Security Technology for Smart Grid Networks

Anthony R. Metke and Randy L. Ekl

***Abstract*—There is virtually universal agreement that it is necessary to upgrade the electric grid to increase overall system efficiency and reliability. Much of the technology currently in use by the grid is outdated and in many cases unreliable. There have been three major blackouts in the past ten years. The reliance on old technology leads to inefficient systems, costing unnecessary money to the utilities, consumers, and taxpayers. To upgrade the grid, and to operate an improved grid, will require significant dependence on distributed intelligence and broadband communication capabilities. The access and communications capabilities require the latest in proven security technology for extremely large, wide-area communications networks. This paper discusses key security technologies for a smart grid system, including public key infrastructures and trusted computing.**

***Index Terms*—Attestation, public key infrastructure (PKI), Supervisory Control And Data Acquisition (SCADA), security, smart grid, trusted computing**

I. Introduction

NEW capabilities for smart grid systems and networks, such as distributed intelligence and broadband capabilities, can greatly enhance efficiency and reliability, but they may also create many new vulnerabilities if not deployed with the appropriate security controls. Providing security for such a large system may seem an unfathomable task, and if done incorrectly, can leave utilities open to cyberattacks.

By building on knowledge, solutions, and standards from other systems and industries, the best security solutions can be utilized for each portion of the smart grid communications network. Clearly, Internet-based protocols, such as IPv4 and IPv6, which have been developed over many years, and which have widespread use, will provide a cost-effective baseline transport. Layering the suite of security protocols developed for IP [such as IPSec and Transport Layer Security (TLS)] on this baseline transport capitalizes on the vast work done in this area by protocol and industry experts.

While the smart grid system is made up of a number of "energy" subsystems (Fig. 1), many of the communications and security components, as listed below, are common between these energy subsystems.

One subsystem which is at the core of smart grid systems is the Supervisory Control And Data Acquisition (SCADA) solution. Multiple vendors offer SCADA solutions, which have varying capabilities and security mechanisms. While some standards exist around SCADA, such as Distributed Network Protocol 3 (DNP3), Generic Object Oriented Substations Events (GOOSE), IEC 61850, and IEC 60870-5, there is still a need to make more consistent the security solutions applied to SCADA deployments.

Manuscript received February 22, 2010. Date of publication May 06, 2010; date of current version May 21, 2010. Paper no. TSG-00032-2010.

The authors are with Motorola, Inc., Schaumburg, IL 60196 USA (e-mail: Tony.Metke@Motorola.com; Randy.Ekl@Motorola.com).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSG.2010.2046347

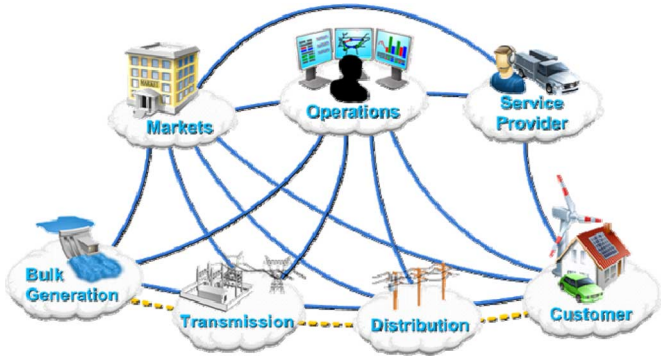

Fig. 1. Smart grid conceptual model.

A second component, key to smart grid systems, is a number of secure, highly available wireless networks. These would include wide area, land mobile radio (LMR) systems, as well as broadband networks, such as WLAN and WiMax.

A third key element is a comprehensive security solution. This paper presents a security solution for smart grid which heavily leverages public key infrastructure (PKI) technology and trusted computing techniques.

II. Security Requirements

The availability of electric power in North America depends in part on the availability of the power grid control systems. As part of the development of smart grid, these control systems are becoming more sophisticated, allowing for better control and higher reliability. Smart grid will require higher degrees of network connectivity to support the new sophisticated features. This higher degree of connectivity also has the potential to open up new vulnerabilities.

According to the Electric Power Research Institute (EPRI) [2], one of the biggest challenges facing the smart grid development is related to cybersecurity of systems. According to the EPRI Report, "Cyber security is a critical issue due to the increasing potential of cyber attacks and incidents against this critical sector as it becomes more and more interconnected. Cyber security must address not only deliberate attacks, such as from disgruntled employees, industrial espionage, and terrorists, but inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters. Vulnerabilities might allow an attacker to penetrate a network, gain access to control software, and alter load conditions to destabilize the grid in unpredictable ways."

There are many organizations working on the development of smart grid security requirements [3] including the North Amer-

TABLE I
LAYER 2 WIRELESS SECURITY CAPABILITIES

Key Security Attributes	802.11i	802.16e	3GPP LTE
End Point Authentication	Mutual or Server EAP (All Types); PMK is derived at both ends	Adapted from DOCSIS BPI+ protocol; PKM-EAP; relies on TLS [5]	AKA; mutual authentication between UE and MME
Session Key Derivation	802.11i 4-Way Handshake	3-Way Handshake[6]	Derived via Key Derivation Functions triggered on authentication via AKA
Encryption	AES-CCMP; 128 bit Key	DES3 and AES; CCMP[5]	Uses AES- 128
Message Integrity	CBC-MAC; MAC calculated across header and payload.	HMAC for message authentication and integrity check; optional CMAC [7]	MAC using AES-128 for control plane, data plane not integrity protected
Replay	40 + Byte IV	PKMv2 RSA Acknowledgement Message; all the Message integrity checks are replay protected [6]	NAS count in NAS signalling messages used for replay protection
Availability	High due to Cert Based Auth. Introduction of AAA for authorization could reduce availability	Driven by infrastructure availability	Depends on HSS availability
Group Security	128 Group encryption key; separate 64 bit TX and TX MIC keys	128 bit GTEK is used to encrypt multicast data packets. [7]	In the clear (between UE and eNodeB)

- DOCSIS – Data-Over-Cable Service Interface Specification
- CCMP – Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
- EAP – Extensible Authentication Protocol
- BPI+ – Baseline Privacy Interface Plus
- PKM – Privacy Key Management
- HMAC – Hashed Message Authentication Code
- GTEK – Group Traffic Encryption Key

ican Electrical Reliability Corporation—Critical Infrastructure Protection (NERC CIP), the International Society of Automation (ISA), IEEE (1402), the National Infrastructure Protection Plan (NIPP), and the National Institute of Standards and Technology (NIST), which has a number of programs.

One prominent source of requirements is the Smart Grid Interoperability Panel (SGiP) Cyber Security Working Group [previously the NIST Cyber Security Coordination Task Group (CSCTG)]. The NIST CSCTG was established to ensure consistency in the cybersecurity requirements across all the smart grid domains and components. The latest draft document from the Cyber Security Working Group, NIST Interagency Report (NISTIR) 7628, entitled "Smart Grid Cyber Security Strategy and Requirements," continues to evolve at the time of this writing. NIST and the DOE GridWise Architecture Council (GWAC) have established Domain Expert Working Groups (DEWGs): Home-to-Grid (H2G), Building-to-Grid (B2G), Industrial-to-Grid (I2G), Transmission and Distribution (T&D) and Business and Policy (B&P).

Cleary there are many groups working on requirements that will be applicable to smart grid. Further, many other standards may apply, including ISO 17799, FIPS 201, other NIST SPs, and DISA Security Technical Implementation Guides (STIGs).

Working with standards bodies, such as NIST and others, will be extremely important to ensure a highly secure, scalable, consistently deployed smart grid system, as these standards bodies will drive the security requirements of the system.

One thing is consistent among the various standards bodies: the security of the grid will strongly depend on authentication, authorization, and privacy technologies. Privacy technologies are well matured. Federal Information Processing Standard (FIPS) approved Advanced Encryption Standard (AES) and Triple Data Encryption Algorithm (3DES) solutions, offering strong security and high performance, are readily available. The specific privacy solution required will depend on the type of communication resource being protected.

As a specific example, NIST has determined that 3DES solutions will likely become insecure by the year 2030. Considering that utility components are expected to have long lifetimes, AES would be the preferred solution for new components. However, it is reasonable to expect that under certain circumstances where legacy functionality must be supported and the risk of compromise is acceptable, 3DES could be used.

Wireless links will be secured with technologies from well known standards such as 802.11i and 802.16e. Different wireless protocols have varying degrees of security mechanisms. A

representative sample of these capabilities and mechanisms are shown in Table I. Wired links will be secured with firewalls and virtual private network (VPN) technologies such as IPSec. Higher layer security mechanism such as Secure Shell (SSH) and SSL/TLS should also be used.

System architects and designers often identify the need for and specify the use of secure protocols, such as SSH and IPSec, but then skirt over the details associated with establishing security associations between end points of communications. Such an approach is likely to result in a system where the necessary procedures for secure key management can quickly become an operational nightmare. This is due to the fact that, when system architects do not develop an integrated and comprehensive key management system, customers may be provided with few key management options, and often resort to manually preconfiguring symmetric keys. This approach is simple for the system designers, but it can be very expensive for the system owner/operator.

What has been learned from years of deploying and operating large secure network communications systems is that the effort required to provision symmetric keys into thousands of devices can be too expensive or insecure. The development of key and trust management systems for large network deployments is required; these systems can be leveraged from other industries, such as land mobile radio systems and Association of Public-Safety Communications Officials (APCO) radio systems. Several APCO-deployed systems provide statewide wireless coverage, with tens of thousands of secure devices. Trust management systems, based on PKI infrastructure technology, could be customized specifically for smart grid operators, easing the burden of providing security which adheres to the standards and guidelines that are known to be secure.

All of the above technologies rely on some sort of key management. Considering that the smart grid will contain millions of devices, spread across hundreds of organizations, the key management systems used must be scalable to extraordinary levels. Further, key management must offer strong security (authentication and authorization), interorganization interoperability, and the highest possible levels of efficiency to ensure that unnecessary cost due to overhead, provisioning, and maintenance are minimized. It is likely that new key management systems (specialized to meet the requirements of smart grid) will be needed.

III. Proposed Solution Part I—PKI

Based on the security requirements for smart grid, as well as the scale of the system and availability required, we believe utilizing public key infrastructure (PKI) technologies along with trusted computing elements, supported by other architectural components, is the best overall solution for smart grid.

We believe that the most effective key management solution for securing the smart grid will be based on PKI technologies. PKI is more than just the hardware and software in the system. It also includes the policies and procedures which describe the set up, management, updating, and revocation of the certificates that are at the heart of PKI [4].

A PKI binds public keys with user identities through use of digital certificates. The binding is established through a registration process, where after a registration authority (RA) assures

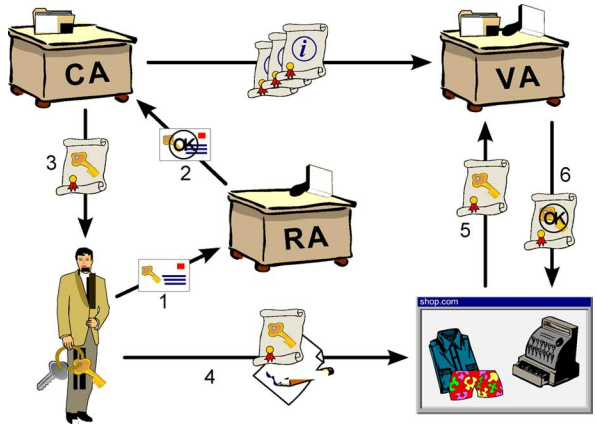

Fig. 2. Basic PKI procedure.

the correctness of the binding, the certificate authority (CA) issues the certificate to the user. Users or devices can authenticate each other via the digital certificates, establish symmetric session keys, and subsequently encrypt and decrypt messages between each other.

The basic steps in utilizing a PKI are shown in Fig. 2. The certificate subject, desiring communication with a secure resource [aka relying party (RP)] begins by sending a certificate signing request (CSR) to the RA. The RA performs a vetting function which determines if the requested bindings are correct, and if so signs the CSR and forwards it to the CA, which then issues the certificate. Later when the certificate subject wishes to access a secure resource, it sends the certificate to the RP. The RP validates the certificate typically by requesting the certificate status from a validation authority (VA), who replies in the positive if the certificate is valid.

PKI allows for a chain of trust, where a first CAs extends trust to a second CAs by simply issuing a CA-certificate to the second CAs. This enables RPs that trusts the first CA to also trust subjects with certificates issued by the second CA. When two CAs issue each other certificates it is referred to as cross signing. In this way, CAs from one organization can extend trust to the CAs from other organizations, thus enabling secure interoperability across domains. CA certificates can contain various constraints to limit the trust being extended by the issuing CA to the subject CA.

In very large systems PKI could be significantly more efficient than shared keys in terms of setting up and maintaining operational credential. This is due to the fact that each entity needs to be configured with its own certificate. This is as compared to symmetric key provisioning where each device may need to be configured with a unique key pair for every secure link.

While PKI is known for being complex, many of the items responsible for the complexity can be significantly reduced by including the following four main technical elements:

- PKI standards
- automated trust anchor security;
- certificate attributes;
- smart grid PKI tools.

Standards are used to establish requirements on the security operations of energy service providers (e.g., utilities, generators,

Independent System Operators (ISOs), etc.) as well as smart grid device manufacturers. Standards will include such items as acceptable security policies (e.g., PKI certificate policies used for issuing each type of certificate in the system), certificate formats, and PKI practices.

Trust anchor security is the basis for all subsequent trust relationships. But often trust anchor management mechanisms are as simple as trusting the IT administrators to install the correct certificate for the root CA in all RP devices, with little or no means of efficiently verifying the correctness of this operation. For systems with thousands or hundreds of thousands of nodes, an efficient and comprehensive trust anchor management system is needed.

Certificate attributes provide an important component to achieving the high availability needed for the power grid. We need to ensure that incorporation of security and device authentication does not unnecessarily impose or extend service outages, due to unreachability of a security server (e.g., AAA). This is why entities must "carry" their complete credential with them in the form of an attribute certificate, or a certificate contains sufficiently detailed policy information to allow an RP to determine the applicability of the certificate holder to a given service.

PKI tools are needed to ease the process of managing the PKI components used to support the smart grid application. These tools will be knowledgeable of the appropriate smart grid certificate policy and certificate format standards, and will be used to programmatically enforce compliance to those standards. Such tools will enhance interoperability, reduce the burden of running the PKI, and ensure that appropriate security requirements are adhered to.

With these elements in place, it will be possible for a smart grid owner or operator to purchase equipment, such as remote terminal units (RTUs), intelligent electronic devices (IEDs), and various forms of communication equipment, from an accredited manufacturer, install these components into their fielded system, and establish high assurance security associations (SAs) with these devices without having to preload shared keys into the device. Such mechanisms will provide highly secure key and trust management in an affordable manner.

We therefore believe that only by including these PKI elements into an overall security architecture, a comprehensive and cost-effective solution for security of the smart grid can be achieved.

A. Smart Grid PKI Standards

PKI is a powerful tool that can be used to provide secure authentication and authorization for security association (SA) and key establishment. PKI can, however, be notoriously difficult to deploy and operate. This is primarily because PKI standards (such as X.509 and IETF RFC 5280) only provide a high level framework for digital certificate usage and for implementing a PKI. For example, they do not specify how a particular organization should vet certificate signing requests, or how the organization should protect each CA. They provide a mechanism for defining naming conventions, certificate constraints, and certificate policies, but they do not specify how these should be used. These standards rightfully leave these details to the organizations implementing the PKI, and working out these details is where a great deal of the expense is incurred.

Some industries (such as the financial services industry) have standardized a model PKI policy. The purpose of a model policy is to define the naming conventions, constraints, policies, and many operational aspects of a PKI for an entire industry. Not only will this have great benefits for interoperability, but just as significantly, it will ease the burden of implementation, as each organization will not have to independently research PKI and determine policies and practices for themselves. They will have been determined by the industry, and they will be known to have desired levels of security.

We therefore propose the development of PKI standards for use by the critical infrastructure industry. The standards would be used to establish requirements on the PKI operations of energy service providers (e.g., utilities, generators, ISO) as well as smart grid device manufacturers. Standards could include such items as acceptable security policies (e.g., PKI certificate policies used for issuing each type of certificate in the system), certificate formats, and PKI practices.

B. Trust Anchor Security

One major component of a secure PKI enabled system is the requirement that each RP (any device that uses the certificate of a second party to authenticate the second party) must have secure methods to load and store the root of trust or trust anchor (TA). The TA is typically a CA at the top of a CA hierarchy. RPs trust certificate holders because they trust the TA, which trusts a CA, which trusts the end certificate holders. This trust is evidenced by a chain of certificates rooted at the trust anchor. If an adversary could change the root of trust for any RP, that RP could be easily compromised.

We propose that each operator will support its own PKI hierarchy with its TA at the top. The challenge for the operator is to ensure that each secure device obtains the correct TA information. One method of doing this without needing to manually preload the TA certificate into every device is as follows. Each accredited manufacture will factory preload the device with a manufactures certificate, identifying the make, model, and serial number of the device, as well as a preprovisioned TA certificate. After a smart grid operator purchases a smart grid device, the manufacturer would issue the operator a TA transfer certificate, which would instruct the device to accept the operator's root CA certificate as the new trust anchor, and only the operator's root CA certificate. The TA transfer certificate would be constrained to specific devices (based on serial number). Tools would automate the entire TA transfer process, reducing the effort to potentially be as simple as turning the device on in the operator's network, sending it the address of the TA transfer repository [possibly via a domain name server (DNS)], and allowing it to automatically request the TA transfer certificate and new TA certificate. For highly critical devices it is recommended that the device must have a FIPS HSM to securely store the TA certificate.

In addition to secure TA management, each PKI enabled smart grid device should have the ability to securely load and store a local policy database (LPD). This LPD is a set of rules

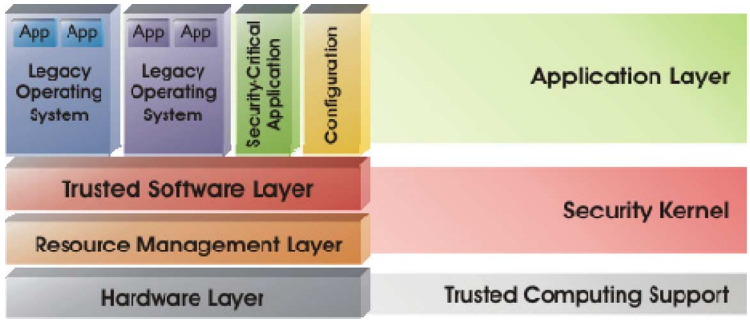

Fig. 3. Trusted computing model.

that define how the device can use its certificate, and what types of certificates it should accept when acting as an RP. The LPD would be a signed object, stored in the HSM, and signed by a policy signing server trusted by the TA. It would be possible for the same PKI tools to automate the management of the LPD as the TA certificate.

C. Certificate Attributes

In order for portions of the smart grid to continue to function while other portions of the grid infrastructure are unreachable, it will be essential for smart grid devices to be able to authenticate and determine the authorization status for each other (as well as human system administrators) without the need to reach a back-end security server (i.e., AAA). In order to do this, two additional capabilities would be required. First, smart grid certificates will require policy attributes to indicate the applicability of the certificate to a given application.

Second, a local source of performing certificate status will be required. This can be accomplished in a number of ways. For example, it would not be difficult or costly to distribute local certificate status servers throughout the grid. A possibly better method involves having each certificate subject periodically obtain a signed certificate status for his own certificate. The certificate subject would store this status and provide it to an RP when authenticating to the RP. The RP would determine, based on local policy, if this status was new enough to accept, and if so, the associated certificate could then be evaluated. It would also be recommended that all certificate subjects were loaded with the chain of certificates between themselves and their TA, and select chains of certificates between the subjects' TA and the TAs of other agencies with which the local agency has cross signed or otherwise trusts. Management of these chains of certificates, and ensuring that devices receive the proper set, would again be automated by tools.

D. Smart Grid PKI Tools

Even with the above standards, smart grid operators would have to familiarize themselves with PKI concepts, terminology, risks, best practices, and the above-mentioned standards. Standards alone may not necessarily provide a cost-effective solution. However, given such a set of standards, it would be possible for vendors to develop smart grid PKI tools which are based on these standards. Such tools would greatly ease the process of managing the PKI components needed to support the smart grid application. These tools will be knowledgeable of the appropriate smart grid certificate policy and certificate format standards, and will be used to programmatically enforce compliance to those standards. Such tools will enhance interoperability, reduce the burden of running the PKI, and ensure that appropriate security requirements are adhered to.

Smart grid PKI tools comprise a set of enhanced functions for PKI components (such as RAs, CAs, and repositories) developed specially for the smart grid industry. The tools could both automate and enforce the appropriate requirements for each PKI operation such as vetting CSRs, or certificate revocation. For example, the tools would know the different requirements for handling CSRs for IED and human system administrators. The tools would aid with system deployment, PKI operations, and system auditing, all in accordance with the standard model policy. Most importantly, these tools will eliminate the need for symmetric key configuration, which is an inherently insecure and expensive process.

The cost of building these tools will not be prohibitive, as they will be similar to tools which already exist for PKI operations, and simply modified for smart grid use.

IV. Proposed Solution Part II—Trusted Computing

The North American power grid is currently undergoing a major transformation. By adding significant new functionality, distributed intelligence, and state-of-the-art broadband communication capabilities, the grid can be made more efficient, more resilient, and more affordable to manage and operate. Unfortunately, these very same capabilities will greatly increase the number and type of threats to which the grid will be exposed. Considering the vast size, scope, and breath of the smart grid, it is reasonable to expect that the cumulative vulnerability of the system may also be vast. Virtually all parties agree that the consequences of a smart grid cybersecurity breach can be enormous. New functions such as demand response introduce significant new attack vectors such as a malware that initiates a massive coordinated and instantaneous drop in demand, potentially causing substantial damage to distribution, transmission, and even generation facilities.

Considering the incredible size of the threat and wide-ranging potential consequences from cyberattacks, the smart grid cybersecurity protection requirements must be extreme. The grid will require a comprehensive security plan that encompasses virtually all aspects of grid operations. One component of such a plan includes trusted computing platforms. Fig. 3 shows a basic trusted computing model [1]. Such platforms and associated mechanisms are used to ensure that malware is not introduced into software processing devices.

There are two categories of devices for which the malware protection problems should be considered: embedded computer

systems and general purpose computer systems. Embedded systems are computer systems that are designed to perform a specific task or set of tasks. They are intended to run only software that is supplied by the manufacture. By contrast, general purpose systems are intended to support third party software purchased by the specific consumer who purchased the system. A PC is an excellent example of a general purpose system. A microwave oven, or cable television set-top box, are examples of embedded systems. This problem of malware protection should be considered separately for each category.

For embedded systems the problem of protecting the system against the installation of malware can be solved with high degrees of assurance. First and foremost the manufacturer must implement secure software development processes; many standard models for such processes are defined in [8]. Second, if the device is intend to be field upgradable, the manufacturer must provide a secure software upgrade solution. The predominant method of doing this is to manufacture the embedded systems hardware with secure storage containing keying material for a software validation. Typically the hardware is configured with the public key of a secure signing server operated by the manufacturer. With this key, the device can validate any newly downloaded software prior to running it. Such a proactive approach can provide higher levels of assurance than can be obtained with a reactive approach such as a virus checker.

Additional security can be obtained by validating the software each time the device boots up. Such techniques are referred to as high assurance boot (HAB). HAB techniques typically rely on core software in secure hardware to validate boot-block code. The boot-block code then validates the operating system (OS), and the OS in turn validates the higher level applications. Each validation step is performed with public key or keys preinstalled in the secure hardware.

For devices which are intended to run for long periods of time (e.g., years) without booting, it is useful to have a method of performing secure software validation on running code. It is possible to have background tasks that can periodically perform such functions without disrupting the operations of the device. It is further possible to couple such background validation steps with other operational aspects of the device, such that if the device is found to be compromised, secure hardware on the device (needed to bring up and maintain security associations with remote entities) will prevent the local device from establishing and maintaining security associations with the remote entities. Many papers, such as [9], are available on methods to provide remote device attestation.

Device attestation is needed to ascertain, for the devices on the network, their true identities, ahead of any manual or automated provisioning at the site.

With device attestation techniques, accredited manufacturers can factory install device attestation certificates in each smart grid device. These device attestation certificates are used only to assert the device manufacturer, model, serial number, and that the device has not been tampered with. These certificates coupled with the appropriate authentication protocol can be used by the energy service provider to ensure that the device is exactly what it claims to be. In order to support device attestation, the device will need a FIPS 140 hardware security module (HSM), and will need HAB functionality.

For general purpose computing devices, such mechanisms that only allow software approved by the manufacture to run have not been popular. Consumers of PCs typically feel that they should not be restricted by the manufacture from loading any software that they want, even if it means having to put up with malware attacks. The predominant means of protecting networked PCs has been to use malware detection and removal software typically referred to as antivirus software. One of the most effective tools that the antivirus software uses to detect malware is a "signature" dictionary. The term "signature" is being used here to refer to a pattern of known recognizable code, as opposed to the cryptographic signature used above. With the signature dictionary, only known viruses can be discovered and removed. Such methods are not helpful in protecting against new or unknown viruses. Clearly with the stakes so high, the smart grid needs a better solution than the reactive antivirus dictionary approach.

To make matters worse, the rapid adoption of cloud computing and sophisticated Internet based applications has resulted in the widespread deployment of a number of "mobile code" technologies. Mobile code is code that is downloaded and run on your PC, typically by your browser, without the user's knowledge. Examples of mobile code include ActiveX, Flash animation, Java, JavaScript, PDF, Postscript, and Shockwave. The Department of Homeland Security (DHS) Control System Security Program [10] recommends tight controls on mobile code in critical control systems for the nation's critical infrastructure and key resources (CIKR).

To address this concern we propose the adoption of, and adherence to, strict code signing standards by smart grid suppliers and operators. Mechanisms for enforcing such standards on general purpose computers, such as PCs, have been put forth by the Trusted Computing Group and are well documented [11]. Such standards should cover all critical devices including field deployed units, such as RTU and IED, network devices, such as router, switches, and firewalls, and control center equipment, such as servers and user consoles. The standards should cover embedded systems, as well as general purpose computers, their operating systems, drivers, and applications, as well as all mobile code. That is, no mobile code should be allowed to run on a critical PC or server that has not been signed by an authority that is able to determine the trustworthiness of the code. Considering that it is certain that hardware and software elements for critical components of the grid will come from many different providers, it is likely that a trust management framework will have to be established for smart grid. This framework will likely require the establishment of a set of criteria that are to be meet by vendors who wish to sell critical components to smart grid operators. Additionally it is likely that one or more accreditation organizations will need to be established to audit suppliers to determine they are meeting the specified criteria.

To some, these measures may seem somewhat extreme, but when we consider what is at stake, and the large potential for vulnerabilities related to malware in the smart grid, it is hard to imagine any other practical way of providing complete malware protection in the grid.

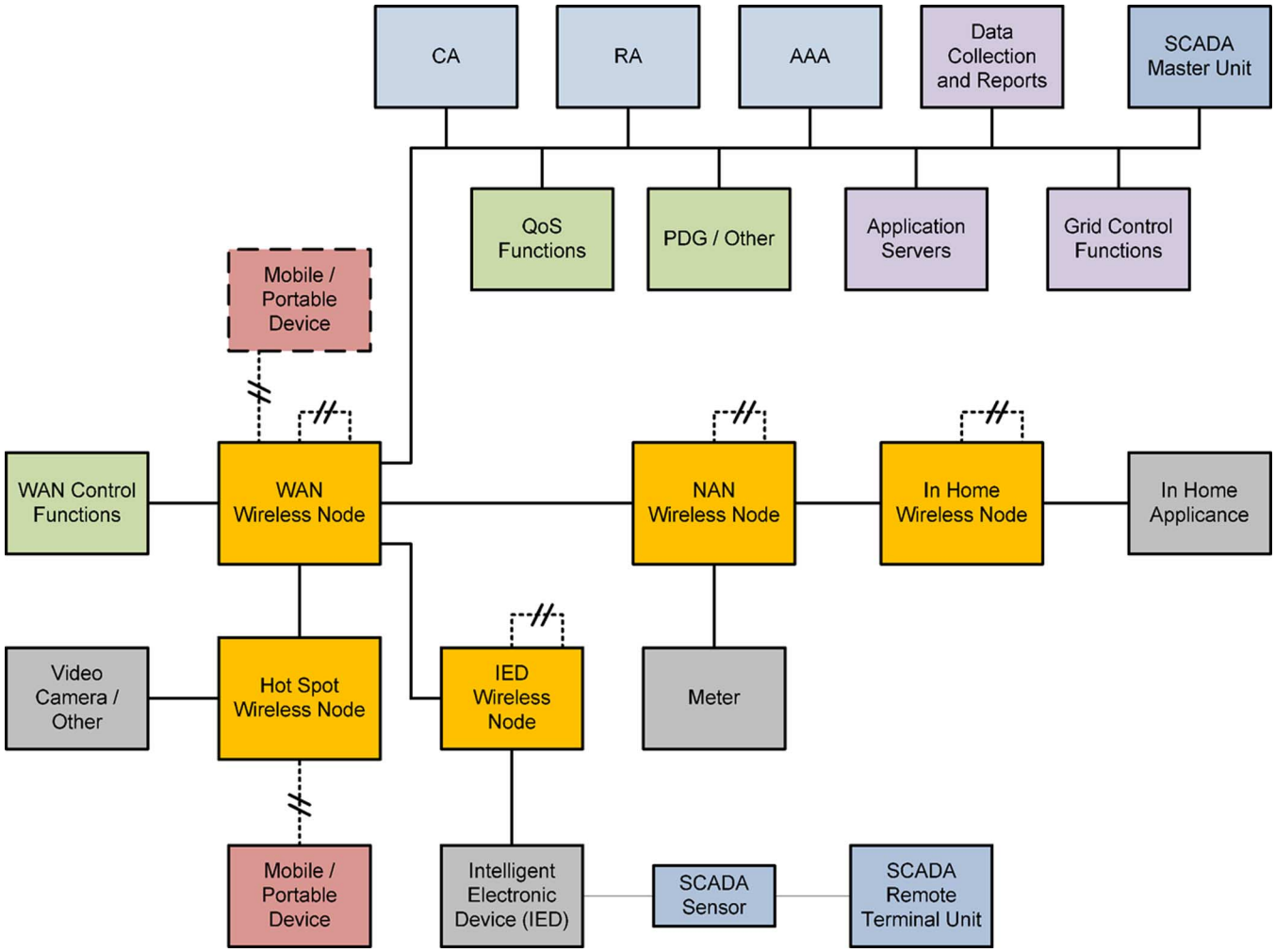

Fig. 4. Smart grid detailed logical model.

V. Other Architectural Components

PKI and trusted computing techniques can provide a very firm basis for a strong and comprehensive security architecture for smart grid. However these technologies alone are only the beginning of the story. A complete architecture will include many other components such as firewalls, strong user and device authentication, and message privacy and integrity. Listed below are a few more components that should be take into account when developing the smart grid architecture.

A. Overall Architecture

There are many views of the overall architecture for smart grid, depending on what the intent is of viewing or analyzing the architecture. We present two architecture views—a high-level conceptual model and a detailed logical model.

High-Level Conceptual Model: The high-level conceptual model (Fig. 1) has been developed by NIST and picked up across the smart grid and utility industry. It simply shows that seven main conceptual entities, along with the intercommunications between them. The blue lines in the diagram are the information flows, and the dotted yellow lines are the energy flows.

Detailed Logical Model: The detailed logical model is comprised of several key elements: networks (wireless and wired), functional subsystems (such as SCADA), endpoints (e.g., computers in the back offices, monitored and/or controllable substation devices), and overlays (such as distributed security functions and elements).

The diagram in Fig. 4 shows an example of the possible interconnection of a subset of the various networks, with a WAN wireless network as the backbone of the entire system. Note that the wireless interfaces between similar devices is shown as a dashed, double-hashed line.

B. Wireless Networks

The smart grid communications network will be comprised of several different subsystems—it is truly a network of networks. These networks include WiMax, WLAN, land mobile radio (LMR), cellular, microwave, fiber optic, dedicated or switched wirelines, RS-232/RS-485 serial links, wired LANs, or a versatile data network combining these media.

Different areas of the smart grid network require different wireless networking solutions. Advanced metering infrastructure (AMI) solutions can be meshed or point-to-point, with local coverage or long range communications. Options for backhaul solutions are fiber, wireless broadband, or broadband over powerline, to name a few. Workforce mobility solutions possibilities include WiMax, WLAN, cellular, and LMR, depending on the reliability, throughput, and coverage desired by the utility.

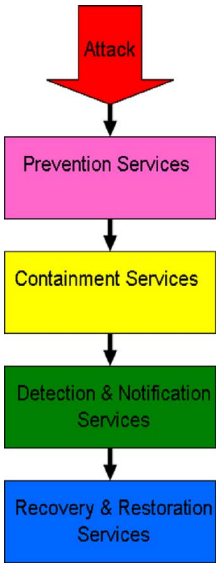

Fig. 5. Incident response plan.

The wireless communications solutions can be either licensed or unlicensed, again depending on the needs of the utility. For the highest reliability, licensed should be chosen. Each of the above options has their advantages and disadvantages, but what is consistently true of any and all of the solutions is the need to have a scalable security solution.

C. Incident Response Plan

The components, systems, networks, and architecture are all important to the security design and reliability of the smart grid communications solution. But it is inevitable that an incident will occur at some point and one must be prepared with the proper incident response plan (Fig. 5). Steps in the incident response plan go from prevention to containment, followed by detection and notification, and finally recovery and restoration [12]. A feedback/process improvement loop can make the system even more secure, and subsequent attacks less damaging, by adding additional prevention and containment checks.

The incident response plan and its implementation can vary between commercial providers and private utility networks. A private utility network is likely to provide better consistency of the incident response plan in the event of a security incident, assuming the private network is build upon a standardized framework of hardware and software. The speed of the response decreases exponentially as the number of parties involved increases. Conversely, a private network would ideally depend on fewer parties; therefore, a more efficient incident response process would provide for more rapid response and resolution. The rapidity of the response is critical during situations that involve a blackout.

Criticalness of the device or system also determines how prone it will be to attacks. History has shown that private networks by their inherent nature are less prone to attacks, and as a result are recommended as the best approach in situations where security is paramount.

D. Device's Scope of Influence

The system must be designed such that if an adversary can impersonate a meter, the scope of his influence is limited to affecting the monthly bill associated with that meter. Many have cited the potential that an adversary may take down the grid by impersonating or hacking into a meter as reason for upgradable cryptographic implementations in the meter. A better approach would be architect a system that would inherently protect against such an attack. A meter should only be able to send packets to a "meter data collection point" and a "meter manager," which in turn can only communicate with specific designated devices for specific designated services. A meter should never be able to send packets to arbitrary components in the system such as IED or distributed control processors located in a substation.

Several methods must be put into place to accomplish this. First, all devices must know who they are communicating with, and who they are supposed to communicate with. This is accomplished through mutual authentication techniques such as TLS or IPSec. During mutual authentication, symmetric session keys are derived which are used to provide message authenticity and integrity for subsequent traffic. Second, logical network segments must be isolated. Controls must be in place within the AMI network to assure that meter traffic cannot make its way into a substation, or some arbitrary network address. Also in the substation or control center, controls must also be in place to ensure that traffic is only admitted from authorized sources. Such a defense-in-depth approach has been the standard in enterprise networks for years. It is tempting to say the best solution is to physically isolate the AMI network from other networks. However, we need to recognize that operational expense will put pressures on utilities to use shared network resources for various purposes. It is therefore incumbent to ensure that the smart grid architecture can support logical isolation of logically disparate networks that share common resources.

VI. Conclusion

As a critical infrastructure element, smart grid requires the highest levels of security. A comprehensive architecture with security built in from the beginning is necessary. The smart grid security solution requires a holistic approach including PKI technology elements based on industry standards, and trusted computing elements. Clearly, securing the North American power grid will require the use of standards-based state-of-the-art security protocols. PKI technical elements, such as certificate lifecycle management tools, trust anchor security, and attribute certificates, are known technologies that can be tailored specifically to smart grid networks, resulting in an efficient and effective solution. The PKI solution supports the trusted computing elements, including device attestation.

To achieve the vision put forth in this paper, there are many steps which need to be taken. Primary among them is the need for a cohesive set of requirements and standards for smart grid security. We urge the industry and other participants to continue the work that has begun under the direction of NIST to accomplish these foundational steps quickly. However, the proper attention must be paid to creating these requirements and standards, as they will be utilized for many years, given the lifecycle of utility components.

REFERENCES

[1] Towards trustworthy systems with open standards and trusted computing European Multilaterally Secure Computing Base, 2005 [Online]. Available: http://www.emscb.com/content/pages/49373.htm

[2] Report to NIST on Smart Grid Interoperability Standards Roadmap EPRI, Jun. 17, 2009 [Online]. Available: http://www.nist.gov/smartgrid/InterimSmartGridRoadmapNISTRestructure.pdf

[3] Draft smart grid cyber security strategy and requirements, NIST IR 7628, Sep. 2009 [Online]. Available: http://csrc.nist.gov/publications/drafts/nistir-7628/draft-nistir-7628.pdf

[4] "Public key infrastructure," Wikipedia Feb. 18, 2010 [Online]. Available: http://en.wikipedia.org/wiki/Public_key_infrastructure

[5] WiMax Security 2010 [Online]. Available: http://www.top-bits.com/wimax-security.html

[6] 802.16e Notes—Mitchell Group, Stanford Univ.. Stanford, CA, pp. 94305–9045, Jun. 6, 2005 [Online]. Available: http://www.iab.org/liaisons/ieee/EAP/802.16eNotes.pdf

[7] L. Cuilan, "A simple encryption scheme based on WiMAX," presented at the Int. Conf. E-Business and Information System Security, Wuhan, China, 2009.

[8] N. Davis, Secure software development life cycle processes Software Eng. Inst., Carnegie Mellon Univ., 2009.

[9] Shaneck, K. Mahadevan, V. Kher, and Y. Kim, Remote software-based attestation for wireless sensors Comput. Sci. Eng., Univ. Minnesota—Twin Cities, 2005, . : , .

[10] Catalog of Control Systems Security: Recommendations for Standards Developers, DHS Sep. 2009.

[11] D. Challener *et al., A Practical Guide to Trusted Computing*. Upper Saddle River, NJ: IBM Press.

[12] J. Sherwood, A. Clark, and D. Lynas, *Enterprise Security Architecture: A Business-Driven Approach*. New York: CMP Books, 2005.

Anthony R. Metke received the B.S. degree in electrical engineering and computer science from the University of Illinois, Urbana–Champaign.

He is a Distinguished Member of the Technical Staff in the Advanced Technology and Research organization, part of the Enterprise Mobility Solutions business of Motorola Inc., Schaumburg, IL. Areas of responsibility include security for smart grid and mission critical broadband systems. His employment experience also includes serving as Director of Network Development for Midway Games, System Architect for US Robotics, and Senior Engineer for GTE. Previous work included PKI, QOS, bandwidth management, WLAN, ad hoc networking, multicast, and IP network design. He has received six U.S. patents.

Randy L. Ekl received the B.S. degree with a triple major in electrical engineering, computer science and mathematics from Rose-Hulman Institute of Technology, Terre Haute, IN, and the M.S. degree with a double major in electrical engineering and computer science from the University of Illinois, Chicago.

He is a Distinguished Member of the Technical Staff and manager in the Advanced Technology and Research organization, part of the Enterprise Mobility Solutions business of Motorola Inc., Schaumburg, IL. Areas of responsibility include aspects of smart grid and mission critical broadband systems. Previous work included cognitive radio for TV white space, WLAN, and performance modeling and simulation. He has 22 granted patents, and many pending, making him a distinguished innovator. He has a number of published papers in IEEE journals as well as other publications, such as *Mathematics of Computation*.

Mr. Ekl is an Associate Member of Motorola's Science Advisory Board and has been elected a Dan Noble Fellow, Motorola's highest honorary technical award.