
**ASSESSMENT REPORT OF THE
NORTH AMERICAN ENERGY STANDARDS BOARD (NAESB)
WHOLESALE ELECTRIC QUADRANT DRAFT TECHNICAL STANDARDS FOR
PUBLIC KEY INFRASTRUCTURE**

August 8, 2006

*Prepared by
Sandia National Laboratories
Information Design Assurance Red Team
for the Department of Energy*

Abstract

This document presents the results of an independent assessment by the Sandia National Laboratories Information Design Assurance Red Team of the “NAESB Wholesale Electric Quadrant (WEQ) draft technical standards for Public Key Infrastructure (PKI),” developed by the North American Energy Standards Board (NAESB). The Sandia Team was tasked not only with performing a thorough assessment of the NAESB draft PKI Standards, but also with suggesting improvements that could be made to the standard.

Sandia is a multi-program laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

Acknowledgments

This document was prepared for the Department of Energy (DOE) by a Working Group of the Information Design Assurance Red Team (IDART) at Sandia National Laboratories. The Working Group has the following members:

David Duggan, Project Leader
Principal Member of the Technical Staff
Sandia National Laboratories
Networked Systems Survivability and Assurance
505-845-8100
dduggan@sandia.gov

Timothy Draelos, Technical Analyst
Sandia National Laboratories
Networked Systems Survivability and Assurance
505-844-8698
ltjrael@sandia.gov

Michael Collins, Technical Analyst
Sandia National Laboratories
Networked Systems Survivability and Assurance
505-284-3017
mjcolli@sandia.gov

Lauren McIver, Technical Analyst
Sandia National Laboratories
Networked Systems Survivability and Assurance
505-284-6962
lmciver@sandia.gov

The working group would like to thank the following individuals from the North American Energy Standards Board (NAESB) for their contributions to this document:

Rae McQuade

North American Energy Standards Board

Executive Director

713-356-0060

DeDe Kirby

North American Energy Standards Board

713-356-0060

Jim Buccigross, Group 8760

Cade Burks, EC Power

Valerie Crockett, Tennessee Valley Authority

Paul Sorenson, Open Access Technology International

Leigh Spangler, Latitude Technologies

Patrick Tronnier, Open Access Technology International

Kathy York, Tennessee Valley Authority

Mike Novak, National Fuel

Lou Oberski, Dominion

This page intentionally left blank.

Contents

EXECUTIVE SUMMARY	vi
1. Introduction	1
2. North American Energy Standards Board Description	1
3. Objective and Purpose of the NAESB Standards	1
4. Critical Success Factors	1
5. Surety Assessment References.....	2
6. Surety Assessment Analysis and Recommendations	3
6.1 Security Issues	4
6.1.1 Deploying the NAESB draft PKI Standard	4
6.1.2 The Certificate Policy for the NAESB PKI.....	4
6.1.3 Cross-Certification.....	5
6.1.4 Security of the CA's signing key.....	5
6.1.5 Certificate Rescission Notices	5
6.1.6 Network Security Controls	6
6.1.7 References to Key Sizes and Cryptographic Algorithms.....	6
6.1.8 NAESB PKI User Declarations	7
6.1.9 Key Pair Generation	7
6.1.10 Unaffiliated Entities.....	8
6.1.11 Certificate Classes	8
6.1.12 Certificate Protection	8
6.1.13 CRL Issuance frequency, validity period, and availability	9
6.1.14 Certificate Application Steps.....	9
6.1.15 Tamper-Evident Hardware	10
6.1.16 Obsolete RFC References.....	10
6.1.17 Use of the Term End Entity	10
6.1.18 Customer Service Center	10
6.1.19 Reasonable Practices	11
6.1.20 Consistent Naming Convention for NAESB PKI Standards	11
6.1.21 Missing Requirement Level Key Words.....	11
6.2 Other Areas for Improvement	11
6.2.1 Missing Definitions	11
6.2.2 Extraneous Definitions	12
6.2.3 Inconsistent Definitions	12
6.2.4 Document Formatting.....	12
7. Summary	12
8. Conclusion.....	13
Appendix A – Abbreviations and Acronyms.....	15

This page intentionally left blank.

EXECUTIVE SUMMARY

This document provides an independent analysis of the draft standards developed by the North American Energy Standards Board (NAESB) related to its PKI Standards described in the document entitled "NAESB Wholesale Electric Quadrant (WEQ) draft technical standards for Public Key Infrastructure (PKI)."

This assessment was performed by Sandia at the request of the Department of Energy, Fossil Energy. The intent is to provide a surety based analysis of the proposed NAESB PKI standards as they relate to electronic commerce within the Energy industry and to provide guidance for addressing specific security issues now and in future documentation. The assessment provides recommendations on the security of the public key infrastructure for the WEQ. The assessment included research into PKI implementations and general PKI standards to be used in comparison with the NAESB draft PKI Standards.

The cooperation and assistance given to Sandia National Laboratories by NAESB during the assessment was greatly appreciated.

The analysis focused primarily on the security of the PKI protocol that is defined in the standards draft document. Vulnerabilities in the standard were identified and described, with general recommendations for improvement generated. Strengths and weaknesses were also identified. The following strengths of the NAESB draft PKI Standard were recognized:

- The NAESB draft PKI Standard was formatted using the outline in RFC 3647, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework."
- The document included headings for all sections in the outline in RFC 3647, even those that had no content in the body of the section. This is in direct compliance with RFC 3647.
- The document referenced all necessary PKI Standards: NIST SP 800-32, RFC 3280, RFC 3647, and RFC 4210.

The following weaknesses in the security of the NAESB draft PKI Standard were identified:

- The document should be modified so that it is a complete Certificate Policy.
- The NAESB draft PKI Standard does not ensure interoperability with other Federal PKI Standards.
- References to specific key sizes or cryptographic algorithms should not be included in the NAESB draft PKI Standards.
- The NAESB draft PKI Standard does not include specifics about cross-certification issues with other PKI Standards

In addition to analyzing the NAESB draft PKI Standards, the Sandia Team also reviewed the two related documents, "NAESB End-Entity Declaration for Public Key Infrastructure" and the "NAESB Qualifying Relying Party Declaration for Public Key Infrastructure." Weaknesses and strengths of those documents are identified in the body of this report.

Recommendations for improvement of this standard include:

- Follow the guidelines set forth in the section entitled "Deploying an Agency PKI" in NIST SP 800-32 during the process of developing the NAESB PKI Standard
- Build on the NAESB draft PKI Standard so that it is a complete Certificate Policy
- Ensure interoperability with the Federal PKI Standard to minimize the cost and time spent by Certificate Authorities (CA) wishing to comply with the NAESB draft PKI Standards in order to become Authorized CA's.

In conclusion, the assessment team believes that the NAESB draft PKI Standards can be modified to represent a reliable PKI Standard for transactions within the WEQ.

1. Introduction

This document provides an independent analysis of the draft documents developed by the North American Energy Standards Board (NAESB) related to its PKI Standards described in the document entitled "NAESB Wholesale Electric Quadrant (WEQ) draft technical standards for Public Key Infrastructure (PKI)" and related documents, such as the "NAESB End-Entity Declaration for Public Key Infrastructure" and the "NAESB Qualifying Relying Party Declaration for Public Key Infrastructure".

The Sandia team operated on the principle that an independent analysis should include a comprehensive assessment and suggested improvements, while incorporating surety engineering concepts throughout the study. Surety can be defined as a measure of the assurance of system reliability, safety, security, and control of use, while balancing denial of unauthorized use with assurance of authorized use within the constraints of risk versus cost.

This assessment was performed by Sandia at the request of the Department of Energy, Fossil Energy. The intent is to provide a surety based analysis of the proposed NAESB PKI standards as they relate to electronic commerce within the Energy industry, and to provide guidance for addressing specific security issues now and in future documentation. Recommendations on improving the security of the public key infrastructure for the WEQ are included. Research into PKI implementations and general PKI standards to be used in comparison with the NAESB draft PKI Standards was also performed.

2. North American Energy Standards Board Description

The North American Energy Standards Board (NAESB) is a nonprofit North American industry association whose mission is to "serve as an industry forum for the development and promotion of standards, which will lead to a seamless marketplace for wholesale and retail natural gas and electricity, as recognized by its customers, business community, participants, and regulatory entities". These standards exist to assist the natural Energy industry in improving customer service, enhancing the reliability of natural energy service, and increasing the competitiveness and efficiency of natural energy markets.

3. Objective and Purpose of the NAESB Standards

The evolution of the Internet into the principal medium for electronic communications in worldwide commerce led NAESB to develop standards for the use of the Internet by the Energy industry to transact business. Energy transmission companies have established Internet sites, including server sites for electronic interchange of files and World Wide Web pages to provide information to shippers and other customers. These sites allow service requesters to place orders and receive scheduled quantity reports electronically.

4. Critical Success Factors

Factors, which are critical to the success of these standards, have been identified during analysis of the NAESB PKI Standards. These factors determine whether the NAESB PKI Standards provide a reasonable level of security in electronic commerce for the Wholesale Electric Quadrant. Critical success factors identified include the following:

- All WEQ transactions are completed using the NAESB PKI Standards
- All Certificate Authorities (CA) involved in WEQ transactions become Authorized CA's
- All vendors involved in WEQ transactions own and use a valid certificate issued by a NAESB Authorized CA
- The NAESB PKI Standard is interoperable with the Federal PKI standard allowing cross-certification by the Federal Bridge CA

5. Surety Assessment References

During the investigation phase, the Sandia Assessment Team found the following standards and documents directly relating to the draft NAESB PKI Standard. These documents will be referred to throughout this report. Each document has a link listed as to the online location of the document.

Federal Standards

FIPS PUB 46-3, "Data Encryption Standard (DES)". Oct 1999. This document provides details on the DES and Triple Data Encryption Algorithm, TDEA, encryption standards.

<http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>

FIPS PUB 140-2, "Security Requirements for Cryptographic Modules." Dec 2002. This document provides the requirements on encryption software and hardware.

<http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>

FIPS PUB 197, "Advanced Encryption Standard (AES)". Nov 2001. This document details the current encryption algorithm AES. When this document was released the Triple Data Encryption Algorithm was removed from the list of standards.

<http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

Industry Standards

RFC 2119, "Key Words for use in RFCs to Indicate Requirement Levels." Mar 1997. This document defines common key words such as "MUST", "SHOULD", and "MAY" that appear in most RFCs.

<http://www.ietf.org/rfc/rfc2119.txt>

RFC 3280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile." Apr 2002. Replaces RFC 2459. This document describes in detail the format for a X.509 v3 certificate and for the X.509 v2 CRL format.

<http://www.ietf.org/rfc/rfc3280.txt>

RFC 3647, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework." Nov 2003. Replaces RFC 2527. This document contains a description and template for those writing CP and CPS. The template can also apply to subscriber and relying party agreements.

<http://www.ietf.org/rfc/rfc3647.txt>

RFC 4210, "Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)." Sept 2005. Replaces RFC 2510. This standard describes the PKI protocol and data structures required for PKI management messages. It also includes a small section about PKI security considerations.

<http://www.ietf.org/rfc/rfc4210.txt>

NIST Special Publications

NIST SP 800-32, "Introduction to Public Key Technology and the Federal PKI." Feb 2001. This document includes a general overview of cryptography and PKI concepts. It also includes a description of the Federal PKI. Most importantly it includes all the necessary steps for an agency to develop its own PKI Standard.

<http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf>

PKI Standards Examples

“European PKI (EuroPKI) Certificate Policy.” Jan 2004. This document defines the pan-European public-key infrastructure. This document was created to be consistent with the structure provided in RFC 2527. RFC 3647 replaced RFC 2527 in November 2003 as the standard framework for Certificate Policies and Certification Practice Statements.

http://www.europki.org/ca/root/cps/en_cp.pdf

FAA-STD-045A, “National Airspace System (NAS) Communications Security Protocols and Mechanisms.” Mar 2005. This document contains all requirements for the NAS Communications Protocol. Also included in this document is the NAS PKI.

<http://nasdocs.faa.gov/nasiHTML/FAAStandards/faa-std-045A/faa-std-045A.pdf>

“Higher Education Certificate Policy Statement (HEPKI) Common Policy Framework.” Jul 2000. This document provides a comparison between the HEPKI CP and other commercial CP’s in order to maintain interoperability with other PKI Standards.

http://middleware.internet2.edu/certpolicies/CPFv005.doc_1.doc

“U.S. Patent and Trademark Office (USPTO) Certificate Policy.” This CP states the PKI Standard that the USPTO uses for transactions with patent and trademark applicants. This document explains the USPTO policy regarding use of Electronic Business Center Certificates and identifies pertinent facts concerning the life cycle and attributes of those certificates.

http://www.uspto.gov/ebc/policy_certificate.html

“U.S. Patent and Trademark Office (USPTO) Subscriber’s Agreement.” This agreement describes the responsibilities of USPTO Electronic Business Center users and should be reviewed before registration. This agreement is unique in that subscribers will only use their USPTO certificate to perform business transactions with the USPTO.

<http://www.uspto.gov/ebc/documents/subscribersagreement.pdf>

“X.509 Certificate Policy for the Federal Bridge Certification Authority.” Jan 2006. This Certificate Policy (CP) defines seven certificate policies for use by the Federal Bridge Certification Authority (FBCA) to facilitate interoperability between the FBCA and other Entity PKI domains.

http://www.cio.gov/fpkipa/documents/FBCA_CP_RFC3647.doc

“X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework.” Feb 2006. This document is the policy framework for the PKI component of the Federal Enterprise Architecture. This document describes six specific certificate policies. This document was created to be consistent with RFC 2527. RFC 3647 replaced RFC 2527 in November 2003 as the standard framework for Certificate Policies and Certification Practice Statements.

<http://www.cio.gov/ficc/documents/CommonPolicy.doc>

6. Surety Assessment Analysis and Recommendations

The analysis focused on the North American Energy Standards Board draft PKI Standard. The Sandia Assessment Team recommends that NAESB consider the following modifications to improve this standard.

6.1 Security Issues

Items listed in the following section deal specifically with areas of opportunity for an adversary, someone who has malicious intentions, within the guidelines set forth by the PKI standard. These issues are in order of importance with the highest ranking security issues listed first.

6.1.1 Deploying the NAESB draft PKI Standard

The guidelines set forth in the section entitled “Deploying an Agency PKI” in NIST SP 800-32 should be reviewed and followed in the process of developing the NAESB draft PKI Standard.

Level: High

Analysis: NIST SP 800-32 devotes an entire chapter to explaining the steps an agency should take to deploy its own PKI. A good overview is found on page 38 of NIST SP 800-32 that outlines how an agency should follow the example of the FBCA Certificate Policy and use the standard formats in RFC 3280 which call for a X.509 v3 certificate and a X.509 v2 Certificate Revocation List, (CRL). “In particular, NIST recommends following the FBCA policy and adhering to the federal certificate profile and CRL extensions profile. It would be best if agencies assume that at some point their PKI will cross-certify with the federal bridge CA, therefore coordinating the development of an agency PKI with the FPKISC is highly recommended.”

A general guideline to the major steps include; analyze data and application for your organization, collect sample policies and base standards, draft certificate policies, select PKI product or service provider, develop CPS (Certification Practice Statement), do a pilot, and apply for cross-certification with the FBCA. For more details on these steps, review NIST SP 800-32, chapter 6, entitled “Deploying an Agency PKI.”

Recommendation: The guidelines set forth in the section entitled “Deploying an Agency PKI” in NIST SP 800-32 should be reviewed and followed in the process of developing the NAESB draft PKI Standard.

6.1.2 The Certificate Policy for the NAESB PKI

The NAESB draft PKI Standard should be modified so that it is a complete CP. This document will then be referred to as the “Certificate Policy for the NAESB PKI.”

Level: High

Analysis: The NAESB draft PKI Standard should be a complete CP. Examples of other PKI standards and implementations include the EuroPKI CP, FPKI CP, FBCA CP, USPTO CP, and HEPKI. All these CP’s illustrate the fact that in order to create a PKI Standard, it is necessary to first formalize a CP. This is also explained in NIST SP 800-32 section 6.3, “Draft Certificate Policy(s).” “The first requirement for an agency developing a PKI is to establish appropriate certificate policy(s). An effective strategy is to adapt and reuse existing policies (especially FBCA) to create policy(s) for the agency. Certificate policies should be at sufficiently high level that the policies will not change too frequently.”

RFC 3647, page 16, provides another example of a CP being created to define a PKI. “For example, the Federal Government might define a government-wide CP for handling confidential human resources information. The CP will be a broad statement of the general requirements for participants within the Government’s PKI, and an indication of the types of applications for which it is suitable for use. Each department of agency wishing to operate a certification authority in this PKI may be required to write its own certification practice statement to support this CP by explaining how it meets the requirements of the CP. At the same time, a department’s or agency’s CPS may support other certificate policies.” RFC 3647 goes on to explain the difference between a CP and CPS. “A PKI uses a CP to establish requirements that state what participants within it must do. A single CA or organization can use a CPS to disclose how it meets the requirements of a CP or how it implements its practices and controls. A CP facilitates interoperation through cross-certification unilateral certification, or other means. Therefore, it is intended to cover multiple CA’s. By contrast, a CPS is a statement of a single CA or organization.” RFC 3647 concludes the section entitled “Relationship Between Certificate Policy and Certification Practice

Statement,” by stating “CP’s and CPS’s play a central role in documenting the requirements and practices of a PKI.”

It is strongly recommended that the NAESB draft PKI Standard be rewritten as a CP that refers to the FBCA CP for most of its standard PKI policies. Thus the NAESB draft PKI will only need to include information specific to the NAESB draft PKI policy. This will ensure that the NAESB draft PKI Standard is interoperable with other Federal PKI’s. This will comply with one of the goals of the document as it states in its “Commitment to Open Standards” section, page 4, “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.” Interoperability with the Federal PKI Standard will reduce the cost and time spent by CA’s wishing to comply with the NAESB draft PKI Standards in order to become Authorized CA’s.

Recommendation: The NAESB draft PKI Standard should be modified to be the “Certificate Policy for the NAESB PKI.” This CP should rely on the FBCA CP for all general PKI Standard details. Only PKI details that are unique to the NAESB draft PKI Standard should be included in its CP. This will ensure interoperability with the most common CA’s CP’s, thus keeping the cost and time spend by CA’s who wish to comply with the NAESB draft PKI Standards in order to become Authorized CA’s down to a minimum.

6.1.3 Cross-Certification

The NAESB draft PKI Standard does not address the issues of cross-certification.

Level: High

Analysis: The NAESB draft PKI Standard will need to include specifics about cross-certification with other PKI Standards to ensure that those applying to become Authorized CA’s will not have to adopt this new CP if their current CP is found, through equivalency mapping, to be on par with the NAESB PKI CP. This will reduce the cost and time spent for CA’s to comply with the NAESB draft PKI Standards. Tailoring the NAESB draft PKI Standard to the outline found in RFC 3647 will ensure that cross-certification will be covered in detail. RFC 3647, page 52, ensures that using this outline will facilitate “Comparison of two certificate policies during cross-certification or other forms of interoperation (for the purpose of equivalency mapping).”

Recommendation: The NAESB draft PKI Standard should include cross-certification to reduce the cost and time spent by CA’s that are only changing their CPS to comply with the NAESB draft PKI Standards.

6.1.4 Security of the CA’s signing key

It is extremely important that the CA impose access controls on its signing key. Anyone that has control of the CA’s signing key is able to issue certificates in the CA’s name.

Level: High

Analysis: Section 2.6, entitled “Publication and Repository”, states “The Authorized CA shall not impose any access controls its signing key, CRL’s, and CPS.” Without access controls on the CA’s signing key, any adversary can obtain the key and create certificates in the CA’s name. This would lead to serious dispute on any transactions that have been conducted using any certificate that was issued by the CA. The CA’s certificate would have to be revoked along with any certificates it has issued. The statement could be corrected by substituting “verifying key” for “signing key” as the CA should make its verifying key public. If the CA’s signing key is compromised, all certificates that are issued in the CA’s name must be revoked because one can not prove who issued the certificates.

Recommendation: Wording should be changed to state: “CA’s should not impose any access controls on their verifying key”. Wording should be added to ensure CA’s impose access controls on their signing key.

6.1.5 Certificate Rescission Notices

Notification time periods for certificate rescission notices are too long.

Level: High

Analysis: The “Certification” section of the document on page 3 states, “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.” Considering the extreme case in which the CA’s signing key has been compromised, these time constraints would allow an adversary to issue invalid certificates for up to 30 days. This is approximately a whole month in which many new end entities can be given invalid certificates. These new end entities could then participate in unsecured transactions in the WEQ during this month time-frame. The end entities that hold certificates that were originally issued by the CA will have up to five days of insecure transactions.

Recommendation: In order to protect WEQ from disputable transactions, the time period for NAESB to rescind a CA’s certificate should be changed from 30 days to 24 hours. The FBCA CP, section 4.9.5 entitled “Time within which CA must Process the Revocation Request”, states that for the FBCA, “all revocation requests must be processed within six hours of receipt of request.” The longest timeframe allowed is 24 hours. It is also advisable to provide this notice in an e-mail to reduce transfer time. Also change the time period for the CA to notify its certificate holders of a rescission notice from 5 days to 24 hours. The CRL should be updated as soon as possible in the instance to avoid transaction disputes. If the CA’s signing key has been compromised in this case, the details of the compromise should be protected until the issues have been resolved.

6.1.6 Network Security Controls

Not enough detail in section 6.7 entitled “Network Security Controls” to maintain adequate security of the networks.

Level: High

Analysis: NIST SP 800-32 section 3.2.3, entitled "Physical Architecture", states "It is highly recommended that the major PKI components be implemented on separate systems, that is, the CA on one system, the Registration Authority (RA) on a different system, and the directory servers on other systems." It would be good to add this requirement to the document. NIST SP 800-32 section 3.2.3 also states, "Placing the CA system behind an additional organizational firewall is recommended." This firewall is in addition to the Internet firewall. It will provide protection from both the Internet and from systems in the organization itself. This is another good practice that can be added to the document.

Section 6.7, entitled “Network Security Controls” states “Remote access and connections from remote computers must be limited to only those absolutely necessary, and must be properly authenticated.” It is important to indicate which computers that remote sites will be able to access. Remote sites should only be allowed to access a directory where the public keys or public certificates are held. This can be set up as a border directory by situating the directory at that border of the organization, for example outside the firewall. The main directory server, located in the organizations protected network will periodically update the certificates in the border directory. Those in the organization will use the main directory server and those at remote sites will use the border directory. The border directory is NOT linked in anyway to the CA or the RA, only to the main directory server. For more information on this topic, refer to NIST SP 800-32.

Recommendation: NIST SP 800-32 section 3.2.3 should be reviewed and additional requirements should be added to the section entitled “Network Security Controls.”

6.1.7 References to Key Sizes and Cryptographic Algorithms

The NAESB draft PKI Standard should not include specifics such as key sizes and cryptographic algorithms as these can change frequently and use of an out-of-date algorithm or key size will severely compromise the security of the transactions.

Level: High

Analysis: Sections 6.1.1 and 6.1.5 mention specific algorithms and key sizes. "3DES" is called out in the document as an acceptable encryption algorithm, however this is not the current standard. The standard to replace DES is formally referred to as TDEA, Triple Data Encryption Algorithm, in FIPS PUB 46-3.

However, this was replaced by AES in November 2001. So it is suggested that AES be used for encryption in the PKI Standard.

The document also requires the use of RSA with 1024-bit keys. This is the current acceptable key size. However, the Federal PKI, in the forward of its CP entitled “X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework”, specifically requires the use of at least a 2048-bit key with RSA. So it is strongly suggested that at least a 2048-bit key is used with RSA. However, in the case of the cryptographic algorithm and the key sizes it would be better to not include specifics and to require the CA to be up-to-date with current standards.

Recommendation: All references to specific key sizes and cryptographic algorithms should be removed from the document. Instead the document should require all CA’s use the current standard key sizes and current cryptographic standards and point to where those standards may be identified.

6.1.8 NAESB PKI User Declarations

The NAESB Declarations, “NAESB End-Entity Declaration for Public Key Infrastructure” and the “NAESB Qualifying Relying Party Declaration for Public Key Infrastructure,” lack a section where the PKI user acknowledges that the identity information provided is complete and accurate. The documents do not ensure that important information is not left out.

Level: High

Analysis: The agreements lack a section in which the PKI user acknowledges that the identity information provided is complete and accurate. This section is important because the PKI user needs to be legally bound to their given identity to prevent identity fraud. The declaration also lacks a section in which the PKI user ensures to provide updates to their information if it should change. Without this section there is no legal responsibility for the PKI user to alert NAESB of any change in identity. The USPTO has a good example of a subscriber agreement though the NAESB PKI would need an agreement that is more detailed because this PKI is more involved than the USPTO PKI.

Since an end entity can either be a subscriber or a relying party, by definition in NIST SP 800-32, it is redundant to have both an agreement for an end entity and a relying party. It is suggested that the documents be renamed the “NAESB PKI Subscriber Agreement” and the “NAESB PKI Relying Party Agreement.” This naming convention would be more consistent with industry standards such as the USPTO PKI and RFC 3647.

The agreements should also be expanded to include more details. They should also follow the outline set forth in RFC 3647, section 3.7, “Set of Provisions” so that they thoroughly cover every necessary topic.

Recommendation: The NAESB PKI Declarations need to be modified so that they are consistent with the USPTO PKI and RFC 3647.

6.1.9 Key Pair Generation

References to specific requirements for FIPS PUB 140-2 Level 3 hardware devices will cause this PKI standard to become out-of-date with other standards.

Level: High

Analysis: Section 6.1.1, entitled “Key Pair Generation”, states specific requirements for FIPS PUB 140-2 Level 3 hardware devices. However, the requirements listed are not found in FIPS PUB 140-2. Therefore to remain consistent with the standards, only a reference to FIPS PUB 140-2 Level 3 is needed. The specific requirements can be removed.

Recommendation: All references to specific requirements for FIPS PUB 140-2 Level 3 hardware devices should be removed to remain consistent with the current standard and to sustain this consistency.

6.1.10 Unaffiliated Entities

The NAESB draft PKI Standard refers to unaffiliated entities but does not list the restrictions on their applications or interactions in the WEQ.

Level: High

Analysis: Section 1.3.3, entitled “End Entities” states “Entities or organizations that may require access to applications secured under the WEQ PKI standards, 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 Unaffiliated Entity.” It is not a secure practice to allow WEQ access to an entity who does not qualify as a WEQ participant unless restrictions are made on the entities interactions within the WEQ. It would be best to not allow unaffiliated entities in the PKI Standard. However, if they are necessary, then a list of restrictions on their privileges in the WEQ should be included in this section. A document should also be created named a “NAESB PKI Unaffiliated Entity Agreement” that legally binds the sponsor to the actions of the unaffiliated entity. This agreement must also list the acceptable and prohibited actions an unaffiliated entity can perform in the WEQ.

Recommendation: Unaffiliated entities should be removed from the NAESB draft PKI Standard, or the section referring to them should include restrictions on their interactions in the WEQ. If unaffiliated entities are accepted in this PKI Standard a document entitled a “NAESB PKI Unaffiliated Entity Agreement” should be created to legally bind the sponsor to its entity’s actions.

6.1.11 Certificate Classes

The number of certificate classes is variable and the description of each certificate does not require it to be consistent with the current certificate standards, X.509 v3, as listed in RFC 3280.

Level: High

Analysis: The Sandia Team was told that NAESB would like to change the number of certificate classes from three to one. If this is the final decision, then section 1.2 entitled “Identification” should be modified to be consistent with this decision. One certificate class is currently sufficient for this version of the document. The smaller the number of certificate classes, the less complex this PKI. However, the next version of the document could include another certificate type if need be.

The “Identification” section of the document does not require the certificates to be of the standard certificate type X.509 v3. It is important that this document require standardized certificates, like those found in RFC 3280, so this PKI Standard will be interoperable with global PKI Standards. Interoperability will ensure simpler cross-certification between CA’s.

Recommendation: Modify the document to only allow one certificate class. The document should also state that certificates will be of the type X.509 v3, to ensure interoperability with other Federal PKI standards.

6.1.12 Certificate Protection

End entities are required to protect the privacy of their certificates to a greater degree than necessary to do business.

Level: High

Analysis: Section 1.3.3, entitled “End Entities” states that end entities must have “established a security policy and procedures to protect the privacy and use of all Certificates issued in the name of the end entity.” The end entities’ certificate will be viewed by relying party to prove the end entities identity in a transaction. In this case, the end entity does not need to protect the privacy of the certificate from the relying party because it would then have no way to prove its identity and therefore no transactions would be done. It is possible that the end entity might want to protect its certificate from any entity that has not completed the “End Entity Certification Authority Declaration Agreement.” However, this protection is not necessary considering the certificate does not contain any information that could not be made public.

The end entity is responsible for establishing “a security policy and procedures to protect the privacy and use” of its private key. As would be expected, the integrity of the certificates an end entity owns should always be protected.

Recommendation: Modify the requirement that the end entity needs to protect the privacy and use of all certificates issued in its name and instead indicate the end entity must protect all private keys issued in its name by an Authorized CA and protect the integrity of its certificates.

6.1.13 CRL Issuance frequency, validity period, and availability

The allotted time frames for the CRL updates and validity period are too long. The CRL availability period is too constraining. The CRL will be maintained on a machine that will have to undergo occasional maintenance at which time the machine will have to be off-line.

Level: Medium

Analysis: Sections 4.4.9 through 4.4.11, describe time constraints for CRLs. They state, “An Authorized Ca must ensure that it issues an up-to-date CRL at least every twelve (12) hours. Additionally, the validity period of a CRL shall not exceed 24 hours. An Authorized CA must ensure up-to-date CRL’s are available 24x7x365 and can be downloaded via the HTTP protocol.” NIST SP 800-32, section 4.4.5 “Certificate Revocation”, states “More frequent generation of CRLs will reduce a CA’s transaction and reputation risk exposure.” Therefore, the CA’s should be requested to maintain a CRL that is updated every six hours and the period of a CRL should not exceed twelve hours. As mentioned in FBCA CP, section 4.9.7 “CRL Issuance Frequency”, an emergency CRL should be issued in under six hours in the case of a revoked certificate. This time constraints are generous considering NIST SP 800-32, page 32, states “several technology firms have developed software that allows a repository to search its records for the validity of a single certificate in real time.”

The CRL should not be required to be available “24x7x365”. This is an unreasonable expectation for a CRL that will be stored on a system that will occasionally have to undergo maintenance which will need to be done off-line. This requirement should be changed to state the CRL should be available “24x7x365”, except for occasional, scheduled, time periods for maintenance.

Recommendation: An up-to-date CRL should be issued six hours instead of every 12 hours. The validity period of a CRL should not exceed twelve hours. The CRL should be made available during all business hours and all other times except for the occasional, scheduled, maintenance outages instead of requiring the CRL to be only available “24x7x365”.

6.1.14 Certificate Application Steps

Certification Application steps are not ordered in a way that ensures the highest level of security.

Level: Medium

Analysis: Section 4.1, entitled “Certificate Application” lists the steps an Authorized CA must perform when an applicant applies for a certificate. The section later states, “These steps may be performed in any order that is convenient for the Authorized CA, and does not defeat security, but all steps must be completed prior to certificate issuance.” It is not advisable to allow CA’s to determine the order of the steps that ensures the highest level of security. The steps should be ordered and listed and the CA should follow the approved ordering to prevent security issues. This suggestion is made in light of the following example. Assume the CA initially completed step two and obtained a signed request file. Then the CA stored this file on one of their off-line machines. Next the CA decides to complete step one and establish and record the identity of the applicant. However, before the CA can complete this step, they find that the signed request file they stored contained a virus that destroyed all the files on that machine. Now the CA has no way to know the identity of the adversary that completed the successful attack on their system. This example illustrates the importance of identifying who one is communicating with, before initiating transactions.

Recommendation: The certification application steps should be ordered in a way that the CA establishes the applicant's identity before completing any other steps. These steps should be completed by the CA as ordered in this document.

6.1.15 Tamper-Evident Hardware

References to "tamper-proof" are inconsistent with the terminology in FIPS PUB 140-2.

Level: Medium

Analysis: FIPS PUB 140-2 does not contain any references to "tamper-proof" devices. Therefore, any references to "tamper-proof" should be replaced with "tamper-evident" so as to be consistent with this standard.

Recommendation: All references to "tamper-proof" should be replaced with "tamper-evident" to remain consistent with the terminology in FIPS PUB 140-2.

6.1.16 Obsolete RFC References

RFC references include obsolete standards.

Level: Low

Analysis: RFC 2510 is obsolete with the creation of RFC 4210. RFC 2527 was replaced by RFC 3647. And "NIST 800-32" is formally referred to as "NIST SP 800-32". Making these three changes in the document would greatly improve its readability.

Recommendation: Update the RFC references so they represent the current standards.

6.1.17 Use of the Term End Entity

The term "end entity" is confusing.

Level: Low

Analysis: NIST SP 800-32, section 3.1 defines an end entity as being made up of two subclasses, a certificate holder and a relying party. (For a definition of these terms, see the section of this document entitled "Inconsistent Definitions.") The term "end entity" is only used once in RFC 3647, more common are the terms relying party and subscriber. It is suggested that the term "end entity" be replaced with certificate holder/subscriber or relying party/certificate user where appropriate in the document to avoid confusion. The appropriate definitions should be included for the terms used in the documents "Definition" section.

Recommendation: The term end entity should be replaced with certificate holder/subscriber or relying party/certificate user where appropriate so the document is more consistent with the standards, RFC 3647 and NIST SP 800-32.

6.1.18 Customer Service Center

The NAESB draft PKI Standard demands that the Authorized CA's Customer Service Center be available "24x7x365".

Level: Low

Analysis: Section 4.10, entitled "Customer Service Center", states "Each Authorized CA shall implement and maintain a 24x7x365 Customer Service Center to provide assistance and services to Subscribers and Relying Parties, and a system for receiving, recording, responding to, and reporting certificate problems within its customers." It is unreasonable to expect that any center which relies on computers will be available at all times. There will be times when the systems need to be backed-up or brought down for upgrades. At these times the machines will all have to be off-line. This statement should be reworded to be less rigid.

Recommendation: The Authorized CA's customer service center should be required to be available at all times, except for the occasional, scheduled maintenance times in which it will be off-line for the minimum duration.

6.1.19 Reasonable Practices

References to commercial internet practices are vague.

Level: Low

Analysis: Section 5.2.2 entitled "Number of Persons Required Per Task" refers to "commercially reasonable practices." In the "Summary" section it states "The standards described in this document achieves the level of security commonly used by other industries engaged in commercial activity across the public Internet." It is recommended that the NAESB draft PKI Standard ensure interoperability with other Federal standards. This will ensure that most CA's will have to change as little as possible to comply with the standards if they already comply with the Federal PKI Standards.

Recommendation: All statements referring to commercial practices should be replaced with Federal standards to improve the clarity and ensure maximum interoperability in this PKI Standard.

6.1.20 Consistent Naming Convention for NAESB PKI Standards

Throughout the NAESB draft PKI Standards, the standard is referred to by multiple, different names.

Level: Low

Analysis: In the NAESB draft PKI Standards, the standard is referred to as the NAESB PKI three times and as the WEQ PKI thirteen times. A consistent naming convention should be used.

Recommendation: Replace any references to the WEQ PKI with NAESB PKI to avoid confusion.

6.1.21 Missing Requirement Level Key Words

Common key words in RFC defining requirement levels throughout the PKI Standard are missing.

Level: Low

Analysis: To improve clarity consider including a section at the beginning of the PKI Standard that defines the common RFC requirement levels. The EuroPKI includes this sentence in the beginning of its CP. "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."

Recommendation: Adding a statement about the requirement level key words at the beginning of the document would improve clarity and be consistent with other PKI Standards and RFCs.

6.2 Other Areas for Improvement

The following recommendations are submitted for consideration in the format and layout of the NAESB draft PKI Standard.

6.2.1 Missing Definitions

Many important PKI terms are used, but left undefined. The following definitions should be added to the document in the "Definitions" section on page 5 to ensure that this section is complete. Also the following standard, NIST SP 800-32, should be referenced just prior to this section as section 3.1 from this document is the source of these definitions.

ARCHIVE – A database of information to be used in settling future disputes. The archive stores and protects sufficient information to determine if a digital signature on an "old" document should be trusted.

CERTIFICATE – A digital document that typically includes the public key, information about the identity of the party holding the corresponding private key, the operational periods of the certificate, and the CA’s own digital signature.

CERTIFICATE REVOCATION LIST (CRL) – A list of certificates that have been revoked. This list is usually signed by the same entity that issued the certificates. The list also documents the historical revocation status of certificates.

REPOSITORY – A database of active digital signatures for a CA system. CA’s post certificates and CRLs to repositories. The purpose of a repository is to provide data that allows relying parties to confirm the status of the digital signatures.

6.2.2 Extraneous Definitions

If the NAESB draft PKI Standard will not be implementing cross-certification, then the definitions of a “CA-certificate” and “Issuing/Subject CA”, in the “Definitions” section, page 6, should be removed from the document as they are no longer relevant. However, implementing cross-certification is strongly recommended.

6.2.3 Inconsistent Definitions

In the “Definition” section on page 6, the definition of “Relying Party” is not consistent with its definition in NIST SP 800-32. An end entity can be broken into two subclasses, the relying party and the certificate holder. NIST SP 800-32, section 3.1.4, refers to “relying party” and “certificate holder”, while RFC 3647, page 7, uses the terms “relying party” or “certificate user” and “subject” or “subscriber”. To be consistent with RFC 3647 and NIST SP 800-32, the term should be referred to as “end entity” throughout the document instead of “end-entity” or “End Entity”. The following definitions are direct quotes from NIST SP 800-32, section 3.1.

END ENTITY -- An organization or individual that uses the PKI, but does not issue certificates. They rely on the other components of the PKI to obtain certificates, and to verify the certificates of other entities they do business with.

CERTIFICATE USER/RELYING PARTY – One who relies on the certificate to know, with certainty, the public key of another entity.

CERTIFICATE HOLDER/SUBSCRIBER – One that is issued a certificate and can sign digital documents.

6.2.4 Document Formatting

Sections 1 and 2 on the opening page should not be numbered as sections since these are really just front matter and not part of the document itself. Section 3, entitled “Recommendation” should become the currently empty section 1.1 “Overview”.

7. Summary

The Sandia assessment team conducted an analysis of the NAESB draft PKI Standard and related documents. The cooperation and assistance given to Sandia National Laboratories by NAESB and its members during this part of the assessment was greatly appreciated.

The analysis focused primarily on the security of the PKI protocol that is defined in the standards draft document. Vulnerabilities in the standard were identified and described, with general recommendations for improvement generated. Strengths and weaknesses were also identified. The following strengths of the NAESB draft PKI Standard were recognized:

- The NAESB draft PKI Standard was formatted using the outline in RFC 3647, “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.”

- The document included headings for all sections in the outline in RFC 3647, even those that had no content in the body of the section. This is in direct compliance with RFC 3647.
- The document referenced all necessary PKI Standards: NIST SP 800-32, RFC 3280, RFC 3647, and RFC 4210.

The following weaknesses in the security of the NAESB draft PKI Standard were identified:

- The document should be modified so that it is a complete Certificate Policy.
- The NAESB draft PKI Standard does not ensure interoperability with other Federal PKI Standards.
- References to specific key sizes or cryptographic algorithms should not be included in the NAESB draft PKI Standards.
- The NAESB draft PKI Standard does not include specifics about cross-certification issues with other PKI Standards.

In addition to analyzing the NAESB draft PKI Standards, the Sandia Team also reviewed the two related documents, “NAESB End-Entity Declaration for Public Key Infrastructure” and the “NAESB Qualifying Relying Party Declaration for Public Key Infrastructure.” The following strengths of these agreements were recognized:

- Both agreements require the PKI user agree to be legally bound to their transactions using the certificate they will be issued by an Authorized CA.

The following weaknesses in the security of the agreements were identified:

- The agreements lack a section in which the PKI user acknowledges that the identity information provided is complete and accurate.
- The agreements also lack a section in which the PKI user ensures to provide updates to their information if it should change.
- An end entity can either be a subscriber or a relying party, by definition in NIST SP 800-32. Therefore, having an agreement for an end entity and a relying party is redundant.
- The agreements do not follow the outline set forth in RFC 3647, section 3.7, “Set of Provisions” so that they thoroughly cover every necessary topic.

General recommendations include following the guidelines set forth in the section entitled “Deploying an Agency PKI” in NIST SP 800-32 during the process of developing the NAESB draft PKI Standard.

It is recommended that the NAESB draft PKI Standard be modified so that it is a complete Certificate Policy. Examples of other PKI Standards are listed above in the analysis section. All these CPs illustrate the fact that in order to create a PKI Standard, it is necessary to formalize a CP. This is also explained in NIST SP 800-32 section 6.3, “Draft Certificate Policy(s).”

It is recommended that the NAESB draft PKI Standard be rewritten as a CP entitled the “Certificate Policy for the NAESB PKI,” or some other appropriate name. This CP should refer to the FBCA CP for most of its standard PKI policies.

Once the NAESB draft PKI Standard has been altered to be a CP, using the outline described in RFC 3547, it is recommended that this CP be examined by an independent analysis, which includes a comprehensive assessment with suggested improvements. This analysis will ensure the PKI Standard defined in the CP does not contain any security issues.

8. Conclusion

This report is intended to contribute to the improvement of NAESB draft PKI Standards and was developed with the best information available at the time.

The assessment team believes that the NAESB draft PKI Standards can be modified to represent the beginnings of a viable PKI Standard for transactions within the WEQ. The document is correct in that it follows the outline provided in RFC 3647 for CP's and includes all necessary references to applicable PKI Standards documents. Therefore, headers preceding empty sections in NAESB draft PKI Standard could be filled out to produce a valid CP that would define the NAESB PKI Standard. Another option is for the NAESB PKI CP to reference the FBCA CP for general PKI Standard details, thus allowing the NAESB PKI CP to remove any sections that include this standard information. This would allow the NAESB PKI CP to be a relatively short document that includes only PKI information that is unique to the NAESB PKI and a reference for all remaining material is contained in the FBCA PKI. This option would ensure that the NAESB PKI was always current with the Federal PKI Standards. It would also ensure the NAESB PKI Standard contains the least amount of security issues possible. This allows interoperability with the Federal PKI and any other PKI's that allowed cross-certification with the FBCA.

Appendix A – Abbreviations and Acronyms

AES	Advanced Encryption Standard
CA	Certification Authority
CMP	Certificate Management Protocol
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DES	Data Encryption Standard
DOE	Department of Energy
EuroPKI	European Public Key Infrastructure
FBCA	Federal Bridge Certification Authority
FIPS PUB	Federal Information Processing Standard Publication
FPKI	Federal Public Key Infrastructure
HEPKI	Higher Education Public Key Infrastructure
IDART	Information Design Assurance Red Team
NAESB	North American Energy Standards Board
NAS	National Aerospace System
NIST	National Institute of Standards and Technology
NIST SP	National Institute of Standards and Technology Special Publication
PKI	Public Key Infrastructure
RFC	Request For Comment
RSA	Rivest-Shamir-Adleman
TDEA	Triple Data Encryption Algorithm
USPTO	United States Patent and Trademark Office
WEQ	Wholesale Electricity Quadrant

ⁱ <http://www.naesb.org/aboutus.asp>