Assessment Report of the North American Energy Standards Board Public Key Infrastructure Program

24 June 2019

Prepared for the Department of Energy and

North American Energy Standards Board

Prepared By

Information Design Assurance Red Team
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185

Acknowledgements

This document was prepared for the Department of Energy (DOE), Office of Fossil Energy by a working group of the Information Design Assurance Red Team (IDART™) at Sandia National Laboratories (SNL). The working group had the following members:

Benjamin Anderson, Project Lead
Sandia National Laboratories
Cyber Systems Security R&D
505-844-9345
brander@sandia.gov

Joshua Daley, IDART Analyst
Sandia National Laboratories
Cyber Systems Security R&D

Ryan Kao, IDART Analyst
Sandia National Laboratories
Autonomous Cyber Systems

Marshall Riley, IDART Analyst
Sandia National Laboratories
Cyber Systems Security R&D

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

Rae McQuade, Executive Director
Jonathan Booe, Executive Vice President & Chief Administrative Officer
Caroline Trum, Deputy Director

In addition, the working group would like to thank the following individuals for supporting the IDART working group meeting held at the NAESB Office in Houston on August 3, 2017:

Jim Buccigross, 8760, Inc.
Christopher Freitas, Department of Energy
Lancen LaChance, GlobalSign
Paul Sorenson, OATI
Leigh Spangler, Latitude Technologies

This page intentionally left blank.

Table of Contents

Executive Summary

The North American Energy Standards Board (NAESB) was formed in 1994 with the support of the Department of Energy (DOE). The purpose of NAESB is to streamline transactions in the natural gas and electric industries by developing voluntary standards and model business practices. These standards and practices are used by participants in the wholesale and retail aspects of the gas and electric markets.

This report provides an analysis of the public key infrastructure (PKI) standards developed by NAESB, including a proposed update to the Accreditation Requirements, and a review of the Certification Practice Statements (CPS) for GlobalSign and OATI, which are the NAESB Authorized Certificate Authorities (ACAs).[1,2]

This assessment was executed by the Information Design Assurance Red Team (IDART™) at the request of program manager, Mr. Christopher Freitas, of the Department of Energy (DOE), Office of Fossil Energy, Office of Oil and Natural Gas. The intent is to provide a surety based assessment of the existing PKI standards, the proposed updates to the Accreditation Requirements, and ensure that the ACAs' CPS are in line with NAESB requirements.

The cooperation and assistance given to IDART by NAESB and their partner organizations was greatly appreciated and was critical to making this surety assessment possible.

Overall, the assessment team found that the NAESB PKI standards, and the proposed updates, provide strong assurance that ACAs are operating in a secure manner, and that only authorized organizations and their representatives can obtain NAESB certificates. (Use of the certificates are examined in a separate report.)

The only weaknesses identified by the assessment team regarding the security of the PKI standards are found in the ACA Certification Practice Statements. The following weaknesses were identified:

- CPS contains NAESB specific language that is drawn from NAESB standards, but is not guaranteed to be updated immediately if there is a change in the NAESB standard
- CPS stated audit log retention periods do not enforce full coverage of all assurance levels as dictated by the NAESB standards

The assessment team feels that these weaknesses are a minor concern as major changes to the PKI system are not expected and can be mitigated by minor changes in the CPS.

[1] Systrends is another ACA but processes its certificates through GMO GlobalSign Inc. and was not independently reviewed.

[2] SSL Corp. d/b/a SSL.com was certified as an ACA in July 2018, which was outside the time frame considered in this report.

1 Introduction

The North American Energy Standards Board (NAESB) was formed in 1994 with the support of the Department of Energy (DOE). The purpose of NAESB is to streamline transactions in the natural gas and electric industries by developing voluntary standards and model business practices. These standards and practices are used by participants in the wholesale and retail aspects of the gas and electric markets.

This report provides an analysis of the public key infrastructure (PKI) standards developed by NAESB, including a proposed update to the Accreditation Requirements, and a review of the Certification Practice Statements (CPS) for GlobalSign and OATI, which are the NAESB Authorized Certificate Authorities (ACAs).[3,4] The assessment team used the Information Design Assurance Red Team (IDART™) methodology to conduct the analysis and assessment of the PKI standards and associated documents.[5]

The assessment team operated on the principle that an independent analysis should include a comprehensive assessment and suggested improvements, while incorporating surety engineering concepts throughout the activity. The team defined surety 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 executed by the Information Design Assurance Red Team (IDART™) at the request of program manager, Mr. Christopher Freitas, of the Department of Energy (DOE), Office of Fossil Energy, Office of Oil and Natural Gas. The intent is to provide a surety assessment of the existing PKI standards, the proposed updates to the Accreditation Requirements, and ensure that the ACAs' CPS are in line with NAESB requirements.

This task involved a review of the following NAESB documents:

- WEQ-012 Public Key Infrastructure, Version 003.1
- Accreditation Requirements for Authorized Certification Authorities – February 18, 2014
- NAESB Authorized Certification Authority Process – December 8, 2016

The assessment team also reviewed the proposed updates to the Accreditation Requirements for Authorized Certification Authorities document that were provided on September 07, 2017.

In addition, as a result of the on-site meeting held in August 2017, the assessment team determined that the CPS for the ACAs should also be reviewed as part of this activity. The ACA documents reviewed by the assessment team were:

- GlobalSign Certification Practice Statement v8.6, December 15, 2017
- OATI webCARES Certification Practice Statement v3.3, October 2017

[3] Systrends is another NAESB ACA but processes its certificates through GMO GlobalSign Inc. and was not independently reviewed.

[4] SSL Corp. d/b/a SSL.com was certified as an ACA in July 2018, which was outside the time frame considered in this report.

[5] Information on the IDART Methodology can be found at: http://idart.sandia.gov/

Note: This report only deals with the establishment of the ACA and the issuance and revocation of certificates. Use of the certificates are examined in a separate report.

2 Objective and Purpose of the NAESB PKI Standards

The increase of electronic communications to conduct commerce requires mechanisms to support authentication, identification, and non-repudiation to ensure that there is some assurance that all entities are who they claim to be, and that their actions cannot be denied. One method to provide these mechanisms is through the use of public key infrastructure (PKI), where a certificate authority provides End Entities with certificates that identify who the entity is, and binds a public key to that identity.

The NAESB WEQ has developed Business Practice Standards and an Accreditation Specification to establish a secure PKI. These standards and specifications:

- Identify the process that is used by NAESB to certify an ACA, and how the ACA maintains that certification
- Provides the technical and administrative details that a certificate authority is required to meet, and comply with, to be a NAESB ACA
- Identify the requirements for an End Entity to achieve compliance with NAESB business practices

Combined, these standards and specifications define a minimum level of authentication and identification in support of Internet data transfers.

3 Critical Success Factors

Factors which are critical to the success of the PKI business practices and standards were identified during the analysis of the documents listed in Section 1. These factors are crucial in determining if the NAESB PKI Standards provide a reasonable level of surety in conducting transactions in the Wholesale Electric Quadrant. Critical success factors identified include the following:

- All ACAs operate in good faith when it comes to meeting NAESB requirements to establish and maintain their accreditation
- ACAs operate in accordance with their CPS including requirements for issuing certificates, revoking certificates, notification processes and procedures, and maintaining the security of their own systems
- ACA CPS verbiage meets or exceeds NAESB requirements
- End Entities operate in good faith when it comes to meeting their obligations as defined in NAESB standards and business practices
- End Entities use appropriate cyber security practices within their organizations to protect their private keys
- All WEQ-012 applications accept legitimate users that present a valid and appropriate certificate from an ACA.

4 Metrics of Importance

Metrics should be collected and analyzed to measure how the implementation of the PKI program increases the security and reliability of electronic data exchanges between trading partners. The following are some examples of metrics related to the PKI program that could be collected for NAESB and industry partners:

- Measure overall ACA activity including the number of new or renewed certificates issued, number of rejected requests, number of certificate revocations, and number of security anomalies[6]
- Measure the best, median, average, and worst time it takes for an organization to detect, report, notify trading partners and the ACA about a compromised certificate
- Measure the best, median, average, and worst time for an updated revocation list to be issued for a compromised certificate
- Measure an organization's level of compliance with updated revocation lists (i.e. – Are they checking for an updated revocation list with each transaction, or are they using some other time period)
- Measure the number of certificate compromises per organization
- Time for an ACA to issue a new certificate if the previous certificate was compromised

For the ACA metrics, NAESB could incorporate these statistics into required reporting during the annual ACA recertification process. For other organizations, these statistics could be self-reported – either to NAESB or maintained on a statistics webpage. If desired, NAESB could collect and tabulate the totals annually and then share the information with participating organizations. If necessary, data could be anonymized while still allowing organizations to rate their own performance against the industry norms.

This data could then be used in life-cycle decisions, trading partner selection, or determining if NAESB standards need to be upgraded or revised.

5 Surety Assessment Research

Research of the NAESB PKI Standards began with the assessment team reviewing the following NAESB documents:

- WEQ-012 Public Key Infrastructure, Version 003.1
- Accreditation Requirements for Authorized Certification Authorities – February 18, 2014
- NAESB Authorized Certification Authority Process – December 8, 2016

The assessment team also reviewed the proposed updates to the Accreditation Requirements for Authorized Certification Authorities document that were provided on September 07, 2017. The team did

[6] A security anomaly would be anything unusual enough, or serious enough, to be noted. For example, a known criminal organization attempting to obtain a certificate.

not examine the results from the 2006 PKI assessment until after they completed the review of the above documentation.

In addition, as a result of the on-site meeting held in August 2017, the assessment team determined that the CPS for the ACAs should also be reviewed as part of this activity. The ACA documents reviewed by the assessment team were:

- GlobalSign Certification Practice Statement v8.6, December 15, 2017
- OATI webCARES Certification Practice Statement v3.3, October 2017

These Standards also reference multiple government and industry documents, including NIST SP 800-32, and SP 800-63; and Internet Engineering Task Force Requests for Comment documents RFC 3280, 3647, 4210, 5280. These, and other reference documents were reviewed by the assessment team to provide context for the information in the NAESB Standards.

From a high-level view, the assessment team found that the processes for establishing an ACA, and for the issuance of certificates, follows industry best practices and provides a high degree of surety that the organization receiving the certificate is the appropriate organization/representative. The team did find a few specific areas where an issue is present; however, the team determined these were minor and unlikely to occur. These issues are detailed in the following section.

6 Surety Assessment Analysis and Recommendations

This analysis focused on the establishment and maintenance requirements for an ACA, and on the requirements for issuance of a certificate to an organization/representative. The assessment team recommends that NAESB work with their ACAs to address the findings listed in this section.

6.1 Security Issues

Items listed in this section deal specifically with vulnerabilities that could provide an opportunity to an attacker wishing to conduct malicious activities that would affect the establishment or maintenance of an ACA and the issuance and revocation of certificates.

For the level of severity: A HIGH value represents a systemic weakness which could allow an adversary to directly and/or covertly conduct malicious activity. A MODERATE value represents a weakness which could allow an adversary to conduct malicious activity and cause considerable degradation of operations. A LOW value represents a weakness which could allow an adversary to conduct malicious activity and cause targeted or limited impact on the mission.

6.1.1 Discrepancy Between NAESB Standards and Certification Practice Statements

Language differences between the NAESB standards and CPS allow for a window of time where the CPS does not match the NAESB requirements and could result in non-compliant certificate operations.

Level: LOW

Analysis: The GlobalSign and OATI CPS's include NAESB specific language that is drawn from various NAESB standards. For example, the GlobalSign CPS includes text regarding the NAESB Authentication Requirements; and the OATI CPS includes text regarding cases where a certificate can be revoked. However, Section 1.5.4 *CPS Approval* Procedures of the GlobalSign CPS indicates the CPS will be updated on an "as needed" basis; and Section 2.3 *Certification Practice Statement Management* of the OATI CPS indicates it will be reviewed "at least annually and updated as necessary to reflect changes to applicable industry standards."

Recommendation: The ACAs should include verbiage in the CPS that indicates a mismatch between the CPS and NAESB standard will default to the NAESB standard. Alternatively, the CPS could be updated to reference the appropriate NAESB standard(s) instead of including the language directly in the CPS.

6.1.2 Possible Incomplete Enforcement of NAESB Standards Assurance Levels

CPS stated audit log retention periods do not enforce full coverage of all assurance levels as dictated by the NAESB standards.

Level: LOW

Analysis: The GlobalSign CPS indicates that they retain audit logs for a period of "at least 10 years" (Section 5.4.3 *Retention Period for Audit Log*). This length of time meets the NAESB requirements for "Rudimentary", "Basic", and "Medium" assurance levels found in Section 4.5.2 of the *NAESB Accreditation Requirements for Authorized Certification Authorities*; however, the retention period for the "High" assurance level is given as 20 years. Since NAESB tools only requires a certificate at the "Basic" assurance level, it is unclear if "High" assurance level certificates have been issued.

Recommendation: Investigate if "High" assurance level certificates have been issued and review if there needs to be changes to the retention period in either the NAESB standard, or in the GlobalSign CPS. (Note: Section 4.4 *Records Retention Policy* of the OATI CPS indicates records will be retained for "time periods required by applicable standards".)

6.2 Strengths of the NAESB PKI Standards

This section details areas that the assessment team identified as practices or requirements that prevent or increase the difficulty of a successful attack or exploitation by an adversary. These are specifically enumerated to ensure that such practices are continued as the target system evolves.

6.2.1 Updated Verbiage to Utilize Latest Version of a Standard

In the updates to the ACA Accreditation Requirements, the document has been modified to refer to the "current version" of applicable standards. This ensures that modifications to the referenced government and industry standards are automatically included in the NAESB standard.

6.2.2 Elimination of Redundant/Unnecessary Conditions

In the updates to the ACA Accreditation Requirements, in the circumstances for certificate revocation, one circumstance was removed, which was revocation of a certificate at the recommendation of NAESB. Since the ACAs already allow outside agencies to recommend revocation due to questionable activity,

this is a redundant circumstance. Removal of these conditions simplifies the updating and maintenance of this standard.

6.3 Review of X.509 Security

This section addresses a request from the NAESB Critical Infrastructure Committee regarding the security of X.509 certificates.

The assessment team examined the Common Vulnerabilities and Exposures (CVEs) published in NIST's National Vulnerability Database (NVD) for calendar years 2017 and 2018 and did not find any vulnerabilities that were in the X.509 standard. The vulnerabilities listed in the NVD affected specific implementations of X.509 functionality in various software packages but did not exist in the X.509 standard itself. The CVEs examined by the assessment team, and the affected technologies, are listed in Appendix B.

Recommendation: The assessment team recommends NAESB review the industry sources such as NIST NVD, ICS-CERT, US-CERT, SANS common weakness enumeration as part of their annual assessment and consider adding verbiage for organizations that rely on X.509 certificates review their systems and software to determine if they are utilizing technologies that are affected by these vulnerabilities (or any others) and update their systems and software to a version that is not affected. As included in the Wholesale Gas Electronic Delivery Mechanism Related Standards and incorporated by FERC in 18 CFR 284.12, updating to the latest versions of available protocols as soon as practicable and not to exceed 9 months is a general best practice that organizations within the wholesale electric quadrant and users of X.509 certificates should also follow. NAESB may want to consider the development of similar wholesale electric business practice standards. Additionally, specific details on individual CVEs can be found in NIST's NVD along with "References to Advisories, Solutions, and Tools" for each CVE.[7]

7 Summary

The assessment team conducted an analysis of the NAESB PKI Program, which included the following documents:

- WEQ-012 Public Key Infrastructure, Version 003.1
- Accreditation Requirements for Authorized Certification Authorities – February 18, 2014
- NAESB Authorized Certification Authority Process – December 8, 2016
- Updates to the Accreditation Requirements for Authorized Certification Authorities document – provided on September 07, 2017
- GlobalSign Certification Practice Statement v8.6, December 15, 2017
- OATI webCARES Certification Practice Statement v3.3, October 2017

The cooperation and assistance given to IDART by NAESB and their partner organizations was greatly appreciated and was critical to making this surety assessment possible.

[7] https://nvd.nist.gov/

The analysis showed that the NAESB PKI Standards, and the proposed updates, provide strong surety that ACAs are operating in a secure manner, and that only authorized organizations and their representatives can obtain NAESB certificates. The only issues identified by the assessment team were related to the ACA Certification Practice Statements.

The following strengths of the NAESB Standards were identified:

- Verbiage to utilize the latest version of a Standard
- The elimination of redundant/unnecessary certificate revocation conditions

The following weaknesses in the security of the PKI Program were identified:

- CPS contain NAESB specific language that is drawn from various NAESB standards, but is not guaranteed to be updated immediately if there is a change in the NAESB standard
- CPS stated audit log retention periods do not enforce full coverage of all assurance levels as dictated by the NAESB standards

Overall, the assessment team feels that these vulnerabilities are a minor concern as major changes to the PKI standards are not expected, and these vulnerabilities can be mitigated by minor changes in the CPS.

8 Conclusion

This report is intended to contribute to the improvement of NAESB PKI Standards and identify any vulnerabilities that could pose a risk to the PKI program. The report was developed with the best information available at the time of the assessment.

Overall, the assessment team found that the NAESB PKI standards, and the proposed updates, provide strong assurance that ACAs are operating in a secure manner, and that only authorized organizations and their representatives can obtain NAESB certificates. (Use of the certificates are examined in a separate report.) However, the team recommends that NAESB work with their ACAs to address the issues discussed in Section 6 since, while minor, they could still result in an ACA being out of compliance with NAESB requirements.

It is also important to note that the assessment team did not identify other areas of concern where incremental improvements to an attacker's tools, techniques, and procedures would allow them to compromise the PKI Program. While it is impossible to determine what new capabilities an attacker might develop, the assessment team is confident that it would require great effort for an attacker to use the PKI Standards as an attack vector on the WEQ.

9 Appendix A: Abbreviations and Acronyms

ACA	Authorized Certificate Authority
CA	Certification Authority
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CVE	Common Vulnerabilities and Exposures
DOE	Department of Energy
FE	Office of Fossil Energy
IDART	Information Design Assurance Red Team
IETF	Internet Engineering Task Force
NAESB	North American Energy Standards Board
NIST	National Institute of Standards and Technology
NIST SP	National Institute of Standards and Technology Special Publication
NVD	National Vulnerability Database
PKI	Public Key Infrastructure
RFC	Request for Comment
SNL	Sandia National Laboratories
WEQ	Wholesale Electric Quadrant

10 Appendix B: X.509 Common Vulnerabilities and Exposures (CVEs) Reviewed

This table is taken as a capture for example of the listings returned from the NIST NVD database published in 2018 when searched for vulnerabilities associated with X.509. The dates listed in the vulnerability ID field do not necessarily reflect the date that a specific vulnerability was published in the database, the CVE vulnerability ID data indicates when the vulnerability was initially reported in some cases, there may be a delay between identification and publication in the database.

Table 1: X.509 Related CVEs Published 2017-2018

Vulnerability ID	Applicable Technology
CVE-2018-16395	OpenSSL library in Ruby before 2.3.8, 2.4.x before 2.4.5, 2.5.x before 2.5.2, and 2.6.x before 2.6.0-preview3
CVE-2018-16253	axTLS version 2.1.3 and before
CVE-2018-16150	axTLS version 2.1.3 and before
CVE-2018-16149	axTLS version 2.1.3 and before
CVE-2018-1000807	pyopenssl version prior to version 17.5.0
CVE-2016-1000030	Pidgin version <2.11.0
CVE-2017-6143	F5 BIG-IP 12.0.0-12.1.2, 11.6.0-11.6.2, or 11.5.0-11.5.5
CVE-2018-8970	LibreSSL 2.7.0 before 2.7.1 (Potentially BoringSSL, as well)
CVE-2018-1000140	rsyslog librelp version 1.2.14 and earlier
CVE-2017-6142	F5 BIG-IP Advanced Firewall Manager versions 13.0.0, 12.1.0-12.1.2, and 11.6.0-11.6.2
CVE-2017-15088	MIT Kerberos 5 (aka krb5) through 1.15.2
CVE-2013-4366	Apache HttpClient 4.3.x before 4.3.1
CVE-2015-5327	Linux kernels 4.3-rc1 and after
CVE-2017-7521	OpenVPN versions before 2.4.3 and before 2.3.17

CVE-2017-2782	InsideSecure MatrixSSL 3.8.7b
CVE-2017-2781	InsideSecure MatrixSSL 3.8.7b
CVE-2017-2780	InsideSecure MatrixSSL 3.8.7b
CVE-2017-9023	strongSwan before 5.5.3
CVE-2017-2801	Randombit Botan cryptographic library version 2.0.1
CVE-2017-2800	wolfSSL through 3.10.2
CVE-2017-2784	ARM mbed TLS before 1.3.19, 2.x before 2.1.7, and 2.4.x before 2.4.2
CVE-2016-6879	botan 1.11.x before 1.11.31
CVE-2017-5334	GnuTLS before 3.3.26 and 3.5.x before 3.5.8
CVE-2016-6892	MatrixSSL before 3.8.6

11 Appendix C: Relevant Document Summary Table

This section summarizes the documents, standards, or business practices – and the relevant section(s) – where any identified issues are located. Also included is a column with the corresponding section from this report that discusses the identified issue.

Relevant Source Document	Relevant Section	Location in This Report
GlobalSign Certification Practice Statement v8.6, December 15, 2017	**Section 1.5.4**: CPS Approval Procedures	Section 6.1.1
OATI webCARES Certification Practice Statement v3.3, October 2017	**Section 2.3**: Certification Practice Statement Management	Section 6.1.1
GlobalSign Certification Practice Statement v8.6, December 15, 2017	**Section 5.4.3**: Retention Period for Audit Log	Section 6.1.2