How PKI Secures Critical Infrastructure Networks against Advanced Attacks

Wholesale Energy Participants Have Shown that Critical Infrastructure (CI) Providers Can Strengthen Cybersecurity by Implementing Standard-Based PKI

GLOBALSIGN WHITE PAPER

Identification of Critical Infrastructures

Following 9/11 and the formation of the Department of Homeland Security (DHS), the federal government identified the United States' Critical Infrastructures (CIs). 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.

The Use of PKI in Securing the Critical Infrastructure

Electric power providers, the wholesale energy market, regulators, and market participants are embracing Public Key Infrastructure (PKI) as a secure, scalable, flexible, and cost-effective method to securely authenticate the many digital identities involved in the wholesale electricity market.

This white paper details how Independent Systems Operators (ISOs), which coordinate, control, and monitor electrical power system operations from state to state, are using PKI based on standards developed by the North American Energy Standards Board (NAESB) to improve security for their cyber-based business processes and transactions. NAESB serves as an industry forum for the development and promotion of standards that will lead to a seamless marketplace for wholesale and retail natural gas and electricity.

It is important to note that although PKI is a robust technology, there is a wide variety of implementation details that can produce either a weak and vulnerable identity management system or a highly secure one. As a result, NAESB has worked with its members to produce a PKI standard that is based on industry best-practices, proven management techniques, and advanced digital-certificate technologies.

This paper will focus on the history of the electric industry, how cybersecurity standards emerged, what those standards are, and how they can be used in other CIs to strengthen security and reduce the risk of harmful cyberattacks.

Critical Infrastructure Cybersecurity Developments

Mounting evidence suggests that cyberthreats to the United States' CIs have increased in frequency or, at the very least, that the number CI providers have reported has increased. As recently as May, major media outlets such as The New York Times reported on the DHS' warning that electric utility grids are "likely" attack targets in the U.S.[1] And in August, National Public Radio (NPR) reported on concerns in Washington about the impact that a cyberattack could have on the power supply.[2]

The truth is, until safe-harbor measures are in place, no one will know the full impact of or the number of attacks to date.

In the wake of an increasing number of cyberattacks designed to disrupt CIs, U.S. providers are stepping up efforts to increase their cybersecurity defenses by formalizing frameworks that emphasize the use of standards, proven best-practices, advanced technologies, and two-way industry-government cyberthreat intelligence sharing.

In the U.S., sectors identified by the DHS as national CIs, which include energy and several others (http://www.dhs.gov/critical-infrastructure-sectors), have been particularly focused on cyber vulnerabilities, as disruption of services or destruction of facilities could have a devastating impact on national economic security, public health, safety, and Americans' general way of life.

The verdict remains out on whether such threats are imminent; however, the current political climate has created enough support for greater government involvement.

President Obama's administration has recognized the need for increased communication between industry and government in terms of sharing unclassified and, where appropriate, classified intelligence about known threats and attacks.

In the Executive Order (EO), Improving Critical Infrastructure Cybersecurity, the Secretary of Commerce directed the National Institute of Standards and Technology (NIST) to lead the effort to develop a cybersecurity framework that would consist of adopting industry best-practices wherever possible. Although use of the framework under the current EO would be voluntary, the industry is expected to implement the standards, methodologies, and procedures outlined through incentives such as reduced liability and, of course, better security. As of this paper, a preliminary draft of the framework includes a compendium with 250 informative references, existing standards, and guidelines, including the Wholesale Electric Quadrant standard for PKI (WEQ-012) NAESB standard.

Recognizing that cybersecurity frameworks have value, electric industry CIs, namely independent system operators (ISOs), have begun to adopt standards for PKI that have been developed by NAESB.

ISOs and Regional Transmission Organizations: Why They Have Chosen Standards

In the late 1960s, the energy industry began to face two primary challenges:

1. How to deal with an unreliable energy supply
2. How to exist in a non-competitive energy marketplace

The New York blackout of 1965 provided the impetus to increase our nation's focus on maintaining a reliable and adequate supply of energy. The incident proved that supply did not always match an insatiable appetite for energy, either because of unstable markets or because of outdated generation, transmission, or distribution systems and processes. By the late 1990s, increased demand and spikes in energy prices led the Federal Energy Regulatory Commission (FERC) to restructure the wholesale electric-power sector with the goal of creating a more competitive wholesale energy marketplace.

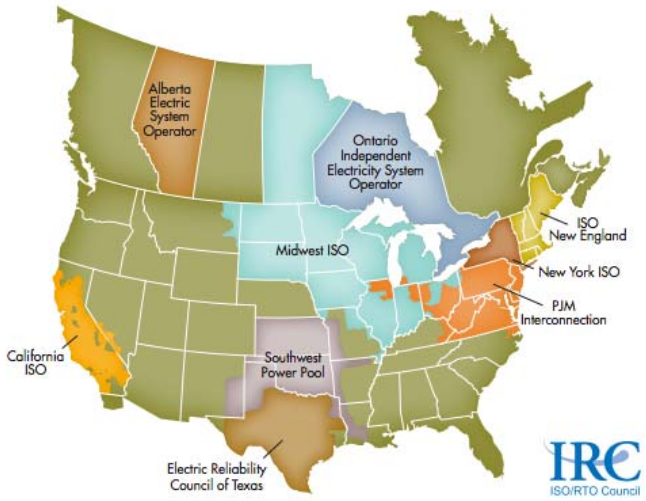
FERC's mandate was to "*operate the transmission systems of public utilities in a manner that is independent of any business interest in sales or purchases of electric power by those utilities*."[3]

Energy generators, transmission providers, and utilities ultimately settled with FERC on a method to provide and manage markets for their given region. The establishment of ISOs and Regional Transmission Organizations (RTOs) were the result of the "Power Pool" participants' proposal to FERC on how best to establish an independent entity responsible for operating a given region's electric grid.

ISOs and RTOs are designed to:

- Coordinate power generation and transmission for their given region
- Control and monitor their regional power-grid transmission
- Coordinate power generation and transmission with other ISOs/RTOs
- Serve as neutral and independent operators for their respective electric markets
- Ensure the safety and reliability of the electric system within their regions
- Be responsible for administering the tariff that facilitates open markets for energy and operating systems
- Be regulated by FERC

The map below shows the ISOs and RTOs operating in North America and their respective territories.



NAESB: Cybersecurity Standards Adoption

As the world advanced into the cyber age, it became apparent that energy supplies and competitive issues were not the only problems ISOs and RTOs had to deal with. Following a series of cyberattacks that attempted (with varying degrees of success) to exploit weaknesses in PKI in order to disrupt power systems, both entities needed to increase focus on cybersecurity.

Key ISO members looked to NAESB as their mechanism to push for enhanced cybersecurity measures. NAESB identified PKI as both a primary line of defense and, if not managed properly, a potential vulnerability. NAESB thus moved to establish and adopt PKI standards.

"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. NAESB works closely with NERC to coordinate the development of business practices and reliability standards for the Wholesale electric industry."

Such a standard was needed, as PKI is a proven security technology and a commercially viable method used to verify identities across untrusted and trusted networks. However, if implemented with outdated cryptographic measures or outsourced critical functions such as identity verification, PKI can produce vulnerabilities that could be exploited. This was proven in some recent, well-publicized Certificate Authority (CA) compromises.

At the urging of key ISO members, NAESB re-convened its PKI subcommittee to revisit the PKI standard for the wholesale energy quadrant (WEQ-012) to include stricter requirements regarding how CAs must deliver and manage digital certificates and supporting CA infrastructure as well as their obligations to users and parties that rely on them.

The updated standard, approved by the NAESB board in November 2012, provides wholesale electric quadrant members higher assurances that the identities of users and systems can be trusted when implemented using the standard.

Today, authorized NAESB CAs issue NAESB-compliant certificates to secure a wide range of applications that support business processes within the wholesale electric industry. In fact, three major business processes that serve the Wholesale Electric Market have incorporated the NAESB standard into their development processes.

1. **Electric Industry Registry**: This is a central repository for commercial industry information that defines the roles played by entities relating to the reservation and scheduling of wholesale power.
2. **e-Tagging**: eTags are used to identify interchange transaction information associated with the physical flow of energy between parties.
3. **Open Access Same-Time Information System (OASIS)**: This internet-based system enables authorized transmission providers to reserve transmission lines to move wholesale electricity

As part of the standard PKI development, NAESB has also adopted an accreditation specification that describes the minimum requirements an authorized CA (ACA) must follow. ACAs must sign affidavits that state they meet the stringent requirements of the accreditation specification as independently verified by a third-party auditor capable of performing a Web-Trust audit or its equivalent. The ACA specification is intentionally separate from the WEQ-012 standard, where it is referenced, to provide maximum flexibility to update as market conditions change. Areas addressed in the specification include:

- Certificate uses
- Assurance levels
- Identity verification
- Certificate life-cycle management
- Facility management
- Operation controls
- Audits
- A wide range of technical and procedural security controls

The graphic below is an illustration of the ACA specification points listed above.

In regards to the WEQ-12 standard referenced above: On July 18, 2013, the International FERC (iFERC) issued a Notice of Proposed Rule Making, FERC Docket No. RM05-5-022, specific to Version 003 of the WEQ standards provided to the Commission on September 18, 2012, and the subsequent updates to the PKI standards submitted by NAESB to the Commission on January 30, 2013. Comments are due to the Commission 60 days after publication in the Federal Register. The NOPR can be accessed from http://www.ferc.gov/whats-new/comm-meet/2013/071813/E-4.pdf, and is summarized in agenda item E-4 in the meeting summary found at http://www.ferc.gov/EventCalendar/Files/20130718100619-summaries.pdf.

Improved Security for All

Through the adoption of these standards, NAESB and its member organizations believe that cyber defenses have been significantly strengthened and that the possibility of a successful attack that could impact the operations or well-being of the nation's electric power supply has been greatly reduced.

"It has become increasingly clear that cybercriminals are targeting the critical infrastructure in an attempt to disrupt our way of life. For this reason, NAESB made it a priority to establish PKI standards to fortify our cybersecurity framework," said Rae McQuade, president of NAESB. "In establishing these standards we hope to provide a strong cybersecurity strategy so that we may best protect the business practices related to the electricity market that is a critical part of the everyday lives of our citizens."

NAESB recognizes the fluidity of cyberthreats and expects the PKI subcommittee to continue to review the ACA specification for areas that might require changes. When such areas are identified, NAESB will make the appropriate changes.

Good for One, Good for All

While most CIs have recognized that they need improved cyber defenses, some have not made the tremendous strides forward that the energy sector has made. In total, there are 16 CIs recognized by the DHS; broken down by sectors, they include: Chemical, Communications, Dams, Emergency Services, Financial Services, Government Facilities, IT, Transportation Systems, Commercial Facilities, Critical Manufacturing, Defense Industrial Base, Energy, Food and Agriculture, Healthcare and Public Health, Nuclear Reactors and Waste, and Water and Wastewater Systems.

All sectors are intricately tied, managed, controlled, and accessible through the world's cyber systems, making all vulnerable to weak IT security and digital forms of attacks. The dynamic nature of cybersecurity standards must be acknowledged in other CI security efforts outside and within the energy sector. Otherwise the possibility of a successful attack that impacts the nation's way of life is certain.

NAESB has demonstrated that cybersecurity standards development can be performed using shared expertise and in concert with the public and private sector. The same can be done for any CI or public or private organization.

Citations:

1. http://www.nytimes.com/2013/05/13/us/cyberattacks-on-rise-against-us-corporations.html?pagewanted=all&_r=0
2. http://stateimpact.npr.org/pennsylvania/2013/08/15/power-companies-weigh-threat-of-cyberattacks-on-electric-grid/
3. www.ferc.gov/legal/maj-ord-reg/land-docs/rm95-8p1-000.txt, Pg 34 UNITED STATES OF AMERICA FEDERAL ENERGY REGULATORY COMMISSION; 18 CFR Part 35 [Docket Nos. RM95-8-001 and RM94-7-002; Order No. 888-A]: "Promoting Wholesale Competition Through Open Access Non-discriminatory Transmission Services by Public Utilities; Recovery of Stranded Costs by Public Utilities and Transmitting Utilities (Issued March 4, 1997)

ABOUT GLOBALSIGN

GlobalSign has been a trust service provider since 1996. Its focus has been, and always will be, on providing convenient and highly productive PKI solutions for organizations of all sizes. Its core Digital Certificate solutions allow its thousands of authenticated customers to conduct SSL secured transactions, data transfer, distribution of tamper-proof code, and protection of online identities for secure email and access control. Vision and commitment to innovation led to GlobalSign being recognized by Frost & Sullivan for the 2011 Product Line Strategy Award. The company has local offices in the US, Europe and throughout Asia. For the latest news on GlobalSign visit www.globalsign.com or follow GlobalSign on Twitter (@globalsign).

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