Case study

ENEXIS

security for smart meters in a fast-changing energy marketplace

The drive to introduce smart meters into the Dutch energy market has accelerated, thanks to the initiative shown by Enexis and a successful data encryption solution delivered by Atos

The energy marketplace in the Netherlands has been restructured significantly in recent years. The country has moved away from regionally based, vertically integrated energy providers to a system in which commercial providers have been separated from the companies delivering electricity and gas.

That enables more than 7 million households in the country to have greater choice about the terms and costs for energy supply, while enabling the major utility companies, of which Enexis is one of the largest, to focus on what they do best: efficient delivery of gas and electricity.

This approach is also designed to manage the much more flexible market that is now emerging. Growing use of renewable energy means that every household can potentially be a micro-generator in its own right, selling power into the national grid as well as taking from it. To make this new market work at its best, smart metering is a basic requirement. This enables customers to manage their energy use more effectively, ensures complete accuracy of billing, permits better and more proactive load-balancing by major providers and also handles two-ways flows of power, making micro-generation a reality.

The Dutch government made the decision in principle to go ahead with the national roll-out of smart meters almost a decade ago, but a range of obstacles has delayed implementation. Perhaps the most important of these has been security, and in particular concerns raised by citizens about the confidentiality of data collected via smart meters by their energy providers. This led to a legal review and the decision that smart meters should not be mandatory but must be left to individual choice by consumers.

Smart and secure

Enexis is one of the leading players in the Netherlands energy market. Of the 7 million households in the country 2.7 million take their power from Enexis, which is both committed to the deployment of smart meters and has the scale and influence to make a real difference to the market.

Enexis management realized that the key to rolling-out smart meters across its customer base was to provide complete assurance that customer data would remain completely private at all times, with no possibility of information being accessed by hackers or identity thieves. In 2008, therefore, they started to investigate ways to ensure complete data security in order to encourage customer acceptance of smart meters, working with Atos and Worldline, an Atos subsidiary, which is a global player in payments and transactional services and European leader in the field.

It was clear from the start that standard server security would not be enough: an encryption solution would also be needed, but the practical requirements were complex. The most important of these was the need for a truly modular solution, as management of meter readings are managed by a partner organization, which did not have a secured and certified key management solution in its software. The Atos team therefore worked closely with Enexis and the partner to develop an approach that would deliver the right results, while ensuring the minimum of disruption at infrastructure level.

Security is largely a matter of trust: in fact the only time you are truly aware of security as an issue is when breaches happen. The key to acceptance of smart meters is that consumers should trust the security systems being used to safeguard their private data. As sensitive private data is transferred from the consumer to the operator or grid provider, to gain trust it is best to use security systems that are proven and certified by third parties. It takes time and effort to build this level of trust, not just between Enexis and its customers but also between Enexis and the Atos team.

During 2009 and 2010, therefore, at the same time as the legal status of smart meters was being discussed and eventually decided, Enexis and Atos team worked together to build an approach that would work under the real conditions of the market. By 2011, Enexis felt ready to send out a call for tender, which was won by Atos and Worldline. In early 2012, the data encryption program was ready to begin.

Smart meters are now being used in a growing range of national electricity and gas markets across Europe. Take up at this stage remains modest but usage is increasing and many European governments are now supporting the concept of rolling-out smart meters nationally. Potential advantages are considerable:

- Accuracy- most householders across Europe are given estimated bills for most of the year. Combined with payment by direct debit, this can mean over-payment in advance, leading to actual financial loss to consumers
- Active management- smart meters mean that individual citizens and families can track their power usage in real time and with complete accuracy. That enables them to adjust their behavior to reduce costs and should lead to a real reduction in energy usage, which is good for society, and a reduction in costs, which is good news for families
- Two-way movement of power- the rise of renewables, and especially the growing use of photo-voltaic panels, means that some families can offset their investment in renewable energy by selling excess power back to the grid, at least on occasion. Without smart meters this would not be possible
- Convenience- it is not necessary for company personnel to enter houses to read meters. This means that customers will no longer need to be at home to ensure accurate billing and will also remove any potential privacy concerns.

The Energy Saving Trust in the UK has calculated that annual savings of up to €200 per household are achievable through active management of usage, enabled by smart meters. That is a prize worth having.

"Smart meters are vital to the future of the energy marketplace and will deliver benefits to households and energy suppliers, alike. To implement smart meters successfully in the Netherlands requires high levels of trust and an effective effort to address current security issues."

Practical, trustworthy and compliant

Based on its cryptographic technology, Worldline has built a solution that is trustworthy and meets the new regulations that govern use of smart meters in the Netherlands.

The real breakthrough in acceptance of smart meters came when Netbeheer Netherlands developed a set of privacy and security requirements, both technology and governance-based, that provided clear, repeatable standards for operation in the market. Known as the Dutch Smart Meter Requirement (DSMR), this standard sets out a clear basis for collection, storage, processing and end-to-end management of data collected from smart meters and subsequently used for preparing bills and other forms of customer contact.

The Cryptoserver solution, developed by Worldline, is compliant with the new standard, and this was an important factor in both encouraging Enexis to go ahead with its smart meter project and in ensuring that Worldline was selected to provide secure encryption. The core requirements within the original tender document were the ability to manage the existing protocols used by Enexis for data collection (known as DLMS / COSEM), backed by complete data security, and certified secure key management. The Cryptoserver meets both requirements.

The only way to deliver truly assured security for data collection is via a cryptographic system that uses cryptographic keys for encoding and decoding the data, while ensuring that non-authorised access is made virtually impossible. Software solutions are available but these always leave open the possibility of hacking from the outside. The only truly tamper-proof solution is, therefore, hardware-based. Cryptoserver contains standalone hardware modules that contain the necessary cryptographic keys that are completely inaccessible to hackers and identity thieves. Data entering and leaving the server is incomprehensible to any outside observer. Cryptographic operations happen only inside the Hardware Security Modules (HSMs). By restricting access to online networks it becomes for practical purposes impossible to look at or steal customer information. These modules are made within the European Union (in Germany) and to accepted international standards, which is a further assurance of their integrity.

Worldline's combined hardware and software approach was chosen as the basis for the Enexis smart meter data security solution, now known as Cryptoserver, and work began on developing and delivering the solution in early 2012.

The power of Cryptoserver

The complete Cryptoserver project was implemented in two phases, as Enexis wanted to move with caution in the early stages in order to ensure that core systems could not be affected by this new departure. The initial focus, therefore, was on encryption of the underlying database, which was completed in September 2012, at which point the second and larger phase of the project was started.

Figure 1 below explains the overall landscape in which the Worldline solution operates.

The encrypted data is transferred to the Central System of the DSO (Enexis). The energy providers, which are responsible for billing and customer service, request the customer data of their customers from the DSO. The cryptographic components are completely separated from core processes.

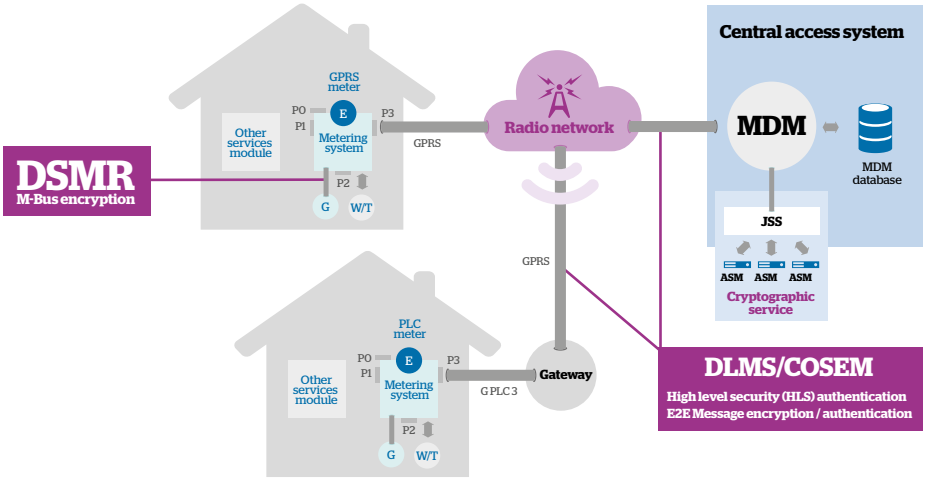

Figure 1 explains the overall landscape in which the Worldline solution operates.

Cryptographic service: Realized by Atos Worldline products JSS & ASM

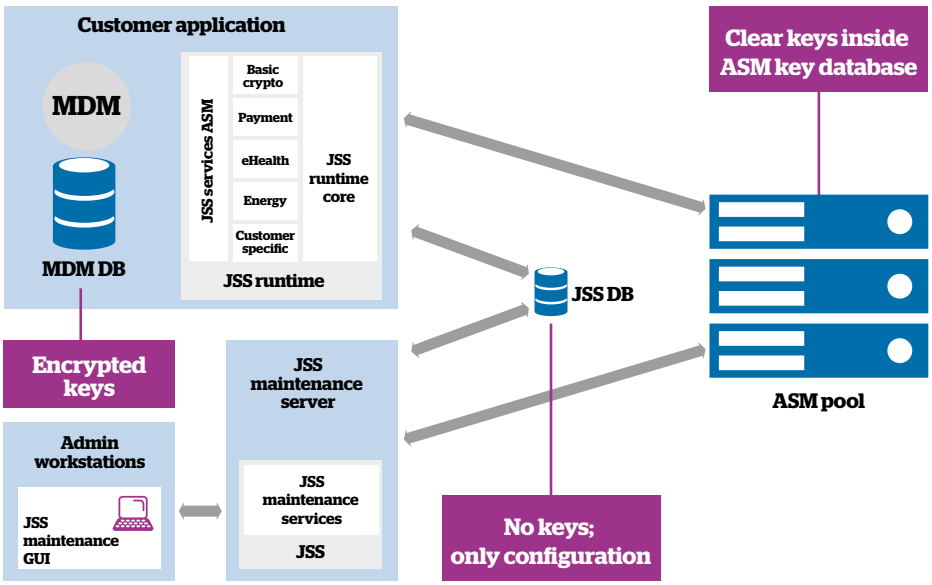

Figure 2 shows in more detail how the interaction between Cryptoserver and core processes is managed.

This demonstrates how the highest levels of security are built into the solution at the deepest level. Encrypted data is stored in the Enexis MDM database and then transferred to the ASM server pool. This comprises the Hardware Security Modules which contain embedded encryption keys, enabling the encrypted data from customers to be turned into data that can be used within core applications to determine the amount of energy used, payment status and other essential requirements for managing the business.

Once again, this shows how encryption works in a system of this kind. Data in transit is always unreadable to the outside world. It only becomes actionable intelligence when decrypted within the Hardware Security Modules. No cryptographic keys or security operations are ever visible to the main servers or the core applications, themselves.

Cryptoserver as a whole includes both the hardware and software components needed to ensure secure operations and seamless, efficient interconnection with core processes. Taken together this permits highly flexible and responsive working, while also ensuring dynamic load-balancing. This is a key factor in enabling high levels of business continuity, with automatic fail-over for all aspects of cryptographic operations.

This is essential for the simple reason that any failure in the security layer will automatically terminate all transactions then in progress, which could lead to disruption.

The high levels of resilience in the cryptographic layer offer a vital safeguard for wider business continuity in delivering customer service.

Delivering positive outcomes

The second stage of the project went live in early summer of 2013 and has proved to be highly successful when measured against all key criteria. There has been no disruption to core systems or customer services, no security failures of any kind, no problems with the Cryptoserver solution and successful connectivity between core processes and security layer from the outset.

The best way to demonstrate success, however, is to look at developments in the marketplace, itself. Currently, 270.000 households have moved to the smart meters on the Enexis network. That represents one in nine of all customers, and take-up continues to accelerate as the advantages of smart metering become more widely understood.

It is clear that customers are starting to accept that it is in their own interests to move to smart metering, and the trust problems that held up the roll-out in the past have been largely overcome.

The Enexis – Atos and Worldline project has wider significance, as well. This Cryptoserver project represents one of the earliest and largest smart meter implementations that is fully based on accepted international standards. It clearly demonstrates that there is a practical and affordable way to improve on standard server security methods to ensure the confidence and peace of mind that ordinary citizens demand. The solution is repeatable, proven and can be lifted and dropped into other settings, other countries and other marketplaces.

Smart meters deliver real benefits for individual customers, energy companies and the nations in which they operate. The main objection to faster roll-out is based on security concerns. Now, Atos and Worldline have shown that these concerns can be, and have been, completely overcome. Progress in the future is likely to be much faster than in the past.

"The successful development and implementation of Cryptoserver has demonstrated that secure and effective use of smart meters on a very large scale is a reality. Atos and Worldline have made a vital contribution to our roll-out of smart meters and we are certain that the cryptoserver solution can and will be used much more widely in the future."

About Atos

Atos SE (Societas Europaea) is an international information technology services company with 2013 annual revenue of €8.6 billion and 76,300 employees in 52 countries. Serving a global client base, it delivers IT services in 3 domains, Consulting & Technology Services, Systems Integration and Managed Services & BPO, and transactional services through Worldline. With its deep technology expertise and industry knowledge, it works with clients across the following market sectors: Manufacturing, Retail & Services; Public sector, Healthcare & Transports; Financial Services; Telco, Media & Utilities.

Atos is focused on business technology that powers progress and helps organizations to create their firm of the future. It is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and is quoted on the NYSE Euronext Paris market. Atos operates under the brands Atos, Atos Consulting & Technology Services, Worldline and Atos Worldgrid.

For more information, visit: atos.net

For more information, contact: dialogue@atos.net