PKI如何保护关键基础设施网络免受高级攻击

批发能源参与者已经表明关键基础设施(CI)提供商可以通过实施基于标准的PKI来加强网络安全

WHITE PAPER

在GlobalSign，我们的服务、合作伙伴和客户数据的安全是我们的首要任务。本白皮书描述了关键基础设施提供商如何通过实施基于标准的PKI来加强网络安全。

关键基础设施的识别

9/11事件和国土安全部(DHS)成立后，联邦政府确定了美国的关键基础设施(CIs)。重要的基础设施对国家安全、公众健康和安全、经济活力和生活方式至关重要;它们包括资产、系统和网络，无论是实体的还是虚拟的，对美国至关重要，它们的丧失能力或被破坏将对安全、国家经济安全、公共健康或安全，或其任何组合产生削弱作用。

我国的关键基础设施之一是能源部门，包括国家电力分配系统(电网)和有助于其运行的物理和虚拟系统。美国能源部门包含超过6,413家发电厂(包括3,273家传统电力公用事业公司和1,738家非公用事业发电公司)，装机容量约为1,075吉瓦。

PKI在保障关键基础设施安全中的应用

电力供应商、能源批发市场、监管机构和市场参与者正在将公钥基础设施(PKI)作为一种安全、可扩展、灵活和成本有效的方法来安全认证电力批发市场中涉及的许多数字身份。

该白皮书详细介绍了协调、控制和监控各州电力系统运行的独立系统运营商(ISOs)如何使用基于北美能源标准委员会(NAESB)制定的标准的PKI，以提高其基于网络的业务流程和交易的安全性。NAESB作为一个发展和推广标准的行业论坛，将导致天然气和电力批发和零售的无缝市场。

值得注意的是，虽然PKI是一种健壮的技术，但有很多实现细节可以产生一个脆弱且易受攻击的身份管理系统，也可以产生一个高度安全的身份管理系统。因此，NAESB与其成员合作制定了一个基于行业最佳实践、经过验证的管理技术和先进的数字证书技术的PKI标准。

本文将重点介绍电力行业的历史，网络安全标准是如何出现的，这些标准是什么，以及如何在其他CIs中使用它们来加强安全性和减少有害网络攻击的风险。

Critical关键基础设施网络安全发展

越来越多的证据表明，针对美国独联体的网络威胁越来越频繁，或者至少CI提供商报告的数量有所增加。就在今年5月，《纽约时报》[1]等主要媒体还报道了国土安全部的警告，称电网"可能"成为美国的攻击目标。8月，**美国国家公共广播电台(NPR)**[2]报道了华盛顿对网络攻击可能对电力供应造成影响的担忧。

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.

随着越来越多旨在破坏CI的网络攻击，美国供应商正在加紧努力，通过正式制定框架，强调使用标准、经过验证的最佳实践、先进技术和双向行业-政府网络威胁情报共享，加强其网络安全防御。

随着越来越多旨在破坏ci的网络攻击，美国供应商正在加紧努力，通过正式制定框架，强调使用标准、经过验证的最佳实践、先进技术和双向行业-政府网络威胁情报共享，加强其网络安全防御。

这种威胁是否迫在眉睫，目前尚无定论;然而，当前的政治气候已经为加大政府干预创造了足够的支持。

奥巴马政府已经认识到，有必要加强产业界和政府之间的沟通，分享关于已知威胁和攻击的非机密情报，并在适当情况下分享机密情报。

在《改善关键基础设施网络安全》行政令(EO)中，商务部长指示国家标准与技术研究所(NIST)领导制定网络安全框架的工作，其中包括尽可能采用行业最佳实践。虽然现行条例下的框架是自愿使用的，但业界预期会透过减少责任，当然还有改善保安等激励措施，落实所述的标准、方法和程序。截至本文，该框架的初步草案包括一个包含250个信息性参考文献的概要、现有标准和指南，包括PKI (WEQ-012)NAESB标准的批发电气象限标准。

认识到网络安全框架的价值，电力行业ci，即独立系统运营商(ISO)，已经开始采用由NAESB开发的PKI标准。

ISOs和区域传输组织:为什么他们选择标准

20世纪60年代末，能源行业开始面临两个主要挑战:

1.如何处理不可靠的能源供应

2.如何在一个非竞争的能源市场中生存

1965年的纽约大停电促使我国更加注重维持可靠和充足的能源供应。这一事件证明，供应并不总是与永不满足的能源需求相匹配，原因可能是市场不稳定，也可能是过时的发电、输电或配电系统和过程。到20世纪90年代末，需求的增长和能源价格的飙升促使美国联邦能源管理委员会(FERC)对批发电力部门进行了重组，目标是建立一个更具竞争力的批发能源市场。

能源发电机、输电供应商和公用事业最终与FERC就提供和管理给定地区市场的方法达成了一致。ISOs和区域输电组织(RTOs)的建立是"电力池"参与者就如何最好地建立一个负责运营某一地区电网的独立实体向联邦电力委员会提出建议的结果。

ISOs 和 RTOs 旨在:

- 协调给定区域的发电和输电
- 控制和监测其区域电网传输
- 与其他ISOs/RTOs协调发电和输电
- 为各自的电力市场提供中立和独立的运作
- 确保所在区域内电力系统的安全可靠
- 负责管理促进能源和操作系统开放市场的关税
- 受FERC监管

下面的地图显示了ISOs和RTOs在北美及其各自地区的运行情况。

联邦电力管理委员会(FERC)的任务是"以一种独立于公用事业公司销售或购买电力的任何商业利益的方式来运营公用事业公司的输电系统。"[3]

NAESB:网络安全标准采用

随着世界进入网络时代，很明显，能源供应和竞争问题不是ISOs和RTOs必须处理的唯一问题。在一系列试图(不同程度地成功)利用PKI的弱点来破坏电力系统的网络攻击之后，两个实体都需要加大对网络安全的关注。

主要ISO成员将NAESB视为推动增强网络安全措施的机制。NAESB认为PKI既是一道主要防线，如果管理不当，则是一个潜在的漏洞。NAESB因此开始建立和采用PKI标准。

> *"NAESB作为一个发展和推广标准的行业论坛，将导致批发和零售天然气和电力的无缝市场，得到其客户，商界，参与者和监管实体的认可。NAESB与NERC密切合作，协调批发电力行业的商业实践和可靠性标准的发展。"*

这样的标准是必要的，因为PKI是一种经过验证的安全技术，是一种商业上可行的方法，用于在不可信和可信的网络中验证身份。然而，如果使用过时的加密措施或将身份验证等关键功能外包，PKI可能会产生被利用的漏洞。这在最近的一些公开的CA (Certificate Authority，证书颁发机构)攻击中得到了证明。

在ISO主要成员的敦促下，NAESB重新召集了PKI小组委员会，重新审议了批发能源领域的PKI标准(WEQ - 012)，包括更严格的要求，要求CA必须交付和管理数字证书，支持CA基础设施，以及它们对用户和依赖它们的各方的义务。

NAESB董事会于2012年11月批准了更新后的标准，为批发电气象限成员提供了更高的保证，即在使用该标准实现时，用户和系统的身份是可信的。

今天，授权的NAESB CAs颁发符合NAESB标准的证书，以保护支持批发电气行业内业务流程的广泛应用程序。事实上，服务于批发电力市场的三个主要业务流程已经将NAESB标准合并到它们的开发流程中。

1. **电业注册处**: 这是商业行业信息的中央存储库，它定义了与批发电力的保留和调度相关的实体所扮演的角色。

2. **e-Tagging**: eTags用于识别与各方之间的物理能量流相关的交换交易信息。

3. **开放同步时间信息系统(OASIS)**: 这种基于互联网的系统使授权的输电供应商能够预定输电线路来输送批发电力。

作为标准PKI开发的一部分，NAESB还采用了认证规范，描述了授权CA (ACA)必须遵循的最低要求。ACAs必须签署宣誓书，声明他们符合认证规范的严格要求，由能够进行网络信任审计的第三方审计机构或同等机构独立验证。ACA规范有意与WEQ-012标准分开，以提供随着市场情况变化而进行更新的最大灵活性。规范中涉及的领域包括:

- 证书使用
- 保证等级
- 身份验证
- 证书生命周期管理
- 设备管理
- 操作控制器
- 审计
- 广泛的技术和程序安全控制

下图是上面列出的ACA规范要点的说明。

关于上面提到的WEQ-12标准:2013年7月18日，国际FERC (iFERC)发布了一份拟议规则制定的通知，FERC Docket No。RM05-5-022，针对2012年9月18日提供给委员会的WEQ标准的版本003，以及NAESB于2013年1月30日提交给委员会的PKI标准的后续更新。评论意见应提交委员会
在联邦公报上公布后60天。NOPR可从 https://www.ferc.gov/whats-new/comm-meet/2013/071813/E-4.pdf访问。

提高所有的安全

通过采用这些标准，NAESB及其成员组织认为，网络防御已经得到了显著加强，成功攻击影响国家电力供应运营或福祉的可能性已经大大降低。

“越来越明显的是，网络罪犯正以关键基础设施为目标，试图破坏我们的生活方式。出于这个原因，NAESB将建立PKI标准作为优先事项，以加强我们的网络安全框架，”NAESB总裁Rae McQuade说。“在制定这些标准时，我们希望提供一个强有力的网络安全策略，以便我们可以最好地保护与电力市场相关的商业行为，这是我们公民日常生活的关键部分。”

NAESB认识到网络威胁的流动性，并希望PKI小组委员会继续审查ACA规范，以确定可能需要更改的领域。当确定这些区域时，NAESB将进行适当的更改。

一个好，大家都好

虽然大多数独联体国家已经认识到他们需要改进网络防御，但有些国家还没有像能源部门那样取得巨大的进步。国土安全部总共承认了16个独联体国家;按行业划分，它们包括:化工、通信、水坝、应急服务、金融服务、政府设施、IT、交通系统、商业设施、关键制造业、国防工业基地、能源、食品和农业、医疗保健和公共卫生、核反应堆和废物以及水和废水系统。

所有部门都被复杂地捆绑在一起，通过世界网络系统进行管理、控制和访问，这使得所有部门都容易受到薄弱的IT安全和数字形式的攻击。网络安全标准的动态性必须在能源部门内外的其他CI安全工作中得到承认。否则，一场影响国家生活方式的成功袭击的可能性是肯定的。

NAESB已经证明，网络安全标准的制定可以利用共享的专业知识并与公共和私营部门协调进行。这同样适用于任何CI、公共或私人组织。

引用:

1. https://www.nytimes.com/2013/05/13/us/cyberattacks-on-rise-against-us-corporations.html
2. https://stateimpact.npr.org/pennsylvania/2013/08/15/power-companies-weigh-threat-of-cyberattacks-on-electric-grid/
3. https://www.federalregister.gov/documents/1996/05/10/96-10694/promoting-wholesale-competition-through-open-access-non--discriminatory-transmission-services-by – 联邦能源管理委员会于1996年10月5日更新的规则

关于GlobalSign

GlobalSign是全球领先的可信身份和安全解决方案提供商，使全球的企业、大型企业、云服务提供商和物联网创新者能够确保在线通信的安全，管理数百万已验证的数字身份以及自动化认证和加密。其大规模公钥基础设施(PKI)和身份解决方案支持数以亿计的服务、设备、人和物组成的万物互联(IoE)。

Tel: +86 021-60952260
.www.globalsign.cn