Federal Energy Regulatory Commission (FERC) Investigation Analysis Report
Summary, analysis and Q/A guide to understanding why FERC initiated and conducted an investigation into electric industry PKI security standards

Table of Contents

Executive Summary

Following 9-11 and the formation of the Department of Homeland Security (DHS), the federal government identified the United States' Critical Infrastructures. Critical Infrastructures are essential to the nation's security, public health and safety, economic vitality, and way of life; they include assets, systems and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof.

Among our nation's Critical Infrastructures is the Energy Sector, which encompasses the national electric power distribution system (power grid) and the physical and virtual systems that contribute to its operations. The U.S. Energy Sector contains more than 6,413 power plants (including 3,273 traditional electric utilities and 1,738 nonutility power producers) with approximately 1,075 gigawatts of installed generation.

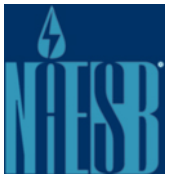
Recent media and industry activity on Capitol Hill has once again brought the Energy Sector into the public spotlight. As a result, there has been a great deal of confusion created regarding the electric grid's strengths and weaknesses and how it is protected against cyberthreats.

To address and dispel misinformation, the Federal Energy Regulatory Commission (FERC), at the request of Sens. Joe Lieberman, I-Conn., and Susan Collins, R-Maine, conducted an investigation into recent allegations that Certificate Authorities (CAs) were placing the Electric Sector in jeopardy by providing digital certificates that did not comply with the North American Energy Standards Board (NAESB) Public Key Infrastructure (PKI) standards. These allegations were proven false.

On August 27, 2012, FERC issued its findings, which concluded that no CAs violated any standards or regulations. FERC further reinforced that allegations claiming the electric sector was in jeopardy due to alleged violations were unfounded. FERC stated: *NAESB standards are aimed at facilitating the security of commercial transactions, and are separate from the obligation of affected utilities under section 215 of the Federal Power Act (FPA) to take steps to ensure the cybersecurity of the bulk-power system.*

This document provides further clarification, insight and understanding of the roles that GlobalSign, CAs and NAESB play in the Energy Sector. Complete with "question and answer" sections, it can be used by any person or entity interested in understanding the relationship between PKI, CAs and electric power providers.

Key Players Defined



About the North American Energy Standards Board:
The North American Energy Standards Board (NAESB) serves as an industry forum for the development and promotion of standards which will lead to a seamless marketplace for wholesale and retail natural gas and electricity, as recognized by its customers, business community, participants and regulatory entities. It is composed of over three hundred corporate members in the energy industry and many more non-member volunteers who contribute to the drafting and adopting of NAESB standards. Within NAESB, the Wholesale Electric Quadrant (WEQ-12) subcommittee is in charge of defining standards for Public Key Infrastructure (PKI) and digital certificates for NAESB member organizations.

About the North American Electric Reliability Corporation:
The North American Electric Reliability Corporation (NERC) is committed to ensuring the reliability of the bulk power system in North America. NERC is a non-government organization which has statutory responsibility to regulate bulk power system users, owners and operators through the adoption and enforcement of standards for fair, ethical and efficient practices.

About the Federal Energy Regulatory Commission:
The Federal Energy Regulatory Commission (FERC) regulates wholesale sales of electricity and transmission of electricity in interstate commerce. It also oversees mandatory reliability standards for the bulk power system. FERC regulates the interstate transmission of natural gas, oil and electricity. FERC is in charge of promoting a strong national energy infrastructure, including adequate transmission facilities. FERC also regulates natural gas and hydropower projects, making sure consumers are obtaining reliable, efficient and sustainable energy services at a reasonable cost through appropriate regulatory and market means.

Defining GlobalSign, PKI and Digital Certificates

1. **What is GlobalSign?**
   GlobalSign is one of the longest-established Certification Authorities (CA) and specialists in PKI deployments and digital certificate security. The company's core function is to verify the identities of machines, people and devices transacting on the Internet, and to act as one of the Internet's most widely accepted third-party trust providers.

   GlobalSign was formed in 1996 as one of the Internet's original trust service providers (technically known as Certificate Authorities). Over the years, GlobalSign has issued millions of trusted digital certificates to people, servers and mobile devices for PKI-enabled solutions and applications.

   GlobalSign digital certificates protect the data and transactions of numerous Fortune 100 companies and governments all around the world. GlobalSign automation technologies allow organizations to transform how they use SSL security across networks and into the Cloud. GlobalSign solutions take the pain out of using cryptography and allow organizations to benefit from secure workflows, increased productivity and the peace of mind.

2. **What is a Certificate Authority (CA)?**
   A Certificate Authority (CA) is an entity that issues Digital Certificates, which are security credentials that authenticate and encrypt Internet communications between devices, servers and humans. CAs also provide portals and Web services to manage the lifecycle of digital certificates. CAs are deemed trusted third parties as they are accepted into, and pre-trusted by, browsers and devices after they show continued compliance to the various industry standards governing trusted certificate issuance, including WebTrust, CA/Forum Baseline Requirements and other specific vertical compliance.

3. **What is a Digital Certificate?**
   Digital certificates are the digital equivalent of a driver's license or any other form of identity issued by a trusted third party. An example of a trusted third-party identity provider is found in the motor vehicle licensing and registration model, which provides drivers licenses and registration certificates that validate identities. Just as physical IDs ensure trust in the real world, digital certificates ensure trust across the Internet, ensuring parties can authenticate to each other and subsequently secure their transactions and communications between servers, systems, machines and humans.

4. **What does a Digital Certificate contain?**
   A digital certificate contains the name of the organization or individual it is issued to, the business address, digital signature, public key, serial number and expiration date. The CA cryptographically binds the data within the certificate to a real-world identity.

5. **What is the responsibility of the Digital Certificate provider for security?**
   Third-party CAs have the responsibility to confirm the identity of the certificate applicant (and subsequently the certificate subscriber) so that people and organizations that rely on the PKI can be assured that Internet communications between devices, servers and humans are secure and trusted.

6. **What is the Public Key Infrastructure (PKI)?**
   A PKI is an all-encompassing term that describes the technology and policy framework that provides and manages digital identities delivered through digital certificates. PKI often refers to the software, hardware, people, policy and communications elements needed to manage the lifecycle of certificates, from application to deployment to renewal.

Defining Why FERC Led an Investigation and Summarizing Conclusions

1. **Why did Sens. Joe Lieberman, I-Conn., and Susan Collins, R-Maine, request a FERC-led investigation?**
   It appears that they may have received false information alleging that some CAs were not meeting cybersecurity standards when it came to issuing Digital Certificates used within the electric industry.

2. **Why would Sens. Lieberman and Collins be involved in this issue?**
   Senator Joe Lieberman is chairman of the Senate Committee on Homeland Security and Governmental Affairs. Senator Susan Collins is a ranking member of the committee.

3. **Why were the Senators concerned?**
   Digital Certificates are vitally important to establishing trust in Internet communications. Attackers have used compromised Digital Certificates to circumvent security measures and access a wide variety of private enterprise and government systems. The Senators were concerned that substandard certificates were being used to protect the security of the electric grid, a part of the Energy Sector, which is recognized by the Department of Homeland Security as a Critical Infrastructure.

4. **Is GlobalSign issuing Digital Certificates being used to protect the electric grid?**
   GlobalSign is not currently issuing any Digital Certificates used to protect the electric grid itself but is working with NAESB to establish standards for Digital Certificates used by electricity wholesalers to secure business applications. It is not yet known if the standards GlobalSign is helping to establish will be used to protect the grid and distributions systems.

5. **What are the standards GlobalSign is helping to establish?**
   The NAESB Wholesale Electric Quadrant (WEQ) WEQ-012 standards are designed to ensure that CAs are working within certain business-practice standards for the issuance of Digital Certificates used to secure electric industry business applications.

6. **Who created the current certification standards?**
   For business applications, pending standards were developed by NAESB and the wholesale electric industry. At the time of the FERC investigation, the WEQ-012 version 3.0 standards governing the use of Digital Certificates to secure business applications such as those used for trading were not ratified, therefore no violations existed. Since then, the ratification process has progressed:

   - On August 21, the NAESB WEQ Executive Committee adopted the WEQ-012 standards recommendation of the PKI Subcommittee.

- The recommended standards were distributed for ratification by the entire NAESB WEQ membership on September 4, 2012. For 30 days following September 4, WEQ members had an opportunity to vote on the standards.

- If approved at the conclusion of the 30-day ratification period, the recommended standards will become a NAESB final action and will be submitted to the FERC.

- If adopted by FERC, the standards will become legally binding.

7. **Has anyone violated NAESB standards that were the subject of the FERC investigation?**
   No, because all the potential certifications and standards are currently pending ratification.

8. **Did GlobalSign participate in the FERC investigation?**
   GlobalSign was 100 percent committed to working with the commission, in conjunction with NAESB, to provide their staff with detailed information on the current standards and to ensure that the information provided to FERC was clear and within the context of the Senators' concerns.

9. **What did FERC conclude as a result of its investigation?**
   The following is an excerpt from FREC's findings, demonstrating that neither GlobalSign nor any CAs violated any NAESB standards related to security of business applications or the electric grid:

   Source:
   REPORT ON USE OF NORTH AMERICAN ENERGY STANDARDS BOARD PUBLIC KEY INFRASTRUCTURE STANDARDS (August 27, 2012)

   The Commission instituted this proceeding to investigate the facts and practices surrounding Certification Authorities' implementation of the NAESB PKI standards. The Commission was investigating allegations that Certification Authorities are issuing certificates that are not compliant with the NAESB PKI standards. Specifically, it had been suggested that entities are issuing certificates without NAESB authorization, without adequate identity authentication, or for too long a duration.

   The *Reporting Order* was issued to determine the nature of any current practices under the NAESB standards and whether the Commission should propose or recommend any changes in applicable law.

   16. While Shift (the accusing entity) raises concerns in its filing, the information received in this proceeding does not provide specific evidence to support the allegations. Thus, we do not believe any further Commission action is warranted on the record here.

   Complete document: http://www.ferc.gov/EventCalendar/Files/20120827175825-EL12-86-000.pdf

10. **When will the standards be finalized?**
    NAESB expects members to ratify the standards on October 4, 2012. Final legalization of the standards is expected by at the beginning of 2013.

11. **What impact do NAESB standards have on electric grid reliability?**
    None. NAESB does not develop standards for the reliability of the electric grid, those standards are developed by NERC. NAESB works with NERC to assure that commercial business practices are complimentary to reliability standards.

How can GlobalSign help?

If you are a Transmission, Generator, Independent Grid Operator / ISO, or market participant in the Wholesale Electric Quadrant (WEQ), GlobalSign can assist with providing a wide range of digital certificates that are compliant with the NAESB standard for PKI; WEQ-012. GlobalSign's NAESB certificates meet the strict requirements as specified in the Authorized CA Accreditation specification required by applications such as Open Access Same-Time Information System (OASIS). As a further benefit, as a pubic Certificate Authority, GlobalSign is uniquely positioned to provide energy sector participants with digital certificates that both meet the strict requirements of WEQ-012, but may also be used in commercial applications that leverage browser and operating trust stores. GlobalSign, an 11-year-old and counting Web-Trust certified Certificate Authority, allows NAESB regulated organizations to rest easy when it comes to issuing and maintaining NAESB compliant digital certificates. GlobalSign's web-based management platform known as Enterprise PKI (ePKI), allows for a quick and easy method to manage the complete lifecycle of multiple digital certificates for the entire organization.

Why choose GlobalSign?

- GlobalSign is an active member of the North American Energy Standards (NAESB) board and is committed to enhancing the security of the electric marketplace by staying in step with the latest in NAESB standard's development.
- History of security innovation and trust: Over 20 million certificates worldwide rely on the public trust provided by the GlobalSign root certificate. The company has been operating a trusted PKI since 1996, and has been WebTrust-compliant for over 10 years.
- Commitment to customer support excellence: You talk to real people when you call GlobalSign.
- Worldwide presence: With GlobalSign technical support offices located around the world, you can expect quicker response times and solutions tuned for your language, region and country.

Call or email GlobalSign today to speak with a specialist who will help guide your organization towards a best-practices-based strategy and provide you with the tools to implement it.

Contact Information

GlobalSign US & Canada	**GlobalSign EU**	**GlobalSign UK**
Tel: 1-877-775-4562	Tel: +32 16 891900	Tel: +44 1622 766766
www.globalsign.com	www.globalsign.eu	www.globalsign.co.uk
sales-us@globalsign.com	sales@globalsign.com	sales@globalsign.com
GlobalSign FR	**GlobalSign DE**	**GlobalSign NL**
Tel: +33 1 82 88 01 24	Tel: +49 30 8878 9310	Tel: +31 20 8908021
www.globalsign.fr	www.globalsign.de	www.globalsign.nl
ventes@globalsign.com	verkauf@globalsign.com	verkoop@globalsign.com

About GlobalSign

GlobalSign was one of the first Certification Authorities and has been providing digital credentialing services since 1996. It operates multi-lingual sales and technical support offices in London, Brussels, Boston, Tokyo and Shanghai.

GlobalSign has a rich history of investors, including ING Bank and Vodafone. The company is now part of the GMO Internet Inc. group of companies. GMO Internet is a public company quoted on the prestigious Tokyo Stock Exchange (TSE: 9449) whose shareholders include Yahoo! Japan, Morgan Stanley and Credit Suisse First Boston.

As leader in public trust services, GlobalSign offers GlobalSign Certificates include SSL, Code Signing, Adobe CDS Digital IDs, Email and Authentication, Enterprise Digital ID Solutions, internal PKI and Microsoft Certificate Service root signing. Our trusted root CA Certificates are recognized by all operating systems, all major web browsers, web servers, email clients and Internet applications, as well as by all mobile devices.

Accredited to the highest standards

As a WebTrust accredited public Certificate Authority, and member of the Online Trust Alliance, CAB Forum and Anti-Phishing Working Group, our core solutions allow our thousands of enterprise customers to conduct secure online transactions and data submission, and provide tamper-proof distributable code as well as being able to bind identities to Digital Certificates for S/MIME email encryption and remote two-factor authentication, such as SSL VPNs.