Security analysis of Dutch smart metering systems

Sander Keemink, Bart Roos
sander.keemink@os3.nl, bart.roos@os3.nl

Universiteit van Amsterdam

July 7, 2008

Abstract

Smart meters enable utility companies to automatically readout metering data and to give consumers insight in their energy usage, which should lead to a reduction of energy usage. To regulate smart meter functionality the Dutch government commissioned the NEN to create a Dutch standard for smart meters which resulted in the NTA-8130 specification. Currently the Dutch grid operators are experimenting with smart meters in various pilot projects. In this project we have analyzed the current smart meter implementations and the NTA using an abstract model based on the the CIA-triad (Confidentiality, Integrity and Availability). It is important that no information can be attained by unauthorised parties, that smart meters cannot be tampered with and that suppliers get correct metering data.

We conclude that the NTA is not specific enough about the security requirements of smart meters, which leaves this open for interpretation by manufacturers and grid operators. Suppliers do not take the privacy aspect of the consumer data seriously. Customers can only get their usage information through poorly secured websites. The communication channel for local meter configuration is not secured sufficiently: consumers might even be able to reconfigure their own meters. Also, the communication channels that are used between the smart meter and gas or water meter are often not sufficiently protected against data manipulation.

It is important that communication at all stages, starting from the configuration of the meter to the back-end systems and websites, is encrypted using proven technologies and protected by proper authentication mechanisms.

Introduction

A smart meter refers to an electricity, gas or water meter that passes its metering data automatically to the utility company on a regular basis. This provides utility companies with new means to monitor their distribution network and gives customers an opportunity to gain insight in their consumption.

In The Netherlands some power grid operators have already started rolling out smart metering systems. In the meantime, the Dutch government has issued a new law that requires grid operators to install a smart meter in every Dutch household. As part of the law there is a technical agreement which defines the minimal requirements for these metering systems.

In this research project, conducted under supervision of KPMG IT Advisory, we will analyze the security aspect of Dutch smart metering regulations and the systems itself. Our research is based on the following research objective:

"Analyze the possible impact of the use of smart metering systems on the security of electricity metering using the CIA-triad and minimum requirements as stated in the NTA-8130 regulation. Compare the NTA and a preferred situation with the smart metering systems that are currently implemented."

Document layout

The first section of this report gives an introduction to smart metering systems, the Dutch energy market, politics and regulations behind smart metering. In the second section an abstract model for smart meter security will be discussed. Next, a theoretical analysis of smart metering systems and regulation follows, based on the abstract model. In the fourth section current implementations of smart metering systems are compared with the theoretical model. The report will conclude with a number of recommendations and a conclusion.

Acknowledgments

This research would not have been possible without the generous help of the following people, who we would like to thank:

Jeroen van Beek, Pieter Ceelen, Hans IJkel and Marc Smeets from KPMG IT Advisory, ICT Security and Control for their guidance and useful comments. Jan Dees from Delta Netwerkbedrijf, Marc van Straaten from Brinck Meettechniek, Hendrik Jan van Roest from Founter and Hilbrand Does from Oxxio for their information and explanation. Josiene Boerdijk from IIR B.V. who kindly gave us the opportunity to attend the Energy Metering and Billing 2008 conference.

Contents

1 Smart metering introduction

1.1 Goals & politics

The Ministry of Economic Affairs initially proposed the smart meter to the Dutch parliament in February of 2006 [48]. The main focus of this proposal was to stimulate the liberalization of the Dutch energy market with the following goals:

- A consumer market which ensures the freedom of choice for the consumer.
- Give an impulse for energy-saving.
- Easy access to metering data services.

The smart meter offers advantages for both the consumer and the energy supplier. Consumers will receive better service and gain insight in their energy usage. Suppliers can introduce new services enabled by the smart meter like providing customers with advice about their usage and energy savings. Grid companies can get a better view in the actual consumer energy usage to improve demand and supply in the energy grid.

The bill of the Ministry of Economic Affairs will result in a change of the Dutch law concerning energy metering. A reference to the Dutch technical agreement concerning the minimal technical requirements of smart metering (NTA-8130 [51]) will be included as part of this regulation. This offers flexibility to change the regulation without having to change the law.

The governement determined the following goals for smart meters [47, 59]:

- Remote readout of consumed and provided energy (metering)
  - Improve the operational management of the suppliers (switching, moving, billing)
  - Improve the insight of the consumer in his actual energy usage and cost
- Remote capacity management (switching)
  - Facilitate operational task of grid managers
  - Disabling of energy supply during emergencies
  - Enabling and disabling of energy supply in case consumers move house (temporary vacancy)
  - Limit supply or disconnection in case of arrears
- Remote measurement and signaling of energy consumption (signaling)
  - Improving operation management for grid managers
  - Detection of energy leaks or fraud
  - Detection of supply fluctuations, discontinuances and link impact
- Online interaction between consumers and suppliers (communication)
  - Online offerings of innovative products and services (energy-saving recommendations, special for certain hours)
  - Consumer can react real time on market, product and price development of suppliers
  - Support for payment methods like prepaid.
- Quick response of energy producers to influence demand

- Connection with home automation appliances
- Connection with decentralized (durable) generation
- Facilitate decentralized supply and demand guidance (coordinate own production with purchases against a favorable rate)

Because of the impact that could be caused by a security breach in the smart metering systems, the Dutch minister of Economic Affairs has stated that scientists may try to break in to the computer equipment of smart metering systems to verify its security. She claims that smart metering must offer a security level as high as for money transfers. [3]

The Dutch house of representatives has come to an agreement on smart metering on June 19th, 2008. Voting will take place on the 1st of July 2008. [67]

In response to the possible impact of smart metering systems on the privacy of consumers, the CBP (Dutch Data Protection Authority) has expressed its concern in an official letter to the minister of Economic Affairs [7]. The minister will discuss the bill with the CBP and report back to the house of representatives before the voting, so the privacy of the consumers can be guaranteed.

If the bill passes, the senate can vote in the autumn of 2008. The act of law will then come into force at the beginning of 2009 [38], the smart meters will then be installed in two separate phases. [49] In the starting phase smart meters that are compliant with the NTA version of august 2007 will be installed:

- in all new housing estates.
- in larger renovation projects.
- on request for houses that have an energy label C or lower but require energy label B [46]. Such installations are referred to as a priority placements.
- in case the grid operator decides to place them on a routine meter replacement or in case they honor a customer request.

On request of the Dutch house of representatives additional features will be added to the NTA, making smart meters even smarter. These improved meters will be installed nation wide during the second phase. A schematic overview of the global planning for smart metering can be seen in figure 1.

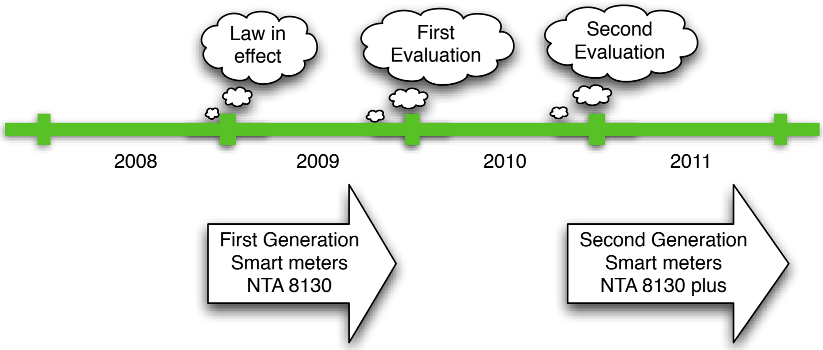

Law in effect
First Evaluation
Second Evaluation
2008
2009
2010
2011
First Generation Smart meters NTA 8130
Second Generation Smart meters NTA 8130 plus

Figure 1: Dutch smart meter planning [58]

All smart meters which are currently being installed in pilot projects and which are not NTA compliant are allowed to stay installed until the end of their economical life, which will be roughly 15 years [58].

1.2 Energy market

Along with the smart metering proposal came the proposal for a new market model for the energy market. This new market model must improve the working of the energy market, which showed some flaws since its liberalization in 2004. A few of the goals of this new model are to make it easier to switch to a new energy supplier, to provide clear and correct billing of energy usage and a single communication channel for consumers. In the new market model the following parties in the Dutch energy market can be identified: suppliers, grid operators and metering companies [48]. The different roles of these parties in the new market model and their role in smart metering will be discussed next.

1.2.1 Supplier

Suppliers are responsible for all customer related processes and are the central point of communication for the customer. A supplier is responsible for the checking and gathering of metering data, which they collect through a certified metering company. Based on the metering data from this metering company the supplier can bill its customers.

1.2.2 Grid operator

Grid operators are the owners of the physical regional electricity grids. They are responsible for the transportation of electricity from various power stations or other grids to the consumer.

In the new market model the meter has been made part of the physical electricity grid. This enables customers to switch from one supplier to another, without having to get a different meter installed. The grid operators are responsible for the administration and the installation of smart meters. They can determine where, by who and when the smart meter will be installed.

1.2.3 Metering company

Suppliers hire metering companies to gather raw metering data from their customers. The metering data is gathered from the various grid operators that have customers from the supplier connected to their grid. Once the data is gathered, the metering company will check and validate this data, after which the clean data is send to the supplier. This flow of information is illustrated in figure 2.

1.3 Dutch standard for smart metering: NTA-8130

The Ministry of Economic Affairs had commissioned the Dutch Normalization Institute (NEN) to determine the minimum set of functions for the metering of electricity, gas and thermal energy at domestic customers. During the process the scope has been narrowed down to electricity and gas only. In April 2007 this effort resulted in the definitive version of the Dutch Technical Agreement (NTA) with reference NTA-8130 [51]. This document defines the legal minimal requirements for smart metering systems that are to be installed in The Netherlands.

To define the minimal requirements for these systems, the concept of ports is used in the NTA. These ports can be physical connections or logical relations between the different components that exist in a smart metering environment. The NTA defines the following ports, which are also shown in figure 3:

- **Port P1** is used for communication between the customer's metering system and one or more modules that can use the information from the meter system. Access to this port is read-only.

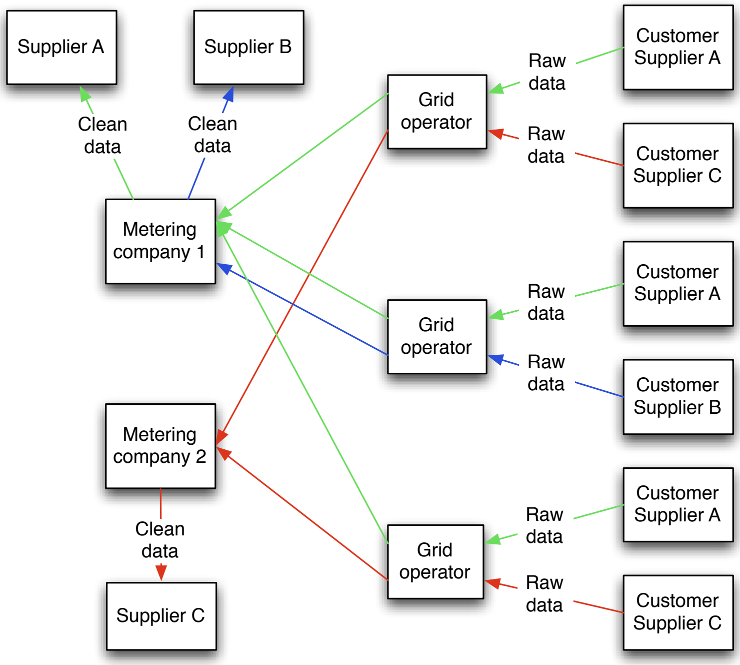


Figure 2: Dutch metering information flow

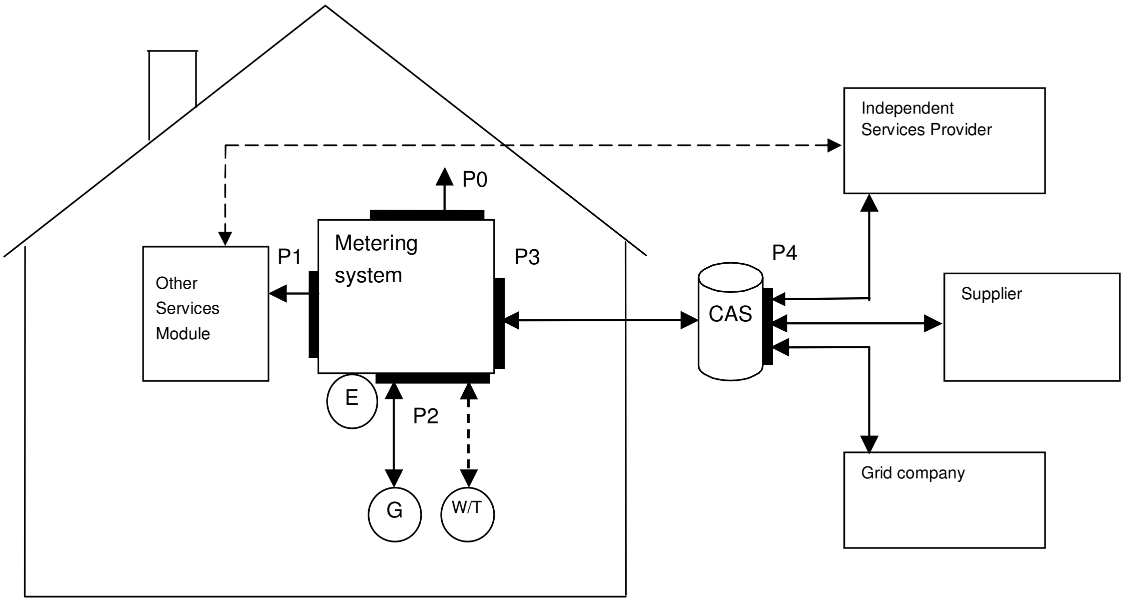


Figure 3: NTA ports

- **Port P2** communicates between the metering system and additional meter sensors, such as a gas or water meter.
- **Port P3** is used for communication between the metering system and a Central Access Server (CAS) that collects metering information from the connected metering systems and can send control commands to the connected devices. Some communication technologies require that the metering system communicates with an intermediate local data concentrator, which will pass the data to the CAS.
- **Port P4** is the port at the CAS which is located at the grid operator and will also be accessible to independent services providers and suppliers.

Besides these four ports defined by the NTA, some smart meters are equipped with a fifth port that provides a connection between the meter and an external device that allows engineers to perform on-site maintenance of the meter. This port is sometimes being referred to as port P0.

From a customer perspective we could also note the supplier's website as a sixth port, P5. This would basically be an extension to port P4 that enables the customer to get information about their energy usage from the supplier.

2 Abstract model for smart metering

ISO/IEC 27002, the Code of Practice for Information Security Management (CPISM), describes information security using the CIA-triad [36]. The CIA-triad defines the following core principles of information security: *Confidentiality*, *Integrity* and *Availability.* To indicate that all three aspects are needed for a secure system, the three aspects are shown in a triangle, hence being referred to as the CIA-triad, see figure 4.

In the CPISM the aspects of the CIA-triad are defined as follows:

- **Confidentiality** “the property that information is not made available or disclosed to unauthorized individuals, entities, or processes”. A breach of confidentiality will occur in case an unauthorized person, entity or process can access the information.
- **Integrity** “the property of safeguarding the accuracy and completeness of assets”. Integrity is closely related to confidentiality. Information that should not be accessible to unauthorised entities should also not be changeable by these entities.
- **Availability** ‘the property of being accessible and usable upon demand by an authorized entity”. Information should be available to authorized entities when the information is needed.

We will use the CIA-triad to identify the different assets of smart metering. The CPISM identifies an asset as anything that has value to an organization. In the case of smart metering the organization contains multiple parties: consumers on one side and suppliers and grid operators on the other.

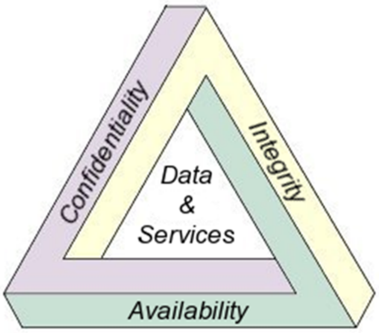


Figure 4: The CIA triad

3 Theoretical analysis

3.1 CIA

Before we will analyze the completeness of the security requirements mentioned in the NTA regulation we will first discuss the importance of security in smart metering using the different aspects of the CIA-triad.

3.1.1 Confidentiality

The detailed metering data from customers is the most important asset that should be considered as confidential in a smart metering system. A complete day-to-day living pattern from each customer can be extracted from this metering data, which is not limited to knowledge about when the customer is at home, at work, on a holiday or when they go to bed. Activities like showering, the use of a washing machine or the use of a toilet, each have a more or less unique pattern in electricity, gas and water usage. This is much more information than the suppliers had before, when a customer reported his usage on a yearly basis; with smart metering the usage can be known from minute to minute. This private information could be useful to criminals like burglars, who can plan their activity using this data. It could also be useful for legal activities such as forensic research by law enforcement.

The CBP also expresses its concerns about all the different systems that hold or can access the consumers usage information and states that all systems holding this private data should be sufficiently protected [7].

According to the goals of the Dutch government the meters must also support a pre-paid payment system. Depending on the implementation of such system this could contain confidential information. In a pre-paid system "energy credits" have to be bought in advance, which could be implemented as a website where the banking information of the customer might be stored. Confidentiality of such data is an important condition.

3.1.2 Integrity

Not only should the metering information of the customer be confidential, also the integrity of the information has to be protected, because this information is used for billing. For both the customer and supplier it is important that this information is correct and not prone to interference in the meter itself or externally in the communication channel towards the utility company. Also, it should not be possible for the customers to modify or generate messages with incorrect usage data influencing their usage totals.

With the introduction of the smart meter customers do not have to report their usage themselves, which changes the relation between the customer and the supplier. First the supplier had to trust the consumer to provide him with the correct usage information, now the customer has to trust both the smart meter and the supplier to register the correct usage information. It is important that the customer can get a detailed view into his actual usage and that he can check the data on the invoice. This is partially covered by the Dutch Measurement Institute (Nederlands Meetinstituut NMi) which approves metering devices to guarantee a correct measurement of energy usage. Customers could check their usage using the display on the meter and using appliances that are connected to the P1 port as defined in the NTA.

Smart meters are placed in the residence of the consumer, which gives the consumer physical access to the meter. Therefore it is important that the integrity of the smart meter configuration is guaranteed. First of all, changes in the communication settings of the smart meter could make it impossible for the utility company to communicate with the meter. The consumer could also try to influence their usage information through the local configuration options of the meter.

3.1.3 Availability

From a customer perspective availability in smart metering systems means the availability of electricity, water and gas itself in the first place. For a grid operator the availability of meter data from the smart metering system would be a second important asset.

Before smart metering was introduced, electricity, water or gas would usually always be available unless there are problems somewhere on the grid or in case the supplier physically disconnected the supply to a customer. Smart meters enable suppliers to remotely switch off customers in case of an emergency or in case customers have not paid their invoices or are committing fraud. This could mean that a customer can be accidentally switched off, that a disgruntled employee switches off customers or that this feature could be used in a "terrorist" attack on the power grid. In case a customer can interrupt the communication of the smart meter the supplier can't receive metering data and would not be able to disconnect the power supply remotely.

By cutting off lots of customers the available power load in the distribution network could become too high, and could cause a cascading effect through the distribution network which could in turn lead to a large blackout. This also works the other way around, by switching a large amount of customers back on at the same time demand could get to high in certain points of the distribution network, which could also lead to a blackout [6, 52].

3.2 NTA

In previous sections the importance of security in smart metering systems has been explained. Next the various security aspects based on the ports as mentioned in the smart metering introduction will be analyzed. This port based view will provide a guidance to cover all aspects of the system where security comes in.

3.2.1 Port P0

Port P0 provides local administrative access to service engineers during installation or maintenance of smart metering systems. Households have physical access to their metering system, and therefore could try to connect to the metering system using the right equipment to interface with the P0 port. Depending on the configuration options that are available through P0, this could lead to a security breach where meter data or tariff settings can be altered, which could affect data integrity. Meter data availability will be affected when communication settings of other connected ports could be modified.

A second implementation of port P0 could be a set of configuration buttons on the meter itself combined with an optional display that allows an engineer to readout or modify meter settings. In case poor protective measures such as a secret key combination are being used to access these administrative features, this could lead to simple to perform attacks that don't require any additional hardware.

As mentioned in the NTA introduction, port P0 is not a part of the NTA specification, which means that there are no legal minimum security requirements available. Because an insecure implementation of port P0 could lead to security breaches on other ports and data integrity, port P0 should really be part of the NTA specification and should have a defined minimum security level. An overview of the possible P0 security risks are displayed in table 1.

Confidentiality	• Disable or alter data security parameters
Integrity	• Reset or alter metering data • Alter tariff settings
Availability	• Disrupt communication to CAS (P3) • Disrupt communication to Gas or Water meter (P2)

Table 1: Port P0 security risks

3.2.2 Port P1

Information about energy usage and various other parameters are distributed every 10 seconds through port P1. According to NTA requirements this port is implemented using a RJ11 connection as its physical form factor and EN 62056-21 mode d (read-only) [32] as its communication protocol. The intended use for this port is to allow a connection to other equipment that will inform users about their energy usage, such as thermostats or specialized displays.

Poorly secured devices that are being connected to the P1 port can introduce new security threats on the confidentially aspect of the CIA triad. This could especially introduce a risk when wireless devices such as energy usage displays are being connected through port P1. Because the explicit definition of a read-only protocol this port should not introduce any integrity or confidentiality issues. An overview of these security risks can be found in table 2.

Confidentiality	• Poorly secured devices connected to P1 • Wireless devices connected to P1
Integrity	N/A
Availability	N/A

Table 2: Port P1 security risks

3.2.3 Port P2

To communicate with other meters such as gas and water meters, the smart meter utilizes the Meter-Bus (M-Bus) protocol, in which the smart electricity meter acts as a master and polls its slave devices regularly to gather meter data. According to the NTA there a two possible communication protocols that can be utilized which are wired M-Bus as specified in EN 13757-2 [15] and wireless M-Bus operating at 868 MHz as specified in EN 13757-4 [17]. This limitation prevents manufacturers from inventing their own proprietary protocols.

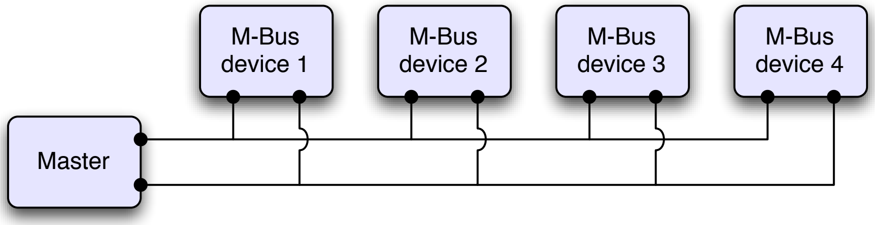


Figure 5: Wired M-Bus as specified in EN 13757-2

The wired M-Bus protocol is implemented as a serial bus, which makes it fairly easy to add extra devices to the bus and tap in to listen to traffic that passes the bus. Because of the master-slave configuration, it is not possible to send commands directly to the smart meter, but manipulating or faking responses to a request from the master device could be possible. Another security threat could be caused by a device on the bus that acts as a rogue master and tries to send commands to the slave devices on the bus. An example of a command that could be sent to a slave device is to close or open the valve of a gas or water meter.

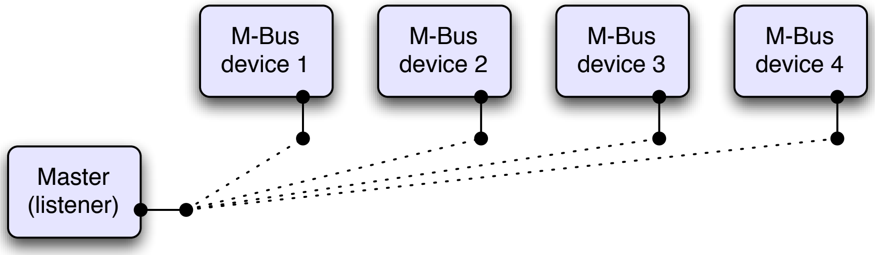


Figure 6: Wireless M-Bus as specified in EN 13757-4

In a wireless configuration the slave regularly, for example once a day, contacts the master (listener), i.e. the electricity meter, to deliver its meter data. This approach is used to enable the slaves to turn their wireless system off most of the day and save battery power. This could be necessary in case gas or water meters don't have access to an AC power supply. Using this configuration it could be possible to send fake meter data to the smart meter and influence meter data. A rogue master could also try to send fake commands to the slave devices when they are online. Table 3 gives an overview of the various P2 security risks.

The EN 13757-2 and 13757-4 protocols define the physical and data-link layers of the M-Bus protocol, and don't include any encryption options. However, the 13757-3 [16] protocol of the 13757 suite describes DES as optional encryption in the application layer. These or other encryption options are not mentioned in the NTA specification.

About P2 security, the NTA notes the following: "The security levels of the M-bus protocol are configured in such a way that interoperability of port P2 is guaranteed". This implicates that encryption is allowed, but compatibility between various devices has a higher priority according to the NTA specification.

Confidentiality	• Wireless M-Bus sniffing
Integrity	• Alter meter data of M-Bus connected meters
Availability	• Block P2 communication to and from meter • Send fake valve close commands to wireless M-Bus gas or water meters • Send fake valve open commands to M-Bus gas or water meters

Table 3: Port P2 security risks

3.2.4 Port P3

The NTA defines that electricity usage will be collected using a 15 minute interval and gas usage using a 1 hour interval. This detailed data will leave the residential environment at least one a day through port P3 and will be collected at an intermediate gateway or will be delivered to the CAS directly.

Using such short intervals has an additional impact on the confidentiality aspect of the CIA-triad, because detailed information about the consumer's living pattern could be extracted from this data. To provide a customer with an accurately monthly bill, sending daily or monthly aggregated metering totals should be sufficient.

The NTA allows the following three communication methods for port P3 communication:

- Power Line Communication (PLC)
- GPRS
- Ethernet

Some companies are using both PLC and GPRS, because PLC is sometimes unusable in old neighborhoods because of the poor quality of power lines, whereas GPRS is not always useable due to poor GPRS coverage in rural areas. The various technologies will be discussed in this section.

PLC

No protocol specification for PLC is mentioned in the NTA, which allows manufacturers to use their own proprietary protocol. It seems that at this time an industry standard for power line communication is not yet available, which causes many companies to implement different protocols. Protocols designed for in-house powerline communication such as those developed by the HomePlug Powerline Alliance [29] are not being used for automatic meter reading.

It is possible that power line signals from multiple households can be monitored at a single location in the neighborhood connected to same local transformer station. Security measures are needed to ensure data privacy and prevent hackers from sending malicious commands to the residential smart meters.

GPRS

GPRS uses the GSM network as a basis and is generally combined with the use of IP. The GSM protocol is generally not considered secure which could make GPRS sniffing theoretically possible, although affordable hardware that could facilitate this isn't widely available yet. Another threat could be a fake GSM/GPRS base station transmitting a stronger signal which causes the smart meter to reconnect to the rogue base station and could be used to gain access to the meter through port P3, or to facilitate a man in the middle attack.

Ethernet

Ethernet could be used for communication over the Internet using a broadband connection that is already available at many households. This would be an attractive medium for hackers, because tools for sniffing and manipulating Ethernet PDU's are widely available.

Requirements

The NTA contains the following general statement about P3 security: "The electricity grid operator will take appropriate measures on identification, authentication and authorization regarding the metering system and encryption of data communication between the metering system and the CAS, independent of the communication medium being used."

These requirements are not defined according to the S.M.A.R.T. principle[1] and therefore it would be hard to measure whether these requirements are met. This could lead to discussions about which measures on identification, authentication and authorization are 'appropriate' and which encryption standard would be strong enough. Therefore the NTA should specifically note measurable security requirements for port P3. An overview of the P3 security risks is included in table 4.

[1] Specific, Measurable, Attainable, Realistic, Time bound

Confidentiality	• Sniffing communication from meter to gateway (PLC) • Sniffing communication from gateway to CAS (PLC) • Sniffing communication from meter to CAS (GPRS, Ethernet)
Integrity	• Alter communication stream from meter
Availability	• Disrupt communications from meter • Send fake control commands to meter systems • Denial of Service attack to meter systems

Table 4: Port P3 security risks

3.2.5 Port P4

Port P4 is located at the back-end of the grid operator and provides suppliers access to meter data and settings of their customers. Security of this back-end system should be very strict, because the CAS functions as a large concentrator and contains metering data and metering settings from many customers. Security breaches at this point could lead to a large scale attack on the availability of public utilities. A security evaluation of the operator's back-end system is beyond the scope of this research project. Table 5 provides an overview of P4 security risks.

The NTA notes the following about P4 security: "The grid operator will arrange identification, authentication and authorization of market parties in such a way that they can only access functions that they are allowed to control."

Confidentiality	• Large scale disclosure of customers' metering data
Integrity	• Corruption of metering data
Availability	• Large scale broadcasting of control commands to meter systems • Denial of Service attack at the CAS

Table 5: Port P4 security risks

3.2.6 Port P5 (website)

One of the goals of smart metering systems is to inform consumers better and more often about their energy usage, which could be implemented as a web application at the suppliers website. The customers could also be given remote access to some of the functions of their smart metering system, such as the ability to switch electricity and gas on or off remotely. When prepaid solutions are rolled out, an interface to upgrade the customer's credit could also be implemented at the suppliers website.

This sixth port is outside the scope of the NTA specifications, and therefore no security requirements are listed. Of course general security guidelines for developing web application should apply. When suppliers fail to develop a secure website this could lead to a serious privacy breach where the metering data of many customers would become public. Because of the privacy aspects the suppliers website should at least use a secure connection (SSL) and access should require a username and strong password. The P5 security risks are displayed in table 6.

Confidentiality	• Shoulder surfing to obtain login credentials • Sniffing on (wireless) LAN to obtain login credentials
Integrity	N/A
Availability	N/A

Table 6: Port P5 security risks

4 Practical analysis

During our research we have gathered information about smart metering systems from various manufacturers. The level of access to information about these metering systems varied per manufacturer, which will influence the specificness of the conclusions that can be drawn about these systems. The practical analysis is based on information from the following manufacturers and grid operators or installation companies that use equipment from these manufacturers:

- Sagem
- Iskraemeco
- Echelon / Enel (Oxxio meter)
- Landis+Gyr (combined with Xemex GPRS module)
- EnergyICT

It is important to note that none of the currently implemented smart metering systems are required to fully comply to the NTA, because they were rolled out before the NTA was completed. Even smart metering systems that are being implemented today are not required to be NTA complaint, because the NTA regulation is not yet in effect.

Feasibility classification

We will use the following classification to indicate the attack feasibility of the different attack vectors as discussed in the theoretical analysis:

- **Research required** We were not able to define the attack feasibility of the corresponding attack vector due to a lack of detailed information.
- **Not feasible** The attack vector mentioned is not likely to occur because appropriate protection is applied to prevent this attack, or because high costs (time or money) are involved to perform such an attack.
- **Feasible** Although we were not able to perform this attack ourselves, the corresponding asset is not protected sufficiently, the equipment needed is available at low costs and the attack can be performed within a reasonably short time.
- **Possible** The attack has been tested and verified during our practical research.

4.1 Port P0

All of the smart electricity meters from the manufacturers that are mentioned before feature an optical interface used for meter reading and programming, as illustrated in figure 7. Some meters, such as those from Sagem, feature a set of buttons that can be used as an additional interface to access programming functions. In this section the implementation of these management interfaces and their security implications will be discussed.

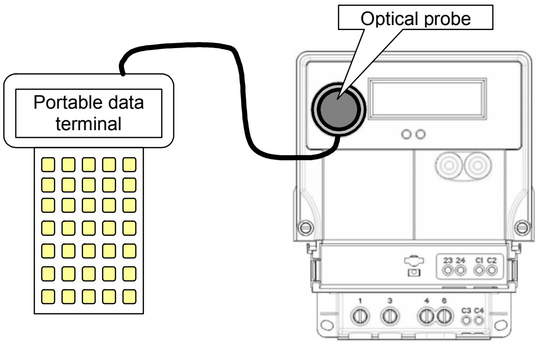


Figure 7: Illustration of a IEC 62056-21 optical probe connected to a meter [61]

4.1.1 Implementation (Optical interface)

The optical interface featured on smart meters from almost every manufacturer is specified in the IEC 62056-21 international standard for meter reading and programming [32]. The protocol defined by this standard is designed to operate not only over an optical interface, but can also be used combined with other media such as modem lines or other wired or wireless connections. Our analysis in this section is based on the information from the IEC standard and documentation received about Landis+Gyr and Sagem meters.

IEC compatible optical interfaces are widely available from suppliers such as Relay GmbH for less then 100 euros [60], and usually feature an USB of RS-232 connector to interface with a personal computer. Models with special connectors to interface with PDA's are also available on the market. The physical form factor of the optical probe is also specified in the IEC standard, which should ensure interoperability between probes and meter systems from different suppliers.

IEC specifications

The IEC specification defines the following set of communication modes:

- **Mode A** supports bidirectional data exchange at 300 baud without baud rate switching. This protocol mode permits data readout and programming with optional password protection.
- **Mode B** offers the same functionality as protocol mode A, but with additional support for baud rate switching.
- **Mode C** offers the same functionality as protocol mode B with enhanced security and manufacturer-specific modes.
- **Mode D** supports unidirectional data exchange at a fixed baud rate of 2400 baud and permits data readout only.
- **Mode E** allows the use of other protocols.

Various commands for communication between the meter and reading device are defined within the IEC protocol, which are: password(P), write (W), read (R), execute (E) and exit/break (B). To access protected data in mode A and B, the password command should first be executed to gain access to this data. For the password command, the following command type identifiers are defined:

- **0** - data is operand for secure algorithm
- **1** - data is operand for comparison with internally held password
- **2** - data is result of secure algorithm (manufacturer-specific)
- **3-9** - reserved for future use

These defined command type identifiers allow static passwords (1) or a manufacturer-specific challenge-response algorithm (0 and 2). Furthermore operation mode C supports manufacturer-specific enhanced security, which is out of the scope of the IEC standard.

The parameter data coding section of the IEC document describes a few examples of parameter data, which include parameter registers for password storage. These storage registers allow passwords varying from 4 to 8 characters. The definition of "character" in this context is unclear.

Besides this password protection, the IEC standard defines a set of security levels for use in combination with mode C. According to the standard, any or all of these may be used by a metering device:

- **Access level 1** only requires knowledge of the protocol to gain access.
- **Access level 2** requires a password to be correctly entered.
- **Access level 3** requires operation of a sealable button or manipulation of certain data with a secret algorithm to gain access.
- **Access level 4** requires physical entry into the case of the meter and effecting a physical change, such as making/breaking a link or operation of a switch, before further communications access is allowed.

IEC implementation

We have compared the password security as defined in the IEC standard with available documentation from Landis+Gyr to gain insight of the implementation of the IEC standard in an actual meter. We examined the user manuals of the MAP110 and MAP120 software which are "able to communicate with all modern electronic meters from Landis+Gyr and also with many units from other manufacturers, which comply with the standards according to DLMS or IEC 62056-21". This tool covers, among others, the following service functions that can be accessed using an optical probe [42, 43]:

- Billing data readout
- TOU (Time of Use) readout and modification
- Billing period reset
- Register and profile resets
- Parameter readout and modification
- Communication input settings
- Analysis and diagnostic functions

Landis+Gyr meters feature several access levels with different security attributes. Level 0 is intended for public access and only allows parameter reading without password protection. Level 1 and 2 are intended for data collection and field service and allow limited write operations using a password.

Password protection for Landis+Gyr meters is adopted from the IEC specification, and allows passwords of exactly 7 or 8 hexadecimal characters, i.e. characters 0-9 and A-F. This results in an effective password strength of 32-bit, which allows 4.294.967.296 possible password combinations.

Level 4 access is intended for extended utility service and allows access to settable and parameterizable data such as register clearing, password setting etc. Access level 4 does not require a password, but requires a correct setting of the security switches that are accessible under the main cover of the meter, protected by a certification seal.

Sagem meters feature a comparable security mechanism: "To avoid any untimely modification, an option can be factory-programmed to authorise optical link programming only when the terminal cover is open."

It is important to mention that not all functions will be available on every meter. Industrial meters will feature more configuration options then smart metering systems found in most households. However, contacts at various grid operators and suppliers confirmed that the optical port is being used to configure tariff and communication settings of smart meters that are being used in The Netherlands. For example the day/night tariff setting of meters from electricity supplier Oxxio can be configured by an engineer during installation through the optical interface using a PDA.

4.1.2 Implementation (Configuration buttons)

Management functions that are accessible through configuration buttons on the metering device are manufacturer-specific, because they are not defined in any standard.

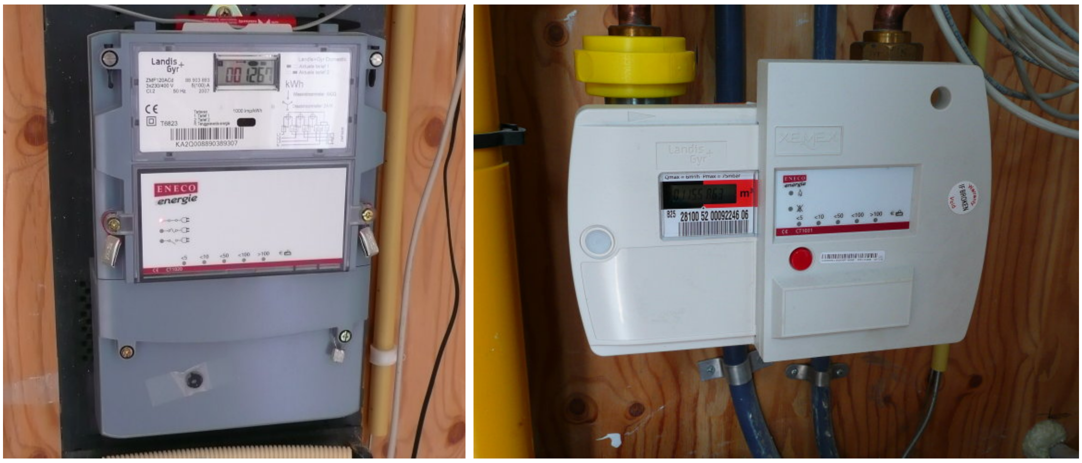
For this research, only user manuals of Sagem meters were available, but other meters are likely to offer similar functionality. The Sagem CX1000 and CX2000 meters support the following operations which are only available when the terminal cover is open, using the configuration buttons [61, 62]:

- Activate (or deactivate) the communication data encryption key
- Date and time setting
- M-Bus device installation
- M-Bus device deinstallation

The most important options from a security perspective are the deactivation of data encryption and deinstallation of M-Bus devices. Deactivation of data encryption could lead to confidentiality breaches, and the deinstallation of connected M-Bus devices could lead to metering data availability breaches.

4.1.3 Practical research

For this research access to a smart metering system, supervised by a supplier or grid operator was not available, which limited the practical research that could be done. We did gain access to a live smart metering system operated by the Eneco grid operator installed at a household in Moordrecht. This smart metering system consists of a modular Landis+Gyr electricity meter type ZMF120ACd, combined with a Xemex GPRS communication module type CT1020 and a



(a) Electricity meter

(b) Gas meter

Figure 8: Landis+Gyr / Xemex smart metering system installed by Eneco in Moordrecht

Landis+Gyr gas meter combined with a Xemex CT1031 wireless RF communication module, as shown in figure 8.

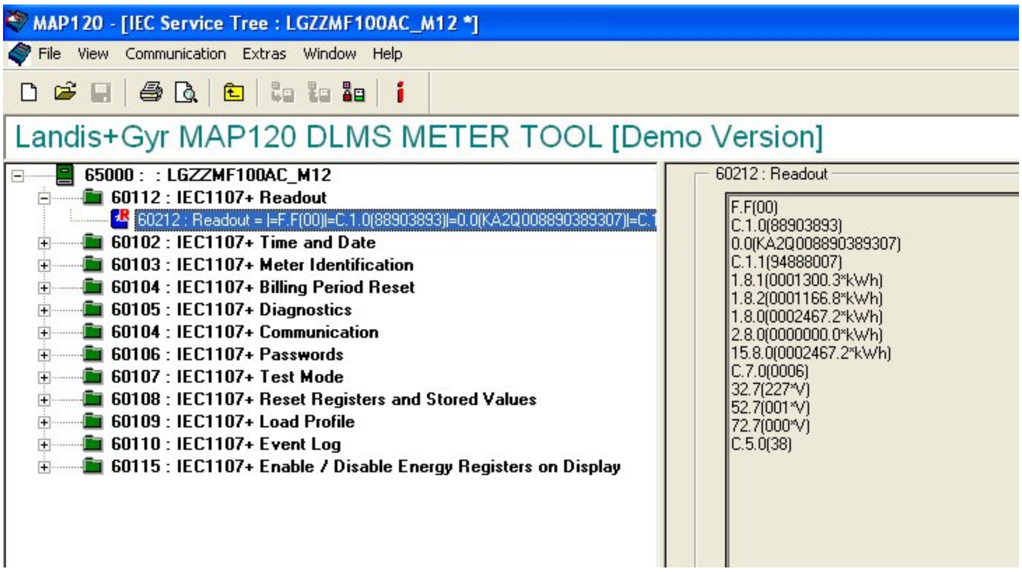
The Landis+Gyr electricity meter features an optical connection, which is the small black window, just below the meter's display. The connection between the meter and the integrated pluggable communication module is a wired connection that uses the IEC 62056-21 protocol to communicate with the meter [44]. The point-to-point nature of the IEC 62056-21 protocol makes it unlikely that direct communication with the Xemex GPRS module is possible through the optical port of the meter.

Most of the intelligence, including external communication through GPRS and internal communication with the gas meter using RF, is handled by the Xemex communication module. This Xemex communication module will probably feature its own management interface which is not accessible from the outside of the module.

It could be possible that some basic settings, such as date/time and tariff properties are available through the optical port of the Landis+Gyr meter. We have tried to interface with the meter using a demo version of the MAP120 software from Landis+Gyr and an optical probe from P+E Technik [56].

Using this software it was possible to do a meter readout, and gather information about the power usage, as shown by the screenshot in figure 9. All other functions such as date and time readout were not functioning. While trying to access these functions, communication between the PC and optical probe was visible using a serial port sniffer, but could not be interpreted by the MAP120 software tool. Sniffing traces from the succeeded data readout and the failed date and time readout are included in appendix A. It seems that the protocol that is being used by both the meter and MAP software does not fully comply to the IEC specifications.

Additional research is needed to analyze the implementation of the IEC 62056-21 configuration commands and security implementations on other smart metering systems. This would be especially interesting with meters that feature a truly built-in communication module where its configuration is likely to be accessible using the optical port.


MAP120 - [IEC Service Tree : LGZZMF100AC_M12 *]
File
View
Communication
Extras
Window
Help
Landis+Gyr MAP120 DLMS METER TOOL [Demo Version]

```
65000 :  : LGZZMF100AC_M12
    60112 : IEC1107+ Readout
        60212 : Readout = |=F.F(00)|=C.1.0(88903893)|=0.0(KA2Q008890389307)|=C.1
    60102 : IEC1107+ Time and Date
    60103 : IEC1107+ Meter Identification
    60104 : IEC1107+ Billing Period Reset
    60105 : IEC1107+ Diagnostics
    60104 : IEC1107+ Communication
    60106 : IEC1107+ Passwords
    60107 : IEC1107+ Test Mode
    60108 : IEC1107+ Reset Registers and Stored Values
    60109 : IEC1107+ Load Profile
    60110 : IEC1107+ Event Log
    60115 : IEC1107+ Enable / Disable Energy Registers on Display
```

60212 : Readout

```
F.F(00)
C.1.0(88903893)
0.0(KA2Q008890389307)
C.1.1(94888007)
1.8.1(0001300.3*kWh)
1.8.2(0001166.8*kWh)
1.8.0(0002467.2*kWh)
2.8.0(0000000.0*kWh)
15.8.0(0002467.2*kWh)
C.7.0(0006)
32.7(227*V)
52.7(001*V)
72.7(000*V)
C.5.0(38)
```

Figure 9: Meter readout using an optical probe and Landis+Gyr MAP120 software

4.1.4 Attack feasibility

We have verified that at least some of the attack vectors as summarized in table 7 are accessible through port P0. Alteration of security settings and disruption of communication to Gas or Water meters are possible on Sagem meters, but require opening of a cover which will break a security seal and possibly activate a tamper switch. Disruption of P3 communication settings could not be verified. Alteration of tariff settings is verified by information received from Oxxio.

C	• Disable or alter data security parameters	Feasible (seal protection)
I	• Reset or alter metering data	Research required
	• Alter tariff settings	Feasible
A	• Disrupt communication to CAS (P3)	Research required
	• Disrupt communication to Gas or Water meter (P2)	Feasible (seal protection)

Table 7: Port P0 attack feasibility

It is questionable whether the security seal and tamper detection of the cover can prevent unauthorised use of programming functions through the optical port. Grid companies have confirmed that tamper switches can generate false positives caused by passing metro trains. Therefore, it is questionable whether grid companies will check every case of tamper detection. Sealing tools are also widely available at low costs at Ebay for example, which could give attackers the opportunity to reseal the meter after reprogramming. Furthermore, disruption of P3 communication could prevent tamper alerts from being send to the grid operator.

The optical port is an easy way to interface with a smart metering system which makes it likely that attacks on this port will be developed by researchers or attackers. The most important meter settings will require breakage of a seal, but it is questionable whether this would stop a dedicated attacker.

4.1.5 Recommendations

Authentication

A first possible solution to prevent the security risks as mentioned above would be to use a unique strong password on each meter that is being installed. Unfortunately this will lead to a serious password management issue when a smart meter is installed in every Dutch household.

Cryptographic authentication could be another option to solve these authentication issues, but it is questionable whether the computational power of smart meters is sufficient to perform these tasks. There are different options to implement cryptographic authentication for smart metering systems.

A first solution would be to use a unique cryptographic certificate for each service engineer that can be verified against a root certificate by the meter itself. This provides additional challenges in certificate revocation and key distribution to the service engineers.

A second solution could be the use of a challenge-response system, where the meter will send a challenge to the reading or programming device. The reading or programming device can encrypt this challenge using a shared secret key and send the encrypted value to the meter as a response.

Another solution would be to use a Kerberos-like protocol [41] in which an engineer would receive a ticket from a ticket granting server (TGS) that can be checked by the meter. An advantage of this algorithm is that the meter itself does not need to have a connection to the ticket server.

Sealing

It is very important that management functions of the meter system are only available after a strong authentication process is completed. Some manufacturers rely entirely on switches that can set the meter in programming mode and are only protected by a security seal. It should not be possible to evade authentication and gain access to management functions only by breaking such seal.

4.2 Port P1

None of the meters from any manufacturer we have seen offers a NTA compliant P1 port. Therefore, a practical research of the security of this port is not possible. Additional research will be necessary when P1 featuring meters and accessories that connect to this port become widely available.

4.2.1 Attack feasibility

No practical research has been done, further research is required when devices become available that make use of the P1 port. This is summarized in table 8.

C	• Poorly secured devices connected to P1 • Wireless devices connected through P1	Research required Research required
I	N/A	-
A	N/A	-

Table 8: Port P1 attack feasibility

4.2.2 Recommendations

In case of wireless devices that connect to port P1, such as an access point that sends usage data to a wireless display it is important to use encryption. When no or weak encryption is used somebody in the perimeter of the resident could get hold of the usage information using a wireless sniffing device.

4.3 Port P2

Communication between the electricity meter and gas or water meters is implemented using port P2. Both wired and wireless implementations are available, which will be discussed in this section.

4.3.1 Implementation

Wired

All of the implementations we have seen during our research which used a wired connection between the electricity and the gas or water meter were using the M-Bus protocol. Companies implementing M-Bus for their smart metering systems are Continuon, Delta and probably others. Almost every manufacturer is offering wired M-Bus compliant devices, which include but is not limited to: Sagem, Iskra-Emeco, Echelon and EnergyICT.

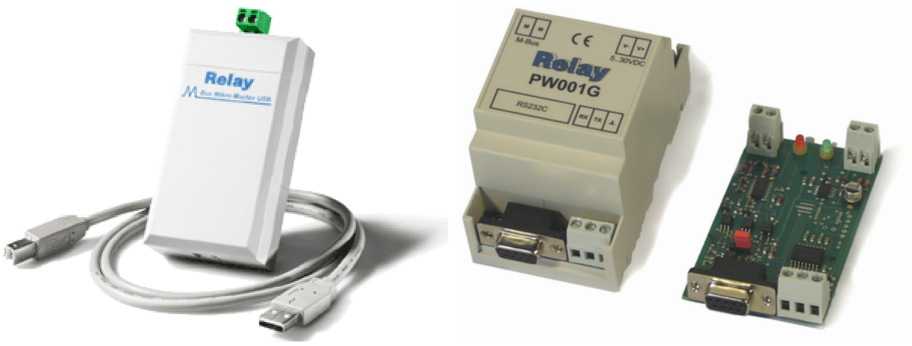
M-Bus is specified in two international standards: the EN 13757-2 [15] defines the physical and data link layer, while the EN 13757-3 [16] specifies the application layer of the OSI stack which can be seen in table 9.

Layer	*Functions*	*Protocol*
Application	Data structures, data types, actions	EN1434-3
Data link	Transmission parameters, telegram formats, addressing, integrity	IEC 870
Physical	Cable, bit representation, bus topology, electrical specs	M-Bus

Table 9: M-Bus protocol layers

The M-Bus application layer defines some basic functionality for data readout of different meter systems. Additional functions such as valve control are not specified in the M-Bus standards as is mentioned in the Application Layer M-Bus Rev.4 standard [45]: “this standard contains only directions how data should be coded. It is beyond the task of an application layer standard to define which data must be transmitted under what conditions by which types of slaves or which data transmitted to a slave must have which reactions. Therefore adherence to this standard guarantees the coexistence and common communication and readout capability of slaves via a universal master software (covering all optional features), but not yet functional or communication interchangeability of meters following this standard.” To summarize, adherence to the M-Bus standards does not guarantee any operability between M-Bus devices from different manufacturers.

Various equipment is available that enables a PC to interact with a M-Bus communication channel. One of the manufacturers of such equipment is Relay GmbH which offers [60] a RS-232 M-Bus slave level converter for 69 euros and a USB M-Bus master for 151 euros as shown in figure 10. A slave level converter could be used to sniff M-Bus traffic and to simulate a M-Bus slave device such as a gas or water meter. The M-Bus master could be used to simulate an electricity meter and to send commands to M-Bus slaves, such as valve control commands for gas meters. Engineers at Delta also use the Relay M-Bus master and its companion software to test M-Bus setups and diagnose M-Bus problems. This makes it realizable for customers whose gas delivery is remotely



(a) M-Bus Micromaster (b) M-Bus Slave level converter

Figure 10: Relay GmbH M-Bus master and slave PC interfaces

blocked by their grid operator to connect a M-Bus master to their gas meter and send a "open valve" control command to reactivate gas supply.

A special signature field is mentioned in the Application Layer M-Bus Rev.4 standard which is reserved for optional encryption of application data. The standard notes that "such an encryption might be required for transmit only wireless meter readout. It is assumed, that each meter (or a group of meters) could have an individual encryption key."

Data Encryption Standard (DES) with Cipher Block Chaining (CBC) is specified as the encryption algorithm for the optional M-Bus security. According to this standard the Initialisation Vector for the CBC should be all zeroes or a combination of the device id, manufacturer id and the current date. The actual message should always start with the current date to prevent replay attacks. However, choosing a predictable initialisation vector is not advised, because it could simplify cryptographic attacks [68].

We haven't seen any of the manufacturers implementing encryption for their wired M-Bus devices, which is confirmed by a Delta engineer. This will enable attackers to send fake meter data to the electricity meter and re-open the valve of their gas meter when closed by their supplier. Finally, an attack on the meter data availability is extremely simple by cutting one of the two wires of the M-Bus connection.

Wireless

Wireless M-Bus was later added to the EN 13757 series which could explain why none of the smart metering systems we have seen has implemented wireless M-Bus. Instead a few proprietary implementations of RF protocols exist for wireless communication between the electricity and gas or water meter.

One of the protocols we have seen is the Radian protocol that operates at 433 MHz and is used by Actaris and the Oxxio smart metering system produced by Echelon. This protocol has been developed by eight players in the metering and radio market (EDF, Gaz de France (GDF), Severn Trent Water, Aquametro, Itron, Schlumberger, Sontex and Viterra Energy Services). The protocol is being promoted as "open", but only members of the Radian Association have access to its specification [2]. Therefore a practical analysis of this protocol was not possible.

The Xemex module that is used by Eneco features its own proprietary wireless protocol which also operates at 433 MHz [70]. This protocol is being referred to as the "WatchTalk Protocol" and can communicate with other Xemex wireless modules, such as the modified Landis+Gyr gas meter as seen in figure 8. No specifications of the protocol were made available, which made a practical analysis of this protocol not possible within our limited timeframe.

It is unclear whether encryption is being used in any of the proprietary RF protocols that are used today, or whether it will be used in NTA compliant wireless M-Bus implementations in the future. Further research is required to verify this. Generic devices that can sniff and simulate wireless signals, such as GNUradio [26] could be used to analyse this.

4.3.2 Attack feasibility

We have seen that simulation of a wired M-Bus master to send fake control commands is possible using a M-Bus Micromaster, making such an attack feasible. It is also possible to simulate a M-Bus slave using the M-Bus slave level converter, which makes simulation of a gas or water meter to send fake meter data feasible.

Although the wireless encryption as defined in the M-Bus specification contains a potential weakness, further research is required for attacks on wireless communication. This is applicable to both wireless M-Bus as well as the various proprietary wireless protocols that are available. An overview of the different attacks is displayed in table 10.

C	• Wireless M-Bus sniffing	Research required
I	• Alter meter data of M-Bus connected meters	Feasible
A	• Block P2 communication to and from meter	Feasible
	• Send fake valve close commands to wireless M-Bus meters	Research required
	• Send fake valve open commands to M-Bus meters	Feasible

Table 10: Port P2 attack feasibility

4.3.3 Recommendations

Encryption and authentication between devices is necessary and should be required by the NTA. Especially in a wireless environment sniffing of meter communication could affect the confidentiality of meter data. Unauthorised control command could lead to a breach of availability when gas or water valves could be controlled from a remote distance.

It would be recommended to update the M-Bus standard to a more modern encryption mechanism which could replace the single DES standard. In case the M-Bus standard defines encryption as mandatory instead of optional, more manufacturers would be likely to implement those features.

4.4 Port P3

Port P3 is defined as the communication port between the meter and grid operator. The NTA defines PLC, GPRS and Ethernet as possible communication technologies. Communication can take place directly from the smart meter to the CAS at the grid operator or through an intermediate data concentrator (DC) which passes it data to the CAS. Besides the technologies mentioned in the NTA we will also describe radio frequency (RF) based systems which are being used in various pilot projects.

4.4.1 Implementation

Ethernet (IP)

Delta Energy is the only grid operator we have found testing a smart metering system which uses a broadband Internet connection as a communication channel. Delta is also the cable network operator in Zeeland, which gives Delta an unique chance to experiment with this technology in a controlled environment. A pilot project has been rolled out at Delta employees. An schematic overview of this pilot is shown in figure 11.

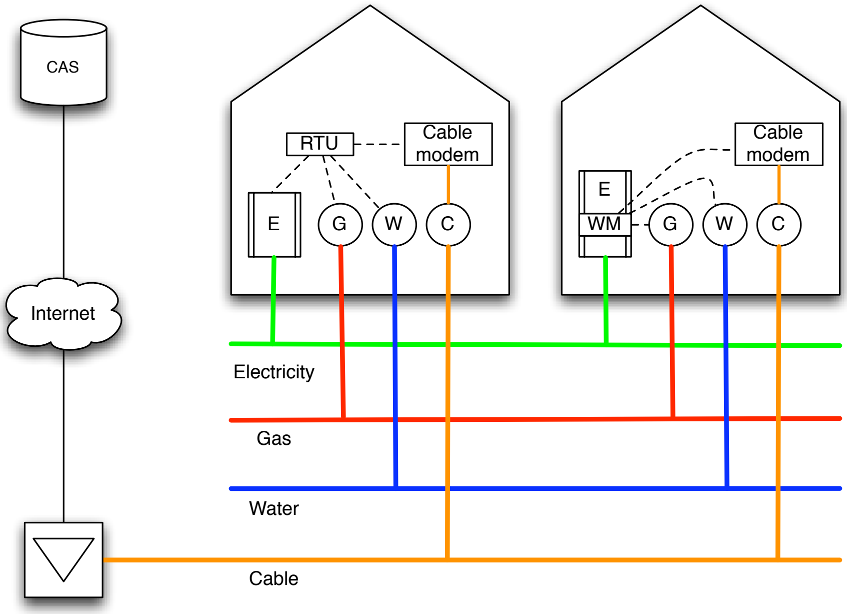


Figure 11: Cable Internet smart metering implementation [22]

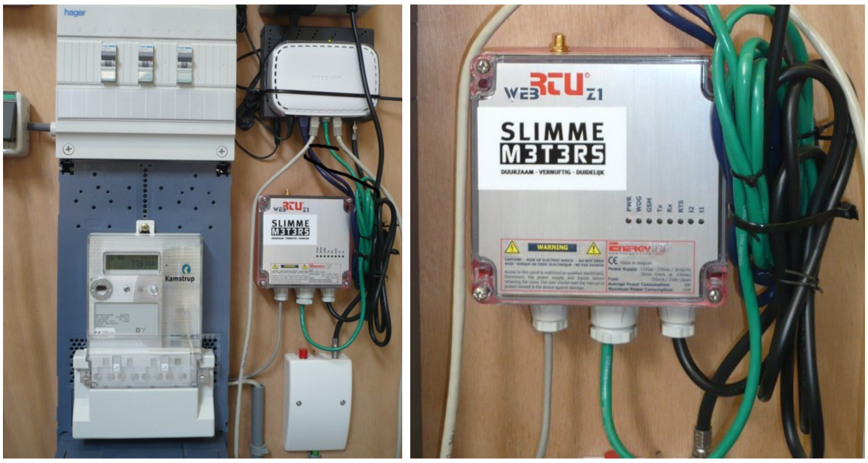
For one of Delta's IP pilots a Kamstrup electricity meter has been used that communicates using wired M-Bus with a WebRTU Z1 data logger as shown in figure 12. A water and gas meter are also connected to the WebRTU using wired M-Bus communication. The WebRTU is connected to a cable modem and is accessible from the public Internet using port forwarding. The WebRTU functions as a data logger and does not provide functionality to control the connected M-Bus devices, such as valve opening or closing.

In this pilot project the EIWeb protocol is used for the communication between the WebRTU and the CAS. EIWeb is "the proprietary, preferred protocol designed by EnergyICT that is used for transferring the stored consumption data from the WebRTU to a central system such as EIServer. The EIWeb protocol is based on HTTP and requires either a CGI application or a Java servlet on the server side." [19] EnergyICT has confirmed that the WebRTU basically utilizes a HTTP POST request to submit its metering data.

One of the configurable parameters in the WebRTU is the URL of the CGI script or servlet that the WebRTU uses to deliver its data. The URL is a standard HTTP URL which provides no encryption by default. To provide data security an encryption key can be set of "16 alphanumeric characters that serve as the key for encrypting the transferred data. The remote server to which you are transmitting the data also needs to have this key for decrypting the data." [20]

EnergyICT did not provide detailed information about their proprietary EIWeb encryption, except that it should be possible to use a different encryption key for each WebRTU. Because both the client (WebRTU) and the server side need to know the encryption key this would most likely be some form of symmetric encryption.

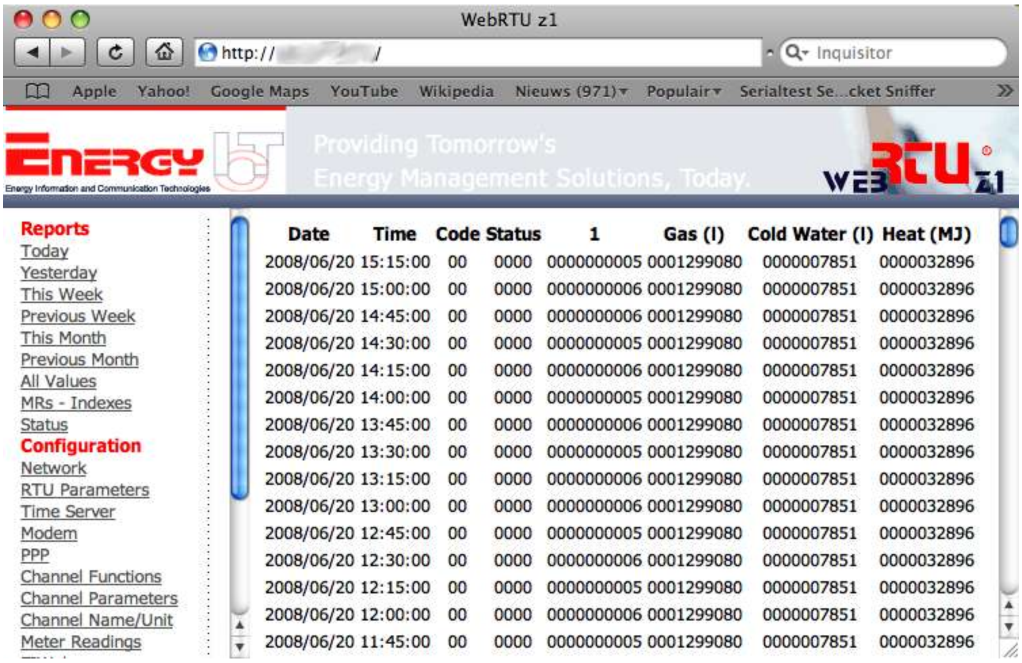
For remote management purposes, the WebRTU devices are accessible from the Internet. No VPN or private subnets are being used to limit access to these devices in the Delta pilot; anyone who knows an IP address of such a device can try to connect to its web interface. This is confirmed by a



(a) Connections (b) WebRTU

Figure 12: EnergyICT WebRTU Z1 installed in a test lab at Delta grid operator

Delta engineer. Furthermore readout of metering data through this web interface is not protected by a password or any other security measure as can be seen in figure 13. This leads to a serious confidentiality issue.



Date	Time	Code	Status	1	Gas (l)	Cold Water (l)	Heat (MJ)
2008/06/20	15:15:00	00	0000	0000000005	0001299080	0000007851	0000032896
2008/06/20	15:00:00	00	0000	0000000006	0001299080	0000007851	0000032896
2008/06/20	14:45:00	00	0000	0000000006	0001299080	0000007851	0000032896
2008/06/20	14:30:00	00	0000	0000000005	0001299080	0000007851	0000032896
2008/06/20	14:15:00	00	0000	0000000006	0001299080	0000007851	0000032896
2008/06/20	14:00:00	00	0000	0000000005	0001299080	0000007851	0000032896
2008/06/20	13:45:00	00	0000	0000000006	0001299080	0000007851	0000032896
2008/06/20	13:30:00	00	0000	0000000005	0001299080	0000007851	0000032896
2008/06/20	13:15:00	00	0000	0000000006	0001299080	0000007851	0000032896
2008/06/20	13:00:00	00	0000	0000000006	0001299080	0000007851	0000032896
2008/06/20	12:45:00	00	0000	0000000005	0001299080	0000007851	0000032896
2008/06/20	12:30:00	00	0000	0000000006	0001299080	0000007851	0000032896
2008/06/20	12:15:00	00	0000	0000000005	0001299080	0000007851	0000032896
2008/06/20	12:00:00	00	0000	0000000006	0001299080	0000007851	0000032896
2008/06/20	11:45:00	00	0000	0000000005	0001299080	0000007851	0000032896

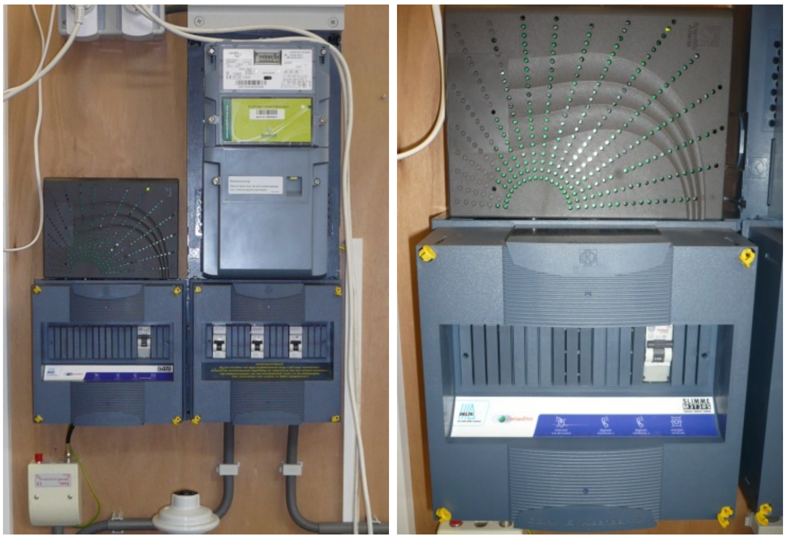
Figure 13: WebRTU web interface accessible from the public Internet

According to new information received from a Delta project manager after reviewing this document, the WebRTU systems which are installed at employees are configured to only allow connections from the IP-address of a central server. This was not the case in the setup we have seen at the Delta test lab and does not seem to be a configuration option in the WebRTU itself. This could be accomplished by firewall rules in the cable modem, but we were unable to verify this. Also, it is important to note that access to the WebRTU settings does require a valid username and password.

A number of attacks on the availability of meter data are possible. First of all, in this setup it would be easy to disconnect the WebRTU from the cable modem. From the outside a denial of service attack could be initiated with the WebRTU or the cable modem as a target. Overloading the connection with random traffic could cause the WebRTU to fail when trying to reach the CAS.

Because of the standard Ethernet setup sniffing would be very easy in this configuration. A man in the middle attack could be difficult as long as the symmetric proprietary EIWeb encryption algorithm or shared key has not been cracked. Other systems that utilize a standard Diffie-Hellman key exchange to generate a shared key could possibly be vulnerable to a man-in-the-middle attack [11].

Currently, Delta is performing tests with a new setup that uses a Landis+Gyr meter with a Windmill Anybridge Smart Client 4200 pluggable module for communication over IP. In this setup all wires are covered and customers only have access to their cable and Internet connection through a so called "media gateway" as shown in figure 14. This is basically a housing that covers the wired connections between the Windmill module and cable modem, and provides a Coax and Ethernet connector to connect the customer's TV and computer.



(a) Overview (b) Cable modem & 'media gateway'

Figure 14: Landis+Gyr / Windmill smart metering with cable modem and Delta's 'media gateway'

Unfortunately we did not get access to documentation of the Windmill module, therefore no conclusions to the communication security of this module can be made. The Windmill Innovation website notes that the AnyBridge platform is based on open IP standards like TCP/IP, SMTP, FTP and that "the AnyBridge platform is based on a unique and patented point-to-point bi-directional e-mail communication method to get messages across" [69]. Most of the attacks that are mentioned could still be possible. Sniffing could be possible using an ARP-spoofing attack or by removing the cover of the "media gateway".

GPRS

Together with PLC, GPRS is one of the main technologies used in smart metering pilot projects by the major grid companies in The Netherlands. Some of the companies that are using or testing GRPS are Eneco, Essent, Continuon, Delta and Oxxio.

General Radio Packet System (GPRS) is an add-on to the Global System for Mobile Communications (GSM) network to facilitate a range of data services for mobile communication. The mobile device registers itself at base station with at least an Access Point Name (APN) and its GPRS authentication credentials to get access to the GPRS network. An APN is a hostname which is associated with the GPRS connection and resolves to the Gateway GPRS Support Node (GGSN) that provides the connectivity between GPRS core network and the telecom operators or corporate router. This connectivity is often, but not necessarily, realized by means of a GRE tunnel between the GGSN and corporate router [34]. A schematic overview of a GPRS smart metering system is shown in figure 15.

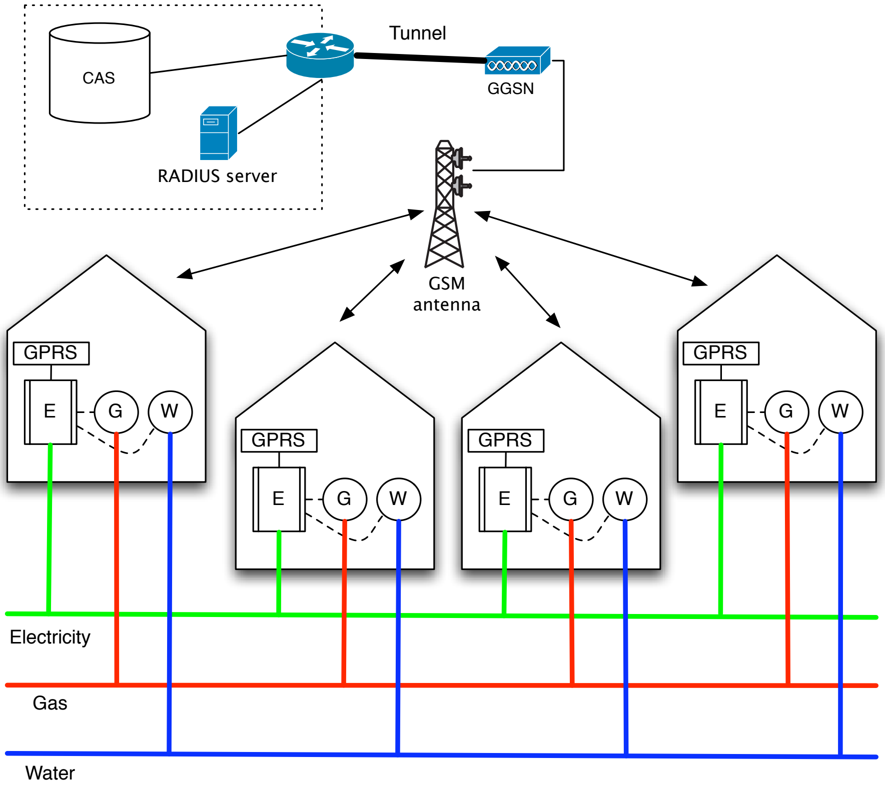


Figure 15: GPRS smart metering implementation

The GSM security model is considered as broken, because of weaknesses found in the A5 stream encryption algorithms that GSM utilizes [57]. The GPRS system uses a new implementation of the A5 stream encryption which should improve the security of the network. Currently, decryption of wireless GPRS signals is not feasible, but could be in the future when details of the new A5 algorithm becomes publicly available [5]. Therefore it is important that besides the GPRS encryption, additional end-to-end encryption between the meter and back-end system is realized.

Some grid operators use the telecom provider's APN for their smart metering systems to connect to, which gives the meter an IP address that could be accessible from the public Internet. Other operators have their own private APN and RADIUS server which gives the meter an internal IP address from the grid operator.

Smart metering systems usually connect only once a day for a small period of time to communicate with the CAS and function only as a client, which makes direct attacks from the public Internet to a smart GPRS meter unlikely.

Attacks on the P3 back-end systems could be possible when someone tries to log in to the grid operator's private APN using a smart meter's credentials. Therefore it is important that every meter uses unique and strong credentials to log into the APN. This risk is even bigger when the grid operator uses the APN of the telecom provider which is accessible to all customers of the same telecom provider. Grid operators should not solely rely on the GPRS authentication to grant access to back-end systems.

Although sniffing of wireless GPRS signals does not yet seems feasible, local sniffing between the meter and an internal or external modem could be possible. We have discovered that some of the smart metering systems use an internal or external RS-232 connection between the metering system and the GPRS modem.

The Xemex CT1020 module which is being used in the Eneco smart meter features a Telit GE863-QUAD-PY GPRS modem that communicates with the Xemex board using an internal RS-232 connection which can be seen in figure 16. This GPRS modem is accessed by the Xemex board using a standard modem AT command set [66]. Sniffing of a RS-232 connection is possible using a simple schematic [4], but is not possible without breaking the casing of the Xemex module.

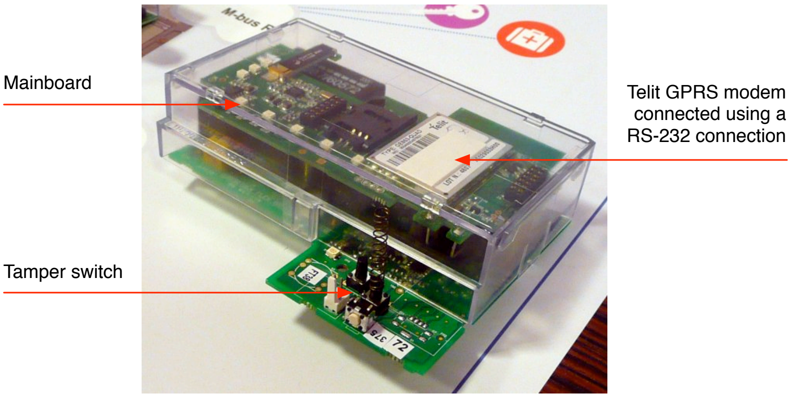


Figure 16: Xemex CT1020 module with Telit GE863-QUAD-PY GPRS modem

Sagem and possibly other manufacturers as well are introducing an external GPRS modem that can be connected to existing PLC meters using a RS-232 connection [63]. This link between the meter and modem could easily be sniffed to obtain more information about the GPRS communication. In case weak encryption and authentication mechanisms are used, data manipulation could also be possible using manipulation of the RS-232 data stream.

Another attack to intercept GPRS communication would be to utilize a GSM/GPRS test station that normally is being used to test cell phones, but could also simulate a fake GSM access point [1]. By broadcasting a stronger signal than the telecom provider's legit access point the test station can force the smart meter to connect to this fake access point. Once the smart meter is connected, analysis of the GPRS communication is possible. However, these devices are very expensive, which would make other attack methods more attractive to most attackers.

The availability of meters that utilize GPRS as their communication channel can easily be attacked using a GSM jamming device which are available for less than 50 euros at Ebay or by placing a Faraday cage around the meter or its external GPRS modem.

Power Line Carrier

Power Line Carrier (PLC) or Power Line Communication is a data communication system which uses the conductor used for electric power transmission as a carrier. The digital data is modulated onto the carrier wave with a high frequency. This is the same system which is used to switch street lights on and off and to switch between day and night tariff in “dumb” electricity meters [9]. PLC uses a frequency of 3 to 148.5kHz which provides an actual performance of a few hundred bits per second with a distance limit of approximately 700 meters.

The smart meter communicates with a Data Concentrator (DC) which is typically located at a local transformer substation. At the substation the medium voltage network is connected to the low voltage "consumer" network. A DC is responsible for collecting the data of the smart meters in the connected low voltage network. The data is communicated from the DC to the grid operators network using IP or GPRS. A schematic overview of a PLC implementation can be seen in figure 17.

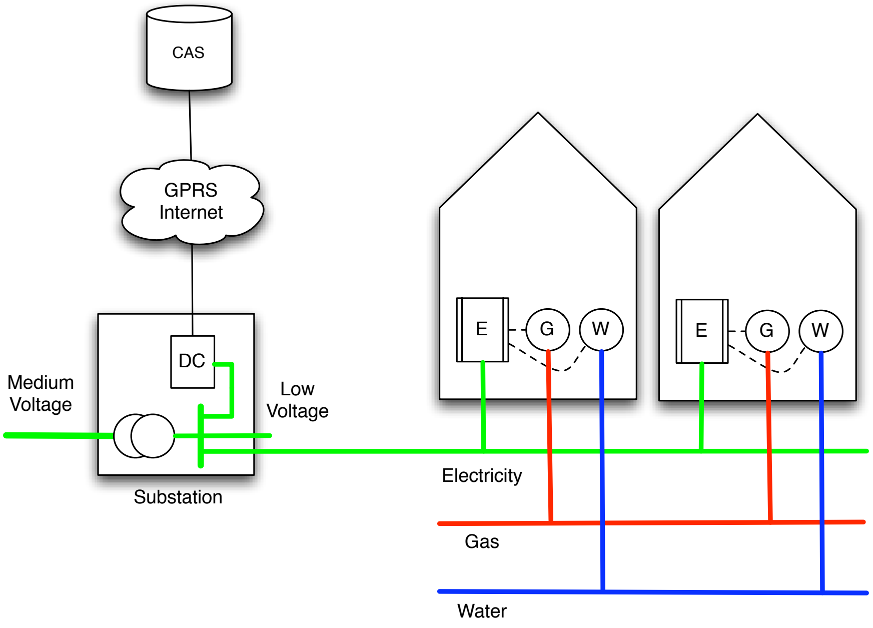


Figure 17: PLC smart metering implementation [22]

Meter to data concentrator

In this paragraph the communication between the smart meter and the DC will be discussed using the 7 layers of the OSI model [37].

All devices using PLC communication must conform to the frequency allocation in CENELEC, Frequency Band Allocation for Europe, defined in EN 50065-1 [14]. The IEC 61334-5 series defines reliable mechanisms for transmission of data on a medium or low voltage transmission or distribution system [21]. The smart meters which we encountered in the pilot projects use the CENELEC A-Band (9-95kHz) and IEC 61334-5-1 [31] standard for the physical layer and the media access control (MAC) section of the data link layer.

PLC uses a shared medium, all residences are connected to the same electricity network. Because PLC signals weaken in strength when the distances increases, smart meters in residences can repeat the signal from and to the DC so that larger areas up to approximately 700 meters can be covered. The DC determines which meters will function as a repeater. Seven of these repeaters can be setup in a chain which should enable the DC to reach even the most distant and most difficult to reach meters, as shown in figure 18 for the Sagem implementation. In practice this means that smart meters receive data from other meters enabling somebody to sniff metering data of these meters.

Consumers are allowed to plug-in any device into the electricity network they like. One of the downsides of the electricity network is that devices plugged into the electricity network can influence the PLC signals that pass the network. From our contact at Delta we heard that an

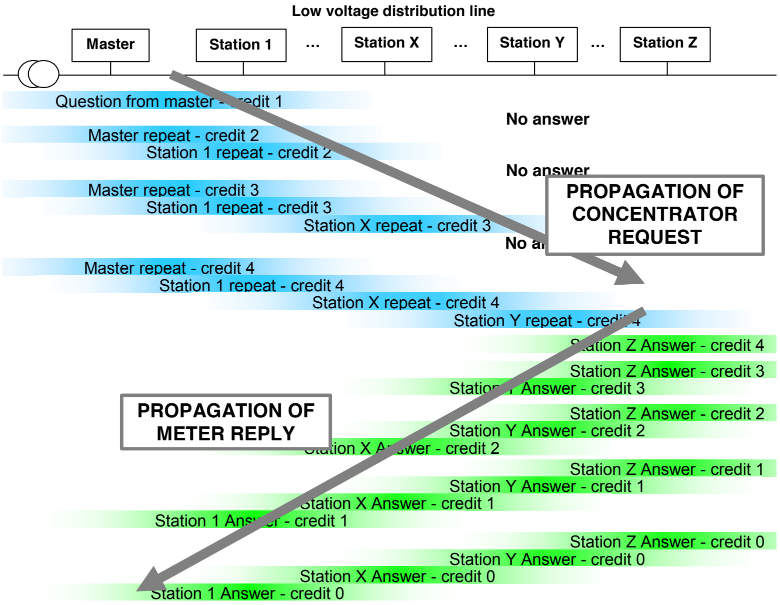

Low voltage distribution line
Master
Station 1
...
Station X
...
Station Y
...
Station Z
Question from master - credit 1
No answer
Master repeat - credit 2
Station 1 repeat - credit 2
No answer
Master repeat - credit 3
Station 1 repeat - credit 3
Station X repeat - credit 3
No answer
PROPAGATION OF CONCENTRATOR REQUEST
Master repeat - credit 4
Station 1 repeat - credit 4
Station X repeat - credit 4
Station Y repeat - credit 4
Station Z Answer - credit 4
Station Z Answer - credit 3
Station Y Answer - credit 3
Station Z Answer - credit 2
Station Y Answer - credit 2
Station X Answer - credit 2
PROPAGATION OF METER REPLY
Station Z Answer - credit 1
Station Y Answer - credit 1
Station X Answer - credit 1
Station 1 Answer - credit 1
Station Z Answer - credit 0
Station Y Answer - credit 0
Station X Answer - credit 0
Station 1 Answer - credit 0

Figure 18: Sagem PLC credits implementation [61]

Uninterrupted Power Supply (UPS) at a school disrupted the PLC signal for all the surrounding residences, making all smart meters in the area unreachable. Delta had to replace the UPS for a UPS of a different brand that did not effect the PLC signal. The source of these kind of problems that are causing black holes in the PLC network are often hard to detect.

According to Delta, PLC based smart meters in the proximity of a variable frequency motor, which are commonly found in industrial areas, are also difficult or impossible to reach. Cheap electricity dimmers can also effect the PLC signals, although not on the same scale as UPS systems or variable frequency motors [22].

At the data link layer manufacturers of smart meters are using different standards [55]:

- IEC 61334-4-32 [30] used by Landis+Gyr and Actaris
- IEC 62056-46 [33] used by Iskraemeco and Sagem
- Local Operation Network (LON) EIA/CEA 709.1-B-2002 [13] used by Echelon

The IEC standards were not available during our project. Further research on the security aspects of these standards could be done.

Currently two higher level protocols are being used in The Netherlands [55]:

- Local Operation Network (LON) EIA/CEA 709.1-B-2002
- DLMS/COSEM [12]

The LON protocol has been developed by Echelon and is used in various industries including: building, home, transportation, utility and industrial automation. LON provides facilities for all layers from the data link layer and up. It is difficult to find any technical documentation on LON and its security implementation. We have found a rapport from 2006 which states the following security issues of the LON protocol: sensitive to denial of service attacks, insecure authentication and encryption mechanism and no authentication for broadcast messages [27]. These security risks were described in 2003 and the latest LON specification is from 2002. Although we did found information stating that the 709.1 standard is being updated, it is unknown how these updates effect the security of the protocol [8].

Because DLMS/COSEM is used by most manufacturers of smart meters and it is not specific to PLC, and also is used over GPRS and IP, it will be discussed in a separate section.

Table 11 shows a summary of the protocols used together with PLC.

Layer	*Protocol*	*Supported by*
Physical	• IEC 61334-5-1	All Dutch PLC meter developers
Data link	• IEC 61334-4-32 • IEC 62056-46 • EIA/CEA 709.1-B-2002	L+G and Actaris Iskraemeco and Sagem Echelon
Transport and Network	Used with Ethernet at link layer	Not used in NL
Application	• DLMS/COSEM • EIA/CEA 709.1-B-2002	L+G, Actaris, Iskraemeco, Sagem Echelon

Table 11: PLC protocols

Using the right equipment one might be able to sniff the PLC network and communicate with the smart meters. Various PLC modems that are compliant to the physical layer protocols are available [50, 28]. One of these modems is the Mulogic PLM-501, which can be seen in figure 19. This modem offers RS-232 and RS-485/RS-422 serial data interfaces to connect to a PC and has support for the IEC 62056 standard, which is used by Iskraemeco and Sagem. In order to effectively sniff data and possibly communicate with the smart meters application level protocol like DLMS/COSEM or LON have to be implemented. United in the Enbin grid operator organisation several Dutch grid operators are working on a DLMS/COSEM standard for the Dutch electricity market [39]. These specifications are available for public and define data types for smart metering applications. No publicly available software or libraries could be found for the DLMS/COSEM standards, which will make PLC sniffing difficult, but not impossible.

Figure 19: Mulogic PLM-501 PLC modem

Data concentrator to CAS

The DC collects the data from all the smart meters that are connected to the low voltage network it services. Although the DC uses the same technologies as discussed before (IP and GPRS) to communicate with the back-office, the impact on confidentiality and integrity would be much larger in case of security breaches, because data of many meters is aggregated at the DC. The higher level communication technology used between the DC and the grid operator's back-office is unclear. We do know that the Founter solution uses a VPN connection [25] and that Sagem offers a solution that uses HTTPS and possibly also VPN [63].

Another aspect of data concentrator security is physical security of the DC which is situated in a substation of the grid operator. If someone could gain access to a substation one could try to connect its own laptop to the DC to collect the data from the connected smart meters. In figure 20 an Iskraemeco DC can be seen in the Delta test environment. On the lower side of the DC four different wires are visible; from left to right: electricity PLC connection, ps2 mouse and keyboard connector, VGA monitor cable and a RJ45 network cable. The Iskraemeco P2PLC runs Windows CE as its operating systems and creates a file for each connected meter with its metering data, keeping backup records of meter readouts up to three months [35]. Whether it is possible for somebody to copy these files from the DC to an external storage device is unclear. The DC does offer additional tools to control and monitor smart meters apart from viewing the metering data.

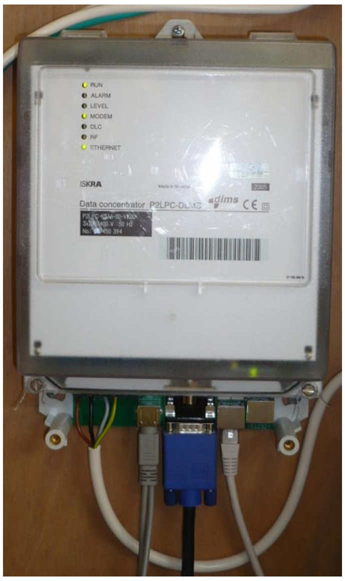


Figure 20: Iskraemeco P2PLC data concentrator at Delta

Meshed RF

Meshed RF is a communications technology which uses radio frequencies to communicate. RF communications requires, like PLC, a data concentrator (DC) which is a central point where all the metering data is collected. Smart meters communicate using RF with the DC, but in case a smart meter is too distant or some kind of interference is influencing communication the meters can form a meshed network where neighbouring smart meters communicate with each other until the DC can be reached. RF communications is based on modified Radian 433 protocol and uses the license free frequency bands between 433.39 and 444.7 MHz [35]. Figure 21 shows a graphical impression of RF communication technology.

In The Netherlands Delta is currently the most active grid operator testing RF communication for smart meters. Delta is testing modular Landis+Gyr smart meters with a Smart Dutch RF module, as shown in figure 22. Smart Dutch is a company that specialises in RF communication for smart meter systems and is also involved in pilot projects at Essent and Eneco [64]. The Smart Dutch RF module uses DLMS/COSEM as its application layer protocol.

Although a different physical medium is used in RF as in PLC it is prone to the same kind of security risks. Consumers can buy or create a RF communication device and develop software

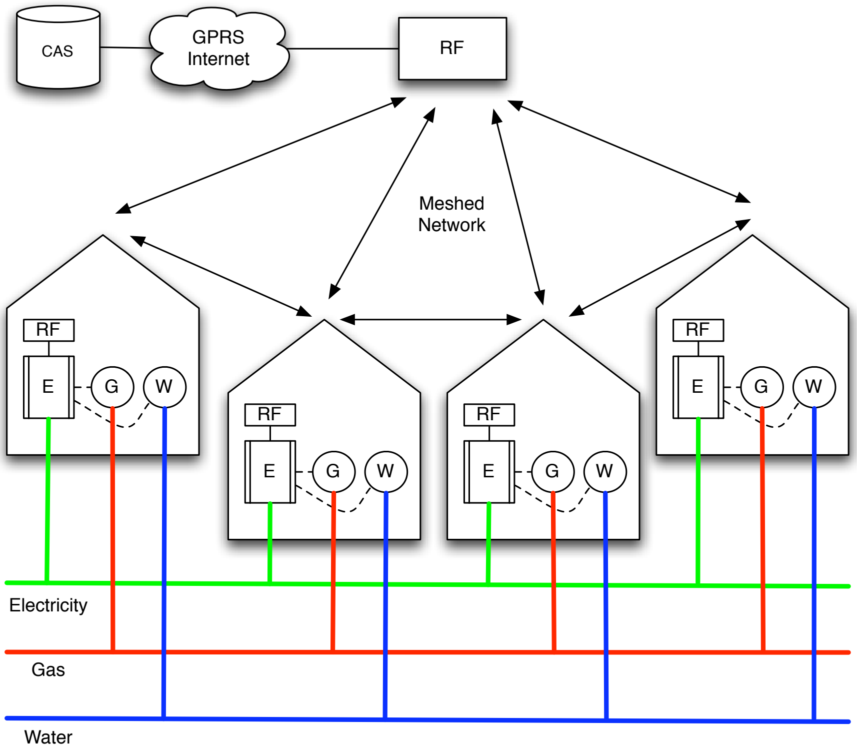


Figure 21: RF smart metering implementation [22]

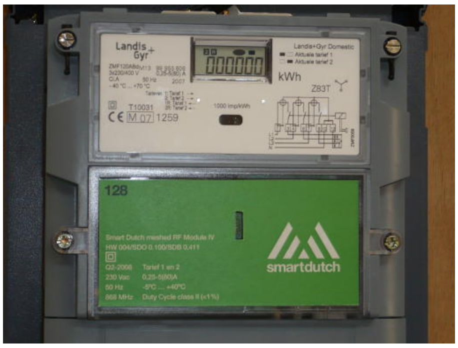


Figure 22: Smart Dutch RF module in a Landis+Gyr meter at Delta

to sniff or communicate using GNUradio for example [26]. The security of RF depends on the application layer implementation. With the usage of radio transmitter, like GNUradio, one might be able to disrupt the data link layer protocol and possibly do a denial of service. The DC used in RF solutions have the same security risks as the DC in PLC. The DC will be placed centrally in neighbourhoods, possibly also at substations and use the same communications technologies as PLC data concentrators to communicate with the CAS: IP and GPRS.

The DLMS COSEM protocol

DLMS/COSEM is a common language which enables partners in the metering industry to communicate in a standard way, and is defined on the DLMS website as follows: [12]:

> DLSM stands for Device Language Message Specifications - a generalised concepts for abstract modelling of communication entities.
>
> COSEM stands for COmpanions Specification for Energy Metering - sets the rules based on existing standards for data exchange with energy meter.
>
> DLMS is:
>
> - An object model, to view the functionality of the meter, as it is seen at its interface(s)
> - An identification system for all metering data
> - A messaging method to communicate with the model and to turn the data to a series of bytes
> - A transporting method to carry the information between the metering equipment and the data collection system

DLMS is long used in the industrial metering industry and is rather large for smart metering. The standard is currently being updated for smart meter usage. DLMS standards are internationalised through IEC standards and can be seen in appendix B on the hand of the 7 layer OSI model, DLMS is not depended on a physical layer. DLMS self uses books to describe its specifications [12]:

- the Blue Book describes the COSEM meter object model and the object identification system
- the Green book describes the architecture and protocols to transport the model
- the Yellow book describes the conformance testing process
- the White book holds the Glossary of DLMS/COSEM terms

DLMS was used mostly in private and closed environments in the past. With smart metering being introduced the data is being transported over public and exposed networks, which has introduced new security requirements. Besides simplifying the DLMS standard for smart metering, various security measures have been introduced. Proven technologies are being used, such as TDES, AES, MD5, SHA1, CBC and GCM [40].

DLSM/COSEM can be used in combination with any communication technology or protocol. In case different meter manufacturers keep using different technologies the Dutch grid operators could get into a vendor lock-in position once the meters are placed. To guarantee interoperability they joint forces to create the Dutch Smart Meter Requirement (DSMR) where specific technical requirements have been made for P3 communication, in contrast to the NTA where no requirements are made.

Currently an agreement exists between the grid operators and four manufacturers on an interoperable DLMS/COSEM standard [55]:

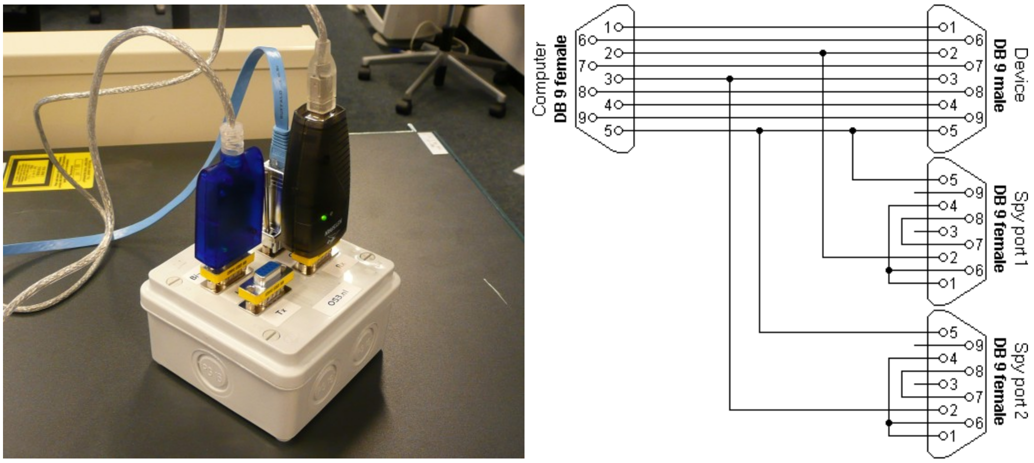
- Actaris
- Iskraemeco
- Landis+Gyr
- Sagem

In the DSMR the authentication and encryption algorithm of choice is AES-GCM-128 and refers to DLMS UA Green Book edition 7 and Blue Book edition 9 for its security implementation. These books are not yet published and on publishing will only be available to members of the DLMS user association and as an IEC standard.

Meters that meet the DSMR requirements and implement DLMS security in a correct matter should provide sufficient application level security. Once the DLMS books, in which the security implementations is described, are published this standard could be analysed in full depth.

4.4.2 Practical research

Unfortunately we did not have access to a smart metering setup at which we could perform any sniffing or other attacks. We did build a RS-232 sniffing device which we could use in case we encountered a smart metering setup that uses an external GPRS modem. We constructed the sniffing box using a simple schematic [4] which is constructed in such a way that it causes no interference to the communication channel. The box features an input and output, and two connections for sniffing both the receiving and transmitting signals. The box has been successfully tested while sniffing a Cisco router console session as can be seen in figure 23.



(a) Test setup (b) Schematic

Figure 23: Testing the RS-232 sniffing box

4.4.3 Attack feasibility

We have seen that sniffing could especially be an attack vector at Ethernet based metering systems and GPRS systems that feature an external RS-232 GPRS module. PLC sniffing does not seem feasible because of the broad range of communication protocols and limited availability of software. Sniffing would only be valuable in case weak encryption is being used.

The alteration of meter data could be possible with IP based systems and possibly GPRS systems that use an external modem in case weak encryption is being used, although additional research is required.

Disruption of communication should be possible with all technologies, whereas DoS attacks could a particular danger in Ethernet based IP networks. More research is required to analyse the possibilities of sending fake control commands to meter systems through the various P3 communication channels. An overview of the feasibility of the different attack vectors is shown in table 12.

4.4.4 Recommendations

A solution to ensure data safety would be to use end-to-end strong encryption between the smart meter and CAS, between the gateway and the meter and between the gateway and the CAS. Cryptographic certificates could be used for the smart meter to verify the authenticity of the CAS or gateway and for the CAS to verify the authenticity of the smart meter or gateway. It is important to verify the certificate of both client and server to eliminate the possibility of man in the middle attacks.

		IP	GPRS	PLC / RF
C	• Sniffing from meter to gateway	-	-	Not feasible
	• Sniffing from gateway to CAS	Research required	Not feasible	Research required
	• Sniffing from meter to CAS	Research required	Feasible (RS232)	-
I	• Alter data from meter	Research required	Research required	Not feasible
A	• Disrupt communications	Possible	Possible	Possible
	• Send fake control commands	Research required	Research required	Research required
	• Denial of Service attack	Feasible	Not feasible	Not feasible

Table 12: Port P3 attack feasibility

4.5 Port P4

Port P4 is the port defined as the access point for the suppliers and metering companies at the grid operator. Through P4 they can control the smart meters and access the metering data of their customers.

4.5.1 Implementation

From different parties such as Delta and Founter and from the speakers at the smart metering conference we understood that most smart metering projects are still in a pilot phase. The primary focus during the pilots is on the meter communication between the smart meter and the grid operator, on the physical placement of smart meter equipment at consumers, and on the customer experience during the smart meter placement process.

The interaction between the grid operator and suppliers or metering companies is still in development. Essent for example is currently implementing their P4 definition [24]. No information is yet available on the implementation of the port P4 besides the information in the NTA.

4.5.2 Practical research

Besides the fact that the P4 port is still in development, data from grid operators and suppliers is required to perform an in depth security analysis of P4. The analysis of P4 is outside the scope of this project but could be done in a future project in cooperation with the grid operators, which are the owners of the P4 systems.

4.5.3 Attack feasibility

No practical research has been performed, which is also shown in table 13.

C	• Large scale disclosure of customers' metering data	Research required
I	• Corruption of metering data	Research required
A	• Broadcasting of control commands to meter systems	Research required
	• Denial of Service attack at the CAS	Research required

Table 13: Port P4 attack feasibility

4.5.4 Recommendations

Though we could not analyse the P4 implementations we are able to state some general recommendations for P4 security:

- **Authorisation** The P4 port should tightly control access to data and to smart meter control. No supplier should be able to read information from other supplier's customers, nor should they be able to control other customers smart meters.
- **Access** The P4 port should only be accessible by suppliers and metering companies. No access should be possible from the public Internet. Because of the small market and parties in the energy market access should be controlled using a private network.
- **Logging** Because of the customers privacy and the impact of security breaches all access and actions should be logged.

4.6 Port P5

Port P5 is the port we defined as the supplier's website which enables customers to get access to their usage data, or possibly upgrade their prepaid credit.

4.6.1 Implementation

At this moment only two suppliers offer access to usage data obtained from smart meters through their website. Other suppliers do offer a personal website for their customers where they, among others, can enter manual yearly meter readings, view their bills and, and view or change personal information. It would be likely that the smart meter readouts will be made available on these websites in the future. The websites which we analysed can be seen in table 14.

Websites with metering data:	• Oxxio [54] • Delta [10]
Websites without metering data:	• Nuon [53] • Essent [23] • Eneco [18]

Table 14: Suppliers websites

4.6.2 Practical research

Web applications are a common victim of cyber crime and is an area in which a lot of research has been done [65]. When a web application is compromised an attacker may be able to steal private and personal information, carry out fraud, and perform malicious actions against other users.

A few common seen techniques to compromise a web application are:

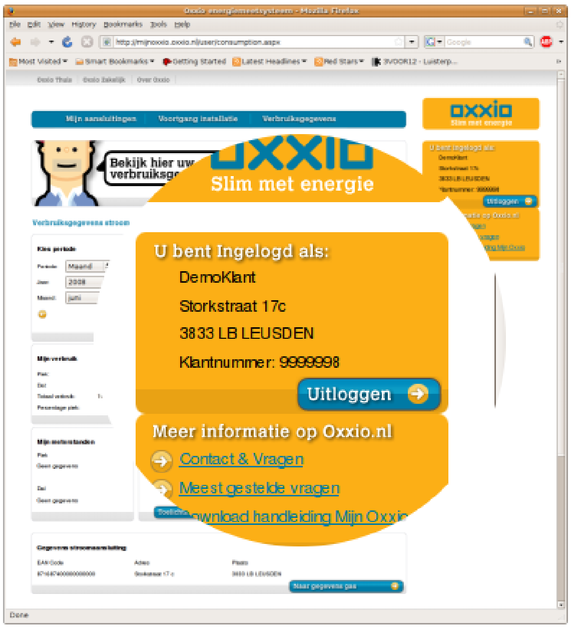
- Broken authentication
- Broken access controls
- Cross-site scripting
- SQL injection
- Information leakage

Because of the information already available on web application security an in depth analysis or penetration testing of the websites is out of the scope of this project. We made a general analysis of the websites and how they could be compromised. Based on the theoretical analysis we looked at the privacy and access aspects of the website:

- What are the credentials that are needed to login.
- How can one request an account.
- How is the privacy of the customer guaranteed.

If a client does not have an account for the website they can request an account on the Nuon, Essent and Eneco websites. This request procedure requires information that in some cases could be publicly available, guessable or could easily be obtained: customer number, zip code and house number. Delta only offers access to customers that are participating in one of their smart metering pilots, and are using a username and password authentication mechanism.

Oxxio has a login procedure which requires a customer number, zip code and house number. The information is inserted at the login web page in clear text and after login these credentials are shown on all web pages which makes it prone to shoulder surfing. This can be seen in figure 24, for a larger version see appendix C. Oxxio stated that they used to have a unique username and password for each client, but that this authentication procedure could be a barrier for customers to visit the "myoxxio" website. User friendliness is the major reason they removed the username and password authentication.



U bent Ingelogd als:
DemoKlant
Storkstraat 17c
3833 LB LEUSDEN
Klantnummer: 9999998

Figure 24: Personal Oxxio website with usage information

A customer number is something that can sometimes be found on the internet but would generally also be noted on all correspondence with the supplier. Somebody could intercept this correspondence or could try an exhaustive search for a correct customer number, which makes it unsuitable as a secure login credential

Only the website of supplier Eneco provided a secure connection with the usage of SSL encryption. The websites from other suppliers are vulnerable to sniffing attacks due to the lack of encryption.

The results of the practical research can be seen in table 15.

4.6.3 Attack feasibility

The feasibility of the security risks as defined during the theoretical analysis as shown in table 6 are summarized for each supplier as can be seen in table 16.

	Metering data	SSL	Password auth.	Secure registration
Oxxio	Yes	No	No	-
Delta	Yes	No	Yes	-
Nuon	No	No	Yes	No
Essent	No	No	Yes	No
Eneco	No	Yes	Yes	No

Table 15: Port P5 security measures

	Shoulder surfing	Sniffing on (wireless) LAN
Oxxio	Possible	Possible
Delta	Not feasible	Possible
Nuon	Not feasible	Possible
Essent	Not feasible	Possible
Eneco	Not feasible	Not feasible

Table 16: Port P5 attack feasibility

4.6.4 Recommendations

The privacy of the customer's data has to be protected using strong SSL encryption for all HTTP data streams. This prevents sensitive data to be communicated in plain text through local (wireless) networks and the internet and could also be used the verify the identity of the website using a server certificate.

Access credentials to the website should at a minimum consists of a username and password which could be only be obtained through a secure registration procedure that uses a out-of-band channel to communicate the users password to the customer.

5 Recommendations

In this section a number of recommendations based on both the theoretical and practical research will be made. Based on the theoretical analysis of the Dutch technical agreement (NTA) some recommendations for a future version of the NTA can be made, which will provide an improved legal and political basis for smart metering security:

Privacy The detailed 15 minute interval for electricity and 1 hour interval for gas allows suppliers to obtain detailed day-to-day living patterns of their customers. The Dutch Data Protection Authority (CBP) has expressed its concern about this sensitive information being send to the suppliers [7]. A possible solution is to send only aggregated data to the grid operators once a week or once a month and to provide consumers with detailed information about their energy usage through devices connected to the P1 port.

Port P0 should be part of NTA Optical management ports and configuration buttons are easily accessible for end-users and can provide functionality to change a meter's configuration. This port should be part of the NTA specification and should have a minimum security level defined to prevent poorly protected systems from being installed at households.

Security aspects should be defined more specifically As seen in the theoretical research, the NTA notes multiple times that grid operators should take "appropriate measures" to ensure a secure smart metering system. The NTA does not note which measures would be appropriate and what data should be secured using which methods. To guarantee a minimum level of security, measurable security requirements should be part of the NTA.

The practical analysis resulted in some specific recommendations that suppliers and grid companies should follow when implementing their smart metering solution:

Do not solely rely on security seals and "do not open" signs Grid companies are used to utilize security seals to visually detect tampering. While metering systems become smarter these companies can no longer rely on security seals and "do not open" signs as their only security mechanisms. We have seen smart meters that can be reprogrammed just by breaking a seal and the push of a button. As long as such options exists there will be hackers that use this knowledge to fraud with metering data. Although most of the meters feature tamper detection mechanisms, the corresponding alerts can easily be blocked using the methods discussed in the practical analysis.

Do not expect a hundred percent availability There are ways to sabotage each of the communication techniques that are used between the smart meter and the grid operator. For example: GSM jammers for GPRS, scissors for Ethernet and variable frequency motors for PLC systems. Grid companies should realize that they probably will not be able to deliver a working smart metering solution for the truly unwilling customer.

Use open encryption standards We have seen that communication between metering devices within residents are often not protected by any encryption mechanism which will enable a number of different attacks. Communication with the grid company is sometimes encrypted using proprietary encryption protocols, which security can't be checked by independent experts. To ensure data safety and integrity manufacturers should use open and proven encryption algorithms for both internal and external communication.

Do not underestimate privacy aspects Customer's day to day living patterns can be extracted from metering data which makes the privacy aspect of metering data extremely important. Grid companies should realize that especially at the Central Access Server (CAS), where data from lots of customers is aggregated, data privacy is an crucial asset.

Use SSL and strong passwords for websites None of the websites we have seen that enable customers to check their usage data are protected sufficiently. Suppliers should at least use a secure connection and strong passwords to secure these websites. Properties such as zip codes and customer numbers are easily traceable and should not be considered as sufficient authentication credentials.

Perform data checks to verify correctness of data During our practical research we have discussed a number of attacks that could be used to alter metering data. Metering companies should perform checks on metering data to verify whether the data received is feasible when normal usage patterns of the customer are taken into account. This would be an important measure to detect anomalies and fraud.

5.1 Future research

Due to the lack of tight cooperation with a grid operator or supplier of metering equipment only very limited practical research was possible during this project. Instead we focused on a more high level overview of the different security aspects of smart metering systems.

More research is needed to gain insight to the security risks of P0 management ports on smart metering systems. Because P1 is not implemented yet, the security of implementations of such devices should be analyzed when they become available. The security of P2 wireless connections between electricity and gas or water meters is unclear and requires further analysis. The connection between the metering systems and the grid operator (P3) also requires additional research, but cooperation from grid operators and manufacturers will be required to perform a detailed analysis.

Before the large scale implementation of smart metering systems takes place, grid operators and suppliers should conduct research into the security of their systems. Because no smart meter solution will be exactly the same, every solution will require its own security analysis. The same applies to the CAS, P4 connected systems and supplier's websites.

Finally, smart metering is still in a pilot phase. The Dutch government has not yet voted and accepted the change in law concerning smart meters. Grid operators are testing new technologies and the manufacturers are making their meters NTA compliant. Because of the missing specifics in the NTA the larger Dutch grid operators have united and are working on more specific smart meter requirements, referred to as the Dutch Smart Meter Requirements (DSRM) [39]. These requirements should be analyzed during future research.

6 Conclusion

During this research we have analyzed the security aspects of the NTA regulation and obtained a high level overview of the different security aspects of smart metering systems that are in use in The Netherlands. Based on our research a few conclusions can be drawn.

Although the security aspects of smart metering systems are considered as an important issue by most politicians, not much of these concerns can be found in the NTA regulation. The NTA does not state which level of security would be appropriate for the different parts of smart metering systems. This gives manufacturers and grid operators the chance to decide which security measures are “appropriate”. The security aspects in the NTA should be defined more specific to guarantee the security level that is needed to meet the requirements of both consumers and politicians.

Besides these security aspects, the need for a 15 minute data collection interval for electricity and 1 hour interval for gas collecting is unclear. These short intervals have a major impact on the privacy of customers, because of the day to day living patterns and other sensitive details that can be extracted from this data. Changing this to a daily or monthly interval could reduce the privacy concerns and still allows suppliers to send a accurate monthly bill to their customers.

Our analysis of smart metering systems that are currently in use in The Netherlands shows that the security measures to ensure full confidentiality, integrity and availability of meter data are not always sufficient.

First of all, the security of meter management functions are not protected by strong authentication mechanisms, but rely on security seals that can be broken easily. Also, communication between the electricity and gas or water meter does not utilize a secure channel in most implementations. Next, we have seen that metering data from individual meters at a pilot test lab are accessible from the public Internet without any authentication. At last we have seen that most suppliers do not use proper authentication and encryption on their website which could expose metering data of customers to attackers.

Most of these problems can be solved with the use of proper encryption algorithms at all communication channels of smart metering systems. This should begin at the management port (P0) all the way through to the supplier’s website (P5).

It is important to note that smart meters are not necessarily easier to fraud with than conventional “dumb” meters. But, because of the detailed information that can be obtained through smart metering systems, data security should be considered as a more important issue. This should especially be the case for the suppliers IT systems where detailed data from many different customers will be stored.

References

[1] Aeroflex. *Racal Instruments Wireless Solutions 6103 AIME specifications.*

[2] Alexander's Gas & Oil Connections. Gaz de France awards Schlumberger large-scale Gas Management Project [online, cited June 29 2008]. Available from World Wide Web: http://www.gasandoil.com/goc/contract/cox93756.htm.

[3] ANP. Slimme meters komen in twee stappen [online, cited June 29 2008]. Available from World Wide Web: http://www.trouw.nl/groen/nieuws/article997011.ece/Slimme_meters_komen_in_twee_stappen.

[4] L. Bies. RS232 serial spy monitor cable [online, cited June 29 2008]. Available from World Wide Web: http://www.lammertbies.nl/comm/cable/RS-232-spy-monitor.html.

[5] G. S. Bjaen and E. Kaasin. Security in GPRS [online, cited June 29 2008]. Available from World Wide Web: http://student.grm.hia.no/master/ikt01/ikt6400/ekaasin/.

[6] B. A. Carreras, V. E. Lynch, I. Dobson, and D. E. Newman. Critical points and transitions in an electric power transmission model for cascading failure blackouts. *Chaos*, 12, 2002.

[7] College Bescherming Persoonsgegens - CBP. Slimme energiemeters achter voordeur consument. beschikbaarstellen gedetailleerde verbruiksgegevens zonder noodzaak of toestemming in strijd met de wbp [online, cited June 29 2008]. Available from World Wide Web: http://www.cbpweb.nl/documenten/pb_20080618_slimme_energiemeters.shtml.

[8] Consumer Electronics Association - CEA. Monthly update [online, cited June 29 2008]. Available from World Wide Web: http://www.ce.org/Standards/2008-04-30CEAStandardsMonthlyUpdate.pdf.

[9] G. Deconinck, D. Bekaert, P. Jacqmaer, T. Loix, T. Rigole, and B. Verbruggen. Studie communicatiemiddelen voor slimme meters. 2007.

[10] Delta. Slimme meters van delta [online, cited June 29 2008]. Available from World Wide Web: http://www.slimmemetersvandelta.nl/.

[11] T. Dierks and C. Allen. The TLS Protocol Version 1.0. RFC 2246 (Proposed Standard), Jan. 1999. Available from World Wide Web: http://www.ietf.org/rfc/rfc2246.txt. Obsoleted by RFC 4346, updated by RFC 3546.

[12] DLMS. Dlms user association [online, cited June 29 2008]. Available from World Wide Web: http://www.dlms.com/.

[13] Echelon. Lonworks [online, cited June 29 2008]. Available from World Wide Web: http://www.echelon.com/developers/lonworks/.

[14] EN. *50065-1 Signalling on low-voltage electrical installations in the frequency range 3 kHz to 148,5 kHz – Part 1: General requirements, frequency bands and electromagnetic disturbances*, 2001.

[15] EN. *13757-2 Communication systems for remote reading of meters. Physical and link layer*, 2004.

[16] EN. *13757-3 Communication systems for remote reading of meters. Dedicated application layer*, 2004.

[17] EN. *13757-4 Communication systems for remote reading of meters. Wireless meter readout*, 2005.

[18] Eneco. Mijn eneco inloggen [online, cited June 29 2008]. Available from World Wide Web: https://prive.eneco.nl/mijn_eneco/inloggen_eneco_online.asp?loginurl=/mijn_eneco/mijn_gegevens.asp.

[19] EnergyICT. *RTU+V6 User Manual.*

[20] EnergyICT. *WebRTU Z1 User Manual.*

[21] E. P. R. I. EPRI. Intelligrid consumer portal telecommunications assesment and specification [online, cited June 29 2008]. Available from World Wide Web: http://www.epriweb.com/public/000000000001012826.pdf.

[22] Eric Verbrugge - Delta Netwerkbedrijf. Slimme meters van Delta. In *Energie Metering & Billing*. Institute for International Research, 06 2008.

[23] Essent. Inloggen op mijn essent [online, cited June 29 2008]. Available from World Wide Web: http://www.essent.nl/content/mijnessent/index.jsp?style=consument&target=https%3A//im.essent.nl/im/consument-inter-site-transfer%3FTARGET%3Dhttps%253A%252F%252Fwww.essent.nl%252Fmijnessent%252Fconsument%252Findex.jsp.

[24] Fons Jansen - Essent. Uitrol Slimme Meteers, een megaklus. In *Energie Metering & Billing*. Institute for International Research, 06 2008.

[25] Founter. Seamless smart metering, bright solution [online, cited June 29 2008]. Available from World Wide Web: http://founter.nl/.

[26] GNU Radio. The gnu software radio [online, cited June 29 2008]. Available from World Wide Web: https://gnuradio.org.

[27] W. Granzer, W. Kastner, G. Neugschwandtner, and F. Praus. Security in networked building automation systems. *Vienna University of Technology, Inst. of Computer Aided Automation, Automation Systems Group.*

[28] Hitechnologies. Power line modems [online, cited June 29 2008]. Available from World Wide Web: http://www.hitechnologies.nl/.

[29] HomePlug Powerline Alliance [online, cited June 29 2008]. Available from World Wide Web: http://www.homeplug.org/.

[30] IEC. *61334-4-32 Distribution automation using distribution line carrier systems - Part 4-512: Data communication protocols - System management using profile 61334-5-1 - Management Information Base (MIB)*, 2001.

[31] IEC. *61334-5-1 Distribution automation using distribution line carrier systems. Lower layer profiles. The spread frequency shift keying (S-FSK) profile*, 2001.

[32] IEC. *62056-21 Electricity Metering - Data Exchange for Meter Reading, Tariff and Load Control - Part 21: Direct Local Data Exchange*, 2002.

[33] IEC. *62056-46 Data link layer using HDLC protocol*, 2002.

[34] Information Risk Management Plc. IRM GPRS & 3G Security Overview [online, cited June 29 2008]. Available from World Wide Web: http://www.gprssecurity.com/.

[35] Iskraemeco. P2plc data concentrator [online, cited June 29 2008]. Available from World Wide Web: http://www.iskraemeco.si/emecoweb/eng/product/AMM_concentrators.htm.

[36] ISO/IEC. *27002 Information technology - Security techniques - Code of practice for information security management.*

[37] ISO/IEC. *7498-1 Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model*.

[38] Jos Hessels. CDA. In *Energie Metering & Billing*. Institute for International Research, 06 2008.

[39] KEMA Consulting. *Enbin - Dutch Smart Meter Requirements*, 2008.

[40] G. Kmethy. *DLMS/COSEM over PLC - security of meter data exchange over open networks*.

[41] J. Kohl and C. Neuman. The Kerberos Network Authentication Service (V5). RFC 1510 (Proposed Standard), Sept. 1993. Available from World Wide Web: http://www.ietf.org/rfc/rfc1510.txt. Obsoleted by RFC 4120.

[42] Landis+Gyr. *MAP110 Service tool user manual*.

[43] Landis+Gyr. *MAP120 Service tool user manual*.

[44] Landis+Gyr. *ZMF120AC technical data*.

[45] M-Bus Usergroup. Dedicated Application Layer (M-Bus) [online, cited June 29 2008]. Available from World Wide Web: http://www.m-bus.com/files/w4b21021.pdf.

[46] Milieu centraal. Informatie over het energielabel [online, cited June 29 2008]. Available from World Wide Web: http://www.energielabel.nl.

[47] Ministerie van Economische Zaken. Eisen slimme meter [online, cited June 29 2008]. Available from World Wide Web: http://www.ez.nl/content.jsp?objectid=150297&rid=150296/.

[48] Ministerie van Economische Zaken. Liberalisering energiemarkten [online, cited June 29 2008]. Available from World Wide Web: http://www.ez.nl/Onderwerpen/Energie/Werking_Kleinverbruikersmarkt/Berichten_en_documenten/28982_51_TK_brief_liberalisering_energiemarkten?rid=150316.

[49] Ministerie van Economische Zaken. Wijziging van de Elektriciteitswet 1998 en de Gaswet ter verbetering van de werking van de elektriciteits- en gasmarkt [online, cited June 29 2008]. Available from World Wide Web: http://parlando.sdu.nl/cgi/showdoc/session=anonymous@3A2409745934/action=doc/query=2/pos=1/KST119011.pdf.

[50] Mulogic. Plm-501 power line modem for cenelec band operation [online, cited June 29 2008]. Available from World Wide Web: http://www.mulogic.com/plm-501.html.

[51] NEN. *NTA (Nederlandse Technische Afspraak) 8130*. Available from World Wide Web: http://www2.nen.nl/nen/servlet/dispatcher.Dispatcher?id=220438.

[52] NOS. Alleen bij VROM gaat het licht uit [online]. Jan. 2007 [cited June 30 2008]. Available from World Wide Web: http://www.nos.nl/nosjournaal/artikelen/2007/1/31/310107_lichtuit.html.

[53] Nuon. Inloggen mijn nuon [online, cited June 29 2008]. Available from World Wide Web: http://www.nuon.nl/system/login.jsp?CT_ORIG_URL=%2Fpersoonlijk%2Findex.jsp&ct_orig_uri=%2Fpersoonlijk%2Findex.jsp.

[54] Oxxio. Mijn oxxio [online, cited June 29 2008]. Available from World Wide Web: http://mijnoxxio.oxxio.nl/.

[55] Paul Cornelissen - Nuon Monitoring. NTA 8130. In *Energie Metering & Billing*. Institute for International Research, 06 2008.

[56] P+E Technik. K1-06 IR - Auslesekopf [online, cited June 29 2008]. Available from World Wide Web: http://petechnik.de/index.php?page=k1-06.

[57] L. Pesonen. GSM Interception [online, cited June 29 2008]. Available from World Wide Web: http://www.tml.tkk.fi/Opinnot/Tik-110.501/1999/papers/gsminterception/netsec.html.

[58] Petra de Groene - Energiekamer. Toezicht en slimme meters. In *Energie Metering & Billing*. Institute for International Research, 06 2008.

[59] Regering.nl. Slimme energiemeter voor iedereen [online, cited June 29 2008]. Available from World Wide Web: http://www.regering.nl/Actueel/Persberichten_ministerraad/2007/september/14/Slimme_energiemeter_voor_iedereen.

[60] Relay GmbH. *M-Bus product pricelist*, 2008. Available from World Wide Web: http://www.relay.de/.

[61] Sagem Communications. *CX1000 User Manual.*

[62] Sagem Communications. *CX2000 User Manual.*

[63] Sagem Communications. *Gateways & Energy Efficiency Department, Meter Management System - Technical Offer, 15-02-2008.*

[64] Smart Dutch [online, cited June 29 2008]. Available from World Wide Web: http://www.smartdutch.nl/.

[65] D. Stuttard and M. Pinto. *The Web Application Hacker's Handbook Discovering and Exploiting Security Flaws.* Wiley Publishing, Inc., 2007.

[66] Telit. AT Commands Reference Guide [online, cited June 29 2008]. Available from World Wide Web: http://www.telit.com/module/infopool/download.php?id=542.

[67] Tweede Kamer der Staten-Generaal. Kamer akkoord met slimme energiemeter [online, cited June 29 2008]. Available from World Wide Web: http://www.tweedekamer.nl/kamerstukken/verslagen/kamer_in_het_kort/slimme_energiemeter.jsp.

[68] V. L. Voydock and S. T. Kent. Security mechanisms in high-level network protocols. *ACM Comput. Surv.*, 15(2):135–171, 1983.

[69] Windmill. *AnyBridge Smart AMR Solution product brochure.*

[70] Xemex. *Technical Specifications Sheet CT1020 2007/1.*

A Landis+Gyr meter data readout

A.1 Metering data readout

Request: 18-6-2008 21:10:31.85264 (+53.7500 seconds)

```
AF 3F 21 8D 0A
```

Answer: 18-6-2008 21:10:33.93064 (+1.0781 seconds)

```
AF CC 47 5A 35 5A 4D C6 B1 30 30 41 C3 2E 4D B1
B2 8D 0A
```

Request: 18-6-2008 21:10:34.94664 (+0.4063 seconds)

```
06 30 35 30 8D 0A
```

Answer: 18-6-2008 21:10:35.97764 (+1.0313 seconds)

```
82 C6 2E C6 28 30 30 A9 8D 0A C3 2E B1 2E 30 28
B8 B8 39 30 33 B8 39 33 A9 8D 0A 30 2E 30 28 4B
41 B2 D1 30 30 B8 B8 39 30 33 B8 39 33 30 B7 A9
8D 0A C3 2E B1 2E B1 28 39 B4 B8 B8 B8 30 30 B7
A9 8D 0A B1 2E B8 2E B1 28 30 30 30 B1 33 30 30
2E 33 AA EB D7 E8 A9 8D 0A B1 2E B8 2E B2 28 30
30 30 B1 B1 36 36 2E B8 AA EB D7 E8 A9 8D 0A B1
2E B8 2E 30 28 30 30 30 B2 B4 36 B7 2E B2 AA EB
D7 E8 A9 8D 0A B2 2E B8 2E 30 28 30 30 30 30 30
30 30 2E 30 AA EB D7 E8 A9 8D 0A B1 35 2E B8 2E
30 28 30 30 30 B2 B4 36 B7 2E B2 AA EB D7 E8 A9
8D 0A C3 2E B7 2E 30 28 30 30 30 36 A9 8D 0A 33
B2 2E B7 28 B2 B2 B7 AA 56 A9 8D 0A 35 B2 2E B7
28 30 30 B1 AA 56 A9 8D 0A B7 B2 2E B7 28 30 30
30 AA 56 A9 8D 0A C3 2E 35 2E 30 28 33 B8 A9 8D
0A 21 8D 0A 03 42
```

A.2 Date readout

Request:

```
AF 3F 21 8D 0A
```

Answer: 18-6-2008 21:13:02.37164 (+1.0625 seconds)

```
AF CC 47 5A 35 5A 4D C6 B1 30 30 41 C3 2E 4D B1
```

Request: 18-6-2008 21:13:03.38764 (+0.4063 seconds)

```
06 30 35 B1 8D 0A
```

Answer: 18-6-2008 21:13:05.41864 (+1.0313 seconds)

```
81 50 30 82 28 B2 B7 B8 C3 B2 39 B1 B1 A9 03 95
```

Request: 18-6-2008 21:13:05.69964 (+0.2188 seconds)

```
81 D2 B2 82 C3 30 30 B1 28 A9 03 12
```

Answer: 18-6-2008 21:13:06.73064 (+1.0313 seconds)

```
82 28 C5 D2 B2 33 A9 03 14
```

Request: 18-6-2008 21:13:06.98064 (+0.2188 seconds)

```
81 42 30 03 71 81 42 30 03 71
```

B DLMS

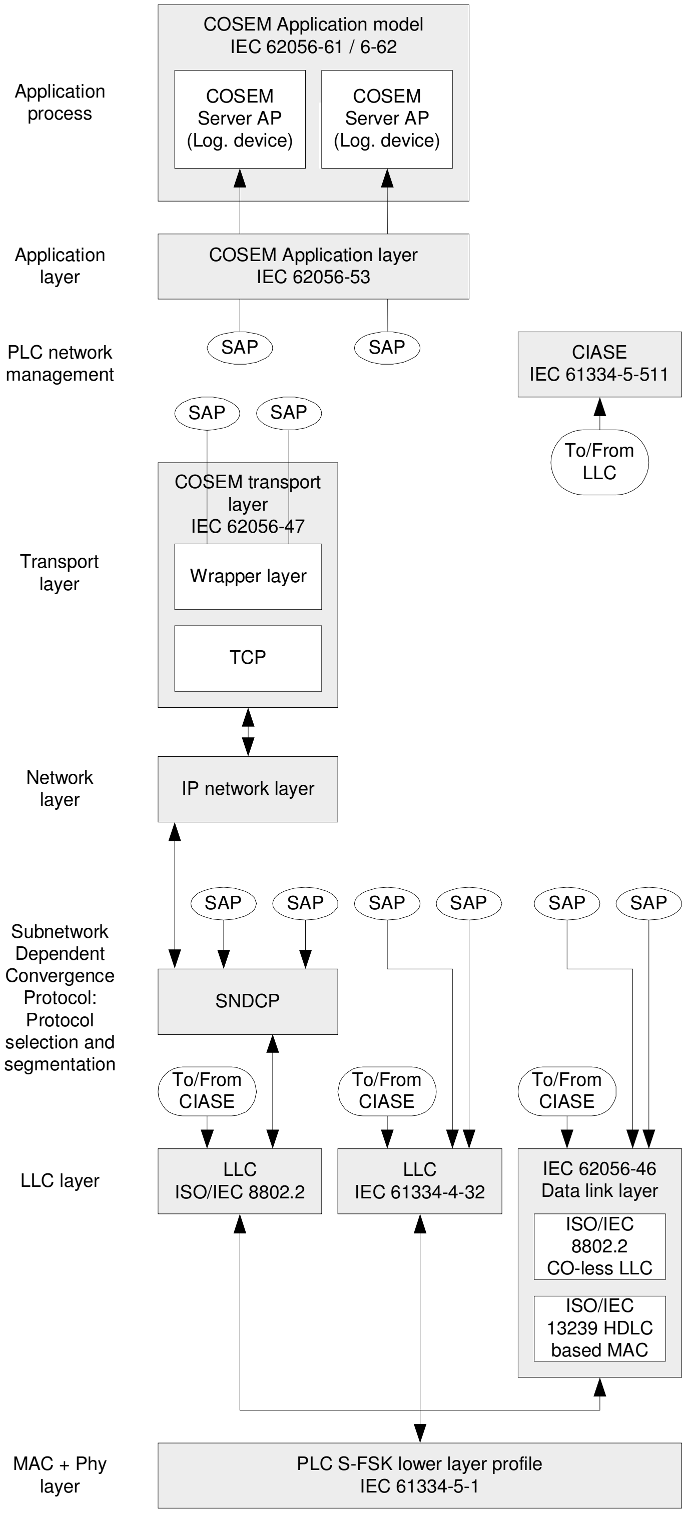
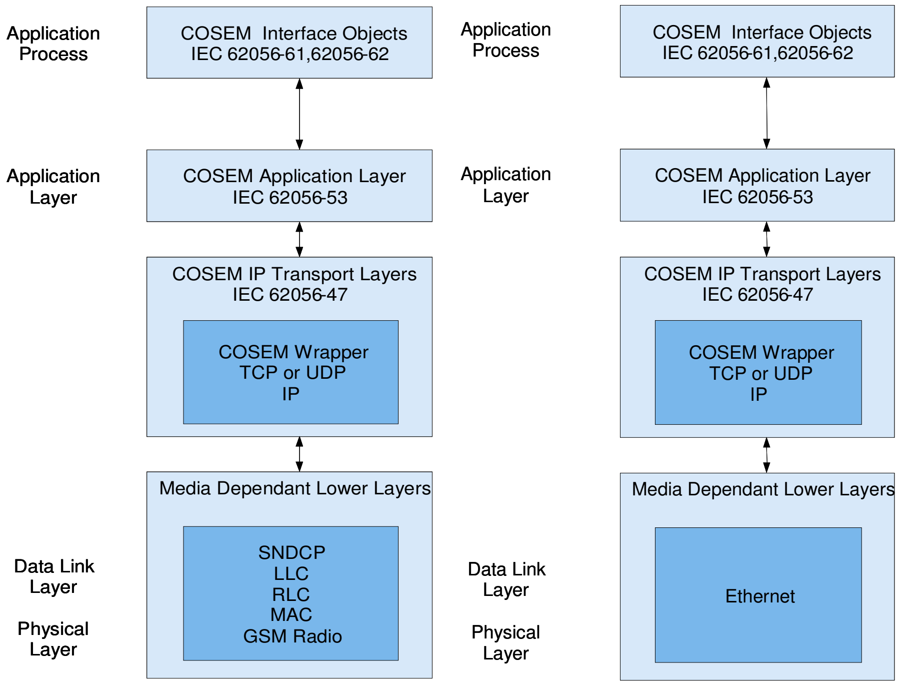


Figure 25: DLMS/COSEM PLC [39]

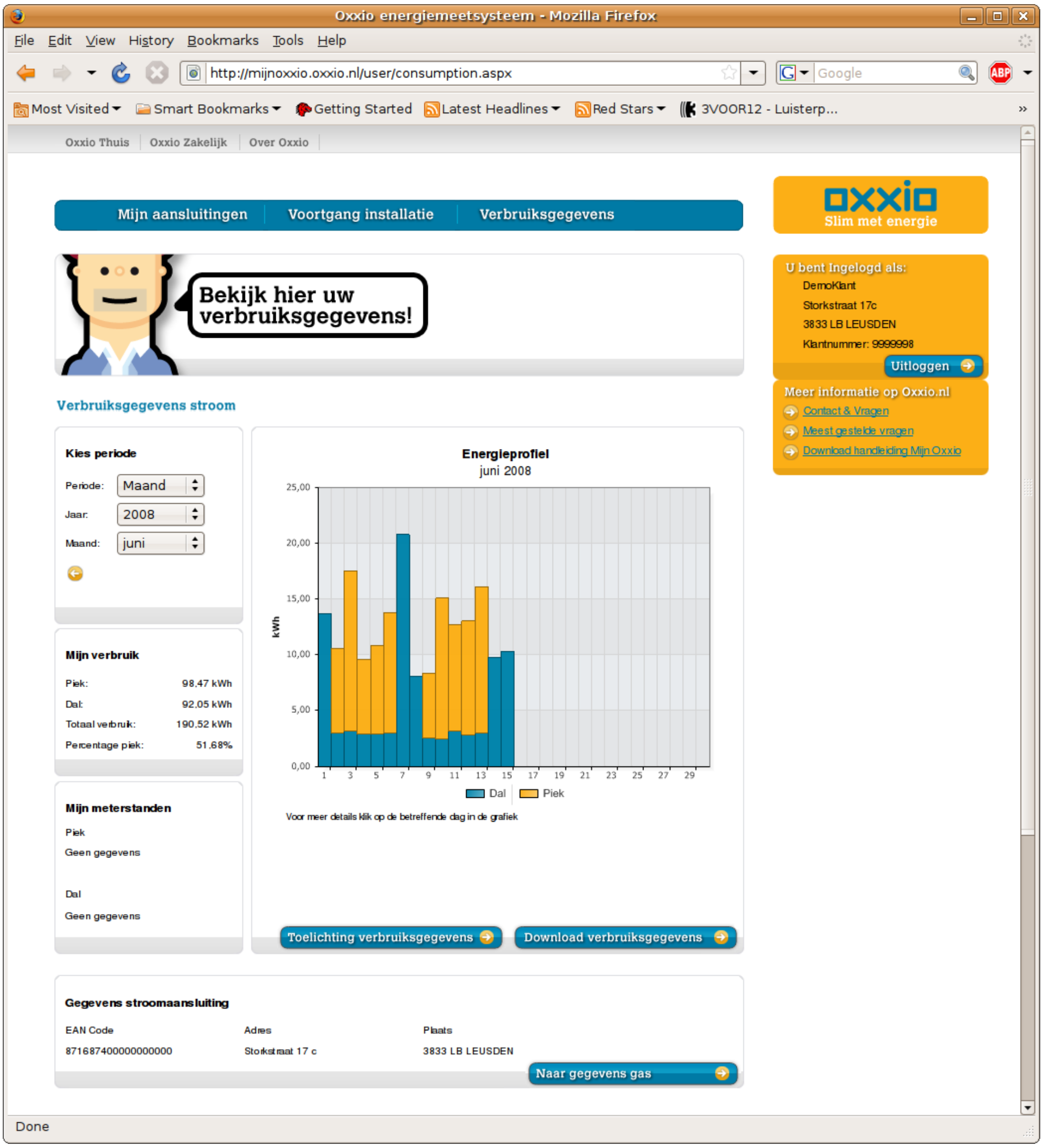

Application Process
COSEM Interface Objects IEC 62056-61,62056-62
Application Layer
COSEM Application Layer IEC 62056-53
COSEM IP Transport Layers IEC 62056-47
COSEM Wrapper
TCP or UDP
IP
Media Dependant Lower Layers
Data Link Layer
Physical Layer
SNDCP
LLC
RLC
MAC
GSM Radio
Application Process
COSEM Interface Objects IEC 62056-61,62056-62
Application Layer
COSEM Application Layer IEC 62056-53
COSEM IP Transport Layers IEC 62056-47
COSEM Wrapper
TCP or UDP
IP
Media Dependant Lower Layers
Data Link Layer
Physical Layer
Ethernet

(a) GPRS

(b) Ethernet

Figure 26: DLMS/COSEM [39]

C Oxxio website



U bent ingelogd als:
DemoKlant
Storkstraat 17c
3833 LB LEUSDEN
Klantnummer: 9999998

Meer informatie op Oxxio.nl
- Contact & Vragen
- Meest gestelde vragen
- Download handleiding Mijn Oxxio

Verbruiksgegevens stroom

Kies periode

Periode: Maand
Jaar: 2008
Maand: juni

Mijn verbruik

Piek:	98,47 kWh
Dal:	92,05 kWh
Totaal verbruik:	190,52 kWh
Percentage piek:	51,68%

Mijn meterstanden

Piek
Geen gegevens

Dal
Geen gegevens

Energieprofiel
juni 2008

Voor meer details klik op de betreffende dag in de grafiek

Gegevens stroomaansluiting

EAN Code	Adres	Plaats
871687400000000000	Storkstraat 17 c	3833 LB LEUSDEN

Figure 27: Personal Oxxio website with usage information, see the upper right corner for login credentials