

**North American Energy Standards Board**

**Request for Initiation of a NAESB Business Practice Standard, Model Business Practice or  
Electronic Transaction**

**or**

**Enhancement of an Existing NAESB Business Practice Standard, Model Business Practice or  
Electronic Transaction**

**Instructions:**

- 1. Please fill out as much of the requested information as possible. It is mandatory to provide a contact name, phone number and fax number to which questions can be directed. If you have an electronic mailing address, please make that available as well.**
- 2. Attach any information you believe is related to the request. The more complete your request is, the less time is required to review it.**
- 3. Once completed, send your request to:**  
Rae McQuade  
NAESB, President  
801 Travis, Suite 1675  
Houston, TX 77002  
  
Phone: 713-356-0060  
Fax: 713-356-0067

**by either mail, fax, or to NAESB's email address, [naesb@naesb.org](mailto:naesb@naesb.org).**

**Once received, the request will be routed to the appropriate subcommittees for review.**

**Please note that submitters should provide the requests to the NAESB office in sufficient time so that the NAESB Triage Subcommittee may fully consider the request prior to taking action on it. It is preferable that the request be submitted a minimum of 3 business days prior to the Triage Subcommittee meetings. Those meeting schedules are posted on the NAESB web site at [http://www.naesb.org/monthly\\_calendar.asp](http://www.naesb.org/monthly_calendar.asp).**

## **North American Energy Standards Board**

**Request for Initiation of a NAESB Business Practice Standard, Model Business Practice or  
Electronic Transaction**

**or**

**Enhancement of an Existing NAESB Business Practice Standard, Model Business Practice or  
Electronic Transaction**

Date of Request: 11 April 2011

**1. Submitting Entity & Address:**

North American Energy Standards Board  
Critical Infrastructure Committee  
801 Travis, Suite 1675  
Houston, TX 77002

**2. Contact Person, Phone #, Fax #, Electronic Mailing Address:**

Name : Jesse D. Hurley  
Title : Chairman, Critical Infrastructure Committee  
Phone : (713) 356-0060  
Fax : -  
E-mail : naesb@naesb.org

**1. Title and Description of Proposed Standard or Enhancement:**

**Title:**

**Authorized Certification Authority Standard and Credentialing Practice**

**Description:**

Recent vulnerabilities, systemic flaws, emerging threats, and attack methodologies that expose critical infrastructure and business transactional information technology assets to high risk of compromise because of inconsistent or inadequate security technology deployment and business practices by certification authorities has prompted an examination of the validity and usefulness of having multiple certification authorities act competitively in serving critical infrastructure constrained markets. Upon inspection, it is clear that having multiple certification authorities serve as authorized certification authorities as defined by the WEQ Standards for PKI in WEQ Version 2.1 Section 012-0.2, necessarily exposes market participants to unbounded critical risks and materially degrades market integrity. This request for standards development examines the evidentiary basis for this finding, and proposes changes to the WEQ PKI standard to expeditiously address this issue in a manner that enhances

transparency of authorized certification authority operation, promotes fairness among market participants, and improves security posture in the dynamically changing context of contemporary cybersecurity threats.

**4. Use of Proposed Standard or Enhancement (include how the standard will be used, documentation on the description of the proposed standard, any existing documentation of the proposed standard, and required communication protocols):**

Introduction

The proposed Authorized Certification Authority Standard would mandate a “single CA” structure to ensure verifiable adherence by the Authorized Certification Authority to the appropriate level of performance, emphasizing reasonability, uniformity, and auditability of authorized certification authority conduct as is expected by the market. This proposed standard modifies the current standard wherein the present practice is to permit multiple certification authorities to be credentialed as an Authorized Certification Authority, and replaces the current, vulnerable model with a resilient and defensible framework that holds a single Authorized Certification Authority to a significantly elevated standard of review. In this regard, unprecedented and extremely stringent procedural and structural safeguards are detailed in the proposed standard so as to limit exposure of market participants to inappropriate or inadequate conduct by the Authorized Certification Authority. .

The proposed Authorized Certification Authority Standard is attached as Attachment A to this request and, upon ratification, would replace in their entirety, WEQ Version 2.1 Section 012-1.3.1 “Certification Authorities” and WEQ Version 2.1 Section 012-1.4.1 “CA Obligations”.

Discussion of Risks; Justifications for Changes

*Lax Practices*

Current information assurance experts have long maintained<sup>1</sup> that lax enforcement of information security practices by certification authorities is responsible for the creation of systemic vulnerabilities where malware can be constructed to circumvent traditional cybersecurity tools, e.g., intrusion prevention, antivirus, intrusion detection and unified threat management services. A prime example of this credible threat is the method of propagation of the Stuxnet vulnerability that is faulted with crippling the control systems for the uranium enrichment infrastructure in the Iranian national nuclear weapons program. The attack vector employed a malicious executable designed to evade detection by antivirus systems by relying on compromised cryptographic keys issued to a legitimate developer of software drivers for Ethernet and network interface card chipsets, namely Realtek® and JMicron®, both of Hong Kong. Improper management, storage and use of subscriber keys and credentials at the targeted manufacturers made it possible to steal or convert their code signing certificates issued by Verisign® on behalf of Microsoft®, enabling the Stuxnet creators to issue malware executables signed with Realtek® and JMicron® certificates. As a result, none of the Stuxnet executables observed in the public domain were traceable by the vast majority of antivirus utilities as the software appeared to be legitimately credentialed as valid drivers by Microsoft. Had Verisign®, Microsoft’s® chosen partner Certification Authority, maintained a Certification Practices Statement and Security Practices Agreement that safeguarded such certificates and had Verisign®, as the CA, vigorously enforced a practice of

assuring policy compliance in subscriber use, such an outcome could have been circumvented.<sup>2</sup> The failure calls into question the practice of credentialing a certification authority where that authority materially fails in its responsibility to protect the integrity of the PKI framework.<sup>3,4,5</sup>

#### *Third Party Responsibility*

The activities of certification authorities can also be compromised by use of downstream agents such as registration authorities (RA) or other service providers such as datacenter owners, operators, or managed security service providers. Most recently, this was demonstrated by a compromise of a major certification authority, Comodo Group. In March, 2011, the certification authority service operated by Comodo was compromised when an Iranian hacker breached the security of a registration authority serving Comodo, and thus enabled the issuance of fraudulent certificates<sup>6</sup>. This type of compromise demonstrates that all parts of the chain of trust must be held to equal standards. In particular, it is now proven that RAs must be held to the same performance requirements as the certification authority's specified standard of care.

Within the PKI framework, the impact of vendors in the security of the supply chain looms large when considering the overall security posture. In a chain of trust, just as with the potential for absolute failure with lax business process, the introduction of vendor hardware and software poses a risk to the certification authority ecosystem. From the manufacturers of physical hardware such as hardware support modules for storing root CA cryptographic keys in a compliant device, to the software vendors "assuring" integrity of keystores in user agents and in fact all software on subscriber devices, all parties participating in the PKI framework are subjected to risk. This risk can be managed and the exposure mitigated by empowering the CA to take swift action when presented with evidence of known security vulnerabilities, particularly when balanced with the interest to ensure the protection of critical infrastructure and key resources. To address this risk, a standard must be enforced for transparency and accountability across CA assets and all elements of the PKI framework from CA through to subscribers as essential to creating a baseline for change management. This orientation will ultimately enable the CA and its framework stakeholders to take appropriate steps to ensure that all systems are properly supported, credentialed, and secured.

#### *Secure Supply Chains & National Security*

Major drivers of risk in the security of supply chains are the point of origin of manufactured hardware and software, as well as the region where support services are performed. In recognition of such risk, certification authorities, their organizational parents, affiliates, joint venture partners, and operating subsidiaries should in all cases be prohibited from entering into corporate relationships with entities and individuals located in or controlled from jurisdictions restricted by US arms trafficking laws; for the same reasons, corporate entities with extant relationships or entanglements with entities or individuals restricted by US arms trafficking laws should be barred from seeking or assuming a role as a certification authority. US federal law prohibits disseminating critical infrastructure information to unauthorized parties, and strictly controls the vendors who may offer hardware and services to countries on restricted registries such as the ITAR list<sup>7</sup> of designated states and foreign nationals maintained by the Department of State Directorate of Defense Trade Controls<sup>8</sup>. To limit exposure of critical infrastructure to national security challenges, including extremely dangerous outside influences, certification should be denied to any entities not fully compliant with the principles outlined above.

A certification authority and its critical infrastructure partners who fail to abide by export policies are or should be at risk for penalty under federal regulations governing critical infrastructure information and the use of restricted services in protection of those systems, e.g., cryptosystems, should restricted third parties be affiliated with or proximate to protected resources.<sup>9</sup> Complaints about the incorporation of hardware, software and services from vendors or joint venture vendors, etc., are not an abstract concern. Recently, Sprint, a US telecommunication services provider, endeavored to contract with Huawei, a Chinese telecommunications gear manufacturer with close and historical ties to China's military, to upgrade its networks' routing and switching infrastructure. Not only was the proposed investment the target of serious Congressional concern and criticism, threatening the full array of Sprint's lucrative US Government contracts, the reputational risk to Sprint with its customers among the Fortune 500 and the threat of enhanced regulation led the company's leadership to reevaluate the cost-benefit analysis of and reverse the proposed purchase from a vendor that was founded by leadership in the Chinese military and financed principally the Chinese government.<sup>10</sup> Nonetheless, such business practices posing a threat to validation of certification authority, much less the national security, would not appear, under the current regulatory framework, to be prohibited.

The deficiency in validation of certification authority business practices can be addressed with a robust framework of auditable compliance and regulatory oversight. As the number of certification authorities rises, the burden of verification and validation of satisfactory practice performance presents a resource challenge when a regulator or group of auditors is required to service the growing pool of authorized certification authorities. Under the new single Authorized Certification Authority model, the chain of trust is unitary and presents a single point of contact for a regulator to reference when working to ensure appropriate compliance levels. This ultimately reduces the cost for downstream consumers as the number of audit actions for the pool decreases proportionately.

#### *Overcoming Challenges*

Comprehensive solutions proposed to address the information assurance deficiencies in existing Authorized Certification Authority business process, are as follows:

1. *Commence Security Audits:* The Authorized Certification Authority must be subjected to annual and spot-check security audits to assess business practice, conformity of process and infrastructural posture with standards requirements, and to enhance the attentiveness of Authorized Certification Authority staff to existing information assurance and protection requirements.
2. *Perform Surety Assessments:* The WEQ PKI standards embodied in Section 012 should be reviewed annually to ensure that the standard is current with the existing state of cybersecurity practice and to assess adequacy of those standards to defend against known threats or high risk attack vectors.
3. *Adopt Executive Attestation Process:* Senior leadership must be held responsible for management of the Authorized Certification Authority and its adherence to the expected standard of care.
4. *Require Continuous Training:* The Authorized Certification Authority must adopt a policy of continuous internal training and external outreach to ensure that staff is properly kept up to date, including a minimum of verifiable hours...

5. *Institute an Indemnification Structure:* The Authorized Certification Authority should cover its customers for incidents caused by the CA's errors and omissions, such coverage should extend to a minimum baseline threshold of \$3MM per year across all incidents, and \$200K per end entity coverage per year, up to the aggregate baseline threshold.
6. *Strengthen Public / Private Partnership:* Regulation and critical infrastructure protection practices are promoting the enhancement of the public / private partnership model for entities that serve critical infrastructure sector functions.
7. *Invest in Cybersecurity and Critical Infrastructure Protection:* The Authorized Certification Authority should demonstrate its commitment to leadership in the protection of the infrastructure held in its trust. A meaningful percentage of the revenues of the Authorized Certification Authority must be invested in research and development activities to promote secure identity frameworks as well as resilient and secure networking, computing, and data storage systems.
8. *Require Compliance Throughout Chain of Trust:* Registration Authorities and other service providers must be held to the same standards as the certification authority to provide an effective and valid chain of trust.

Because of reliance on the integrity of information stored in the Electronic Industry Registry (EIR) under the WEQ Standards, the organization that acts as the EIR Administrator must have an arms-length relationship with Authorized Certification Authority activities, and excluded from acting as the Authorized Certification Authority.

*Technological Incompatibilities per WEQ PKI Standard*

Name Uniqueness (012-1.9.2) makes it impossible to ensure duplicate X.500 namespace collisions will not occur when multiple certification authorities are serving certificates. *No repository synchronization capability presently exists technologically to prevent multiple CAs from issuing duplicate certificates in the context of the globally unique identifier requirement.*

Safeguards and Benefits

The proposed Credentialing Practice will provide a framework to enable NAESB to certify compliance of the Authorized Certification Authority with the requirements embodied in the WEQ PKI Standards. Once certified, the Authorized Certification Authority will be issued an operating license by NAESB, and notice shall be sent to FERC and NERC identifying the Authorized Certification Authority.

The proposed Credentialing Practice is appended hereto as Attachment B to this request, and upon ratification, would establish the process of credentialing under the NAESB PKI Certification Program referenced by WEQ Standard 012-0.2.

**5. Description of Any Tangible or Intangible Benefits to the Use of the Proposed Standard or Enhancement:**

1. Eliminates commoditization of security where excellence in conduct is cannibalized in favor of cost structures.
2. Minimizes the attack surface of the critical infrastructure by centralizing key resources and ensuring a strong chain of trust protection for sensitive assets.
3. Reduces regulatory oversight burden and establishes a clear line of control for federal oversight to promote fairness and transparency.
4. Enables rapid, uniform design and deployment of cybersecurity and information assurance technologies and practices throughout all aspects of the electric sector ecosystem. This approach lowers overall costs to consumers while ensuring the ability to address emerging threats is strengthened.
5. Creates a framework to ensure reasonable pricing charged to the industry because of the requisite pricing analyses and binding voluntary submission by the Authorized Certification Authority to FERC oversight required by the standard.
6. Establishes and promotes evidentiary bases for security mandates issued by the Authorized Certification Authority.
7. Removes the “profitability” disincentive experienced by market participants for cybersecurity enhancements by referencing critical infrastructure improvements to be offset to federal tariffs.
8. Enhances public-private partnership as endorsed by the states and US Government by compelling the Authorized Certification Authority to engage in liaison activities with appropriate cybersecurity and critical infrastructure protection authorities at the federal and state levels, e.g., NERC, DHS, and DOD.
9. Strongly incentivizes the Authorized Certification Authority to promote market integrity as a condition of its singular license, which for the first time would establish a positive financial motive for promoting the security of the electric sector and to defend against foreign and domestic critical infrastructure threats.
10. Eliminates the possibility of foreign influence in the operations and intelligence artifacts generated by the Authorized Certification Authority by barring corporate relationships with companies organized in or controlled by countries enumerated on the ITAR list.

**6. Estimate of Incremental Specific Costs to Implement Proposed Standard or Enhancement:**

None – May actually reduce costs through streamlining processes.

**7. Description of Any Specific Legal or Other Considerations:**

Please consult legal review attached as Schedule D.

**8. If This Proposed Standard or Enhancement Is Not Tested Yet, List Trading Partners Willing to Test Standard or Enhancement (Corporations and contacts):**

Not Applicable

9. If This Proposed Standard or Enhancement Is In Use, Who are the Trading Partners :

Not Applicable

10. Attachments (such as : further detailed proposals, transaction data descriptions, information flows, implementation guides, business process descriptions, examples of ASC ANSI X12 mapped transactions):

**Attachment A: Proposed Authorized Certification Authority Standard**

The standard will be developed collaboratively by the NAESB Critical Infrastructure Committee, the Certification Committee, NERC, and the JESS.

**Attachment B: Proposed Credentialing Practice**

The standard will be developed collaboratively by the NAESB Critical Infrastructure Committee, the Certification Committee, NERC, and the JESS.

**Attachment C: Evidentiary Report**

---

<sup>1</sup> <http://www.schneier.com/paper-pki-ft.txt> Provides an analysis of typical defenses used by substandard or underperforming CA service providers and proposes mechanisms to correct deficiencies.

<sup>2</sup> [http://www.f-secure.com/weblog/archives/Jarno\\_Niemela\\_its\\_signed.pdf](http://www.f-secure.com/weblog/archives/Jarno_Niemela_its_signed.pdf) Questions the lack of vigorous CA inspection of credentials and assesses the risk of “commoditizing” the CA verification process for PKI frameworks.

<sup>3</sup> [http://blogs.cisco.com/security/stuxnet\\_exploiting\\_trust\\_relationships\\_and\\_expected\\_behavior/](http://blogs.cisco.com/security/stuxnet_exploiting_trust_relationships_and_expected_behavior/) Describes Verisign’s<sup>®</sup> and Microsoft’s<sup>®</sup> role in Stuxnet propagation as an example of “chain of trust” failures due to lax practices by a certification authority in conforming to an adequate standard of care.

<sup>4</sup> <http://www.blackhat.com/presentations/bh-usa-09/SOTIROV/BHUSA09-Sotirov-AttackExtSSL-PAPER.pdf> Challenges utility of “Extended Validation” certificates issued by Verisign<sup>®</sup> – resulting in fake credentials being used as trusted and “validated by Verisign<sup>®</sup>”

<sup>5</sup> <http://tools.cisco.com/security/center/viewAlert.x?alertId=18752> Describes a cryptographic weakness in certificates issued by Verisign<sup>®</sup> that enable a malicious third party to present fake credentials as legitimate due to improper use by the certification authority of a compromised hashing algorithm (MD2).

<sup>6</sup> [http://www.wired.com/threatlevel/2011/03/comodo\\_hack/](http://www.wired.com/threatlevel/2011/03/comodo_hack/) This article describes in detail the successful attempt by an Iranian hacker to gain access to privileged resources on Comodo’s secure certification authority network, ultimately enabling the attacker to issue fraudulent certificates that were used in Internet transactions.

<sup>7</sup> [http://www.pmdtc.state.gov/embargoed\\_countries/index.html](http://www.pmdtc.state.gov/embargoed_countries/index.html) Enumerates the countries which are embargoed by the US Government for trade in materials regulated by US export restrictions.

---

<sup>8</sup> <http://www.pmdtc.state.gov/> Identifies the US Government agency office responsible for managing the export controls and corporate relationship structure restrictions for vendors of materials and services that are classified as munitions or of interest to the national defense. Vendors of critical infrastructure services and encryption systems and services are governed by these regulations for restricted foreign trade oversight. Cryptosystems, such as PKI systems and the services that offer them are generally considered munitions under federal law.

<sup>9</sup> <http://www.bis.doc.gov/> Office of the Department of Commerce that enforces export restrictions.

<sup>10</sup> <http://www.ft.com/cms/s/0/a5f99bb2-4699-11e0-967a-00144feab49a.html#axzz1I7zFjKzH> Article describes the demise of the Sprint / Huawei deal.