



FORNETIX

The Looming Surge in Smart-Metering Encryption

**UNDERSTANDING THE CYBER SECURITY NEEDS OF A
RAPIDLY-EXPANDING AND EVOLVING ELECTRICAL GRID**



Utility meters are an important part of modern life that are often overlooked.

Every modern home or workplace has them to keep track of water, gas, and electricity usage. We typically assume this data is being used for billing, but measuring consumption also allows the companies providing resources to plan and adjust output. As demand increases or decreases, so too must the supply. This is most prevalent with the generation of electricity where it is far cheaper to create just enough power to meet demand, rather than try to store excess and use it later. The more information a producer of electricity has regarding when and where power is being used, the more efficient they can make their business. This is especially true as these companies incorporate multiple sources of power such as wind and solar that are not constant. Given how valuable this data is to companies, traditional analog utility meters are being replaced with "smart meters" that feature highly-advanced controls and network connections.

Smart Meters At-a-Glance

Smart meters allow for the ongoing monitoring of energy flows. Instead of a meter being used strictly for billing, utility companies can use smart meters to understand the ebb and flow of energy usage throughout the day. With the use of smart meters as part of a smart grid, costs of over-producing or under-producing can be minimized.

Additionally, usage of renewable resources like solar, wind, and water to produce power can be maximized, reducing the impact on the environment caused by more conventional methods such as coal or natural gas. These factors are why the European Union has mandated that 80% of all electricity metering utilizes smart meters by 2020.

Security Considerations in the European Union

The EU is leading the way in deploying smart grids and smart meters. They are also leading the way in protecting Personally Identifiable Information (PII) in regulations such as the General Data Protection Regulation (GDPR). Because energy usage data is considered private and in some cases PII, it must be encrypted to comply with EU laws. This is a good practice as tampering with this data could cause a variety of issues. Inflating usage numbers can cause consumers of energy to face large bills for energy they didn't use. Producers of energy can overproduce and waste precious resources in an attempt to keep up with a supply that is not there. Similarly, if usage was shown to be zero then we might see brownouts or supply problems as the producers react to the perceived lack of demand. Perhaps the simplest problem with not protecting the data is that a bad guy would be able to see when someone is home or sleeping just by looking at their power usage.



Effective Deployment Strategies to Support Security and Scale

Deployments of smart meters can be quite large and, as such, the encryption management requirements can be very large as well. There are two solution methodologies that are being employed for modern smart metering systems today. The first is to leverage HSMs and custom-built management software to integrate with the head end systems. This models much of what the financial industry has done in the past when needing to perform rapid cryptographic functions for things like PIN processing. There are a few standards-based specifications that have rules for communicating between the head end system and the various meters and systems that connect to the HES, but they have no standards for key management. This means that with each smart grid deployment, new key management systems are being created and customized for the deployment.

Standards Offer an Easier Path to Success

To some, it may seem to make sense to build out a custom system for each smart metering deployment to boost performance, but history and experience in other industries tells us that repeatable solutions are ultimately better. The second solution methodology for dealing with key management in the smart



metering industry is to leverage a KMIP-enabled server. KMIP, Key Management Interoperability Protocol, is a standard held by the non-profit group OASIS, the Organization for the Advancement of Structured Information Standards. It gives a repeatable, interoperable approach for handling key management in any industry. KMIP was created to provide a standard protocol to replace the many different ways of handling key management when interacting with IT storage and backup systems from various vendors. Prior to KMIP, setting up encryption in these systems was costly, time consuming, and potentially insecure, especially if a company needed to change vendors. By leveraging a standards-based approach, deployment becomes easier, as multiple vendors are able to interoperate by design. Additionally, deployments are repeatable with re-usable systems, allowing for a simplified supply chain and support of various smart grid initiatives.

Exploring a bit more into the actual key management components of smart metering, every standard used

today seems to leverage a few of the same key components. The first is the ability to manage the full lifecycle of AES symmetric keys as these are fundamental for securing the communications to and from smart meters... but not just regular AES keys. Key Wrapping is used heavily in the smart grid industry, so any key manager utilized for smart metering should support several different block ciphers, including NIST Key Wrap, CCM, and GCM. KMIP, as of version 1.4, supports 18 different block ciphers, including the most common ciphers used in smart metering. It is not enough to be able to manage the lifecycle of the keys; a system performing key management for smart metering must also be able to handle the encrypt and decrypt functions leveraging these keys, which KMIP supports. Further, asymmetric key pairs must be supported for the signing and verification of configurations. As the industry becomes more savvy, companies are adopting elliptical curve key pairs over RSA key pairs. Again, KMIP 1.4 supports both types of key pairs as well as cryptographic signing and verification.



Challenges and Considerations



One might think if a KMIP server is able to support all of the functionality that an HSM combined with custom management software and a key management database supports, then a KMIP server should be leveraged for every deployment. With KMIP, there are two challenges that organizations face when deciding which deployment methodology to use:


- 1) The ability of a KMIP server to perform cryptographic functions at the speed of an HSM.**
- 2) The ability to scale to the massive number of keys required for smart metering.**



With COSEM/DLMS, each smart meter has a minimum of 4 keys associated with it. Many deployments have at least 8 keys, 4 per role. This means that even a small deployment of 250,000 meters will exceed the capacity of most commercial KMIP servers at 2,000,000 cryptographic objects to be managed. In order to read each of those meters in a standard business day, a KMIP server must perform a minimum of 6 KMIP operations for each read (Locate*2, Get*2, Encrypt, and Decrypt). If we extrapolate that out: 6 KMIP operations x 250,000 meters / 8 hours / 60 minutes / 60 seconds = ~52 KMIP operations per second. Even with the ability for KMIP to batch operations, the speed required is beyond the capabilities of most KMIP servers today.

However, Fonetix has created VaultCore, an out-of-the-box solution capable of meeting both the capacity and the speed requirements to support the smart meter industry for deployments of this size and much larger. Ultimately, the smart grid industry and so many others would prefer to deploy a more secure, interoperable, and standards-based solution instead of creating new proprietary implementations for every project. Fonetix is happy to be leading the way in creating technology that meets the requirements of not only the smart grid industry, but the requirements of all industries that need encryption management for IoT devices.



-  Fonetix.com
-  Facebook.com/fonetix

-  Linkedin.com/company/fonetix
-  Twitter.com/fonetix

-  **1-844-539-6724**
-  **5728 Industry Lane,
Frederick, MD 21704**