05/16/2013

**Recommendation from the NAESB PKI Subcommittee Regarding 2013 WEQ Annual Plan Item 4.a.ii**

**Introduction**

This document is prepared by the North American Energy Standards Board (NAESB) Public Key Infrastructure (PKI) subcommittee (“PKI Subcommittee”) to provide analysis regarding issues identified in the Report on Use of NAESB PKI Standards, Docket No. EL12-86-000, issued on August 27, 2012 (“Report”),[[1]](#footnote-2) and to serve as the recommendation to the Wholesale Electric Quadrant (WEQ) Executive Committee (EC) for 2013 WEQ Annual Plan Item 4.a.ii. Specific to the Report, concerns were raised that the lifespan of the root key was too long, which can be seen in the quotes noted and excerpted from paragraph 16:

* “…the 20-year lifetime of the root keys and certificates is too long”
* “…concerned that this time period may present an unacceptable risk of compromise and therefore recommends that NAESB consider this issue through updates in its standards in an expeditious manner.”
* “Such long life spans increase the likelihood of a user’s keys or certificates being compromised.”

The PKI Subcommittee would like to emphasize that the NAESB Accreditation Requirements for Authorized Certification Authorities Specification (“Accreditation Specification”) requirement for a maximum 20 year validity period only applies to certificates and key materials for the highly secure Root Certificate Authority (CA).

The PKI Subcommittee understands the critical importance of strong cyber-security to protect and ensure the wholesale electric market-based transactions and the reliability of the bulk-power system. The PKI Subcommittee takes seriously its charge to develop PKI standards that will provide such protection including the stability in business operations. The PKI Subcommittee has performed extensive review and discussion of the Report and considered the need for additional updates to the WEQ-012 PKI Business Practice Standards and Accreditation Specification. This document sets forth the reasons for the PKI Subcommittee’s recommendation that no changes to the existing lifetime of the root keys and certificates be made at this time. It also provides background on the PKI Subcommittee’s adoption of the WEQ-012 PKI Business Practice Standards and Accreditation Specification, a discussion of the technical parameters of PKI, and how industry best practices were used as a basis to guide the modifications to the WEQ-012 PKI Business Practice Standards that are available now as final actions, and to be published in Version 003.1 scheduled for second quarter 2014.

**Recommendation and Support**

In its review of the Report, the PKI Subcommittee does not recommend any changes to the existing maximum lifetime of the Root Certificate and associated keys for the following reasons:

1. The PKI Subcommittee recognizes that PKI technology is ever changing and evolving; flexibility is needed in order to respond to incorporate new technology as appropriate. To that end, the PKI Subcommittee established the separate Accreditation Specification that can be revised quickly and efficiently to respond to changes in PKI technology. The current structure of separating the technical details in the Accreditation Specification from the actual WEQ-012 PKI Business Practice Standards facilitates the ability of the PKI Subcommittee to modify the accreditation requirements for Authorized Certificate Authorities (ACAs) in the future when appropriate.
2. The PKI Subcommittee thoroughly analyzed and discussed the issue of Root Certificate key lifetimes, as well as other related issues, during the standards drafting process. The PKI Subcommittee spent considerable time across multiple meetings discussing acceptable Root Certificate key lifetimes. As a result of this deliberate review, the language that an ACA “must have a minimum of 10 years with no security breaches to Certificate Authority operations which resulted in compromise of Certificate Authority keys” was added to make sure the security track record of the CA was taken into consideration.
3. The PKI Subcommittee recognizes that responding to cyber-security threats is a matter of critical concern and requires the ability for quick and flexible responses. Regardless of a CA’s Root Certificate key lifetime of 10, 15, 20 years or longer, each CA who has applied for NAESB ACA status has confirmed processes in place to issue new Root Certificates and new root keys in an expeditious manner in response to any verified cyber-security threat or real danger. Knowing that a CA can setup a new Root Certificate should need arise reduces the need for “what if” cyber-security scenarios that speculate on root key compromises in the future.
4. The PKI Subcommittee acknowledges that the 20 year lifetime of Root Certificate keys is a theoretical maximum. The Accreditation Specification establishes that lifetime ceilings cannot exceed this maximum. However, there is no prohibition to retiring Root Certificates and keys earlier than the 20 year lifetime, and the PKI Subcommittee recognizes the strong likelihood that the existing Root Certificates and associated keys will be retired prior to the 20 year expiration date.
5. The WEQ-012 PKI Business Practice Standards and Accreditation Specification require the use of Certificate Revocation Lists (CRLs) in all certificates and thus certificate types (CA, Client and Server) can be revoked and replaced at any time should the need arise.
6. A permanent, recurring agenda item on the NAESB’s Annual Plan is the PKI Subcommittee’s review of the WEQ-012 PKI Business Practice Standard and Accreditation Specification that includes an evaluation of Root Certificate key lifetimes. The annual (at minimum) review will examine the existing WEQ-012 PKI Business Practice Standards and Accreditation Specification in light of new technologies and procedures, and any changes to the threat landscape. A discussion of the known threats and vulnerabilities and the appropriate actions that need to be taken represent a more balanced way of mitigating threats than arbitrarily setting a Root Certificate key lifetime at this time. Furthermore, by establishing these regular reviews, the PKI Subcommittee will more effectively balance the concern for security with the potential disruption of the industry with frequent Root Certificate changes.
7. As explained below, the PKI Subcommittee’s approach takes a more cautious approach than commonly accepted industry best practices used by several federally governed Certificate Policies.

**Background**

NAESB ratified the initial version of the WEQ-012 PKI Business Practice Standards and published them as part of WEQ Version 001 in 2007, which included requirements to develop and implement standards for a Certification Program to review and approve Certification Authorities. The WEQ-012 PKI Business Practice Standards included in WEQ Version 001 also involved the implementation of an electronic registry to identify ACAs and End Entities. The WEQ-012 PKI Business Practice Standards included in WEQ Version 001 also sought a revision of the Business Practices Standards that support OASIS, Electronic Tagging, and other new applications that would benefit from the use of the WEQ-012 PKI Business Practice Standards compliant digital certificates.

FERC incorporated by reference into federal regulations the NAESB WEQ Version 001 Standards in 2008 via FERC Order No. 676-C.[[2]](#footnote-3) The order included the WEQ-012 PKI Business Practice Standards, and FERC coordinately issued FERC Order No. 676-D, clarifying that further explanation and requirements were expected, effectively holding application of the standards in abeyance until such requirements were developed and approved, which occurred with the NAESB accreditation of ACAs.

Throughout 2011 and 2012, the NAESB PKI Subcommittee worked to revise the WEQ-012 PKI Business Practice Standards included in WEQ Version 001 to ensure they are consistent with current technology. In addition to enhanced technical requirements, the PKI Subcommittee split the WEQ-012 PKI Business Practice Standards into two separate but corresponding documents: the WEQ-012 PKI Business Practice Standards and the NAESB Accreditation Specification, both of which are referenced by the Board Certification procedure for ACAs.[[3]](#footnote-4)

1. The WEQ-012 PKI Business Practice Standards establish the obligations for both ACAs and End Entities.
2. The Accreditation Specification describes the technical and procedural requirements a CA must meet in order to qualify as an ACA.

The Board Certification Committee ACA Process ties the documents together and details the process by which a Certificate Authority becomes an ACA.

The new WEQ-012 PKI Business Practice Standards were adopted by the NAESB Executive Committee on August 21, 2012, and were ratified by a near unanimous vote of NAESB members on October 4, 2012. The standards are now considered final actions and will become part of Version 003.1 scheduled to be published in second quarter 2014. A status report on the final actions and the final actions themselves were filed with the FERC on November 30, 2012 and January 29, 2013, respectively.[[4]](#footnote-5) The Accreditation Specification is referenced within but is not part of the set of WEQ-012 PKI Business Practice Standards filed with the Commission. As such, it can be modified independently of the standards, and on an accelerated timeline.

**Identifying Industry Best Practices**

A primary objective of upgrading the WEQ-012 PKI Business Practice Standards was to seek out industry best practices in PKI implementations that had been introduced since the WEQ-012 PKI Business Practice Standards included in WEQ Version 001 was published, and to incorporate such practices into WEQ-012 PKI Business Practice Standards to be included in WEQ Version 003.1 and Accreditation Specification, as appropriate. The PKI Subcommittee identified several robust PKI implementation models used in government and the private sector. Each model had broad overlap in functionality, as recommended by IETF 3764 [1] and similar operational characteristics (e.g. minimum key sizes of 2048 bits beyond calendar year 2010). After careful analysis it was determined that the Federal Bridge Certification Authority Model [2] represented the most appropriate model for the energy industry and was therefore used as the basis for the revised WEQ-012 PKI Business Practice Standards and Accreditation Specification. The operational characteristics for key sizes and lifetimes specified in the WEQ-012 PKI Business Practice Standards to be included in WEQ Version 003.1 and Accreditation Specification were taken directly from the Federal Bridge model. Further support for the key sizes and lifecycle specified in the Business Practice Standards and Accreditation Specification was provided by the National Institute of Standards and Technology Security Publication 800-57 [3].

The PKI Subcommittee also cites Department of Energy Grids CA Certificate Policy and CPS (Section 6.3.2 pg 75) [http://www.doegrids.org/Docs/CP-CPS.pdf [4](http://www.doegrids.org/Docs/CP-CPS.pdf%20%5B4)] that describes certificate validity requirements as follows:

“For CAs that issue end-entity certificates, the lifetime must be no less than two times of the maximum life time of an end-entity certificate and should not be more than 20 years.”

As such, the WEQ-012 PKI Business Practice Standards, and the final actions[[5]](#footnote-6) that will amend WEQ Version 003 when WEQ Version 3.1 is published in second quarter 2014, are consistent with policies defined by the U.S. Department of Energy and the National Institute of Standards and Technology, as well as directions defined by leading international standards bodies.

**Technical Discussion**

The primary purpose of PKI is to encrypt and authenticate electronic data. The PKI lifecycle includes the request, installation, configuration, management and revocation of digital certificates. Authenticating user identities with PKI is the first step in communication between two entities that wish to do business, and is just one of many levels of security used to protect against cyber-security threats (other levels of security, that are outside the scope of this document, include for example username/password policies, network security, robust internal security practices and procedures, etc.).

There are four primary PKI roles:

* “End Entities” (end users via their browsers, email program, etc.) are parties that use digital certificates to prove their identity;
* “Relying Parties”are parties that rely on a certificate and/or a digital signature;
* “Registration Authorities” (RA) are parties that verify the identity of the End Entities, and manage the issuance and revocation of certificates; and
* “Certificate Authorities” (CA) are parties that are trusted to bind the verified identity of the Digital Certificate Owner into a digital certificate via the CA’s digital signing process.

There are also four primary types of digital certificates. Server Certificates are installed on web servers, and are used by websites to prove their identity and to secure and encrypt data. Client Certificates are installed on end user computers and are used to verify an end user’s identity and to secure and encrypt data. Issuing Certificates are used to digitally sign Server and Client Certificates. Finally, Root Certificates are at the top of the PKI “trust chain” and are used to digitally sign subordinate CA Certificates.

The first step in establishing a PKI trust chain is for the CA to create a Root Certificate. The Root Certificate is at the head of the trust chain, and all subordinate certificates issued under the Root Certificate are chained to it. The Root Certificate is generated pursuant to a strict process, typically called a root generation ceremony. The ceremony ensures that the Root Certificate is set up correctly, and with the requisite amount of security and procedural controls to ensure the reliability and integrity of the Root Certificate. The root generation ceremony is carefully documented, multiple personnel are involved, and each with separate and distinct roles with enforced separation of duties.

Root Certificates are physically stored in FIPS 140-2 level 3 hardware security modules. Level 3 modules are designed to prevent unauthorized access, and require multiple personnel to present their independent credentials prior to accessing the Root certificate. Specifically, Level 3 modules include the use of strong enclosures and tamper detection/response circuitry that zeroes all private key material if the covers/doors of the cryptographic module are opened without authorization. In addition, logs of on-line activity are monitored and audited as part of Web Trust audits. The Root key pair and Certificate’s validity period are set during the root generation ceremony. This validity period cannot be changed, although (as discussed below), the Root Certificate and key pair can be retired at any time. The Root key pair includes a mathematically related public and private series of characters called “asymmetric keys.” The public key is made public, while the private key is stored in the FIPS certified storage device. The Root Certificate, which includes its public key, must be disseminated to all End Entities participating in the PKI trust chain. This is a time consuming and intensive process, requiring action by all entities participating in the chain.

Once a Root Certificate is generated, the CA establishes an Issuing Certificate[[6]](#footnote-7) that is chained to the Root Certificate and digitally signed and verified by the Root Certificate. The Issuing Certificate, which is protected by the same FIPS 140-2 level 3 requirements as the Root Certificate. The Issuing Certificate is used to digitally sign, verify and issue Client and Server Certificates to an End Entity or issue additional subordinate CAs if the Root CA Pathlength parameter allows. When an End Entity requests a Client or Server Certificate, a key pair consisting of a public and private key is generated. Both keys are linked to a single End Entity. Public keys are made public, and private keys are kept confidential and always remain with the End Entity. When the End Entity initiates a certificate request from with the CA, the End Entity must present its public key embedded as part of its certificate request. The CA uses the public key to digitally verify the identity of the End Entity. If digital verification is successful a certificate is returned to the End Entity who links it to the private key so it can be used for secure communications. The process the CA uses of comparing the public and private keys is called digital signature verification and if it fails (i.e. if the keys do not match), identify of the End Entity cannot be verified and no certificate is issued. If digital signature verification succeeds, the End Entity is issued a certificate that it can use to securely communicate with other End Entities participating in the PKI trust chain.

Under the revised WEQ-012 PKI Business Practice Standards and Accreditation Specification, new Root Certificates and keys must have validity periods not to exceed 20 years. This designated period is a mandatory ceiling, and does not preclude CAs from retiring Root Certificates prior to the end of the 20 year period. Root Certificates and keys will expire at the end of their respective maximum validity periods. CAs can also retire their Root Certificate and keys at any time prior to the end of the root’s validity period. Client and Server Certificates and keys, by contrast, only have a two year maximum validity period, and will expire automatically at the end of the two year period, and can be revoked at any time prior to their expiration. When a Client or Server Certificate expires or is revoked the End Entity or device using the certificate will be excluded from digital communication with other End Entities in the PKI trust chain (See Figure 1 following).

**Figure 1: Lifecycle of NAESB Keys**



Simply put, in hierarchy of keys, for the NAESB WEQ-012 PKI Business Practice Standards and Accreditation Specification, the Root Certificate validity period cannot exceed 20 years, the Issuing Certificate validity period cannot exceed the Root Certificate validity period, and the Client and Server Certificates validity period and keys cannot exceed 2 years.

**Conclusion**

The PKI Subcommittee appreciates this opportunity to review and provide analysis explaining the existing WEQ-012 PKI Business Practice Standards and the final actions to be applied in the Version 003.1 publication scheduled for release in second quarter 2014. For the reasons stated above, the PKI Subcommittee concludes that the WEQ-012 PKI Business Practice Standards to be included in WEQ Version 003.1 and the Accreditation Specification, including the 20 year maximum lifetime of Root Certificates and keys, sufficiently protects against cyber–security risks by implementing strong procedural and technical controls pertaining to PKI.

The analysis provided and the WEQ-012 PKI Business Practice Standards themselves, accompanied by the Accreditation Specification and the Certificate Authority process, demonstrate a balance of trust and risk. The trust is provided through procedures, key lengths and the key lifespan. The Accreditation Specification is set aside as separate from the standards. The accreditation requirements can be more quickly updated to reflect market conditions and technology changes, to support additional industry business processes as applications of the standards are broadened, to recognize industry accepted changes in cyber-security practices, or to address vulnerabilities that would require quick responses. The standards themselves can be modified in as little as three months if the modifications are well understood, industry supported, and consistent with applicable regulatory practices. The accreditation requirements and the standards will be reviewed by the PKI Subcommittee for modifications on an annual basis unless needed more frequently.

As such, the PKI Subcommittee recommends that no further updates to the current WEQ-012 PKI Business Practice Standards and Accreditation Specification regarding the lifetime of the root keys and certificates are needed at this time. The PKI Subcommittee will, however, remain vigilant of this issue, and will recommend changes at the appropriate future time.

**References**

[1] IETF, RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, which can be accessed from <http://www.ietf.org/rfc/rfc3647.txt>

[2] X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA) Version 2.24 February 25, 2011

[3] NIST Special Publication 800-57 Recommendation for Key March, 2007 Management – Part 1: General (Revised)

[4] Department of Energy Grids CA CP and CPS v3.1

1. Report on the Use of NAESB Public Key Infrastructure Standards, Docket No. EL12-86-000, issued on August 27, 2012 is available at: <http://www.naesb.org/pdf4/update031413w2.pdf> [↑](#footnote-ref-2)
2. The FERC adopted NAESB standards in FERC Order No. 676-C on July 21, 2008 and the order can be accessed from the FERC web site or through this link: <http://elibrary.ferc.gov/idmws/file_list.asp?accession_num=20080721-3055> [↑](#footnote-ref-3)
3. [↑](#footnote-ref-4)
4. North American Energy Standard Board Status Report to FERC Regarding Public Key Infrastructure (PKI) Efforts (Docket No. RM05-5-022), *available at*: <http://www.naesb.org/pdf4/ferc113012_naesb_pki.pdf> (submitted November 30, 2012), and North American Energy Standard Board Report to FERC Regarding Modifications to the Public Key Infrastructure (PKI) Standards (Docket No. RM05-5-022), *available at*: <http://www.naesb.org/pdf4/ferc012913_pki_standards_report.pdf> (submitted January 29, 2013). [↑](#footnote-ref-5)
5. The three final actions that amend Version 003 for the WEQ-012 Standards and related standards are (a) 2012 WEQ Annual Plan Item 4.b, Part 1 - Develop Public Key Infrastructure (PKI) Standards Requirements for e-Tagging (Part 1) - Ratified December 28, 2012: <http://www.naesb.org/member_login_form.asp?doc=fa_weq_2012_ap4b_part1.doc>, (b) 2012 WEQ Annual Plan Item 4.a - Develop Public Key Infrastructure (PKI) Standards for OASIS -Ratified November 28, 2012: <http://www.naesb.org/member_login_form.asp?doc=fa_weq_2012_ap4a.doc>, and (c) 2012 WEQ Annual Plan Item No. 4.c.i-ii/R11014/R11015 (Part 2) Final Action - Ratified October 4, 2012: <http://www.naesb.org/member_login_form.asp?doc=fa_weq_2012_ap4ci-ii_r11014_r11015.doc>. [↑](#footnote-ref-6)
6. Issuing CA certificate may be issued by an intermediate CA signed by the Root CA [↑](#footnote-ref-7)