiple assurance levels issued and not represented by OID. Not dictating OIDs was originally intended to not disrupt otherwise qualifying CA certificates that met the single assurance level of WEQ-012 at that time.

Comment [PT24]: OATI believes certificate classes and assurance levels are difficult to define and technically challenging to implement by the adopting applications. OATI recommend the use of categories of certificates based on Key Usage and Extended Key Usage which are well known, natively supported by SSL/TLS, easily supported by applications including web servers, browsers, email clients, etc. and can be easily validated up a certification path.

Comment [TW25]: OATI: The Accreditation document outlines assurance levels. It does not address what was stipulated in original WEQ-012 relating to acceptance of certain level assurance certificates in connection with given application. If OASIS requires use of a BASIC assurance level, the original standard stipulated that use of certs at that assurance level and all higher assurance levels would be allowed. So, a HIGH level cert could be u ... [2]

RECOMMENDATION TO NAESB EXECUTIVE COMMITTEE

For Quadrant: Wholesale Electric Quadrant
Requesters: WEQ PKI Subcommittee
Request No.: 2012 WEQ AP Item 4.c.i-ii/R11014/R11015
Request Title: Develop modifications for WEQ-012 as needed to reflect current market conditions (Authorized Certification Authority Standard and Credentialing Practice (R11014). Technology Review and Upgrade for NAESB Public Key Infrastructure Standard WEQ-012 (R11015))

012-1.3 COMMUNITY AND APPLICABILITY ~~STANDARDS ARE SPECIFIED IN THE ACCREDITATION DOCUMENT~~

012-1.3.1 CERTIFICATION AUTHORITIES STANDARDS ARE SPECIFIED IN BOTH THE ACCREDITATION DOCUMENT AND THIS 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~~ using authentication specified 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 a qualified wholesale electricity market participant~~ as an un-Affiliate Entity.

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

Comment [TW26]: OATI: Per comment on 1.2

Comment [TW27]: OATI: The Accreditation document addresses the process for establishing certification of an ACA. Use of the new Registry could be an industry practice and not officially part of the standard, depending on where and what QRP requirements are set forth in this standard vs. relegated to being set in each individual application's standards for use of WEQ-012.

Comment [PT28]: OATI: All other RFC cross references have been removed from this document.

Comment [TW29]: OATI: JESS has discussed and no longer is seeing a need for the 'sponsorship' obligation for an un-Affiliated entity to prove 'need to know or to be included in EIR.

RECOMMENDATION TO NAESB EXECUTIVE COMMITTEE

For Quadrant: **Wholesale Electric Quadrant**
Requesters: **WEQ PKI Subcommittee**
Request No.: **2012 WEQ AP Item 4.c.i-ii/R11014/R11015**
Request Title: Develop modifications for WEQ-012 as needed to reflect current market conditions (Authorized Certification Authority Standard and Credentialing Practice (R11014). Technology Review and Upgrade for NAESB Public Key Infrastructure Standard WEQ-012 (R11015))

012-1.3.4 APPLICABILITY STANDARDS ARE SPECIFIED IN THE ACCREDITATION DOCUMENT

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/Subscriber Obligations (RFC 3647 Section 9.6.3)

Each End Entity organization shall acknowledge their understanding of the following obligations to the Business Practice Standards WEQ-012 through their Authorized Certification Authority.

A. End Entity recognizes and acknowledges the electric industry's need for secure private electronic communications meeting the goals of:

- 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.

B. End Entity recognizes 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.

C. End Entity has reviewed these Business Practice Standards WEQ-012 with respect to industry guidelines for establishing a trusted PKI.

Comment [TW30]: OATI: Applicability should be addressed as related to the parameters of NAESB guidance. As stated above in Comment 7, additional industry standards may apply or may be specified to apply to add security to this area. Each application/ business process should be reviewed for such treatment.

Comment [TW31]: OATI: Per comment on 1.2

RECOMMENDATION TO NAESB EXECUTIVE COMMITTEE

For Quadrant: **Wholesale Electric Quadrant**
Requesters: **WEQ PKI Subcommittee**
Request No.: **2012 WEQ AP Item 4.c.i-ii/R11014/R11015**
Request Title: Develop modifications for WEQ-012 as needed to reflect current market conditions (Authorized Certification Authority Standard and Credentialing Practice (R11014). Technology Review and Upgrade for NAESB Public Key Infrastructure Standard WEQ-012 (R11015))

D. 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 industry recognized "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.~~

Comment [TW32]: OATI: This requirement was in the original WEQ-012 standards but has now been removed in these standards.

Entities shall ~~also~~ be required to identify, through the NAESB EIR, the specific Authorized Certification Authorities they have selected to use as their Authorized Certification Authority(ies) and acknowledge the following accompanying obligations:

- End Entity has executed 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.
- End Entity complies 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.
- End Entity affirms the establishment of a PKI certificate management program, has trained all affected employees in that program, and 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)
- End Entity correctly represents the type of Subscriber (I.e., individual, role, device or application) and represents that all information provided in each Certificate request is complete and accurate.

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.

Comment [TW33]: OATI: OATI strongly disagrees with placing this obligation on the application to define. Alternatively, this section should be reinstated and contain the key elements—such as validating identity – like check the CRL (or OCSP) for revocation, proper assurance level, etc. Could probably word it that 'Unless stipulated as part of the standards or specification associated with use of WEQ-012 in specific applications or business transactions, the following minimum obligations must be met to be considered a QRP."

The biggest "teeth" that was put into the WEQ_012 standard was in this section that bound end entity to the electronic transactions (to the extent one can ever bind another to something they dispute doing) they entered into with a cert that was verified to meet all QRP obligations.

RECOMMENDATION TO NAESB EXECUTIVE COMMITTEE

For Quadrant: **Wholesale Electric Quadrant**
Requesters: **WEQ PKI Subcommittee**
Request No.: **2012 WEQ AP Item 4.c.i-ii/R11014/R11015**
Request Title: Develop modifications for WEQ-012 as needed to reflect current market conditions (Authorized Certification Authority Standard and Credentialing Practice (R11014). Technology Review and Upgrade for NAESB Public Key Infrastructure Standard WEQ-012 (R11015))

012-1.4.5 **REPOSITORY OBLIGATIONS STANDARDS ARE SPECIFIED IN THE ACCREDITATION DOCUMENT**

Comment [TW34]: OATI: The portion of the standard addressing what is obligated to be part of EIR has been removed from the standard. The QRP obligations include requirements for verifying certs against the EIR. If each application has to set QRP obligations, then does each application have to set forth EIR obligations to make sure they are enforceable? Somewhere in WEQ-012, should stipulate exactly what the requirements for the EIR relative to WEQ-012. Adding EIR obligation on ACAs to 1.3.1 would suffice; EIR obligation on End Entities set in 1.3.3.

012-1.5 FEES

Fees charged by an ACA are not within the scope of the Business Practice Standards WEQ-012.

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 Authorized Certification Authority, or designated RA, 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]. 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 Authorized Certification Authority services. In addition, personal information submitted by Subscribers:
    - Must be made available by the Authorized Certification Authority to the Subscriber involved following an appropriate request by such Subscriber
    - Must be subject to correction and/or reasonable and appropriate revision by such Subscriber
    - Must be protected by the Authorized Certification Authority in a manner designed to ensure the data's integrity and confidentiality
    - Cannot be used or disclosed by the Authorized Certification Authority for purposes other than the direct operational support of Business Practice Standards WEQ-012 unless such use is

[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.

RECOMMENDATION TO NAESB EXECUTIVE COMMITTEE

For Quadrant: **Wholesale Electric Quadrant**
Requesters: **WEQ PKI Subcommittee**
Request No.: **2012 WEQ AP Item 4.c.i-ii/R11014/R11015**
Request Title: Develop modifications for WEQ-012 as needed to reflect current market conditions (Authorized Certification Authority Standard and Credentialing Practice (R11014). Technology Review and Upgrade for NAESB Public Key Infrastructure Standard WEQ-012 (R11015))

authorized by the Subscriber involved or is required by law, including judicial process
- All confidentiality requirements specified in the Accreditation Document

012-1.8 INTELLECTUAL PROPERTY RIGHTS

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

Comment [MB35]: OATI: Intellectual Property Rights are not identified in the Accreditation Document. That document must be revised appropriately.

012-1.9 INITIAL REGISTRATION

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

Comment [MB36]: OATI: Use of "Certificate/s" is confusing—is it a client certificate/server certificate/etc. Clarification/ definition/consistency must be added. This comment applies throughout this document.

- 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

Comment [PT37]: OATI: These subscriber types, along with appropriate key usage and extended key usage, should define the categories of certificates available under this standard (not classes or assurance levels). Recommend rewording to reflect this approach.

An Authorized Certification Authority is not required to support the application and issuance of all these Certificate types, but the Authorized Certification Authority shall be required to disclose to any End Entity those specific Certificate types they do support.

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 employ 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 TSIN registry~~.

Comment [TW38]: OATI: Removal of the requirement that the cert Subject include a registered Entity Code should probably be removed. If it is retained, the standard must indicate a uniform, standard place the information must be presented otherwise it has no value to applications that might use this information. Suggested, though, that the guidance (use of 'should') as to the form of the common name may be useful to the standard and should be reinstated.

012-1.9.2 **RESERVED**

RECOMMENDATION TO NAESB EXECUTIVE COMMITTEE

For Quadrant: **Wholesale Electric Quadrant**
Requesters: **WEQ PKI Subcommittee**
Request No.: **2012 WEQ AP Item 4.c.i-ii/R11014/R11015**
Request Title: Develop modifications for WEQ-012 as needed to reflect current market conditions (Authorized Certification Authority Standard and Credentialing Practice (R11014). Technology Review and Upgrade for NAESB Public Key Infrastructure Standard WEQ-012 (R11015))

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

Comment [MB39]: OATI: Difference between routine rekey, reissue, and renew needs to be clarified 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~~

Comment [TW40]: OATI: Per comment to 1.2

RECOMMENDATION TO NAESB EXECUTIVE COMMITTEE

For Quadrant: **Wholesale Electric Quadrant**
Requesters: **WEQ PKI Subcommittee**
Request No.: **2012 WEQ AP Item 4.c.i-ii/R11014/R11015**
Request Title: Develop modifications for WEQ-012 as needed to reflect current market conditions (Authorized Certification Authority Standard and Credentialing Practice (R11014). Technology Review and Upgrade for NAESB Public Key Infrastructure Standard WEQ-012 (R11015))

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~~

Comment [TW41]: OATI: Per comment to 1.2.

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

RECOMMENDATION TO NAESB EXECUTIVE COMMITTEE

For Quadrant: Wholesale Electric Quadrant
Requesters: WEQ PKI Subcommittee
Request No.: 2012 WEQ AP Item 4.c.i-ii/R11014/R11015
Request Title: Develop modifications for WEQ-012 as needed to reflect current market conditions (Authorized Certification Authority Standard and Credentialing Practice (R11014). Technology Review and Upgrade for NAESB Public Key Infrastructure Standard WEQ-012 (R11015))

012-1.21 PHYSICAL CONTROLS ~~STANDARDS ARE SPECIFIED IN THE ACCREDITATION DOCUMENT~~

Comment [TW42]: OATI: Per comment to 1.2.

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~~

Comment [TW43]: OATI: Per comment to 1.2.

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 MANAGEMENT ~~STANDARDS ARE SPECIFIED IN THE ACCREDITATION DOCUMENT~~

Comment [TW44]: OATI: Per comment to 1.2.

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

RECOMMENDATION TO NAESB EXECUTIVE COMMITTEE

For Quadrant: **Wholesale Electric Quadrant**
Requesters: **WEQ PKI Subcommittee**
Request No.: **2012 WEQ AP Item 4.c.i-ii/R11014/R11015**
Request Title: Develop modifications for WEQ-012 as needed to reflect current market conditions (Authorized Certification Authority Standard and Credentialing Practice (R11014). Technology Review and Upgrade for NAESB Public Key Infrastructure Standard WEQ-012 (R11015))

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~~

Comment [TW45]: OATI: Per comment to 1.2.

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 ~~RESERVEDSUBJECT ALTERNATIVE NAME~~

Formatted: Heading 3, Left, Indent: Left: 0", Tab stops: 1", Left

~~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.~~

Comment [TW46]: OATI: Think it is inappropriate for an application to require specific information to be contained within the certificate without identifying what that information may be in the WEQ-012 or Accreditation document. This should be referenced to Accreditation document if Subject Alternative Name is cited there, or mark this as RESERVED otherwise.

012-1.26.5 CRL DISTRIBUTION POINT STANDARDS ARE SPECIFIED IN THE ACCREDITATION DOCUMENT

RECOMMENDATION TO NAESB EXECUTIVE COMMITTEE

For Quadrant: **Wholesale Electric Quadrant**
Requesters: **WEQ PKI Subcommittee**
Request No.: **2012 WEQ AP Item 4.c.i-ii/R11014/R11015**
Request Title: Develop modifications for WEQ-012 as needed to reflect current market conditions (Authorized Certification Authority Standard and Credentialing Practice (R11014). Technology Review and Upgrade for NAESB Public Key Infrastructure Standard WEQ-012 (R11015))

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)

ii) Technology Review and Upgrade for NAESB Public Key Infrastructure Standard WEQ-012 (R11015).

b. Description of Recommendation:

Technology Review and Upgrade for NAESB PKI WEQ-012 Standard

c. Business Purpose:

RECOMMENDATION TO NAESB EXECUTIVE COMMITTEE

For Quadrant: **Wholesale Electric Quadrant**
Requesters: **WEQ PKI Subcommittee**
Request No.: **2012 WEQ AP Item 4.c.i-ii/R11014/R11015**
Request Title: Develop modifications for WEQ-012 as needed to reflect current market conditions (Authorized Certification Authority Standard and Credentialing Practice (R11014). Technology Review and Upgrade for NAESB Public Key Infrastructure Standard WEQ-012 (R11015))

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

September 22, 2011 PKI Subcommittee Meeting Minutes
October 20, 2011 PKI Subcommittee Meeting Minutes
November 10, 2011 PKI Subcommittee Meeting Minutes
December 8, 2011 PKI Subcommittee Meeting Minutes
January 4, 2012 PKI Subcommittee Meeting Minutes
January 26, 2012 PKI Subcommittee Meeting Minutes
February 16, 2012 PKI Subcommittee Meeting Minutes
March 8, 2012 PKI Subcommittee Meeting Minutes
March 22, 2012 PKI Subcommittee Meeting Minutes
April 26, 2012 PKI Subcommittee Meeting Minutes
May 31, 2012 PKI Subcommittee Meeting Minutes
June 14, 2012 PKI Subcommittee Meeting Minutes (pending)
July 3, 2012 PKI Subcommittee Meeting Minutes (pending)
July 9, 2012 PKI Subcommittee Meeting Minutes (pending)

Page 2: [1] Comment [MB8] **8/10/2012 3:38:00 PM**

OATI: Prior to the identification of specific examples, each should be studied/reviewed to identify the application of other industry standards (such as NERC CIP) that may also apply. In that case, NERC/NAESB/the industry must consider the impact of such security provisions if PKI Digital Certificates are allowed that are not located in NERC CIP compliant environments.

Page 6: [2] Comment [TW25] **8/10/2012 3:38:00 PM**

OATI: The Accreditation document outlines assurance levels. It does not address what was stipulated in original WEQ-012 relating to acceptance of certain level assurance certificates in connection with given application. If OASIS requires use of a BASIC assurance level, the original standard stipulated that use of certs at that assurance level and all higher assurance levels would be allowed. So, a HIGH level cert could be used in OASIS. Was it subcommittee's intent that each application has to state that in their standards?