

# Securing the Smart Grid



## Securing the Smart Grid

Security is a hot topic for the smart grid market—generating consumer, government and industry concerns about the safety of digitizing the electric grid. This white paper examines how public wireless smart grid projects are integrating best-of-breed security protocols to ensure the highest level of safety for the grid, while limiting management complexity. It will also discuss how IPsec, secure platform technology and public key infrastructure (PKI), the same layer of security used by governments and financial institutions, will provide utilities and businesses with a future-proof, industry-proven, secure smart grid solution that can quickly be taken to market while reducing costs.

There is a dramatic push in the deployment of smart grid solutions, fueled by concerns like cost-reduction, energy efficiency, and energy independence. Frequently, many trials and early deployments are taking place without security considerations. Unfortunately, security is not an afterthought and something that can be added on at a later stage— good, robust security has to be integrated right from the start. Without adequate security measures, utilities are vulnerable to fraud, service theft and process interruption (possibly leading to equipment damage and personal injury), affecting consumers facing unexpected service interruption and loss of consumption data privacy. Utilities are exposed to liability claims if they are not protecting the consumer's privacy in compliance with various international laws

The vulnerability of the smart grid infrastructure to cyber-attacks is expected to drive a boom in cyber-security spending for utilities. According to a February 2010 report from Pike Research, the smart grid cyber security sector will increase from \$1.2 billion in 2009 to \$3.7 billion by 2015. During the period from 2010 to 2015, the research firm anticipates that a total of approximately \$21 billion will be invested in global smart grid cyber security deployments.

### Focus on Utilities

Securing a brand new infrastructure that plugs into an existing infrastructure, as is the case with the smart grid, is a tremendous task. Fortunately, there is plenty that can be learned from securing IT networks. The security services that need to be provided in an Advanced Metering Infrastructure (AMI) are exactly the same as the ones provided by Virtual Private Networks (VPN)—data confidentiality and privacy, data integrity, service availability, authentication and authorization of communicating entities, livelihood, secure firmware upgrades as well as defense against sophisticated attacks like man-in-the-middle, replay, and reflection attacks.

Solutions that provide these security services exist today, but they have to be adapted to smart grid architectures. When making a choice, it is important for utilities to realize that good security solutions need to be open and proven (note that, from a business case point of view, they also need to be future-proof and scalable). Open solutions are better than secret or proprietary solutions, because they have been thoroughly tested by academia and hackers, and have withstood them successfully.

It is an illusion to think that secret systems can remain secret for long—there is a consensus among the security community that security through obscurity is bound to fail. Secondly, when making a choice, it is always advisable to go for the proven solution, again, because these systems have been studied, tested, and deployed so many times that the risk of a hidden security flaw (possibly leading to a security exposure) is much lower than with new, unproven, and insufficiently tested systems.



Such proven technologies and solutions include VPN solutions, Public Key Infrastructure (PKI) solutions, and secure platform technology. As a logical conclusion, the best way for utilities to manage risk is to rely on proven solutions from proven vendors. Even when working with trusted solutions, utilities should not forget to take an overall approach to risk management, encompassing implementation, deployment and operation, with continuous testing and improvement at every stage.

This makes the low-cost public IP network, with its high available bandwidth and its proven and trusted security solutions, a better candidate for AMI deployments.

### **Using Public Wireless Networks**

Intuitively, one may be tempted to think that private networks need to be less secured than public networks, because attackers cannot easily access them. Examples of private networks include telecommunication operators' core networks, or campus networks owned by big enterprises. However, history shows that a determined attacker will gain access, regardless of the network's nature. This is even more so when using private networks for the smart grid, because the connected endpoints are in people's homes, and therefore accessible to attackers.

Although using private networks seems to be a compelling option, it will not significantly improve the security level. In addition, from a scalability point of view (the need to connect an increasing number of endpoints per household), low bandwidth private networks are less suitable for AMI deployments. This makes the low-cost public IP network, with its high available bandwidth and its proven and trusted security solutions, a better candidate for AMI deployments.

### **AuthenTec's Security/Encryption & SmartSynch's Solutions**

The first steps in a secure AMI is the ability to identify connected devices, to authenticate these devices (i.e., to verify that these devices are really the devices they pretend to be) and to authorize these devices (i.e., allowing them access to the network based on the authentication results and the utility's security policy). This challenge is similar to the one met with in services and applications like e-commerce, pay TV, defense systems, and banking applications. The solution of choice that provides this identification and authentication service is the Public Key Infrastructure (PKI). A PKI is an infrastructure (i.e., the whole of organizations, people, equipment, software and protocols) that is capable of issuing revocable certificates (or digital identities), and verifying the validity of these certificates.

Certificates are the credentials of a meter, or of any other connected device (electric cars and batteries, solar panels, windmills and smart home appliances that can take advantage of cheaper time- of-use-based billing services). They are more secure, more scalable, and easier to manage versus using symmetric keys as a credential. Certificates are issued by trusted entities called Certificate Authorities (CA). A utility may choose to take on the role of a CA, but it can also outsource this task. Certificates are generated by high security appliances called Hardware Security Modules (HSM), which are capable of injecting digital certificates during the manufacturing process without human intervention (and thus without security risk).

The second step in a secure AMI is secure communication. When using a public IP network, the traditional, tested solution of choice is IPsec. This communication security protocol provides all desired security services—data confidentiality and privacy, data integrity, certificate-based (or other) authentication, liveliness, and defense against man-in-the-middle, replay, and reflection attacks.

A third cornerstone for building secure smart grid solutions —especially when deploying scalable and future-proof home gateway based architectures—is secure platform technology. Secure platform refers



to the ability to detect and defend against attacks. A secure platform will always control its system firmware to check if the software is original or an authorized update. This is called secure boot. Optionally, a secure platform can also check its system software integrity at runtime, called runtime integrity checking. Secure platforms also offer secure storage services (sensitive data are always encrypted when stored) and defend against attacks such as rollback (returning to an old version of the system software to exploit a known security flaw that has been patched in more recent versions) and cloning (cloning of compromised or hacked software on other devices).

Finally, secure platforms enable secure firmware upgrades, and, optionally, they enforce application separation, to avoid an application accessing and potentially tampering with sensitive data of another application. AuthenTec's technology has been successfully deployed by leading vendors to create secure platforms in consumer devices such as smartphones.

Smart grid security needs to be addressed—SmartSynch and AuthenTec are leading the charge to provide open, widely tested and approved security solutions based on PKI, secure communications, and trusted platform technology. Public wireless networks, when secured using AuthenTec's security solutions, are as secure as private networks and cost less to maintain. Utilities can mitigate security risks by proactively implementing these best-in-breed, secure solutions.

