Draft Version 04/16/2013 – Edited 4-30-13

**Recommendation from the NAESB PKI Subcommittee to the 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-1) and to serve as the recommendation to the Wholesale Electric Quadrant Executive Committee for the 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 WEQ-012 Standards requirement for a maximum 20 year validity period only applies to certificates and key materials for the highly secure off-line (network unattached) 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 Standards. 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 ratification of the WEQ-012 Standards, a discussion of the technical parameters of PKI, and how industry best practices were used as a basis for the WEQ-012 Version 003 Standards and guided the modifications 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 keys and certificates for the following reasons:

1. The PKI Subcommittee recognizes that PKI technology is ever changing and evolving; flexibility is needed to respond to incorporate new technology as appropriate. To that end, the PKI Subcommittee established the separate Accreditation Requirements for Authorized Certificate Authorities (ACA), which can be revised quickly and efficiently to respond to changes in PKI technology. The current structure facilitates the ability of the PKI Subcommittee to modify the Accreditation Requirements for 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 the balance between Root Certificate key lifetimes and corresponding risks. 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 considered before longer key lifetimes were allowed.
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 immediately issue new Root Certificates and new root keys in response to any verified cyber-security threat or real danger. Knowing that a CA can setup a new root key or complete PKI on short notice reduces the need for “what if” cyber-security scenarios which 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 requirements establish that lifetime ceilings cannot exceed this maximum. 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 certificates and keys will be retired prior to the 20 year expiration date.
5. One of the goals of shorter Root Certificate key lifetimes is to reduce the window in which the keys are used to encrypt or sign important or otherwise highly sensitive data. Theoretically, the longer a key pair is used, the higher the probability of a brute force or other type of compromise where previously encrypted data can be unencrypted or previously signed data can be re-signed. However, if the important or otherwise highly sensitive data are in existence for a very short time then this type of vulnerability is significantly less of a concern. Since nearly all certificates issued in the Wholesale Energy Industry are exclusively used for encrypting SSL/TLS session keys, and not for long term encrypting or signing important or otherwise highly sensitive data, the lifetime of a key becomes a less critical factor in the overall security of the PKI.
6. The main vulnerability of longer Root Certificate key lifetimes is Server Certificates being issued from fraudulent Issuer CAs. The PKI Subcommittee realizes that in the past, options to address this were mainly limited to revoking the CA Issuing Certificate and all certificates issued from it. However, newer security measures have been developed to greatly mitigate risks more efficiently. With the creation of “Untrusted” Certificate Stores, and other advances associated with browser provider CA certificates distribution programs, fraudulent certificates can be neutralized within hours across an industry or across the globe. As technology continues to evolve, the PKI Subcommittee will endeavor to explore and implement additional practices and procedures that mitigate security risks with greater efficiency, flexibility and lower impact to the industry.
7. Root Certificates are only used to sign CA intermediate or CA Issuing Certificates which sign Client and Server Certificates of a much shorter duration. Further, the WEQ-012 Standards require the use of Certificate Revocation Lists (CRLs) and thus all certificate types (Root, Client and Server) can be revoked and replaced at any time should the need arise.
8. The PKI Subcommittee plans to recommend adding evaluation of Root Certificate key lifetimes as a permanent, recurring agenda item on the NAESB’s Annual Plan. The review will examine the existing WEQ-012 Standards in light of new technologies and procedures, and any changes to the threat landscape. An annual discussion of the known threats and vulnerabilities and the appropriate actions which 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 annual reviews, the PKI Subcommittee will more effectively balance the concern for security with the potential disruption to the industry with frequent Root Certificate changes.
9. The PKI Subcommittee’s approach follows or takes a more conservative approach than several federally governed Certificate Policies as sited later in this document.

**Background**

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

FERC incorporated by reference into federal regulations the NAESB Version 001 Standards in 2008 via FERC Order No. 676-C.[[2]](#footnote-2) The order included the WEQ-012 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 Authorized Certificate Authorities.

In the past year the NAESB PKI Subcommittee has been working to revise the WEQ-012 Standards to ensure they are consistent with current technology. In addition to enhanced technical requirements, the initial version of the WEQ-012 Standards has been split into two separate but corresponding documents: the WEQ-012 Business Practice Standards and the NAESB Accreditation Requirements for ACAs (“Accreditation Specification”), augmented by the Board Certification procedure for ACAs.[[3]](#footnote-3)

The WEQ-012 Standards form a framework for secure PKI infrastructures in the electric industry for application to wholesale electric market-based transactions. The WEQ-012 Business Practice Standards document establishes the obligations for both Authorized Certificate Authorities and End Entities. The corresponding Accreditation Specification describes the technical and procedural requirements a Certificate Authority must meet in order to qualify as an ACA. A third document, the Board Certification Committee ACA Process, details the process by which a Certificate Authority becomes an ACA.

The new WEQ-012 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-4) The Accreditation Specification is referenced within but is not part of the set of WEQ-012 Business Practice Standards. As such, it can be modified independently of the standards, and on an accelerated timeline.

**Identifying Industry Best Practices**

One of the main objectives in upgrading the WEQ-012 Standards was to seek out industry best practices in PKI implementations that had been introduced since the original WEQ-012 Standards were published, and to incorporate such practices into the WEQ-012 Version 003, 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 WEQ-012 Version 003 Standards. The operational characteristics for key sizes and lifetimes specified in WEQ-012 Version 003 Standards were taken directly from the Federal Bridge model. Further support for the key sizes and lifecycle specified in WEQ-012 Version 003 Standards was provided by the National Institute of Standards and Technology Security Publication 800-57 [3].

The PKI Subcommittee would also like to cite 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 Version 003 Standards, and the final actions[[5]](#footnote-5) that will amend Version 003 when 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 provides security of 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.

There are four primary PKI roles: “Digital Certificate Owners” (end users via their browsers, email program, etc.), and “Relying Parties” (web/application servers, devices, etc.) which use digital certificates to prove their identity; “Registration Authorities” (RA) which verify the identity of the Digital Certificate Owners and Relying Parties, and manage the issuance and revocation of certificates; and “Certificate Authorities” (CA) which are trusted to bind the verified identity of the Digital Certificate Owner or Relying Party into a digital certificate via the CA’s digital signing process.

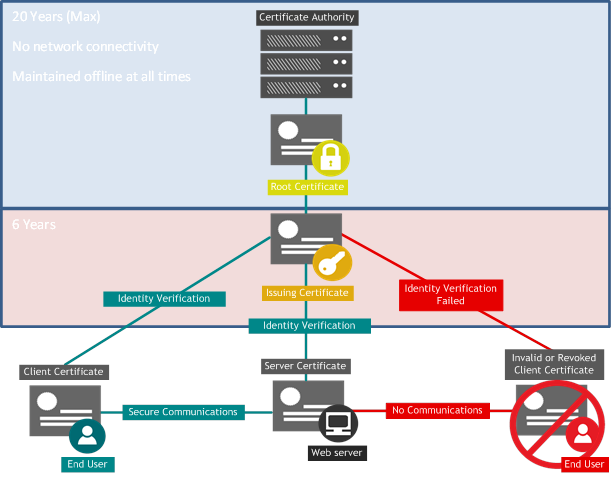
There are also four primary types of digital certificates. Server Certificates are installed on web servers, and are used by websites to prove their identity and to secure and encrypt data. Client Certificates are installed on end user computers and are used to verify an end user’s identity and to secure and encrypt data. CA 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 CA Issuing 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 CAs are secured in FIPS 140-2 level 3 hardware security modules and are difficult for an attacker to access. 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 a special, highly secure 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 intensive process, requiring action by all entities participating in the chain.

Once a Root Certificate is generated, the CA establishes an Issuing Certificate which is chained to the Root Certificate and digitally signed and verified by the Root Certificate. The CA, which is protected by the same FIPS 140-2 level 3 requirements as the Root, then uses the Issuing Certificate 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 communication with the CA, the End Entity must present the public key embedded in 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 of comparing the public and private keys is called digital signing and verification and if it fails (i.e. if the keys do not match), no secure communication link is established.

Under the WEQ-012 Standards, 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 Standards, the Root Certificate validity period cannot exceed 20 years, the Issuing Certificate validity period cannot exceed 6 years, and the Client and Server Certificates validity period and keys cannot exceed 2 years. Subordinate validity periods are, through widely accepted industry practices, at least half the time period of the parent. As such, shortening the periods will have a cascading effect on the subordinates – if the Root Certificate validity period were 10 years, then the Issuing Certificate validity period would be 5 years or less, and the Client and Server Certificates validity period and keys would be 2 years or less, with the added restriction that the Root Certificate Authority could not issue certificates to the issuing Certificate Authority for longer than the life of the Root Certificate, nor could the issuing Certificate Authority issue certificates for longer than the life of the issuing certificate – thus possibly requiring Client and Server Certificates to be issued/reissued every year.

**Conclusion**

The PKI Subcommittee appreciates this opportunity to review and provide analysis explaining the existing WEQ-012 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 current WEQ-012 Standards, including the 20 year maximum lifetime of Root Certificates and keys, sufficiently protect against cyber–security risks by implementing strong procedural and technical controls pertaining to PKI.

The analysis provided and the WEQ-012 Standards themselves, accompanied by the accreditation requirements 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 requirements are 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 Standards 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-1)
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-2)
3. NAESB Authorized Certification Authority Process, *available at*: <http://www.naesb.org/pdf4/certification_process.docx> (adopted September 20, 2012) and NAESB Accreditation Requirements for Authorized Certification Authorities Specification, *available at*: <http://www.naesb.org/member_login_check.asp?doc=certification_specifications.docx> (adopted August 21, 2012) [↑](#footnote-ref-3)
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-4)
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-5)