Radboud University Nijmegen

# Beyond Smart Meters
## Legal compliance of Home Energy Management Systems

H.C.B. (Christiaan) Hillen

August 12, 2013

**Master Thesis Information Science**
Graduation Number 187 IK

Radboud University Nijmegen
Institute for Computing and Information Sciences

**Supervisor**
Prof. mr. dr. M. Hildebrandt
Radboud University Nijmegen
M.Hildebrandt@cs.ru.nl

**Second reader**
Prof. dr. M.C.J.D. van Eekelen
Radboud University Nijmegen
M.vanEekelen@cs.ru.nl

## Abstract

With the introduction of Smart Meters in the Netherlands, a new market is developing: Home Energy Management Systems. These systems allow users to gain insight into their energy consumption with enough detail to facilitate self-regulation, or in other words, to consume less energy. This thesis identifies the legal requirements for Home Energy Management Systems with regards to the processing of personal data and compares these requirements with five systems that are currently available in the Netherlands. The comparison is performed by exploring documentation and questioning client support services and developers of these systems. This comparison shows that none of the five systems conforms to all the legal requirements, with the biggest issues being a lack of personal data protection and the notification of the Dutch Data Protection Authority on the intent to process personal data. Suggestions for the mitigation of these issues are then given in recommendations on how to comply with the legal requirements as identified.

# Contents

# List of abbreviations

| | |
|---|---|
| 29WP | Article 29 Working Party |
| AES | Advanced Encryption Standard |
| CA | Certificate Authority |
| CBP | College Bescherming Persoonsgegevens |
| DES | Data Encryption Standard |
| DPD | Data Protection Directive |
| EAN | European Article Number |
| EDSN | Energie Data Service Nederland |
| EEPROM | Electrically Erasable Programmable Read-Only Memory |
| GDPR | General Data Protection Regulation |
| GPRS | General Packet Radio Service |
| HAN | Home Area Network |
| HEMS | Home Energy Management System |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Hypertext Transfer Protocol Secure |
| IEEE | Institute of Electrical and Electronics Engineers |
| PLC | Power Line Communication |
| PSK | Pre-Shared Key |
| SDRAM | Synchronous Dynamic Random-Access Memory |
| SMP | Slimmemeterportal.nl |
| SMU | Slimmemeteruitlezen.nl |
| SSID | Service Set Identifier |
| SSL | Secure Socket Layer |
| ToS | Terms of Service |
| VAS | Value-Added Service |
| VPN | Virtual Private Networking |
| WBP | Wet Bescherming Persoonsgegevens |
| WiFi | *see WLAN* |
| WLAN | Wireless Local Area Network |
| WPA | WiFi Protected Access |
| WPA2 | WiFi Protected Access 2 |

# 1 Introduction

For most people, most of the time, their energy consumption is invisible. Lights turn on, computers work, electric cars are charged. The only feedback households used to get on what amount of energy they were consuming, were the electricity and gas bills every few months.

But with the introduction of Smart Meters and their capabilities to offer detailed information on power consumption, this rate of feedback is changing. Not only can consumers see what is being consumed, but also when, a feature that old style meters do not offer unless observed continuously. With the increase in feedback and data creation however, comes the danger of this data falling into the wrong hands. No longer is your energy consumption only visible by looking directly at the spinning disk or blinking light in your electricity meter and the rotating numbers on the gas meter.

Energy consumption data can be shared with your supplier via wired or wireless communication protocols, making it possible to create accurate bills, but also to see, in detail, how much energy a household is consuming or through photovoltaic cells, is producing. Through non-intrusive load monitoring (NILM), it is possible to deduce a lot of information on what is happening behind the Smart Meter. There is an active line of research in this particular area, building device libraries and refining detection algorithms for NILM purposes.[1] Given enough details in this data, it is even possible to identify different appliances in the home by creating load signatures of devices, which can be seen as an electrical fingerprint of this device.[2] From this, the conclusion is drawn that *"the detailed readings of a home allow someone, who gains access, to draw extensive conclusions about the residents"*.[3]

The Smart Grid itself has been extensively researched with regards to security[4]; the Smart Meter has been explored in depth[5]; but there remains one open end, the data that actually will leave the relative security of the Smart Meter and enter the systems that will offer the consumer feedback. The devices giving the feedback, being either purely software, or with the aid of hardware are also known as Home Energy Management Systems (HEMS') and are the focus of this thesis.[6] [7] What data is being made available, to

[1] Efthymiou & Kalogridis (2010), Lam et al. (2007).

[2] Hart (1989), Hart (1992), Carluccio et al. (2011), Greveler et al. (2012).

[3] Kirmse (2012).

[4] For instance: Khurana et al. (2010), McDaniel & McLaughlin (2009), Metke & Ekl (2010).

[5] For instance: Cleveland (2008), Molina-Markham et al. (2010), Garcia & Jacobs (2011).

[6] Inoue et al. (2003), Son et al. (2010).

[7] Not all Home Energy Management Systems require a Smart Meter to gather energy consumption data, utilizing sensors instead. The result however, is still the same as this information is highly granular and is combined with identification codes. Because these

whom, what devices are used, and do these devices offer enough protection against unlawful processing of this data?

Home Energy Management Systems are being widely installed on normal meters and used to process energy consumption data they are included in this thesis.

## 2 Research design and methodology

Due to the multidisciplinary nature of the research topic, the choice is made to work on two distinct domains, both the legal and the technical, or European data protection legislation and data security technology to be more precise. It is from these two perspectives that the HEMS' are examined. The main topic of research is:

> Do the HEMS' that are currently available in the Netherlands comply with the current legal framework? And if it turns out that there are compliance issues, what can be done to mitigate these compliance issues?

To answer these questions, the legal framework is explored in detail, with the prime focus on data protection on the one hand, and the grounds for the introduction of the Smart Meter and required capabilities on the other. From this legal framework, a set of legal requirements is distilled which is used in the technical domain to examine current implementations of HEMS'. Thus, the following sub questions are answered.

> What is personal data and is energy consumption data personal data?

> What are the legal requirements to processing personal data?

The technical domain is explored by examining a selection of five currently available options in the Netherlands. The focus in particular is on the communication of data from the Smart Meter to the HEMS, all the intermediate stations this data passes along the way and any forms of technical data protection that are implemented such as encryption and digital certificates. To get this information, manuals, promotional materials and other documentation are examined detailing the HEMS', the Dutch implementation of the Smart Meter and the Dutch system of data transmission from the Smart Meter. In addition customer services and employees from the various organizations involved in the HEMS' are contacted. This is done to answer the following sub questions:

> Where is personal data stored within the HEMS, who are the controllers and processors, and who can access this information?

> What data flows are present in the HEMS, and are these secure?

Finally, to answer the main research question, the implementations, their accompanying documentation and all other information to be found on these implementations are compared with the legal requirements, and a proposal is made for the mitigation of the found compliance issues.

The Information Science perspective of this research is something which should be kept in mind while reading this thesis. This perspective concerns itself with the design of information systems, and as such requires knowledge on the components that make up such systems, as well as knowledge on the organizations and people who are going to use these systems. This means that an information scientist needs to understand both the domain of information technology, and the domain of business administration and management. As such, detailed knowledge on either domain is not obtained, but a working proficiency is required to move within these domains.

A key skill for any information scientist is to be able to obtain this working proficiency in new fields in order to be able to communicate with the experts in these fields. Next to the independent performance of scientific research, this is what this thesis shows: the obtaining of a working proficiency in the fields of data protection legislation and digital security. Therefore, neither section is as detailed and in-depth as it would have been with either a legal or digital security master student. However, few will discuss both the legal and technical perspective and translate legal requirements into technical requirements, because they are specialists in one or the other, but rarely in both.

Information scientists are able to acquire the mindsets of specialists and 'think like one of them' and 'understand where they are coming from' without becoming specialists in these fields themselves. This allows information scientists to become intermediaries between fields, which is their actual speciality

Due to this nature of information science and information scientists, the research done in this thesis is quite unique. There are not many researchers who bridge gaps between technical and non-technical domains, in particular between law and technology, with the translation of legal requirements into technical requirements.

# 3 Smart metering basics

The Smart Meter (hereafter also simply called 'Meter') is a device that is currently being issued as a replacement for the traditional 'dumb' meter that is installed in households to meter energy consumption. The benefits for the end-user of having a Meter installed are hoped to be:[8]

- Universal access to affordable energy
- Reliability and availability of energy
- Detailed energy consumption feedback to the end-user, and expected ensuing reduction in greenhouse gasses
- Correct and timely billing
- Improved competition and efficiency in energy markets
- Flexible pricing strategies
- Load balancing
- Detailed information concerning energy consumption and pricing
- Transparency about the share of renewable energy in energy consumption
- Generation of renewable energy resources

This meter is not actually a 'smart' device, for it has very little digital or artificial intelligence. The main features of the meter, which are of interest and is its claim to being smart, are that the meter can be monitored and controlled remotely and that it can provide real-time energy consumption data which facilitate Smart Meter analytics. However, it is also possible to 'smarten' a dumb meter by retrofitting it with sensors and a communication capability, thus allowing for most of the features of Smart Metering to be available with a dumb meter.[9] Although a smartened meter is still better than a dumb meter with regards to insight into energy consumption, it is insufficient with regards to the other hoped benefits such as those involved with the production of energy and serving this back to the grid and the two-way communication allowing for remote control of the Meter.

No longer does one have to check the meter by hand, the meter can communicate with the grid operator directly either through wired or wireless technologies.[10] Also, clients can receive real-time feedback on their

[8] Morch et al. (2007), Hildebrandt (2013) p.25.

[9] Darby (2010).

[10] Kamstrup 162 - Generation J Smart Meter data sheet. Mentioning M-bus, PLC (Power Line Communication) TCP/IP, GMS/GPRS, radio and S0 pulse as means of

consumption, which has been indicated as being essential for the realisation of consumption reduction.[11] The customer gets a greater insight in his energy consumption through the use Home Energy Management Systems and he might monitor his power consumption from outside of the home as well, using web portals from the suppliers or value-added services (VAS), which process the energy consumption data gathered by the meter and present them in a visually attractive manner.

The benefit for the energy suppliers is that they can provide detailed billing to the customer, whilst the network managers can use aggregated consumption data for load balancing purposes.

A Home Energy Management System (HEMS) is a system that process energy consumption data and presents this to the end-user in an understandable way, for the purpose of gaining insight into energy consumption such that a greater degree of awareness can be achieved on the amount of energy consumed. A HEMS can take the form of for instance an in-home display (IHD) connected to the Meter or a web portal that is run by a company processing the meter data. The systems can operate solely within the Home Area Network (HAN)[12] or simply make use of this network in data transmission.

One problem with the Meter itself, that indirectly affects its security, is the choices made in production based on economics. Given the amount of meters to be installed, which ranges in the millions, any savings that can be done in the cost to construct such a meter will quickly add up. Thus, the computational resources of the Meter are limited to only a slow CPU and a small amount of memory, when compared to smart devices. Such a limited system is barely suitable for strong encryption protocols which require extensive calculations.[13] [14] Combined with the problem of managing keys to millions of meters in case root access it needed to perform software updates, the difficulties of smart metering from a security perspective become clear.[15]

communication although some are optional and must be built in or added through modules. Typical for Dutch meters is communication through GPRS (as is the case with the meters supplied by Oxxio) or PLC.

[11] KEMA (2010), Intelligente meters in Nederland; herziene fianciele analyse en adviezen voor beleid. p.55.

[12] A Home Area Network or HAN, is a computer network on a small scale, typically consisting of just the personal computers within a household, along with the router and modem which connect this network to the Internet. Most of these networks have wireless capabilities so that smart devices and laptop computers can use this network to connect to the Internet as well.

[13] Kirmse (2012).

[14] Encryption is the act of making data unintelligible such that this action can be reversed if one knows the key. A very simple example is a=1, b=2, . . . ,z=26, such that '7,8' spells 'hi'. a=1 etc. is called the key, '7,8' is called the cyphertext, and 'hi' the plaintext.

[15] Anderson & Fuloria (2010).

## 3.1 Ports and data streams

From the meter, the data is passed on through various ports. Ports can take the form of physical or virtual ports, which can be compared to hardware versus software. A physical port is a piece of hardware, something one can touch and feel, and has substance and mass. A virtual port is a piece of software, it can not be touched or felt, and has no substance or mass, it exists only as computer code.

Within the Smart Meter architecture, energy consumption data has two ports of origin, the P1 port, and the P4 port, each of which will be described in detail in the following sections. Although there are two ports of origin for energy consumption data from which HEMS can receive data, there are more ports within the Smart Meter architecture, as seen in Figure 1.

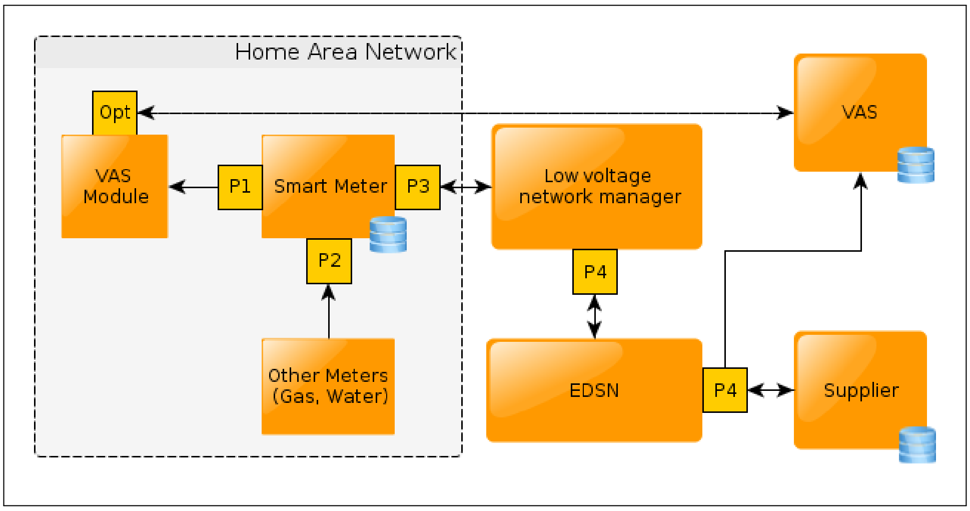


Figure 1: An overview of the ports on the Smart Meter and the information flows within the smart metering system concerning the data from the meter. The end-user resides within the Home Area network and has access to the Smart Meter. Connected to the P1 are devices supplied by Value-Added Services, with an Opt(ional) data stream to and from the Value-Added Service. The cylindrical symbols are storage locations. Based on te Paske et al. (2012).

### 3.1.1 The P1 port

The first port of interest is the P1 port, a physical port on the meter itself which allows devices to be connected directly to the meter. This port is also called the consumer port and provides the end-user with real-time energy consumption data with a ten-second interval.[16] Because of the short

[16] Netbeheer Nederland, P1 Companion Standard (final), p19.

interval between measurements, P1 data can be described as having a high granularity.

Because the P1 port is located on the meter itself, and the meter usually resides somewhere behind the front door, the end-user has direct access to this port.[17] In Figure 1, the end-user is not displayed, but is located within the Home Area Network.

The physical access to the meter and thus access to the P1 port means that at any time, the end-user can simply connect a device to listen to this port or disconnect a device that is listening to the port in order to prevent further data from being processed outside of the Meter. Any device capable of listening to and activating the P1 port can receive this data which takes the form of a telegram as shown below that is sent out by the port every ten seconds:

```
/KMP5 KA6U001660297912

0-0:96.1.1(204B413655303031363630323937393132)
1-0:1.8.1(00024.000*kWh)
1-0:1.8.2(00005.000*kWh)
1-0:2.8.1(00026.000*kWh)
1-0:2.8.2(00001.000*kWh)
0-0:96.14.0(0002)
1-0:1.7.0(0000.03*kW)
1-0:2.7.0(0000.00*kW)
0-0:17.0.0(999*A)
0-0:96.3.10(1)
0-0:96.13.1()
0-0:96.13.0()
0-1:24.1.0(3)
0-1:96.1.0(3238313031353431303034303232323131)
0-1:24.3.0(121030140000)(00)(60)(1)(0-1:24.2.1)(m3)
(00024.123)
0-1:24.4.0(1)
!
```

Each telegram starts with a forward slash and the type identifier of the meter, and ends with an exclamation mark. Between this first line and the exclamation mark are numerous lines in the form of `reference(value)`,the exact meaning of which can be determined by looking up the references in the P1 Companion Standard.[18] This tells us that `0-0:96.1.1` is the equipment

[17] Although it is possible that the meter is not accessible to the end-user due to policy of the landlord or because of the architecture of the building. In the Netherlands however, the meter is usually located within the home, a few feet from the front door. This thesis makes the assumption that the end-user has unrestricted physical access to his meter.

[18] Netbeheer Nederland, P1 Companion Standard (final), p12.

identifier reference, and `204B413655303031363630323937393132` is thus the unique identifier of this meter. As can also be seen in this telegram, the meter is currently registering the actual power delivery of just .03 kw (reference `1-0:1.7.0`). The very low readings in this telegram are because of the test system used to generate this telegram: a Meter for demonstration purposes with a single device attached to it, which was the power adapter for a laptop used to retrieve the telegram. No PV-cells are attached to register energy production, nor is there an ongoing base consumption as one would expect with a Meter in situ.

The purpose of the telegram is to inform the end-user about his real-time consumption. Given the format of these telegrams however, a method is still needed to collect and interpret consecutive telegrams in order to create an energy consumption graph. For this purpose, devices are made available commercially that can connect to the P1 port. The other option is to build a device oneself, although this requires knowledge on electrical engineering and computer programming as no dedicated hardware or software is readily available.

### 3.1.2 The P4 port

The second port of interest is the P4 port, a virtual port, which makes this port less obvious. This port is not actually located on the meter itself, but is located at the low-voltage energy supplier as seen in Figure 1. The P4 port offers energy consumption data formatted in XML[19], with an interval of fifteen minutes.[20] Because of this long interval between measurements, P4 data can be described as having a low granularity.

The fifteen minute data is an aggregate of the P1 data during this time interval, and is stored on the meter itself for a limited duration of ten days. After these ten days, the data is aggregated further, to represent a time period of twenty-four hours, and is stored on the meter itself for the limited duration of forty days. A last round of aggregation is then performed, to represent a time period of one month, and is stored on the meter itself for the limited duration of thirteen months. After thirteen months, the data is removed from the storage.

Although the P4 data is stored on the meter, it is not available from the meter directly. This is because the only party other than the end-user to have access to the meter is the low-voltage network manager.[21]

[19] XML or Extensible Mark-up Language, a language used to define the structure of data with existing and user-defined tags. This structure can then be interpreted by a web browser or by other pieces of software.

[20] P4 data is not made available to end-users, and as such, there is no example in this thesis of the P4 data format.

[21] Low-voltage network managers are one of the three types of network managers within the Netherlands. At the highest level there is TenneT, who manages the high-voltage network or grid that connects the regional nets together, and connects the Dutch grid to

|  | P1 Port | P4 Port |
|---|---|---|
| Recency of data | Real-time | Batchrequests: 1 day delay<br>Current: <1 hour delay |
| Granularity | 10 seconds | $\geqslant$ 15 minutes |
| History | No | Last 10 days with a granularity of 15 minutes<br>Last 40 days with granularity of 1 day<br>Last 13 months with granularity of 1 month |
| Other data | No | Statusinformation such as switch states, max throughput, etc. |
| Controllermessages | No | Yes, turning on/off, altering max throughput, displaying of message on meter display |
| Relevant legislation | WBP | WBP, Electriciteitswet, Gaswet |
| Controlling authority | CBP | Nederlandse Mededingingsautoriteit (NMa) and CBP |

Table 1: Differences between P1 and P4, adapted from te Paske et al. (2012).

Once the low-voltage network manager receives the data from the meter they pass this data on to Energy Data Services Netherlands (EDSN). This organization can be seen as a facilitator of administrative processes, they are the data brokers and are the interface between the low-voltage network manager and the energy suppliers and VAS'. Therefore, the only way meter data can become available to anyone but the end-user or the low-voltage network manager is either via P1, controlled by the end-user, or via the P4 port, in which case data can be requested from EDSN. It is also through EDSN that turn on/off and altering of max throughput commands are passed on to the meter.

As the low-voltage network manager is the only party who has a two-way communication connection with the Meter, they are the only ones who are technically capable of communicating with the meter and issue commands.[22] Accordingly, any commands from energy suppliers go through EDSN, who passes them on to the low-voltage network manager who then issues these commands to the meter.

The purposes of P4 data are numerous, first and foremost it can be used by energy suppliers for billing purposes, but it can also be utilized in load balancing. It is also used by the VAS' and the energy suppliers to provide the end-user with a current energy consumption overview, although in this case there will be a delay in the readings. Lastly, it can be used for a historical overview, consisting of the data up to thirteen months ago, in order to compare monthly consumption against the same month in the previous year.

### 3.1.3 Other ports

Next to the P1 and P4 ports, Figure 1 also depicts ports P2 and P3. P2 is a physical port on the meter itself, which allows for the connecting of for example a gas meter or water meter to the Meter in order to add these consumption data to the data stream. To utilize this port, a physical gas or water meter must also be present, and capable of making its data available in such a way that the P2 port can interpret this correctly. This port is not further discussed in this thesis.

P3 is the psychical port that actually provides the P4 type data, but does so only towards the low-voltage network manager as already mentioned. The two typical methods of communication with this P3 port are General Radio Packet Service (GPRS) and Power Line Communication (PLC). GPRS is in

the surrounding countries. At the middle level are the middle-voltage network managers, who manage the regional branches. Finally, the low-voltage network managers form the connection between the regional branches and individual households (meters).

[22] Although any party with sufficient technical capabilities and in possession of the needed security items such as private keys and equipment identification codes might be able to spoof communications and commands, although this has not been done successfully yet.

fact, the same method as used by mobile phones. PLC is a form of communication that uses pulses over the power lines themselves. PLC messages are collected in a data concentrator which is usually located at the distribution point within a neighbourhood. This data concentrator then passes the gathered data on to the low-voltage network manager via GPRS. Because of the various forms of communication offered, the P3 port can take on the form of a GPRS antenna, a module connected to the power lines for PLC purposes, or other forms as required for the used technologies. Each meter equipped accordingly can send and receive PLC pulses, and due to the nature of power lines, anyone who has a connection to the line these pulses travel over can listen in on these pulses, just as eavesdropping on GPRS is possible using a suitable antenna. However, both these channels are secured using encryption.[23] This thesis abstracts from these two methods of communication, although eavesdropping is possible.

### 3.1.4 Optical Sensors

The last possible source of energy consumption data is not depicted in Figure 1, because it is not a part of the Smart Metering architecture. Those people who want to gain insight in their energy consumption, but do not have a Meter, can opt to fit their dumb meter with optical sensors.

Because this data is not subject to standardization, the recency of data, its granularity, and the availability of other data than just the energy consumption data are unknown as each device can implement its own specifications. Nevertheless, as with P1 and P4 data (see Table 1), the Dutch Data Protection Act (Wet Bescherming Persoonsgegevens or WBP) still applies and the Dutch Data Protection Authority (College Bescherming Persoonsgegevens or CBP) is still the controlling authority.

## 3.2 Privacy impact of energy consumption data

In the previous section, the three sources of energy consumption data have been identified: the P1 port, the P4 port and optical sensors placed on dumb meters.

Whilst P4 data is protected using digital certificates and an IP whitelist[24] to ensure that only authorized parties have direct access to this data via EDSN[25], P1 and sensor data do not have such a de facto protection. It is up to the HEMS supplier to provide security in accessing P1 and sensor data as there are no standards or mandatory requirements other than those stipulated by law. That is to say, although there are legal requirements,

[23] PLC is encrypted using single DES, the encryption on GPRS is unknown to the author.

[24] An IP whitelist is a list of Internet Protocol (IP) addresses. Each IP uniquely identifies a computer, and only the IP's that are on the list are allowed access.

[25] te Paske et al. (2012).

there are no mandatory technical or organizational requirements described in order to fulfil these legal requirements. Due to the high value of detailed energy consumption data, malicious attempts to access this data are to be expected.[26] However, not only malicious access is attempted: *"History has shown that where financial or political incentives align, the techniques for mining behavioural data will evolve quickly to match the desires of those who would exploit that information"*.[27] Each of the three sources will be explored in detail to identify privacy issues in the processing of this data.

### 3.2.1 P1 data

The most detailed data available, P1 data is sensitive and highly prized and contains a host of information including make of the meter, its unique identification code and real-time consumption data. Anyone who gets access to this information can decipher patterns about a household and given access to enough P1 data sources, can construct profiles on energy consumption and use this information to classify households.

If the access is managed in near-real-time (seconds from the actual event), not only can a profile be created, but it can be used to identify the location and activity of the data subject within the home. As such, P1 data is very sensitive data.

An important factor in P1 data is that the data subject can, at any time, decide to no longer share this information by unplugging the connector on his Meter.[28] This places the data subject in a position of direct control over the availability of his data. However, once the P1 data has left the Meter and is communicated towards the HEMS, it is out of direct control of the data subject.

A real threat to data security from P1 data is the method of communication between the device that is plugged into the P1 port and whatever HEMS is used to display this information. In some cases it is a closed system where the P1 data does not actually leave the HAN, although any wireless communication is sniffable given the right tools. In this case, only those within the HAN are able to gain access.[29] In other cases, the P1 data is sent over the Internet to remote servers and made available on a web portal or smart device style HEMS.

When P1 data is sent to a server, a myriad of potential vulnerabilities exist. Each communication pathway and each storage location is susceptible to malicious intentions, mistakes in implementation of digital security measures, or unintentional actions. Web portals themselves might also be at risk if not secured properly, as is the database that is used to store login

[26] Knyrim & Trieb (2011).

[27] McDaniel & McLaughlin (2009).

[28] The same holds true for sensor data.

[29] Or in case of wireless transmissions, those within range of these transmissions.

data. The media has shown countless examples of databases filled with login data being stolen by hackers because of for instance SQL-injection vulnerabilities or passwords that can be found with simple dictionary attacks.[30] That such vulnerabilities still exist even though these particular exploits have been known for a long time indicates that keeping up with technical data protection deserves attention, as this is a part of the legal obligation as well.

### 3.2.2 P4 data

P4 data is much better regulated than P1 data in that the only way to access it is through a request with EDSN to obtain this data. The procedure for this is highly regulated and requires that the VAS provider presents an accountant statement to the low-voltage network operator (or, in the first four months, a declaration by the board of directors of the VAS) and a signed list of EAN codes[31] of customers by whom the VAS has been mandated to remotely read the meter. EDSN checks the board statements whilst the low-voltage network manager checks the accountant statement.[32] [33]

Technical authentication of VAS and suppliers happens through certificates which have to be collected in person with EDSN, for which an identification document such as a passport is also needed; an accompanying PIN code is sent through e-mail. Finally, only fixed IP's have access to the P4 port.[34]

After verification that the VAS is legitimate, no further checks are done; the list that the VAS provides is not compared to the data that is actually requested. Research has not indicated that the low-voltage network managers check this list either.[35] No checks are made to verify that the data subject has actually mandated the VAS to start monitoring energy consumption on the P4 port, the VAS' are simply trusted to do the right thing. Someone with malicious intent might thus feign the role of VAS, write their own director's statement (as a one-man VAS company), search for the EAN codes he wants to monitor using the EAN codebook[36], get a certificate from EDSN, and start monitoring energy consumption data. This is not a very likely scenario but it is a vulnerability in the system.

More likely is the scenario of data leakage by the insecure processing of

[30] For instance http://www.itworld.com/open-source/366287/ubuntu-forums-hacked-tux-penguin-joins-nra and http://money.cnn.com/2012/06/06/technology/linkedin-password-hack/index.htm.

[31] EAN or European Article Number is a 13 digit identification code.

[32] te Paske et al. (2012) p.18.

[33] EDNS, Procedurebeschrijving Portal P4 Leveranciers en ODA's, versie 1.4 (definitief), June 7th, 2012, section 4.

[34] Ibidem.

[35] te Paske et al. (2012) p. 19.

[36] To be found at www.eancodeboek.nl, a service provided by EDSN.

data by the VAS. As discussed in the previous section, a web portal might prove insecure, a database might be vulnerable to (yet unknown) exploits possible that will cause the P4 data to be leaked.

### 3.2.3 Sensor data

Unlike P1 and P4 data, sensor data contains only the energy consumption data as it observes from the meter, there is no identification code for the meter being observed. There is however, an identification code for the hardware that is being used to register this data, to facilitate processing by the VAS. The granularity of sensor data can vary, as a spinning disk can be nearly continuously monitored, allowing for second by second updates. It is unknown how frequent the sensor-based HEMS actually do register the energy consumption data, but a frequency of at least every ten seconds is to be expected.

## 3.3 Feedback on consumption

One of the prime benefits for the consumer is the possibility to gain detailed insight in his energy consumption. This feedback can take several forms, with the main distinction being between direct and indirect feedback. Direct feedback is given through an in-home display or website which receives its data from P1 or through sensors, the real-time nature of this feedback is what distinguishes it from indirect feedback. Indirect feedback is given through websites or even on paper. This feedback is based on P4 data, making it at least 24 hours old.

Through web-based applications, the supplier of this service (the energy supplier, or a VAS) has access to and control over the data that is made available. Because this information is already under control of the VAS, he has the option to also offer a smart application that serves the same purpose as the web portal. This can be done to partially overcome the problem of engagement by customers, causing them to regularly access this information, as web portals alone have shown limited customer engagement.[37]

In general, savings of 0-10% are expected from indirect feedback, with a Dutch study using a web portal yielding an 8.7% conservation.[38] Direct feedback yields savings of 5-15% although it does take about three months for new consumption and savings practices to become habitual.[39] The prime motivation for consumers to conserve energy is the financial benefit, although the environment is a strong second.[40]

[37] Darby (2010).

[38] Benders et al. (2006).

[39] Darby (2006).

[40] KEMA (2010), Intelligente meters in Nederland; herziene fianciele anayse en adviezen voor beleid. p.55-56.

## 3.4 Data storage

Figure 1, the overview of datastreams, depicts several storage locations. The first location for data storage is within the meter itself using EEPROM storage.[41] The data stored within the meter is the history data available on the P4 port as described in Table 1.[42]

The second storage location lies with the energy supplier who uses P4 data for billing purposes and (in)direct feedback depending on legal obligations and the consumer's preferences. It is not always clear however, how long this data is stored exactly, and what measures are in place to prevent issues concerning confidentiality, integrity and availability.

The last storage location lies with the VAS (or energy supplier doubling as a VAS), who uses this data to offer a service to the customer. Given that a VAS might receive P1 or P4 data, this raises concerns as this is the only location outside of the household where P1 data is sent. If there is no storage unit connected to the P1 port within the home area network, the database of the VAS is the only location where P1 data might be stored. Transparency in how the VAS' processes P1 and P4 data depends largely on how the VAS' set up their services and offers the data subject insight. There is a risk here that data subjects do not receive effective insight into the stored data, leaving them uncertain as to what is being processed and so, what the VAS' actually know about the data subject and what purposes the data is actually used for.[43]

Aside from these long-term storage locations, there is also the short-term location that lies with EDSN. For a party to gain access to P4 data, they must request this data from EDSN, who in turn requests this data from the low-voltage network manager. This data is then requested from the P3 port on the meter by the low-voltage network manager, passed back to EDSN and cached, waiting for the requesting party to retrieve this data, EDSN removes the data from their own system once it has been collected by the requesting party, thus the P4 data is now only with the requesting party and EDSN no longer has a copy. For every storage location, be it temporary through caching, or for longer term use, it is unclear if practice indeed follows the legal requirement that data be removed once it is no longer needed for the purpose it was collected.

[41] EEPROM or Electrically Erasable Programmable Read-Only Memory. This type of storage will retain its data even if disconnected from a power source, a useful feature considering the possibility of a blackout and the vital need for the data on the meter for billing purposes.

[42] The meter should delete data which is not needed to construct the history, although whether this is actually done can not be verified without either looking into the meter software or actually reading the EEPROM memory by extracting this from the meter and exploring it, which lies beyond the scope of this thesis but might prove interesting to pursue.

[43] te Paske et al. (2012).

In this, the consumer will have to trust the data controllers and processors that they indeed have all the proper security features in place to safeguard the data. The consumer will also have to trust the low-voltage network managers and EDSN in that these parties will not store energy consumption data for longer than is necessary to fulfil the purpose of making this data available on the P4 port.[44]

The consumer is only protected through codes of conduct and guidelines, and will just have to trust the data controllers to actually live up to these expectations in a form of centralized trust.[45] [46]

## 3.5 Profiling

With the aid of Meter data, it is quite possible to construct a profile of a household. Using NILM techniques to identify certain patterns within the data that can indicate daily routines and the presence of certain devices has been possible for decades already. Through the load monitoring of the dumb meter in several households, Hart (1989) was capable of identifying devices such as a refrigerator, a failed underground septic tank pump and a water-bed, even being able to distinguish between this bed being made or uncovered. These devices were identified through their typical energy consumption profiles.

Two German security researchers demonstrated that a television will consume different amounts of energy depending on what film is being watched for energy consumption of a screen is in direct correlation with brightness and contrast of that screen.[47] This fingerprint is unique, and with it, they were possible to identify when this particular film was being watched within a complete household energy profile consisting of several days of data.

Profiling does not stop with just the devices, complete households can be profiled using the available data. The, by now classical example, of a devout Muslim getting up at five in the morning for daily prayer, perhaps combined with a family name which can quite easily be obtained, makes it easy to see how certain groups of people could be 'singled out' by exploring the data.[48] Daily behaviour, time of getting up, having breakfast, showering, leave the premises to go to work, come back home, and going to bed can all be inferred from an energy consumption graph.[49] Depending

[44] This thesis assumes that indeed these parties do not store this data longer than is needed to fulfil this purpose, as the storage or removal of data by these parties is unverifiable by the author.

[45] Garcia & Jacobs (2011).

[46] Netbeheer Nederland (2012) Code of Conduct for the processing of personal data by Grid Operators in the context of installation and management of Smart Meters with private consumers. Entered into force May 19, 2012.

[47] Carluccio et al. (2011)

[48] Interpretation of load graph from Quinn (2009) made in Kursawe (2012).

[49] Knyrim & Trieb (2011).

| **Question** | **Characteristic** | **Granularity** |
|---|---|---|
| Does the consumer live alone? | pattern for a single or multiple occurring events | hours/minutes |
| When is the consumer working? | no power activities for long time during the day | hours/minutes |
| Does the consumer use a microwave or oven? | oven: long pre-heating phase with heating for temperature hold. microwave: short heating phases of wave generator | seconds |
| How often does the consumer wash his clothes? | heating phase of washing machine with subsequently spin cycle | minutes |
| How often is a hot drink consumed? | usage of water boiler: high consumption for short time | minutes/seconds |
| Which TV program did the consumer watch? | matching pattern of specific TV program | minutes/seconds |

Table 2: An overview of questions concerning private information that can be inferred from energy consumption data with various granularities (Kirmse, 2012).

on the granularity of data, certain basic questions can be answered about a household as can be seen in Table 2. With the advancements of data mining and big data techniques, complex patterns and profiles can be created to categorise households and cater to needs identified with these categories, going beyond the basic questions from Table 2. Although the benefits of profiling might be interesting, as services can be offered that are likely to be of interest, the dangers for a household of receiving a certain label and thus being subject to decisions based on this label are not to be underestimated. Furthermore, with the possibility to identify certain appliances and noticing that they start to slowly decrease in efficiency (a fridge that cycles more frequently or uses more power now than it did last year) this information can be used for targeted (fridge) advertisement.

Some consumers might experience these recommendations as beneficial and be grateful that imminent breakdown or inefficiency was noticed, whilst others might experience this as a form of intrusion into their private domain.[50]

Recommendations according to certain labels that might be received due to the conformity of a household with a profile may lead to households that correspond to different profiles being treated in different ways. With the right of access however, the data subject has the right to obtain from the data controller, *"knowledge of the logic involved in any automatic processing*

[50] Garcia & Jacobs (2011).

*of data concerning him at least in the case of automated decisions"*.[51] Thus, if energy consumption data is used to create profiles and to automatically label households based on these profiles, the data subject has the right to know how this is being done. The data subject also has the right *"not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc."*[52] Thus, although profiling is not explicitly prohibited by law, data subjects do have the right not to be subjected to profiling if its legal effect has significant impact on their person.

Regarding the reasons for profiling; in the Q&A session of the 28C3 talk by security researchers Dario Carluccio and Stephan Brinkhaus concerning the hacking of a Smart Meter, Nikolaus Starzacher, the CEO of the German Smart Meter supplier Discovergy, actually stated the reason for collecting detailed energy consumption data to be *"to see if you have an old fridge or an old washing machine"*. He went on to explain that their income model was currently based on the installation and subscription fees, but in the future they would be exploring the possibility of commissions when recommending energy supplier switching to current customers and commissions on appliance replacement recommendations.[53]

## 3.6 Stakeholders

Within HEMS', two main stakeholders can be identified, who's interests are in conflict with one another. On the one hand there are the consumers, who are generating energy consumption data. Their interest is in getting as much detail as possible in order to get an accurate picture of their energy consumption, but at the same time controlling who has access to his data. On the other hand there are the service providers (VAS and energy suppliers in this role), who have a keen interest in this energy consumption data for marketing purposes. With more detailed consumption data, more detailed information can be deduced from this data and better offers can be made accordingly.[54]

In this tension between the service providers and customers, a balance must be found for each customer individually. Some do not want anyone to process their personal data, whilst others just want the best possible service and have no problem with the service provider processing their personal data. Therefore it is a trade-off between keeping personal data for oneself

[51] Directive 95/46/EC. Art. 12.

[52] Directive 95/46/EC, Art 15.

[53] A video recording of this talk can be found on youtube at https://www.youtube.com/watch?v=YYe4SwQn2GE, last referenced on July 25 2013.

[54] Kirmse (2012).

and providing (parts of) this personal data to service providers so they can provide more accurate services; for if a VAS only has access to P4 data, he can not provide services that would require P1 data.[55]

### 3.7 Dutch energy suppliers market

Within the Dutch borders there are numerous energy suppliers, at least seventeen but it is hard to get a complete list of suppliers as not all offer their services within the entire geographical area of the Netherlands and suppliers come and go. Different suppliers cater to different needs, not only based on geographical factors, but also with regards to the demand on electricity created strictly through 'green' methods such as wind and solar power. Every household has a choice of several suppliers competing against each other for the consumer's favour. This can be done for example via the aforementioned 'green' branding, by making special offers with regards to pricing flexibility or the promise to keep a price fixed, even when the laws of supply and demand dictate that the price should be increased.

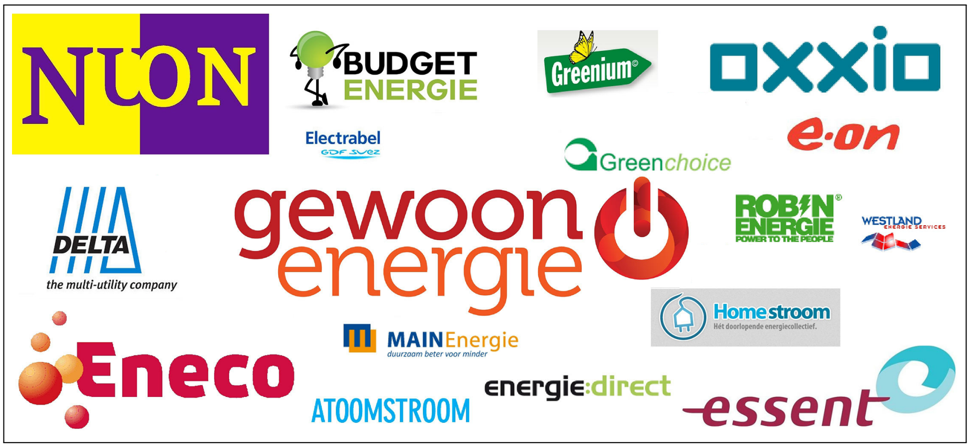


Figure 2: Logo's of most of the energy suppliers in the Netherlands. Due to ever changing markets this overview is incomplete and merely serves as an indication of the number of suppliers in the Netherlands which, combined with not all suppliers being available for every household, makes for a complex market.

Some suppliers are already offering HEMS services, either in the form of an IHD or through a web portal and smart device application. However, there are also services that are not directly offered by the energy suppliers but rather by VAS, who have no direct link with the energy market other than offering such a service. As such, these services do not have a need for the data in the light of load balancing or for billing purposes. Their interest

[55] Ibidem.

| Name | Description |
|---|---|
| Toon (Eneco) | An IHD, P1 device and web portal by supplier Eneco |
| mijnOxxio (Oxxio) | A web portal by supplier Oxxio |
| e-inzicht (Essent) | A web portal by supplier Essent |
| E-manager (Nuon) | A web portal by supplier Nuon |
| plusdata (Anode) | A web portal by supplier Anode |
| Qurrent Qbox mini | A P1 device and web portal by VAS Qurrent |
| i-CARE | A web portal and possibility for a P1 device depending on the package, by VAS enerGQ |
| myNet2Grid | A P1 device and web portal by VAS Net2Grid |
| SWYCS | A set of monitored wallplugs and web portal by VAS dsp-innovation |
| Wattcher | An optical sensor and an IHD by VAS wattcher |
| Smile P1 | A P1 device and web portal by VAS Plugwise |
| Slimmemeteruitlezen.nl | A web portal by VAS Enepa |
| Slimmemeterportal.nl | A web portal by VAS EnergyAlert |

Table 3: A selection of HEMS available on the Dutch market, either via one's own energy supplier or as a value added service. Note that not all of these HEMS actually utilize P1 or P4 data, some use sensors to collect energy consumption data from dumb meters.

lies in making money from this information by creating added value for their customers and finding new business models for this information.

Table 2 offers an overview of HEMS that are available on the Dutch market to gain insight in household energy consumption.[56] Some of these devices are available through the energy supplier only, whilst others are available to anyone. At the time of writing this thesis, no device was found that interfaces only with P1, without using the HAN or the Internet.

[56] Source: http://www.milieucentraal.nl/thema%27s/thema-1/energie-besparen/slimme-meter-en-energieverbruiksmanagers/energieverbruiksmanagers-inzicht-in-energieverbruik/, last referenced June 3 2013.

# 4 Legal framework

The legal framework surrounding smart metering covers various topics. First, the third energy package is explored, being the legal ground for the introduction of Meters, and the roll-out of Meters in the Netherlands. Second, the examination of the definition of personal data is performed and checked against energy consumption data. Third, the data quality principles concerning the processing of personal data are detailed and applies to energy consumption data. Fourth, transparency is discussed with regards to energy consumption data and the creation of profiles. Fifth, this transparency principle is discussed in light of the ePrivacy Directive and prior informed consent. Sixth, because appropriate technical measures should be taken in protecting personal data, the data security goals are discussed. Finally, legal requirements are derived that will be used in the next chapter to test legal compliance of HEMS.

For meters to fulfil their potential, they will be processing energy consumption data, which will be examined to see if personal data is involved in this processing and what grounds are likely to legitimize this processing. This chapter is concluded with requirements for the processing of this data within the context of the legal framework in order to comply not only with data protection regulations, but also to comply with the minimal requirements concerning providing the customer insight in his consumption data as lies within the capabilities of the meter and is demanded by legislation.

As is the case with European Directives, these Directives have to be transposed into national law as stipulated in The Treaty on the Functioning of the European Union:*"A directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods."*[57] In particular, the Dutch transposition of the Data Protection Directive is the Dutch Data Protection Act or 'Web Bescherming Persoonsgegevens'(WBP). The transposition of Directives into national law is complete, in that although the form and methods are left to the Member States, no (part of an) article may be omitted or altered, nor additions be made. Directives differ from regulations in that regulations have direct applicability on Member States and do not require the transposition into national legislation.

In this section, various Opinions by the Article 29 Working party (29WP) are also cited. The 29WP is set up according to article 29 of Directive 95/46/EC: *"A Working Party on the Protection of Individuals with regards to the Processing of Personal Data, hereinafter referred to as 'the Working Party', is hereby set up. It shall have advisory status and act independently."*. This article then continues with a dictation of the composition

[57] Treaty on the Functioning of the European Union, Art. 288.

and methods of the 29WP. Although the Opinions themselves have no official legal status, they are highly regarded by the field of law and the 29WP is considered to be an authoritative source; in daily practice the Opinions are tuned to for advice and interpretations of legislation concerning matters of personal data processing.

## 4.1 Third Energy Package and the Dutch case

The introduction of the Meter has its roots in the Third Energy Package.[58] This package contains two Directives, setting forth rules for the international electricity market and setting forth rules for the international natural gas market. Directive 2009/72/EC prescribes that EU member states should equip at least 80% of consumers with Smart Meters by the year 2020.[59] The prerequisite for this is that an economic assessment is performed, which should be performed prior to September 3, 2012.[60] This economic assessment on behalf of the Dutch Ministry of Economic Affairs was performed in the Netherlands by KEMA in 2010 which was positive.[61]

A new assessment was performed in 2012, taking into account the Meters already equipped to Greenhouse horticulture and heavy industries as part of the baseline.[62] [63] This assessment was positive regardless of climate policy or decentralized energy production; as in almost all scenario's the cost-benefit analysis was positive.

Because of the positive assessment, Meters were to be rolled out in the Netherlands, but met with considerable problems. Because of the underlying goal of energy efficiency to be accomplished with the meter, and the ensuing initial neglect of consumer privacy issues, this resulted in unanticipated public resistance which had to be mitigated in order to successfully introduce the Meter such that no more than twenty percent of customers would reject the meter.

[58] Consisting of: Directive 2009/72/EC; Directive 2009/73/EC; Regulation (EC) No 713/2009; Regulation (EC) No 714/2009; Regulation (EC) No 715/2009. Which entered into force in September 2009 giving member states 18 months to transpose it into national law.

[59] Directive 2009/72/EC, annex 1.2 states "intelligent metering systems" which essentially are Smart Meters, legislation generally uses broad terms to prevent being bound to certain technologies and unforeseen developments.

[60] Directive 2009/72/EC Recital 55 and Annex 1.2.

[61] KEMA Nederland (2010), Intelligente meters in Nederland, Herziene financiele analyse en adviezen voor beleid. The conclusion of this report was that roll-out on a voluntary basis was financially positive, however, when more than twenty percent of consumers reject the Meter, the result would no longer be positive. Which might actually be a possibility due to the recent discussions on privacy matters. See also Kamerstuk "Brief aan de Tweede Kamer over de geactualiseerde kosten-batenanalyse van de slimme meter", September 3 2010.

[62] CE Delft & KEMA (2012).

[63] Hildebrandt (2013).

Introduction of the meter consisted of three phases, the first phase led to the development of the NTA 8130 Smart Meter Standard.[64] The second phase of the roll-out was detailed in a bill[65], which met with severe criticism in parliament. Finally, in the third phase this bill was modified and the pilot roll-out commenced.[66] The critical issue here, and mitigation of the privacy critiques, can be condensed to the right of the consumer to refuse having a Meter installed or have it administratively turned off such that remote metering is denied.[67] One of the important articles in the criticism on smart metering is article 8 of the European Convention on Human Rights (the Convention) which reads:

> "Everyone has the right to respect for his private and family life, his home and his correspondence."

A paper by Koops and Cuijpers further details the Dutch case and the testing of the Dutch Meter against the Convention and coming to the conclusion that the Meter indeed infringes privacy as stipulated in the Convention.[68] More details on the specifics of the introduction of the Meter in the Netherlands, the troubles parliament faced, and the privacy issues raised can be found in Cuijpers (2011) and Braat (2011).

## 4.2 Smart Meter legislation

According to article 9(1) of Directive 2012/27/EC *"member states shall ensure that, in so far as it is technically possible, financially reasonable and proportionate in relation to the potential energy savings, final customers [. . . ] are provided with competitively priced individual meters that accurately reflect the final customer's actual energy consumption and that provide information on actual time of use"*.

Directive 2012/27/EC also explicitly connects the installation of a meter with *"the security of the smart meter and data communication, and the privacy of final customers meter"* with the relevant data protection and privacy legislation, further stressing the importance of data protection and privacy within the domain of Smart Metering.[69] As the meter has the capability to keep a detailed record on consumption, the end-user should *"have the possibility of easy access to complementary information on historical consumption allowing detailed self-checks"*.[70] Furthermore, the end-user shall *"receive all their bills and billing information for energy consumption free*

[64] NEN (2007).

[65] See Wetsvoorstel 31320, Wetsvoorstel 31374.

[66] Hoenkamp et al. (2011), Wetsvoorstel 32373, Wetsvoorstel 32374.

[67] Hoenkamp et al. (2011).

[68] Koops & Cuijpers (2009).

[69] Directive 2012/27/EC, Art 9.2(b).

[70] Ibidem, Art. 10.2.

*of charge and [...] have access to their consumption data in an appropriate way and free of charge."*[71] and be *"properly informed of actual electricity consumption and costs frequently enough to enable them to regulate their own electricity consumption. That information shall be given by using a sufficient time frame, which takes into account the capabilities of the customer's metering equipment. No additional costs shall be charged to the consumer for that service"*.[72] Finally, *"comparisons of the final customer's current energy consumption with consumption for the same period in the previous year, preferably in graphic form"* and a *"comparisons with an average normalised or benchmarked final customer in the same user category are made available to final customers in clear and understandable terms"* should be presented.[73]

## 4.3 Personal Data

In this section the Data Protection Directive (95/46/EC), also referred to as 'the Directive' and considered a *lex generalis* concerning the processing of any personal data, is examined to see if it applies to metering data. The Directive is titled *on the protection of individuals with regard to the processing of personal data and on the free movement of such data* which states its principle purposes. The Directive defines a completely harmonized level of personal data protection throughout all the member states on the one hand, and on the other the free flow of such data within Europe for the sake of economic interest.[74] The Directive in its second recital also states that *"data-processing systems are designed to serve man"*, as such, it facilitates personal data processing given certain restrictions rather than in principal prohibiting personal data processing save specific situations.

The processing of data as defined by the Directive is effectively described as anything that can be done with this data, including collection, storage and erasure.[75] Within the data flows as described in the previous section, operations are performed on data that clearly fall under this processing, starting out with the storage of energy consumption data on the meter, and the transmission of this data between the meter and the low-voltage network manager. More operations are performed throughout the network that are of similar nature although all of these operations which involve personal data are restricted according to the Directive which stipulates inter alia the preconditions under which personal data processing is legitimate.

If these data flows consist of personal data, their processing can only be performed under the terms as stated in the Directive with the exclusion of

[71] Ibidem, Art 11.1.
[72] Directive 2009/72/EC Annex 1.1(i).
[73] Directive 2012/27/EU, Annex VII 1.2(b) and (c).
[74] Schnabel (2009) p.516, Kuner (2007) p.20.
[75] Directive 95/46/EC, Art. 2(b).

processing concerning public security, defence, State security and in areas of criminal law and in processing by a natural person in the course of a purely personal or household activity.[76] For metering data to be identified as personal data, the definition given in the Directive is scrutinized and conclusions are drawn accordingly.

The Directive defines personal data as *"information relating to an identified or identifiable natural person"*.[77] This definition consists of four components, each will be discussed in turn. The division can take place as follows:

- "any information"
- "relating to"
- "an identified or identifiable"
- "natural person"

This division follows the Opinion "on the concept of personal data" by the Article 29 Working Party[78] in which they also elaborate on these *"building blocks [which are] closely intertwined and feed on each other"*.

### 4.3.1 "any information"

The term "any information" is a broad one, implying that any statement that is made about a person is to be considered, as opposed to statements about objects and non-tangibles. This information can be both of an objective (age) and subjective (credit assessment) nature, and need not actually be true, as false information can still be linked to a person. Indeed, information has a very broad scope up to and including information stored within the memory of a computer in the form of binary code.[79] [80] As such, the content of this information is not relevant, as long as it is information, or in other words data. Personal data *"includes information touching the individual's private and family life [...] but also information regarding types of activity undertaken by the individual."*[81]

As, although the activity itself of turning an appliance off or on does not seem to fall under the information about a person directly, this activity does indicate that a person had interaction with this appliance or that at the very least this application is present within a household as some appliances automatically switch on and off such as thermostats and refrigerators.

[76] Directive 95/46/EC, Art. 3.2.
[77] Directive 95/46/EC, Art. 2(a).
[78] 29WP, Opinion 4/2007.
[79] Nouwt (2008).
[80] 29WP, Opinion 4/2007 p.7.
[81] 29WP, Opinion 4/2007 p.6.

Through careful monitoring of energy consumption, it is quite possible to identify individual appliances within a household from amongst the detailed accumulated energy consumption data. In one study it was even shown that through this monitoring, performed with an optical sensor on a dumb meter, the researcher could tell if a water bed was made or uncovered due to differences in its electric heater cycles.[82]

A meter will register the switch of an appliance as a change in power consumption, and over time, the accumulated power consumption is stored on the meter itself, thus this data is processed.[83] Thus, the conclusion is that the switching activities within a household as registered by a meter through changes in energy consumption and is stored on this meter is information (on a data subject).

### 4.3.2 "relating to"

The 29WP states that *"information can be considered to 'relate' to an individual when it is* about *that individual"*.[84] In the case of the smart metering, at its core, the information gathered by the meter is strictly information on how much energy is consumed within the household, that the meter is connected to. To assert that indeed, this information relates to an individual, the 29WP describes three elements should be explored, these are 'content', 'purpose' and 'result'.[85] 29WP also states that *"data relates to an individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated"*.[86]

The 'content' of energy consumption data is not directly about an individual for it does not contain a name, personal identification number, or other direct relation. The relation is indirect, as energy consumption data contains a unique identifier that belongs to a specific Meter from which the data originated, akin to a signature. This signature is related to a specific energy consumer, who will be billed according to this specific energy consumption data, but the content of this data is not directly about a person but rather about the specific combination of appliances that consume energy within the household.

The 'purpose' of energy consumption data conforms to what the 29WP describes as *"to evaluate, treat in a certain way, or influence the status or*

[82] Hart (1989).

[83] As the meter itself contains an EEPROM memory chip, which can be seen as similar to a flash-card or USB stick, although not removable from the meter, storage (thus, processing) takes place in the form of binary code as it does with all computers.

[84] 29WP, Opinion 4/2007 p.9.

[85] 29WP, Opinion 4/2007.

[86] 29WP, Working document on data protection issues related to RFID technology. January 19 2005.

*behaviour of an individual"*[87] For indeed, processing of this data is done for the purpose of, amongst others, influencing the behaviour of the individual concerning his energy consumption.

'Result' implies that the data in question, when processed, will have an impact on a person, specifically on his rights and interests. With smart metering, this is the case for it is in the interest of the specific person that his energy consumption data be correctly processed, for billing purposes and for real-time feedback. Also, energy consumption data might be used to indicate that a person is at home or not, and thus perhaps fulfilling or breaking an obligation to being at home. This is not the intended purpose of this data, but it is possible and thus have an impact on the person. The data might also be used to treat the specific person differently, that is, provide him with certain services depending on his energy consumption data and the profiles that can be created using this data.

Although 'content' and 'purpose' are not clearly linked to the person in the case of energy consumption data, this is the case with 'result'. Therefore, the conclusion is that energy consumption data relates to a person.

### 4.3.3 "an identified or identifiable"

*In general terms, a natural person can be considered as "identified" when, within a group of persons, he or she is "distinguished" from all other members of the group. Accordingly, the natural person is "identifiable" when, although the person has not been identified yet, it is possible to do it. This second alternative is therefore in practice the threshold condition determining whether information is within the scope of the third element.*[88] This rather long quote exactly indicates what it means to be either identified or identifiable. Article 2.a of the Directive gives further indication towards the interpretation of identifiable in that *"an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identification number[...]"*. Lastly, recital 26 of the Directive states that *"to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person"*.

With energy consumption data, the data itself contains a unique identifier in the form of a signature from the Meter, that is, a number that is unique to this meter, such that data from it can be distinguished from data generated by any other meter. Because of this unique signature and the usage of the energy consumption data to bill a natural person, the consumption data makes it possible to distinguish a household indirectly, through which the indirect identification of a person is possible. Although prima facie it might not be possible to identify a data subject, perhaps through the removal of

[87] 29WP, Opinion 4/2007 p.10.

[88] 29WP, 4/2007 p.12.

the unique signature from the data, when deliberate action is undertaken to single out this data subject from the collected data on numerous households, identification is still possible, although indirectly, for instance by comparing consumption data with social media activity, known (public) schedules or even direct observation of a household and comparing information gathered in this way, with patterns contained within the energy consumption data. Thus, with the linking of devices, what was considered no longer identifiable or identified (and thus no longer personal data) may turn out to still be identifiable.

The conclusion is that identification through energy consumption data is possible, due in part to the unique signature contained within the data, although identification is also possible without this signature by comparing energy consumption with other sources of information such as social media.

### 4.3.4 "natural person"

A natural person is a living human being, referring to article 6 of the Universal Declaration of Human Rights which states that *"Everyone has the right to recognition everywhere as a person before the law"*. This is a clear distinction from a legal person, which is not covered by the Directive, as stated in recital 24. As members of a household are living human beings, they are natural persons under law.[89]

### 4.3.5 Energy consumption data is Personal Data

Given the above four building blocks, the conclusion is made that energy consumption data is personal data for indeed this data is *"[...] information relating to an identified or identifiable natural person"*. In their opinion 12/2011 on Smart Metering, the 29WP comes to the conclusion that energy consumption data is personal data, due to the fact that: 1) the data contains a unique identifier, such as the meter identification number, 2) the data relates to a consumer's energy profile in the context of their energy usage, and 3) the data is used to facilitate the objective of reduction of overall energy consumption, which will require individual consumers to be targeted.[90]

## 4.4 Grounds for data processing

Having asserted that energy consumption data is personal data, the Directive states the legal criteria under which data processing might take place. In a nutshell, these criteria are (a) unambiguous consent, (b) to fulfil a contract (c) legal obligation, (d) vital interest of the data subject, (e) public

[89] For ease of discussion, the assumption is made that only humans are members of a household, domestic animals and pets are ignored.

[90] 29WP, Opinion 12/2011 p.8.

interest, and (f) legitimate interest of the data controller.[91] Each of these grounds by themselves are enough to legitimise the processing of personal data. In the following subsections, each of these grounds will be explored and linked to energy consumption data where relevant. The specific grounds as utilized in practice will be explored in a later section, when each specific HEMS is scrutinized.

### 4.4.1 (a) Consent

The Directive defines consent as *"any freely given specific and informed indication of [the data subject's] wishes by which [he] signifies his agreement to personal data relating to him being processed"*.[92] There are three requirements for consent given in this definition, namely "freely given", "specific" and "informed".

Firstly, freely given consent denotes that the data subject is truly free to exercise this choice *"without risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent"*.[93]

Secondly, specific consent indicates that the data controller has stated exactly what the purpose of the data processing is; the data controller has made a clear, closed-ended and exact purpose statement. This is opposed to the so called 'blanket consent' in which the data controller asks for consent to do as he pleases with the data once he has it, perhaps finding new and innovative uses for it along the way that have nothing to do with the initial purpose of collection.

Lastly, consent can only be given if the data subject is informed. Thus, not only does the controller need to indicate a clear purpose statement, but the data subject also needs to be informed about this and made aware of the implications of data processing.

Consent can be given implicitly and explicitly. Explicit consent in general terms means that a data subject has to undertake a specific action to denote his consent such as placing a signature, pressing a button for this specific purpose or otherwise take action. Implicit consent in generally takes place when a data subject, through inaction, indicates consent. This is a troublesome form of consent as ambiguity exists as to whether the subject was properly informed or even possessed knowledge on the existence of the consent.

In energy consumption data, implicit consent takes place when a data subject has a Meter installed in his home, and this meter's standard setting is to allow energy consumption data to be gathered through P4. In other words, the low-voltage network manager will have consent to remotely read data, unless consent is specifically withdrawn. The practical implementation

[91] Directive 95/46/EC, Art. 7.

[92] Directive 95/46/EC, Art. 2(h).

[93] 29WP, Opinion 15/2011 p.12.

of this is that any data subject may object to data collection, although the default setting is that P4 data is gathered. The action of having a meter installed would be implicit consent to utilize the functionality of P4, which is an unsure ground for consent as the data controller can not prove that the data subject has given consent, he can only assume this to be the case.

Although the Directive only states three requirements for consent, 29WP considers another requirement in its Opinion on the definition of consent regarding informing the data subject.[94] [95] The presented information should be of such a quality, that the data subject can understand it, and the information should be accessible and visible.[96]

In the case of energy consumption data, the data controller should realise that his data subjects come from all walks of life and statistically, the chance is small that the data subject has received training in the legal and technical domains with enough depth and detail to comprehend the full scope of smart metering and the data contained herein. Also, although computers and the Internet are common in households these days, the data controller can not presume that every household has access to online Terms of Service and other sources of information upon which consent is being based. ”For more information, see our website” is thus not enough as a means of information accessibility. Although it stands to reason that anyone who wants to use a web-based HEMS, will have access the Internet and thus be able to access the Terms of Service online.

In conclusion, consent should be given explicitly, freely, for a specific purpose about which the data subject is informed in for him understandable and available terms, or may be implied if the action taken clearly indicates that the data subject agrees.[97] Only in this way can the data controller be sure that indeed consent as a legal basis for data processing is present.

### 4.4.2 (b) To fulfil a contract

The Directive in considers a contract to be legitimate grounds for data processing is *”[this] is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering a contract”*.

Necessity within the smart metering domain depends on which party has a contract with the data subject, and what that contract entails. This is something that will have to be judged on a case-by-case basis examining each contract. If, for instance, a contract entails that the data controller

[94] 29WP, Opinion 15/2011 p.20.

[95] See also Kuner (2007) p.67.

[96] Visibility also includes a large enough font, that is easily legible.

[97] Such as is the case with buying an item online. Through this action, the data subject agrees to having his name and address processed in order to acquire the item, for without it, this would be impossible.

makes available to the subject a visual representation of the data subject's P4 data, this data will have to be processed in order to perform the contract. On the other hand, if the contract only requires the supply of energy and bimonthly billing and a final bill or restitution at the end of the year based on the actual meter reading which the data subject provides once a year, the data controller has no need for P4 data.

A clear example of the need to process personal data is the ordering of an item in an online store. In order to perform the sales contract, the online store will have to process the address of the client, it is "necessary" to do so. *"Data protection authorities interpret this provision strictly, and are not likely to view the processing of data as 'necessary' to perform the contract unless such processing is truly central and unavoidable in order to complete the transaction"*.[98]

The HEMS which are discussed within section five all provide visualizations of energy consumption data and have a need for this information stemming either from P1 or P4 if offering the visualization is part of the contract.

### 4.4.3 (c) Legal obligation

There is a discrepancy here between the capabilities of Meters and the ensuing obligation of energy suppliers to provide accurate billing and consumption feedback which is on par with the facilities offered by the Meter on the one hand, and the consent of the data subject on the other. This discrepancy lies with the interpretation of Directive 2007/72/EC Annex 1.1(i) stating the obligation to "*[energy consumption data] shall be given by using a sufficient time frame, which takes into account the capabilities of customer's metering equipment and the electricity product in question."* This can be interpreted from an inclusive and an exclusive perspective. In the inclusive perspective, any data that the meter is capable of producing should be presented to the customer. In the exclusive perspective, the customer can not hold the energy supplier to the obligation to provide certain data if the meter is not capable of producing this data. Although the exclusive interpretation seems more logical, this issue remains unclear. Examining the Dutch Gas Act, and in particular article 95lb, stipulating that frequency of billing and making available of energy consumption data are designated by order in council.[99] Nevertheless, the energy supplier has the legal obligation to process meter readings for the purpose of billing, although for this purpose, detailed consumption data is not needed.

[98] Kuner (2007) p.244.

[99] Dutch: Algemene Maatregel van Bestuur.

### 4.4.4 (d) Vital interest of the data subject

Vital interest is not a criterion that is part of the processing of energy consumption data concerning the data subject. The processing of energy consumption data is not a matter of life and limb, no lives are at stake.[100] One vital interest is that of the availability of energy and the protection of critical infrastructure to facilitate this availability. Currently, as load balancing is not being done on a wide-spread level, there is no danger to availability or the critical infrastructure as far as the Meter and HEMS are involved. If however, data gathered trough remote metering becomes vital for load balancing, then the vital interest of the data subject will become a criterion. Although load balancing and infrastructure management are of vital interest to the grid operators, they fall outside of the scope of this thesis. This criterion will therefore not be explored further.

### 4.4.5 (e) Public interest

Public interest is not a criterion that is part of the processing of energy consumption data unless in such cases where this data can be processed under governmental authority or under the authority of law enforcement. However, according to article 14(a) of the Directive, the data subject still has the right to object against processing of data under this criterion. Due to the restrictions this criterion will therefore not be explored further.

### 4.4.6 (f) Legitimate interest of the data controller

Also called the f-ground or 'balancing of interests', the legitimate interest of the data controller is often used as a default ground for companies to process personal data, claiming that this is in the legitimate interest of the company as it is it's core business. However, even if this criterion is legitimate, the data controller still has the restriction of only being allowed to process personal data legitimately, and in doing so may not override the fundamental rights and freedoms of the data subject.[101]

In the Smart Metering domain, the core business of the low-voltage network manager is the functioning of that part of the grid for which it is responsible. As is being shown on a daily basis, although there are few Meters from which the network manager receives data, the network is functioning properly. From this the conclusion is drawn that there is no compelling legitimate interest for the network manager to process this data; they are doing quite well without it. However, in order for the Smart Grid to become reality, data processing will be vital in order to fulfil the promises of the Smart Grid.

[100] Directive 2007/72/EC, Annex 1.1(i).

[101] Kuner (2007) p.245.

For the energy supplier, the same holds true. Without Smart Meters and the processing of the personal data, households are still billed for the energy they consume and meter readings are still available, albeit far less frequent than would be the case with remote readings combined with the legitimate processing of P4 data.

The last group of interest are the VAS', who's complete business model revolves around the processing of P4 (and possibly P1) data. For them to be able to do so, they must have access to this information, although typically they will obtain the consent of that data subject, and have a contract with the data subject for which data processing is needed. As such, although the f-ground might still apply, consent and contract will most likely already apply as well.

## 4.5 Data quality principles

In the previous two sections, it has been asserted that energy consumption data is personal data and the grounds for processing have been explored. Given that such data can legally be processed, there are five principles which must be adhered to as stipulated in article 9 of the Data Protection Directive.[102] These principles exist next to the grounds for processing, both articles 6 and 7 of the Directive need to be adhered to when processing personal data. Each of the principles stipulated in article 6 will be explored in detail with regards to the Energy Consumption Data.

### 4.5.1 (a) Fair and lawful processing

Personal data must be *"processed fairly and lawfully"*. Two elements are contained in this principle, which together with article b is also seen as the legitimate purpose principle.[103] In the matter of lawful processing, this is already covered in the grounds section of the legal framework. Personal data processing is only allowed in accordance with the Data protection Directive, and in accordance with article 8 of the European Convention on Human Rights.[104] [105]

Fair processing means that data subjects are informed on what is being processed and why. These two elements combine to form transparency, the data subject is informed what is being processed, why this is being

[102] Directive 95/46/EC, Art. 6(a) through (e).

[103] Kuner (2007) p.90.

[104] Koops & Cuijpers (2009)

[105] Article 8 - Right to respect for private and family life: 1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

processed, and on which legal grounds, such that the data subject can make an informed decision regarding consent if this is applicable or decide whether to enter into a legal relationship with the potential data controller or not based on the available information.

In order for processing to be fair, the data controller will have to be honest and open about his identity, inform the data subject about the intention of the data processing, and process the data only in accordance with those purposes that the data subject can reasonably expect.

Within the domain of energy consumption data, it is reasonable to expect that the data controller uses personal data for billing purposes and grid management such as load balancing and does so only with legitimate grounds. In contrast, customers will not expect that the data controller uses the data to construct profiles which he uses to predict the capability of the data subject to pay his bills on time and will take pre-emptive measures accordingly, although this is possible with the Smart Meters and can be seen as a marketing-related purpose.[106]

### 4.5.2 (b) Purpose specification

Personal data must be *"collected for specified, explicit and legitimate purposes and not further processed in ways incompatible with those purposes."* This principle lies at the basis of data collection and is the *raison d'être* of the processing to take place and is also known as the 'purpose limitation principle'.[107]

Specified purpose entails the purpose being *"sufficiently defined to enable the implementation of any necessary data protection safeguards, and to delimit the scope of the processing operation"*.[108] The would-be data controller will therefore have to know beforehand exactly what his plans are with the data and why this data is needed. The specification is strict in that no data should be collected that is not necessary, adequate or relevant for the purpose. Furthermore, specification *"must be determined at the time of collection of the data"* at the very latest, but preferably prior to collection.[109]

The detail of specification should be great enough to determine the boundary between what processing is and what processing is not performed on the collected data, and to allow legal compliance to be assessed and data protection safeguards to be applied.[110] As examples, "to provide a better user experience" and "for marketing purposes" as specifications of purpose are therefore not detailed enough without further explanation. However,

[106] As mentioned in the Gedragscode Leveranciers Slimme Meter 2012, article 5.3.1.

[107] 29WP, Opinion 03/2013 p.4, and Kuner (2007) p.99.

[108] 29WP, Opinion 03/2013 p.12.

[109] Directive 95/46/EC, Recital 28.

[110] 29WP, Opinion 03/2013 p.15.

this does not mean that a highly detailed, perhaps technical or legal, specification will be sufficient for such explanations can become unreadable for the data subject. On the other hand, a reference to 'commercial purposes' is considered to be inadequate.[111]

Explicit purpose entails the purpose being *"sufficiently unambiguous and clearly expressed"*; it must be *'manifest' (explicit) and specific (concrete).*[112] This explicitness is further reflected in articles 10 and 11 on information and articles 18 to 21 on notification which require that the data subject and the Data Protection Authority are explicitly informed on the specified and legitimate purposes for the processing of personal data.[113]

Legitimate purpose entails the purpose going *"beyond the requirement to have a legal ground for the processing under Article 7 of the Directive and also extends to other areas of Law"*.[114] Thus, not only the Directive is to be adhered to when processing personal data, but the entirety of legal sources should be taken into account, including such domains as contract law, the European Convention on Human Rights and case law.

In smart metering in the Netherlands, purpose limitation is described in the Code of Conduct Smart Meters 2012.[115] Note that this document applies to energy suppliers and companies who process data wherein the energy suppliers are the data controllers; it does not apply to VAS, as these are not suppliers.[116] However, since the Code of Conduct is an interpretation of the WBP, which in turn is the transposition of the Data Protection Directive into national law, VAS' will have to abide by the WBP. And as the Code of Conduct is an interpretation with regards to the specific field in which the VAS' operate, there is no reason why they should not comply with this code, as in doing so they will most likely abide by the WBP.[117]

The Code of Conduct is recognized by the CBP as a correct interpretation of the WBP and other legal acts concerning the processing of personal data.[118] It describes the purposes for processing of personal data within the context of Smart Metering in article five. These purposes are:

1. Standard regime

2. Other services

[111] Kotschy (2010) p.52.

[112] 29WP Opinion 03/2013, Kotschy (2010) p.51.

[113] Directive 95/46/EC, Art. 10, 11, 18 through 21.

[114] Directive 95/46/EC, Art. 7.

[115] Gedragscode Leveranciers Slimme Meters (2012).

[116] Although a supplier may act as a VAS as well, in which case he will still have to comply to the Code of Conduct.

[117] Although in cases of doubt, the WBP is the primary legal source and the Code of Conduct an interpretation of this act.

[118] *"het College bescherming persoonsgegevens, [...] Is voornemens te verklaren: Dat de Gedragscode, gelet op de bijzondere kenmerken van de sctor, een juiste uitwerking vormt van de Wbp en andere wettelijke bepalingen betreffende de verwerking van persoonsgegevens."* Staatscourant, 23 November 2012, Nr. 23975.

3. Marketing related purposes
4. Internal administrative purposes
5. Processing of interval readings

The Standard Regime consists of purposes such as billing and taking readings in case of contract termination or switching of suppliers. The Other Services consists of such purposes as advising on savings and production, variable tariff systems and answering client questions. For these Other Services, grounds must be present as described in article 3.4.1 of this Code of Conduct, which are interpretations of article 8 of the WBP, regarding legal grounds for data processing. The marketing related purposes are limited to the own services of the supplier, and may only use the data for marketing services other than his own in the case of unambiguous consent. The Internal administrative purpose is limiting in that the supplier is not allowed to process personal data for these purposes unless this purpose can not be served with the processing of non-personal data. Last, the Processing of interval readings is only allowed with the unambiguous consent of the data subject.[119]

### 4.5.3 (c) Adequate, relevant and not excessive

Personal data must be *"adequate, relevant and not excessive in relation to the purpose for which they are collected and/or further processed"*. This is also known as the 'minimization' or 'proportionality' principle and entails that no more data must be collected than that which satisfies the purpose of collection, or in other words, no more than the minimal amount of information may be processed.

Adequacy here, means that the amount of data collected should be allowed to be large enough to make it possible to fulfil the purpose for which this data is collected as specified according to article 6.b of the Directive as mentioned in the previous section.

Relevancy of this collected information means that the data collected must be directly related to the purpose of collection. It should be noted that this relevancy is limited in that if it is possible to fulfil the purpose without the processing of personal data (by processing non-personal data for instance) this must be done although the personal data might be is relevant to the purpose. If the possibility exists of applying a different method to fulfil the purpose that does not involve the processing of personal data, this method should take precedence.

[119] Typically this will be P4 data, unless the supplier presents the data subject with a P1 device, or the data subject sends the supplier the P1 data through other means.

Not excessive here means that the amount of data collected is kept at a minimum needed to fulfil the purpose. This is the balancing act with adequacy, as there should be enough data collected, but no more than that.

A clear example in the Smart Grid is that of load balancing, which is one of the hoped benefits. Although real-time readings of meters directly would facilitate load balancing, this can also be done without the need for personal data, but rather with aggregated data collected on a neighbourhood level.[120]

### 4.5.4 (d) Accurate and up to date

Personal data must be *"accurate, and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purpose for which they are collected or for which they are further processed, are erased or rectified."*

As personal data relates to a person and is often processed in order to provide this person with a service, accordingly it is in the best interest of the processor and the data subject that this information is up to date and accurate insofar any decisions made using this information will influence the data subject, such as the choice to restrict electricity throughput in the meter because of (false) information on unpaid bills.

Accuracy of the data means that collected personal data corresponds to the factual status of the data subject. Up to date depends on the purpose of the data collection, in the case of age and judgement on if a person is a minor or has a certain other age, this data needs regular correction. Data such as name of biological parents typically does not need to be corrected. Accordingly, if data is accurate and current, depends on the purpose for which it is collected.

Again, for billing purposes, if information is outdated or inaccurate, bills will not reflect the exact amount of energy consumption, or in case of a few very sunny days, the amount of electricity pushed back to the grid. Furthermore, if household number 38 has PV-cells on their roof and pushing electricity back to the grid, indeed household number 38 should receive the benefits, and not household 83, who has no PV-cells.

### 4.5.5 (e) Limiting identification

Personal data must be *" kept in a form which permits identification of data subjects no longer than is necessary for the purpose for which they are further processed."* This principle entails that as soon as personal data has served its purpose, it should be anonymized such that it is no longer possible to determine the identity of the data subject, effectively turning the personal data into non-personal data that accordingly is no longer bound by the Data Protection Directive. However, it should be noted that anonymization of the

[120] Kursawe et al. (2011).

data itself does not automatically mean that it no longer relates to an identifiable natural person, because it is possible to combine this anonymous data with other data to produce a larger dataset that allows for re-identification of the data subject.

### 4.6 Transparency

After exploring the two principles of grounds and data quality, the third principle to be explored is that of transparency. This is the obligation of the data controller to inform the data subject on the processing of his data.[121] According to the Directive at the very least *"The controller or his representative must provide a data subject [...] with at least the following information:*
*(a)The identity of the controller and his representative if any;*
*(b)The purpose of the processing for which the data are intended;*[122]
If needed to guarantee fair processing, the data controller also has to provide further information.[123] *"Because of the obligations of the data controller, the data subject knows about his/her personal data, who has stored it, who will process it and for what purpose(s)"*.[124]

In the case of HEMS, this entails that the data subject is informed on the identity of the data controller, and of the data processor(s) if any, and on the purpose of processing such as described in the Code of Conduct.[125]

The processing of energy consumption data is not always transparent, although the act of processing itself and the visualisation of this data clearly indicates that consumption data is being processed. The problem lies with who the controller and processor are, which is not always communicated to the data subject as will be seen in chapter five. Furthermore, informing may be vague, such as statements on purpose being 'for marketing', which does not let the data subject know what the actual purpose is other than that the controller will be using data to make money in some form. The last issue with transparency is that there is no stipulated location where this informing should take place. The result is identity and purpose being buried inside Terms of Service and Privacy Statements that are not always easily located on the website of the HEMS supplier as also will be seen in chapter five. In conclusion, although informing the data subject is an obligation of the data controller, there is a lack of detail as to how the data subject should be informed.

[121] 29WP, Opinion 1/2008 p.22.
[122] Directive 95/46/EC, Art. 10(a) and (b).
[123] Ibidem. Art. 10(c).
[124] Schnabel (2009) p.562.
[125] Gedragdcode Leveranciers Slimme Meter 2012, Art. 5.

## 4.7 Prior informed consent

According to article 5.3 of the ePrivacy Directive, storage of or access to information stored in the terminal equipment of a subscriber or user is only allowed *"on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing"*.[126] However, an exception is made for *"any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user"*[127]

The data subject still has to give his consent, as *"Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website."*[128] Note the use of the phrases 'freely given' and 'informed' which can also be found in the definition of consent in the Data Protection Directive.[129] This signifies that consent has to be given prior to the starting of data processing.[130] This also signifies that consent should be 'informed', thus referring back to the transparency principle. The exception that is described entails that the 'subscriber or user' has specifically requested a certain service.

However, when requesting this service, the subscriber or user will have given his consent as seen in article 6.3 of the ePrivacy Directive stating that *"For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data[...] if the subscriber or user to whom the data relate has given his/her consent"*.[131] This entails that consent is needed, but also that it 'has [been] given', indicating the timing of consent to be prior to processing. Combining this with the transparency principle, the data subject should be provided with 'clear and comprehensive information', prior to giving consent, which results in prior informed consent.

Within the scope of HEMS, it therefore makes good sense to inform users on the identity of the controller and the purpose of processing (transparency) *prior* to obtaining consent from the user to process information. This also entails that consent will often be the legal ground upon which personal data processing is legitimised.[132]

[126] Directive 2002/58/EC, Art. 5.3.

[127] Ibidem.

[128] Directive 2002/58/EC, Recital 17.

[129] Directive 95/46/EC, Art. 2(h).

[130] As also stated by the 29WP in Opinion 15/2011 p.31.

[131] Directive 2002/58/EC, Art. 6.3.

[132] As also stated by the 29WP in Opinion 2/2010 p.10.

## 4.8 Data security goals

Throughout the digital security literature, an acronym is used to indicate the three high level security requirements: CIA, which stands for Confidentiality, Integrity, and Availability.[133] These are however, not the only requirements of data security that should be kept in mind; there are two more; Authenticity and Non-repudiation. In this section, these five security requirements and how they are involved in HEMS.

In the proposed General Data Protection Regulation currently being a work in progress, entry in to force of which is expected in 2016, articles are included that will make is mandatory to notify the supervising authority and the data subject in case a personal data breach has taken place.[134] Under current legislation, the data controller has no such obligation.

### 4.8.1 Confidentiality

Confidentiality is defined as *”an obligation to protect some other person’s or organization’s secrets if you know them”*.[135] This means that unauthorized access is not possible and eavesdropping is unsuccessful; the data should be kept secret from parties who do not have the legitimate right to access this information. Confidentiality in general is obtained using encryption, such that, only those allowed access to the information, hold a special key used to disclose (decrypt) the obfuscated (encrypted) information.

This way, unless one obtains the key, the cyphertext can be obtained, but decryption to obtain the plaintext is infeasible. It should be mentioned that there is only one perfectly secure cryptographic protocol, the one-time pad, and this is only secure when used properly.[136] Perfectly secure entails that even against adversaries with infinite computational power the plaintext can not be retrieved. All other protocols are only secure in that it takes a very large amount of computational power and a lot of time to decrypt without having the key. In practice, cryptographers rely on this computational complexity to design cryptographic protocols that take millions of years to bruteforce using more computers than there are atoms in the universe. This is however, based on current technology and as technological capabilities increase, so does the speed at which bruteforce attacks are able to successfully attack a cyphertext.

A cryptographic protocol is considered broken when a method has been found that allows for decryption in fewer attempts than is needed with a bruteforce attack. Because of the increase in computational power or the discovery of a weakness, what was once considered secure (Such as the DES

[133] Anderson (2008), Metke & Ekl (2010), Khurana et al. (2010).

[134] Proposed GDPR, Art. 31 and 32.

[135] Anderson (2008) p.13.

[136] Kahn (1967), pp.398-400.

encryption protocol[137].) is now no longer secure as devices can outlast cryptographic tools' lifetimes.[138] However, just because a protocol is broken does not mean it is insecure in practice. For example, although methods have been identified on AES-128[139] which are faster than bruteforce, these methods are still impractical. Although they reduce the time and computational power needed, it still takes millions of years and a huge number of computers.[140] Although keys might be compromised, that is, become available to a party that should not hold this key, this does not mean that a cyphertext can always be decrypted. Not only the key needs to be known, but also how to use it.

With energy consumption data, confidentiality is obtained when only those parties that have a lawful reason to process the data are actually capable of doing so, or in more technical terms; have access the plaintext data. Only the data subject himself should be able to access his consumption data on a HEMS web portal, and should not be able to have access to consumption data of his neighbour. Also, the neighbour should not be able to listen in on the communication the HEMS has with the Smart Meter, or if listening in is possible, only encrypted data should be obtainable, keeping the secret protected.

### 4.8.2 Integrity

Integrity is about the verification of data, such that accidental or malicious changes are prevented, yet if changes do take place for whatever reason, they do not go unnoticed. To enforce integrity, some form of check should be in place to ensure that any loss of integrity is noticed. This can be done by keeping data in different locations and looking for differences that occur.

In computer systems, integrity can be protected using hashes or signatures. Hashes are one-way functions that produce fixed-length outputs. These outputs will differ widely even if the input is only slightly altered. This is easiest to explain via an example, using the SHA1 hashing function.

```
'hello' --SHA1--> f572d396fae9206628714fb2ce00f72e94f2258f
'Hello' --SHA1--> 1d229271928d3f9e2bb0375bd6ce5db6c6d348d9
```

As can be seen, the input of the function differs only in the case of the first character, yet the output is very different. If the same input is run through the function again, the same hash is outputted. A hash function

[137] Van De Zande (2001)

[138] Khurana et al. (2010).

[139] AES-128 or Advanced Encryption Standard with 128 bits key is an encryption algorithm.

[140] Bogdanov et al. (2011) for instance.

can be applied to data of any size, and yields a unique hash.[141] Given that the output stays the same if the input stays the same, any alteration will be noticeable, preventing accidental changes in the data from going unnoticed.

However, given that SHA1[142] is available to everyone, someone with malicious intent could alter data, recompute the hash function and replace this hash as well. To solve this issue of malicious changes, digital signatures can be used.

Signatures can be compared to hash functions in that the output is unique. The digital signature schema consists of three algorithms.

- A key generator that can create public/private key pairs
- A signing algorithm
- A signature verification algorithm

To use signatures, a public/private key pair must be generated. The public key is distributed to those who need to verify signatures, along with a statement about who generated this key, such that anyone verifying the signature can verify that the one who signed the data is the holder of the private key. The private key is kept in a safe place.

Inputting the private key and the data into the signing algorithm yields a signature, much like a hash. This hash, along with the data is then sent to the party needing this data. Because the private key is needed to generate the signature, if the data is altered in transit this will be noticed.[143]

With the public key, the data, and the signature, the verification algorithm can verify or reject the claim to authenticity. If the signature and the data do not match, integrity and authenticity can not be confirmed.

This schema also works the other way round. Using the public key, anyone can encrypt data, but only the holder of the private key can now decrypt the data. This ensures that messages intended for the holder of the private key, are kept confidential. This can also be used to create a signature, and send both the encrypted data and the plaintext data to the holder of the private key, who can then check the integrity of the plaintext against the signature.

In energy consumption data, if no integrity checks are in place it might be possible to alter actual consumption data in order to increase or decrease consumption amounts without this being noticed. This is clearly not in the best interest of the consumer or the supplier.

Integrity works together with confidentiality in that if a party can not alter the plaintext and only has access to the cyphertext, they might be

[141] The SHA1 hash is 160 bits long, and usually expressed in forty alphanumericals. There are thus $2^160$ possible hashes. A finite set of hashes will eventually cause two different inputs to collide onto the same output HASH.

[142] And other hash functions such as MD5, SHA3, and GOST.

[143] Assuming that the private key is secure and not compromised.

able to alter the cyphertext, but have no idea what the effect would be on the plaintext. This might result in a successful alteration that changes the plaintext into something that would slip past the checks, but it is more likely that a change in the cyphertext will result in something that makes no sense at all when decrypted.

### 4.8.3 Availability

Availability means that the data and the system resources are available (ready to use) when needed, to those parties which are authorized. In terms of system security, availability of the system is related (in terms of security) with preventing DoS[144] attacks in general.

In energy consumption data, the data on the Smart Meter should be available to the low-voltage network manager for the purpose of remote metering if they have such an agreement with the data subject. The same goes for the availability of this data to the energy supplier for billing purposes. For this to be possible, the means of access should not be disrupted, intentionally or accidentally. From the data subject's perspective, if he utilizes a HEMS, he should have the data available to gain insight in his energy consumption such as is gathered by the HEMS.

### 4.8.4 Authenticity

Authenticity means that you believe that the data that you received came from a genuine and authorized source, and you can actually verify that. *"In the academic literature on security protocols, authenticity means integrity plus freshness: you have established that you are speaking to a genuine principal, not a replay of previous messages."*[145]

Authenticity is typically achieved using cryptographic keys such as described with the digital signatures. Certificates are used to bind keys to identities and makes key management simpler as keys themselves do not contain identities.

For certificates to work, the Certificate Authority (CA) needs to be trusted, or the CA that signed the certificate of the CA needs to be trusted in what is called a chain of trust. Following this chain one works one's way up to root CA's, who signed their own certificate rather than having another CA sign it.[146] The public key of the root CA is publicly known.

[144] DoS or Denial of Service is a type of attack on a system that causes this system to become unavailable, for instance by making this system use all its resources. A variation on this is DDoS, where the first 'D' stands for distributed. In this, the attack does not come from a single source but distributed across various sources.

[145] Anderson (2008) p.14.

[146] Symantec Group, Comodo, Go Daddy Group, and GlobalSign are the largest CA's in the world and function as Root CA for the majority of SSL certifications.

CA's work by issuing certificates to parties after these parties have positively identified themselves towards the CA, which entails personally identifying oneself by means of a legal identification document such as a passport, stating the purpose of the certificate, and paying a large sum of money. In such a certificate it is stated who the CA is, who they issued the certificate to, when it was issued, and when it expires, along with digital signatures to check the integrity of the certificate.

In simplified terms, when a browser attempts to connect to websites that are secured with SSL (Secure Socket Layer) certificates: 1) The browser asks the webserver to identify itself. 2) The webserver responds with sending a copy of its SSL certificate. 3) The browser checks this certificate with its internal list of trusted CA's and if the digital signature is correct, and sends a message to the webserver if the checks are true. 4) The webserver responds with a signed acknowledgement (using the key in its certificate) to start the SSL encrypted session. 5) Further communication during this session between the browser and webserver is now encrypted.

This encryption is done using symmetric cryptography using a symmetric session key that is agreed upon between the browser and webserver and AES encryption is used to encrypt the further communications. SSL is considered to be secure although cracks are slowly starting to appear in this twenty year old protocol.[147]

### 4.8.5 Non-repudiation

The last security goal is that of non-repudiation meaning that an action can not be denied; if a party undertakes an action it can not, at a later moment in time, deny that it undertook this action, because this action has been logged in some way. Typical use cases are accessing, altering, removing or copying data. For non-repudiation to work, the authenticity of the acting party must be unquestionable, integrity of the associated data must be maintained, and freshness of the action must be confirmed. Freshness entails that an action took place at a certain time (or within a certain limited time-frame) and is not a replay of a previous event or something that happened outside of the limited time-frame.

In energy consumption data, the act of consuming energy is something which should be subject to non-repudiation, as is the act of signing a contract and consenting to data processing. If a consumer could successfully (yet falsely) deny having consumed energy or having signed a contract, the entire relationship between supplier and customer would be jeopardised. A supplier would never be sure as to what amount of energy would have been consumed or that indeed a contract would have been signed for the supply of this energy and the remote metering of consumption. With respects to freshness, billing

[147] Metke & Ekl (2010).

for energy consumption should be based on the energy consumption data within the time-frame of the bill, and not about the same time-frame a year ago. Non-repudiation is also important in consent, as a data subject should not be able to repudiate having given his consent to data processing.

## 4.9 Deriving legislative requirements

Within the Smart Metering system, the HEMS play a key role. According to Directive 2012/148/EU, Recital 3.a: *"Smart Metering system' means an electronic system that can measure energy consumption, adding more information than a conventional meter, and can transmit and receive data using a form of electronic communication."* and according to legislation, customers should be properly informed on this energy consumption information.[148] Meters by themselves however offer very limited information on energy consumption, that is, although they store it internally, this data is not accessible by consumers without the use of further technology. Although one of the popular meters (Kampstrup type 162 J NTA) does have a small display, the information it displays is limited to current consumption in the low or high tariff, and the current production in low or high tariff[149], which by no means can compare to the data that the meter can actually provide through its ports.

For a better exploitation of the advantages such meters provide, an efficient local interface is needed if the consumer is to interact in real-time based on data on actual time of use. However, given that meters tend to reside in basements or other non-frequented areas of the home and the display on the meter itself is too small, it will not suffice and so an external display can be deemed mandatory.[150] The mandatory nature of this display can also be derived from legislation for without such a display it is quite impossible to achieve the requirements as stipulated, and as such, this display is an essential part of the Smart Metering architecture.[151] This external display can take on two basic forms, either an actual physical display within the household (IHD) or a web-based application.[152]

Currently, no Smart Meter in the Netherlands is equipped with a standalone physical display by default, the only method of accessing P1 data is through building your own device, or by opting for one of the few commercially available solutions that are being offered. The less granular P4 data can be accessed through web portals that VAS make available.

A last but important legal requirement has to do with the processing

[148] Directive 2009/72/EC, Annex 1.1(i).

[149] Manual for Kamstrup Smart Meter type 162 J NTA of 382 J NTA, p.1, as supplied with demo meter received from Kamstrup in June 2013.

[150] Benzi et al. (2011).

[151] Directive 2009/72/EC Annex 1.1(i).

[152] Darby (2006).

of personal data within the Dutch borders. According to Article 27(1) of the Dutch Data Protection Act *"the fully or partly automated processing of personal data intended to serve a single purpose or different related purposes, must be notified to the Data Protection Commission (Commissie Bescherming Persoonsgegevens, CBP) or the officer before the processing is started."*[153]

Concluding this chapter, the following requirements can be distilled from the legal framework concerning personal data, legal grounds for processing, and the minimal requirements making energy consumption data available to the end-users. Energy suppliers are required to:

1. have grounds upon which data processing is legitimised;[154]
2. process personal data only for a specified purpose;[155]
3. notify the data subject on this data processing, in for the data subject understandable language;[156]
4. notify the CBP on the intent to process data;[157]
5. make detailed consumption data available to the data subject, in an understandable format and in a timely manner, as to facilitate self-regulation by the data subject;[158]
6. present such data free of charge;[159]
7. implement appropriate technical and organizational measures to protect this personal data.[160]

[153] Unofficial translation from the Dutch legal source: *Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens.*

[154] As described in Directive 95/46/EC Art. 7 and detailed in section 4.4 of this thesis, and as described in WBP, Art 8.

[155] Such as stipulated in the "Gedragscode Leveranciers Slimme Meters 2012" (Code of conduct Smart Meter suppliers), being accepted by the CBP as an accurate interpretation of the Dutch Data Protection Act towards this specific sector (Staatscourant 23 November 2012, Nr. 23975), and in Directive 95/46/EC art. 6(a) and (b) with regards to a specified, explicit and legitimate purpose, adequate, relevant and non-excessive (purpose limitation and data minimization).

[156] This includes the identity of the controller, the purpose of processing, what data is being collected, and the existence of the right to access and rectification as stipulated in Directive 95/46/EC, Art. 10. and WBP, Art. 33, and WBP, Art. 7 concerning the explicit description of purpose.

[157] Directive 95/46/EC Art. 18 and 19, and WBP, Art. 27 and 28 concerning the obligation of notification and the contents of notification.

[158] As stated in Directive 2007/72/EC, Annex 1.1(i).

[159] As stated in Directive 2007/72/EC, Annex 1.1(i): *"No additional costs shall be charged to the consumer for that service"*.

[160] *"[Protection against] accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involved the transmis-*

In the case of VAS, less requirements are described as they do not have the obligations regarding the making available of consumption data. VAS process personal data and are bound by contract with the customer to provide certain services. These services do not include the mandatory availability of consumption data in a timely manner, with a level of detail corresponding to the capabilities of the Smart Meter, nor do they need to be free of charge.

However, all the other requirements mentioned above do still hold true. Of particular interest concerning VAS, is the way they generate revenue and how personal data is involved in this. As their primary source of income is likely the processing of energy consumption data or selling devices that facilitate this processing, the broader the scope of processing, the more opportunities arise to generate revenue such as through profiling and offering targeted services according to these profiles.

*sion of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risk represented by the processing and the nature of the data to be protected."* as stipulated by Directive 95/46/EC, Art. 17.1, and as stipulated in WBP, Art. 13.

# 5 Current home energy management systems

Having concluded the legal framework, having formulated requirements based on this framework, and having explained the basic goals of data security and vulnerabilities of the data types, five current HEMS are examined within this chapter to see what they do, which data are processed, and how end-users are informed.

For each device, the following questions will be answered:

1. What is 'in the box', or what does the consumer get for his money?
2. Where and how does the data flow? This includes the protocols used.
3. Do the Terms of Service and/or Privacy Statement contain oddities?
4. Is it made clear what data is being collected and for what purpose?
5. Is our data safe? Or, can the neighbour capture our energy consumption data?
6. Does this HEMS comply with the legal requirements as identified?

## 5.1 Toon

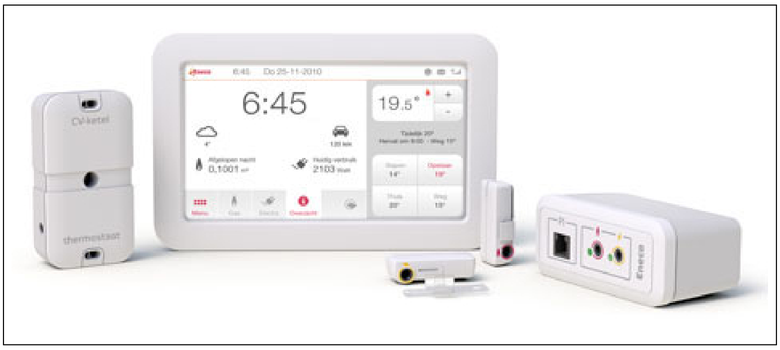


Figure 3: The Toon HEMS. From left to right: the central heating module (not discussed in this thesis), the IHD, the two sensors for gas and electricity meters, and the gateway.

Toon is an IHD developed by Quby and marketed by Eneco. The complete system consists of the IHD, a wireless module near the meter that collects the energy consumption data, two sensors and a central heating module. Toon costs 120 euro's with a further 75 euro's in installation costs, although installation is given for free, and Toon itself is free with a new contract. A further 3.50 euro's is billed monthly as a subscription fee, regardless if Toon itself was free or not. Subscriptions can be cancelled after one year, at which point the system will still function as a display for energy consumption data, but the extra functions will no longer work and software updates will no longer be available.

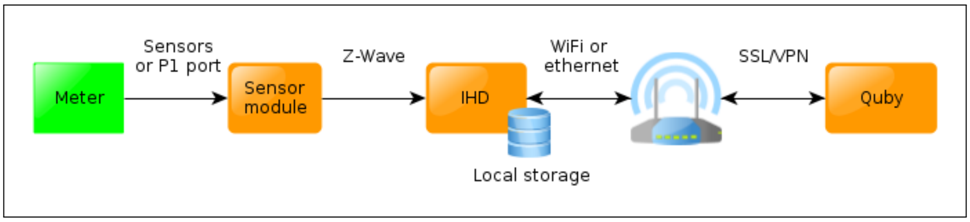


Figure 4: Dataflow within the Toon HEMS.

In case a Smart Meter is present in the household, simply connecting to the P1 port is enough to provide electricity consumption data. If no Smart Meter is present, consumption data can still be gathered by using two optical sensors that 'look' at the spinning disk or blinking light in non-smart electricity meters and the rotating last digit of the gas meter. The drawback of these optical sensors is that they can not distinguish between forward and backward spinning, registering both as consumption and thus skewing the results for those households which are producing energy through photovoltaic cells (PV-cells) and supplying this back to the grid. A backwards spinning disk is possible when the PV-cells are actually producing more energy than the household is consuming.

Lastly, there is also the option to use 'Toon op afstand' (Toon from a distance), with which one can view energy consumption data as read by Toon, but from a location other than the own home. With 'Toon op afstand', P1 data is accessible.

### 5.1.1 The Z-Wave protocol

Toon uses the Z-Wave protocol to communicate between the IHD and the module next to the Smart Meter. Z-Wave is proprietary wireless communication protocol aimed at the residential control and automation market. This proprietary nature is its downfall, implementation is limited to those who are willing to do so down to the level of detail dictated by the Z-Wave alliance.[161]

In order to set up an initial connection between this module and the IHD, they have to be within short range of each other, some sixty centimetres at most, due to low power communications during the initiation process. Although short is a relative term here as near-field communication typically takes place within a decimetre, compared to the communication distance between two nodes that can be more than thirty meters, sixty centimetres is short range.[162] The devices 'whisper' as it where whilst pairing, to prevent

[161] Galeev (2006).

[162] Ibidem.

eavesdropping. In this pairing, the controller gives its unique identifier to the slave, an identifier which is used throughout the network. This identifier is essential in all further communications and only those devices that know this identifier are able to communicate within the network. Each controller contains this unique identifier hard-coded within the Z-Wave chip, and so it can not be altered if compromised. All devices that want to join an existing Z-Wave network will have to go through the initial connection procedure with the controller. This is another drawback of the Z-Wave protocol, as each new device will have to communicate with this controller within short range, which is problematic in larger networks or when the controller is connected to a computer as controller and new node will have to be physically brought together.

Once a connection has been established, broadcasting with normal power settings are made, and the IHD can be placed within the network at any location as long as at least one other node of the network is within range as the Z-Wave network has a mesh topology.

At this moment, there are four different generations of the Z-Wave chip. The first (100) generation chip has the possibility to encrypt the broadcasting messages using DES encryption. The second and third generation do not have encryption possibilities as according to the manufacturer, clients rarely if ever used this encryption functionality.[163] Thus *"in [this] specification, Z-Wave no longer has security"*.[164] The fourth generation does implement encryption again, using AES-128 encryption, however, this chip is one-time programmable, limiting its application.

Due to the one-time programmable restriction of the fourth generation, Quby opted to use the third generation or 300 chip in the Toon HEMS.[165]

As can be seen in Figure 5, the Transport frame contains the Home ID, which is actually the unique identifier that is used to verify that a node is part of the network. With the implementation of the 300 chip in the Toon HEMS, this entails that the unique identifier is being broadcast as part of every frame, thus eavesdropping this identifier is possible, along with all the other content of each frame.[166]

### 5.1.2 Connecting to the Internet

Toon offers various services that need information gathered from servers outside of the HAN. Also, the software of Toon frequently gets an update as it matures. For these things to happen, Toon needs an Internet connection and so the IHD contains both a WiFi module and an ethernet port. For most

[163] Knight (2006).

[164] Ibidem.

[165] Expressed during a telephone call with the CTO of Quby, Arjen Noorbergen, on June 28 2013.

[166] Knight (2006).

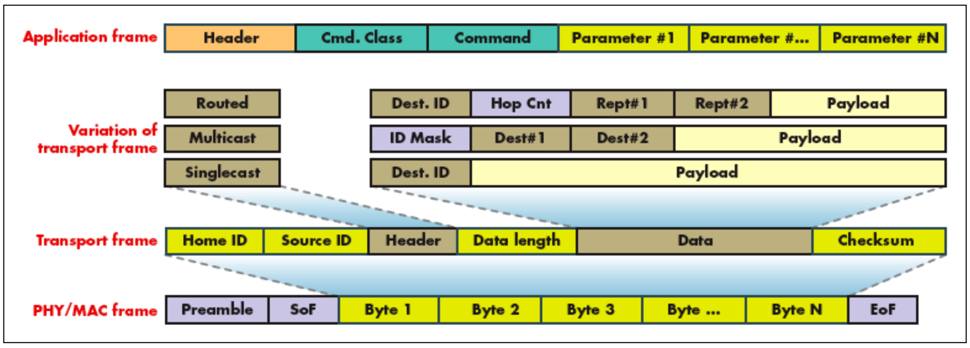


Figure 5: The Z-Wave protocol frame structure. Each PHY/MAC frame starts with a synchronization preamble, followed by a Start of File (SoF), the payload data in N bytes, and ends with an End of File (EoF). The maximum payload is 64 bytes. Payload data is preceded by a frame header containing Home ID, Source ID, frame type, and length of the data. Verification is done using a checksum byte after the payload. (Galeev, 2006)

households, there will be no ethernet cable going to their current thermostat, and so either a cable will have to be run to this point, or Toon will have to use its wireless capabilities.

The purpose of this connection is mainly one-way, software updates are sent, as well as specific contract information such as tariffs and estimated consumption figures based on previous consumption figures as gathered for billing purposes. This extra information allows for the expression of consumption data not in kilowatt hours, which means little to most people, but rather in euro's. Further services are a weather application and traffic information, the weather application in particular is very popular according to Quby.

Communications between the Eneco servers and Toon all goes via Quby, who use SSL (digital certificates) and VPN to protect these communication lines, and are considered to be secure.[167]

In case the 'Toon op afstand' app is used, a username/password combination is used together with a HTTPS connection with Quby. Quby checks the username/password with an Eneco database which returns a contract number if the check is successful. The Quby webserver then requests the Toon belonging to this username/contract to forward its P1 data via an SSL connection towards the app. Both the Quby and Eneco servers are secured using digital certificates to authenticate them towards each other.[168]

[167] Metke & Ekl (2010).

[168] Expressed in e-mail communication with the CTO of Quby, Arjen Noorbergen, on August 9 2013.

### 5.1.3 Storage on the In-home Display

The IHD of the Toon HEMS contains a 128MB flash memory, upon which information is stored next to the operating system. With the operating system in place, some 64MB is left to store data. Data storage is accomplished through a round robin style implementation such that old data is overwritten in time. There are three rounds to this implementation, data with a granularity of ten seconds is stored for a week, data with a granularity of five minutes is stored for a month, and then there is the last round of storage with a granularity of one hour, which is stored for five years. This gives a total of 60480 10-second readings, 8760 5-minute readings and 438000 1-hour readings for a total of 113040 possible data points, entailing that each datapoint is roughly 0.5kB or 512B in size when taking into account the available storage space. A sample telegram taken from a Kamstrup meter made into a file within the Linux operating system turns out to be 435B.[169] With compression techniques and removal of the non-essential data in a telegram such as unused references, overall size on the flash memory can be further reduced, allowing room for future expansion of the functionalities of the Toon system. The data stored on Toon can be removed using a factory reset, something which the end-user can do himself. As part of policy, neither Eneco nor Quby access the data which is stored on Toon, although there are is no technical measure in place which absolutely prevents this from occurring.[170]

### 5.1.4 Terms of Service and Privacy Statement

Terms of Service (ToS, Dutch: Algemene Voorwaarden) are available on the website of Eneco, although not easily findable. Once found, it turns out that the ToS of Toon date back to May 2012. Accessibility is made difficult not only in finding this document, but also in reading it for it is very fine print and in 'legalese', not something the regular customer would, or could manage. No particularly strange statements were found in the ToS.

The Privacy Statement concerning Eneco can be found on their website, a link in the footer of their homepage providing direct access.[171] The statement is available both in Dutch and in English, and is not in 'legalese'. What becomes clear immediately is that with the sentence *"Eneco reserves*

[169] Filesize was determined by writing the single telegram as seen in section 3.1, taken from a demo Kamstrup meter to file via the command line interface of a Linux distribution and examining its size using the ls command. Depending on the number of references in a telegram, the size may vary however. In the P1 companion standard on pages 17 and 18, a telegram is listed that contains 36 references, resulting in a telegram of far greater size.

[170] Expressed during a telephone call with the CTO of Quby, Arjen Noorbergen, on June 28 2013.

[171] Toon Privacy Statement: https://thuis.eneco.nl/privacystatement/.

*the right to change the Privacy Statement"* at the end of the page, and the absence of a version number or date of last change, the reader can never be sure if this page is the same page as he might have read yesterday. To solve this problem, Eneco mentions in their Privacy Statement that if the statement is 'significantly changed', this will be mentioned on their website, and the date of the most recent change will be mentioned at the bottom of the statement itself. However, although the version number of the statement (ie, '052012 91') does hint at the last change being made in May of 2012, causing this statement to be iteration number 91, there is no mention on the actual meaning of the version number. Also, there is no mention of the most recent change date at the bottom of the statement as there should be according to Eneco. Although not explicitly mentioned, Eneco has informed the CBP on the intent to process personal data, which can be found in the CBP's public registry with number 1397543.[172]

A concerning statement is that it is demanded that in case the consumer has a Smart Meter, this meter is activated on 'Mijn Eneco' such that Eneco can send energy consumption data from the low-voltage network manager to Toon. [173]

The Privacy Statement includes a section on what personal data will be processed by Eneco, which includes name and address, product data and contract data. The purpose of this processing is stated to be for the processing of sales, to deliver the Toon services, and for billing and support purposes. Eneco states it may also be processing data for marketing purposes, although it is unclear what this purpose entails exactly. The Privacy Statement also include a section on what data will *not* be processed. This is data on the Internet connection itself, settings concerning temperatures, and energy consumption data which was been collected by Toon.

### 5.1.5 Data security

As shown in Figure 3, communication between the sensor module and the IHD is accomplished using the Z-Wave protocol. In the section on this protocol it has already been stated that Toon implements the third generation Z-Wave chip, which entails data packets being transmitted in plaintext. Confidentiality is not assured within these transmissions. As the IHD stores energy consumption data locally and does not transmit this data to Quby, the wireless connection that is typically used between the IHD and the home router will not be used to pass along energy consumption data. Accordingly,

[172] https://www.collegebeschermingpersoonsgegevens.nl/asp/ORDetail.asp?moid=8088898d80, last referenced July 27 2013.

[173] *In case you have a Smart Meter, the activation of your Smart Meter on Mijn Eneco is mandatory. Eneco then transmits the energy consumption data from your low-voltage network manager to Toon." Translation from Dutch by the author.* Privacy statement Toon by Eneco, version 052012 91.

although such a WiFi connection can be sniffed, confidentiality remains intact. Lastly, the communications that do occur between Quby and the home router (and through that towards the IHD) are set up using VPN and SSL and is thus considered to be confidential.

Looking at authenticity, within each first packet of a set in the Z-Wave protocol, the shared network key can be found, which is the unique identification code as set by the network controller and distributed in the inclusion process of each new node. This key is used as part of the authentication process, and any device holding this key can communicate with the network. Thus, if this key is obtained, packets can be injected into the network. Authenticity is thus debatable, as replay attacks are possible.[174]

Z-Wave does not operate on the frequencies that for instance WiFi and bluetooth use (around 2.4 GHz) but broadcasts in the 900 MHz range.[175] This means that anyone wanting to eavesdrop on Z-Wave communications will need dedicated hardware capable of listening in on this frequency range.

Regarding data integrity, energy consumption data is only stored on the Toon IHD itself. Z-Wave transmissions from the sensor module towards the IHD can be altered however, as they are in plaintext, thus adding unauthentic data to the data stored on the IHD and compromising integrity. A factory reset will remove all the stored data, however, it is unknown if a reset can also be performed remotely. It is also unknown if the stored data can be altered. Either way, this will only result in the loss of integrity of data used to visualize consumption, it does not influence billing, but will probably go unnoticed if alterations are done subtly.

Data availability in Toon is independent of the servers of Quby and only relies on the IHD itself for historical data, and the sensor module connected to the meter for real-time data. A factory reset would make data stored on Toon permanently unavailable, and a powerful jamming signal in the same frequency range as Z-Wave might be able to disrupt availability of real-time data. These two disruption possibilities are hypothetical however, and would need further exploration to see if indeed it would be possible for an attacker to perform these operations without having physical access to the HEMS.

Non-repudiation is of little interest in the Toon HEMS, as the data subject contacts Eneco with the request for the placement of the Toon HEMS and accepts the ToS as part of becoming a consumer of this HEMS service by Eneco. From the combined act of ordering Toon, having it installed, and making use of its services, it can be assumed that the data subject can not repudiate the acceptance of the ToS.

[174] Knight (2006).

[175] Gungor et al. (2011).

### 5.1.6 Legal compliance of Toon

The Toon HEMS does not completely comply with the legal requirements as the service is not for free, and the measures to protect personal data are not adequate.

| | | | | | | |
|---|---|---|---|---|---|---|
| grounds | purpose | transparent | CBP | presentation | free | protected |

Table 4: Fulfilment by the Toon HEMS of the legal requirements as described in section 4.6.

Eneco does have legal grounds for processing (consent and to fulfil the contract with the end-user) and states the purposes for processing in their Privacy Statement which is easily obtained from their website. The documentation provided allows for the transparency of data processing as the identity of the controller and the purpose for processing are stated. The CBP has also been informed on the intent to process personal data. The Toon IHD, web portal and app each provide understandable interpretations of energy consumption data in understandable format and in a timely manner. However, Eneco does not offer any such service free of charge, as Toon requires a subscription fee as well as an initial investment unless Toon is supplied and installed for free under certain conditions.[176] Lastly, the protection of the energy consumption data is inadequate as Z-Wave transmissions using the third generation chip is insecure.

## 5.2 E-manager

The E-manager by Nuon is a portal-based HEMS that offers insight via either a website, or a smart device application. This device is made by Greenwave Reality (GR), and also offers various additional devices that can interact with the E-manager gateway such as light bulbs and intelligent power strips that can be controlled wirelessly, although these options are not a part of the basic package such as available from Nuon. The basic package costs 149 euro's, plus a monthly subscription fee of 2.95 euro's.

The subscription plan that comes with the E-manager entails the following benefits: Insight in consumption on a protected web portal and smart device application. Storage of this consumption data on the servers of Nuon, to allow for a comparison with other days, months and years. Comparison of daily usage with other comparable households, or households in your neighbourhood, town, province or in the rest of the country.[177] Daily predictions on monthly and yearly consumptions and an estimation on the achievement

[176] Which does not exempt the end-user from having to pay the monthly subscription fee.

[177] This is a privacy risk if the number of comparable households is low.

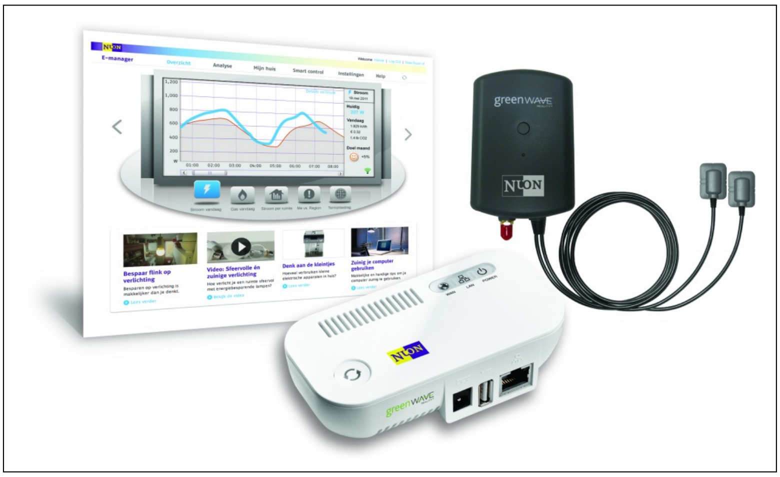


Figure 6: The Nuon E-manager. From left to right: the web portal, the gateway, and the sensor module with sensors attached.

of energy savings goals. The ability to extend the plan to include the controlling of devices and central heating.[178]

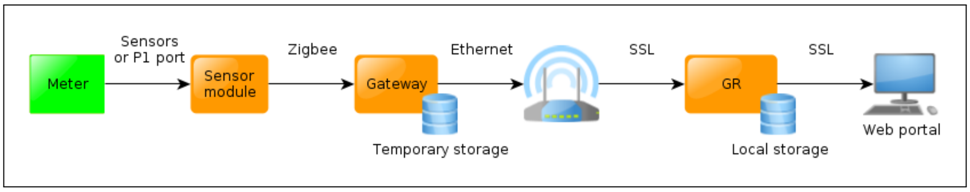


Figure 7: Dataflow within the E-manager HEMS.

The E-manager connects to meter via a P1 port if present, and also has sensors that can view a dumb meter. These two sensors or P1 cable are plugged into a sensor module, that wirelessly transmits this information to the E-manager gateway using the Zigbee protocol, that in turn passes the gathered data on to the servers of GR. As such, all data, inter alia energy consumption data and device data, are stored on the servers of GR. These servers are situated on at least three different continents as GR has offices in Denmark, The United States and Singapore and clients in each region. It is unclear as to where precisely the data from the E-manager is stored, it might well be on all three continents in a distributed fashion or as remote back-ups, or be kept on the European servers only.

The E-manager gateway is capable of communicating with devices using Z-Wave and Zigbee protocols. As Z-Wave has already been discussed in section 5.2.1 only the Zigbee protocol will be examined further. The E-manager

[178] Source: http://www.nuon.nl/energie-besparen/E-manager/inzicht-pakket.jsp, last referenced July 10 2013.

uses the Zigbee protocol to communicate between the sensor module and the gateway. As the basic package which is most often sold by Nuon only contains the sensor module, the gateway, and a power supply, communication by the gateway with other devices is ignored in this thesis, however, both Zigbee and Z-Wave devices can be connected to the gateway.

### 5.2.1 Zigbee

Zigbee is a low power and low data-rate wireless communication protocol with a maximum throughput of 250 Kbps, a small stack of just 120 KB with a range of ten to one hundred meters that builds upon the IEEE 802.15.4 standard.[179] It has become one of the leading communication protocols, due to its low energy consumption, low cost per node, and strong marketing efforts.[180] The Zigbee protocol allows for the forming of star, mesh, and tree like topologies with routers acting as repeaters to relay messages that two nodes can not directly send to each other in so called multihop routing and route discovery functionalities. Each device within the network gets its own 16-bit address, which it receives from its parent node.

Within a Zigbee network, there exists exactly one coordinator, and any number of end-devices and routers although this number is determined and fixed by the coordinator, who fixes not only the number of children (both routers and end-devices) each router may have, but also the maximum depth of the tree. In a tree network the coordinator is the root of the network, the routers intermediate nodes and the end-devices are the leaves. Both the coordinator and the routers are full function devices, whilst the end-devices are reduced function devices.

To set up the network, the first node to be powered up is the controller, after which child nodes can join in the network. The installation manual provided with the E-manager states that the first device to be powered up is the so called gateway, which also sets up the connection to the Internet. From this, the conclusion is drawn that with the E-manager, the gateway is the coordinator; whether the sensor module has full functions or reduced functions is unknown.

According to the Zigbee protocol standard, the implemented encryption for Zigbee packets is AES-128 as specified in FIPS Pub 197, using the CCM*-mode.[181] [182] The CC2530 chip, a second generation Zigbee chip, in the E-manager *"allows the user to encrypt and decrypt data using the AES algorithm with 128-bit keys. The core is able to support the AES operations required by IEEE 802.15.4 MAC security, the ZigBee network layer, and the*

[179] Baronti et al. (2007).

[180] Slootweg et al. (2011), Farhangi (2010).

[181] ZigBee Specification Document 053474r17, January 17, 2008

[182] For more details on CCM*, a variation of 'Counter with Cipher block chaining Mode', see Struik (2005).

*application layer"*.[183] Note the use of the words 'allows' and 'able', which suggest that encryption is not enforced, merely supported and optional.

Unlike Z-Wave, that operates on the relatively quiet frequency of 868.42 MHz, Zigbee typically operates in the 2.4 GHz range (although it can also handle the 868 MHz range) which is also used by for instance WiFi networks, bluetooth, and microwave ovens.[184] The CC2530 chip only supports the 2.4 GHz range however. Despite the heavy use of this frequency, the Zigbee radio does not seem to have any problems with communication despite this being a possibility and concerns having been raised towards this issue.[185] Because Zigbee operates on radio frequencies, it is possible to use dedicated hardware to capture these packages and examine them, although encryption will be in place which will have to be dealt with in order to get to the content of each package.

In the case of the E-manager, there are a number of questions that are left unanswered because no information is available. How is the encryption protocol implemented, is it actually used? How is the Zigbee protocol implemented, what stack version? Is there a random key for each coordinator that is produced by GR, or is there a limited set or even just a single key that all devices use? Where is this key stored, and can it possibly be extracted from the controller? If mistakes are made in the implementation or use of the protocols or key management, although the protocols elves are secure, in practice things turn out to be less than secure and are susceptible to exploits.

In general, the Zigbee specification offers means to achieve the following security requirements: Freshness, message integrity, authentication and encryption.[186] If and how these means are implemented in the E-manager is unknown. As the E-manager is not testable by the author, all that can be done is make assumptions on the security of the implementation.

Even if the implementation is secure, an attacker still has the possibility to compromise availability by flooding the bandwidth at which Zigbee is communicating, although this tactic probably works with just about every wireless communication protocol.[187]

However, with the deficiency in network and link key management in the Zigbee protocol, it is possible to obtain these keys from any device that has been connected to the network, compromising confidentiality and authenticity.[188] *"Upon leaving the network (or being forced to), a node still remains able to access communications because the onboard keying material*

[183] CC2530 datasheet, available at www.ti.com/lit/ds/swrs081b/swrs081b.pdf, last referenced Augstust 10 2013.

[184] Zigbee Alliance (2007), Lewis et al. (2009).

[185] Zigbee Alliance (2007), Gungor et al. (2011), Lewis et al. (2009).

[186] Baronti et al. (2007).

[187] Lewis et al. (2009).

[188] Dini & Tiloca (2010).

*is not properly revoked. A node leaves the network when it is dismissed, sent to maintenance, lost, compromised, or supposed so. In all these cases, the keys stored on the device may be compromised, and thus, if they are not properly revoked, an adversary may exploit them to mount severe attacks against the network and application level."*[189]

If the implementation of the Zigbee protocol in the E-manager HEMS is secure, remains unknown, although with the possible compromise of confidentiality and authenticity due to key management deficiencies, and the compromise of availability by flooding the bandwidth, the assumption that Zigbee indeed is insecure can be backed up. It is better to assume insecurity and be proven wrong, than to have a false sense of security, therefore the assumption is made that the implementation of Zigbee in the E-manager is insecure. Further research, and reverse engineering of the actual hardware might tell if the implementation actually is secure.

### 5.2.2 Data storage on servers and locally

Little is known about the storage of data on the GR servers other than that these servers are used to store the data gathered by E-manager. What data exactly is stored, can not be determined other than relying on the ToS and Privacy Statement made by Nuon.

A small statement in the ToS stipulates that in the case of a loss of connectivity towards the Internet, energy consumption data will be temporarily stored locally and be transmitted as soon as the connection is function again. Nowhere in the E-manager manual is any mention made of this local storage, what is stored exactly, and when (or if) this temporary storage is emptied. The assumption is made that this storage is located within the gateway, as it is the controller of the Zigbee network, which should be verifiable by reverse engineering the device.

### 5.2.3 Terms of Service and Privacy Statement

In the ToS, Nuon states that the web portal is a secured electronic Internet environment, although the means of security are not stated. It does state however that services of third parties are used, for which they will receive personal data of the customer, which will be communicated in encrypted from. Regarding purpose of processing, the ToS states that processing is done for the purposes of handling orders, fulfilling agreements, customer relations and for marketing. For the purpose of services, personal data will also be shared with third parties, and it is not clear who these parties are. This statement is in conflict with the statement that data will be stored on the web portal and only be accessible to the data subject and Nuon. Technically, a web portal is the front-end of a server and so information

[189] Ibidem.

will be stored on the server and not on the portal. The web portal for the E-manager service is located on the domain of GR[190], which raises the question if GR might have access to this data.

The Privacy Statement makes it clear that Nuon has informed the CBP on the intent to process personal data; which indeed can be found in the CBP registry under numbers 1110536 and 1110548.[191], [192] Nuon specifically states that personal data is stored on a secured server, which protects against processing by those without permissions and that 'personal data is only used for purposes for which it was collected, or for purposes that are compatible with this purpose'. The closing statement reads that the Privacy Statement can be altered at any time and the consumer is advised to regularly check the Privacy Statement. There is however, no version number or date of last change to be found on the statement so it is unclear to the consumer if something has changed or not.

### 5.2.4 Data security

Judging data security with the E-manager is troublesome as GR is unavailable for comments. The only information available is through Nuon, who state that the connection between the HAN and the GR servers is set up using SSL. From the web portal itself can be concluded that the connection between the servers and the browser is also protected using SSL. This leaves the connections within the HAN as possibly non-confidential. As the connection between the gateway and the router is made using an ethernet cable, listening in on this communication is not feasible.

When using the Zigbee protocol to communicate between the sensor module and the Gateway however, the assumption is made that communications are insecure because of the possibility of compromised network and link keys.[193]

Regarding data integrity, as nothing is known about the temporary storage within the HAN as mentioned in the ToS accompanying the E-manager, the possibilities of tampering with this storage are unclear. With the vulnerability of the Zigbee connection however, packet spoofing might be possible which will compromise data integrity and produce false readings on the web portal. This data is however only used for information purposes and not for billing. Thus, an attacker may be able to gain insight into energy consumption data and alter this data, but billing will still be correct.

[190] https://nuon.greenwavereality.com.

[191] https://www.collegebeschermingpersoonsgegevens.nl/asp/ORDetail.asp?moid=808f808e8b, last references July 27 2013.

[192] https://www.collegebeschermingpersoonsgegevens.nl/asp/ORDetail.asp?moid=808f808e8e, last referenced July 27 2013.

[193] Dini & Tiloca (2010).

### 5.2.5 Legal compliance of the E-manager

The E-manager HEMS does not completely comply with the legal requirements as the service is not for free, and there is doubt as to whether the measures to protect personal data are adequate.

| | | | | | | |
|---|---|---|---|---|---|---|
| grounds | purpose | transparent | CBP | presentation | free | protected |

Table 5: Fulfilment by the E-manager HEMS of the legal requirements as described in section 4.6

Nuon does have legal grounds for processing (consent and to fulfil the contract with the end-user) and states the purposes for processing in its ToS and in its Privacy Statement, both of which are easily obtained from their website. The documentation provided allows for the transparency of data processing as the identity of the controller and the purpose for processing are stated. The CBP has also been informed on the intent to process personal data. The E-manager web portal and provides understandable interpretations of energy consumption data in understandable format and in a timely manner. However, Nuon does not offer any such service free of charge, as the E-manager requires a subscription fee as well as an initial investment. Lastly, the protection of the energy consumption data is doubted as there are issues with the security of the Zigbee protocol. It is better to assume insecurity and be proven wrong, than to have a false sense of security. Therefore, the E-manager HEMS is marked as not complying with the requirements of adequate protection.

## 5.3 Smile P1

The Smile P1 (hereafter called 'Smile') by Plugwise is a small device that connects directly to the P1 port of a Smart Meter, and thus can not function with a meter that does not have this port. The Smile accepts telegrams from the meter, and passes these on via WiFi or an ethernet cable to the home modem, which in turn passes this information on to the Plugwise servers. It is these servers that provide the information to the app that is running on a smart device. It is also possible to connect directly to the Smile using a WPA/WPA2 PSK protected WiFi connection for installation purposes. For this, the pre-shared key (PSK) is needed which is an eight-letter password that is found on the back of the device. The Smile costs 99.99 euro's; the subscription to the service is free for the first six months, and from then on costs 12 euro's a year.

The set up of the Smile can take place using either a connection with the Smile device itself using its WiFi capabilities, or through an ethernet connection. Because of this wireless connection possibility and the use of that same connection for setting up the device, the WiFi network that the

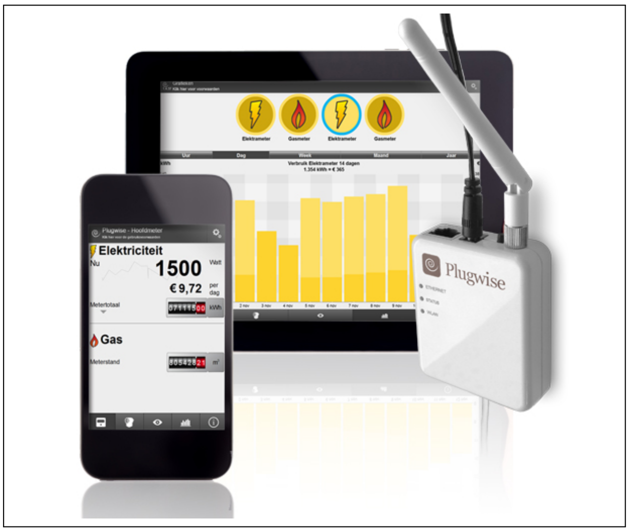


Figure 8: The Smile P1 device, together with two smart devices running the app that can be used to interface with the Smile.

Smile creates is always on if no ethernet cable is plugged in. If an ethernet cable is used to connect the Smile to the HAN, the WiFi network is shut down.[194]

### 5.3.1 WPA/WPA2 PSK

In order for the Smile to communicate with the HAN and to set up the configurations for the Smile, the Smile generates a wireless network if no ethernet cable is plugged in, broadcasting its service set identifier (SSID, or more commonly known as the network name), which for the Smile, always starts with ”smile_” and is followed by six alphanumericals for a total SSID length of 11. The PSK with the Smile is located on a sticker on the back of the device and is hardcoded into the device itself, thus, it can not be changed by the end-user.[195] In the Smile, this PSK consists of eight lowercase letters, allowing for a total of $26^8$ possible passwords.[196]

The establishment of a connection between a WPA/WPA2 PSK access point and a device is done through a four way handshake that involves the PSK, the SSID and other pieces of data as is described in the IEEE 802.11i

[194] Expressed during a telephone call with Plugwise customer service on August 9 2013.

[195] During a phone call with the Plugwise service desk on August 9 2013, a question about wanting to change the SSID and the PSK on the Smile was met with the answer ”Why would anyone want to do that”. After further questioning it turned out that indeed the PSK and SSID are unchangeable in the device. The only option was to buy a new device.

[196] Plugwise Smile P1 installation manual, downloaded from www.Plugwise.com/nl/idplugtype-f/smile-p1-handleiding on July 26 2013.

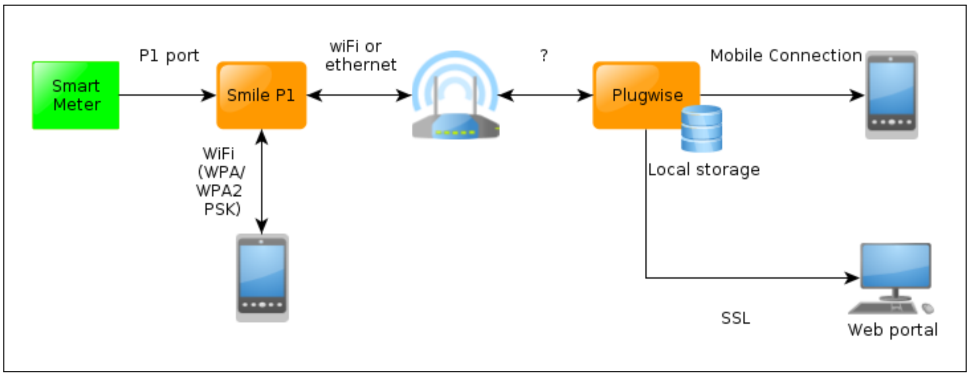


Figure 9: Dataflow within the Smile P1 HEMS.

standard.[197] This standard includes a minimum length for the PSK, which is eight characters, which corresponds to the PSK length in the Smile.

WPA/WPA2 PSK connections can be bruteforced if one knows the SSID of the network and the keyspace is small,[198] it simply requires capturing the four-way handshake to initiate the network, which can be done at any time a device connects to the network. This four-way handshake, a set of four messages that is being passed between a connecting device and an access point, which can easily be captured using software such as Wireshark.[199] Once this handshake has been captured, it can be used to speed up the bruteforce significantly as the network itself is no longer needed to confirm the PSK.

With the Smile, the SSID is broadcast, and the key is limited to eight lowercase characters entailing $26^8$ keys in the keyspace. With a conservative estimate of 400.000 passwords checked each second, trying out every single key in the keyspace of the Smile would take:

$$\frac{(\frac{26^8}{400000})}{60*60*24} \approx 6 \text{ days}$$

Which is entirely feasible, as not only does this take very little time, but as mentioned, it can also take place off-site as the network itself is not needed. Thus, WPA/WPA2 PSK, with such a small keyspace is to be considered insecure. Whoever holds the PSK, has access to the energy consumption

[197] 802.11i-2004 - IEEE Standard for information technology-Telecommunications and information exchange between systems.

[198] A keyspace is the set of all possible keys given a certain grammar of this key, the cardinality or number of elements in the set is the size of the keyspace.

[199] Tutorials on how to crack WPA/WPA2 connections can be found all over the Internet. A quick search on Google on August 9th 2013 using the search term 'WPA2 cracking' gave 337,000 results. Some results are for services that will retrieve the PSK for you, if you provide them with the captured handshake.

data and can modify the settings within the Smile device, if within range of its WiFi network.

### 5.3.2 Unclear communications

Within the HAN, a smart device can be used in combination with the PSK to connect to the Smile directly for set up purposes. The viewing of energy consumption data always takes place using the data that is stored on the Plugwise servers, if the end-user is within the HAN or outside of it. This is concluded from the lack of storage space in the Smile device itself as it contains no EEPROM memory and just 32 MB of SDRAM[200], from which can be concluded that no local storage can take place, because this would mean that data would be lost.[201] This conclusion is confirmed by the Plugwise site stating that P1 data will be sent to a secured server.[202]

The Plugwise customer service was very vague and reluctant to answer questions concerning the flow of information and the security features of the Smile HEMS. In particular, the question as to what security features were in place to safeguard the connection between the HAN and the servers of Plugwise was met with the response that they were not going to tell how this was done.[203] However, upon viewing the Plugwise app and going through the installation, various mentions were made that *"Your energy consumption- and/or production data is always stored anonymously. Data is send over a secure connection (SSL)"*.

Although the device is capable of receiving telegrams every ten seconds, data packets are supposedly pushed only once an hour, containing only hourly measurements which are stored on the servers of Plugwise. Nevertheless, even from outside of the HAN, the application is capable of displaying information with a granularity of fifteen minutes. Plugwise did not have an adequate answer to how such a feat was accomplished and was hesitant to reveal details on data collection and communication protection.[204]

The smart device application does have the option to turn off the sharing of energy consumption data with Plugwise, but it is not clear if this also means that Plugwise can no longer set up a connection with the Smile device. Without getting access to a Smile device and examining it in detail as to

[200] SDRAM or Synchronous dynamic random-access memory is a type of memory that looses its contents if a power loss occurs.

[201] See the Smile P1 technical specifications at http://www.Plugwise.com/nl/idplugtype-f/node/903, last referenced August 9 2013.

[202] *"In a few steps, you can add the Smile P1 to your own wireless network using the user-friend app. The Smile P1 will then send your meter readings to a server which complies with strict securityfeatures for the storage of data"* Translation from Dutch by the author. Source: http://www.Plugwise.com/nl/idplugtype-f/node/903, last references August 9 2013.

[203] So called 'security by obscurity', which is never a good sign as this does not allow for the examination of the methods and protocols.

[204] Expressed during a telephone call with Plugwise customer service on June 28th 2013.

what is being transmitted over the ethernet and WiFi networks, one can only guess as to what is really going on.

### 5.3.3 Terms of Service and Privacy and Cookie Policy

The ToS explicitly mentions that Plugwise has the right to let (parts of) the contract between the customer and Plugwise be performed by third parties. Therefore, it is unclear who is actually performing the data processing.

Plugwise retains the right to alter the software that is running on the Smile, as long as this alteration is necessary according to Plugwise. This implies that Plugwise has access to the device itself in some way, although customer service was not willing to discuss this when asked.

A particularly interesting statement is that 'the customer holds responsibility for the security of the Plugwise system'. This is quite impossible as although the customer is responsible, he is not given the means to actually act out on this responsibility. Although sharing the PSK with strangers will compromise the system, there is no way to change the PSK to something more secure.[205] So, although Plugwise places this responsibility with the customer, the customer is not given the means to secure his system. As such, this responsibility can not be placed with the consumer. Upon contacting customer service, it was explained that this has to do with the security of the HAN, which is entirely unclear from the ToS.

Regarding the processing of personal data, the Privacy and Cookie Policy states that energy consumption data will be processed after being anonymized, unless the data subject gives explicit consent to store this data with a connection to his identity. The purpose of this processing is the delivery of services, including software updates to the Plugwise systems[206], and for marketing purposes. This processing can also be performed by third parties, whilst Plugwise remains the responsible.

The Privacy and Cookie Policy ends with the date of last alteration which was on January 20th, 2009, also making it clear that changes will not be announced, and that the client will have to check the statement regularly.

### 5.3.4 Data security

Although the Smile has the option of using both the wireless and wired connections with the HAN, in case the wireless version is used, the implementation of WPA/WPA2 PSK leaves the Smile vulnerable. Because of the use of a very small PSK, that can not be changed by the end-user, and a SSID that can not be changed as well, this is a vulnerability that is even

[205] Upon contacting customer service with the question if the PSK was changeable, the response was "No you can not, why would you want to do that anyway?". The only way to change the PSK was to buy a new Smile.

[206] The ToS and Privacy and Cookie Policy are not about the Smile specifically, but about all the devices and services that Plugwise offers.

easier to exploit, and once the key is compromised, there is no way to re-secure the Smile. If a malicious party can gain access to the Smile through this connection, they can change consent indication such as the sharing of unanonimized data with Plugwise, changing availability of this information outside of the HAN. Thus, if the wireless connection is used to connect the Smile with the HAN, confidentiality, availability, integrity, authenticity, and non-repudiation all are compromised.

If the wired connection is used, compromising the wireless network of the Smile itself is impossible. Considering that the data is sent from the HAN to the servers of Plugwise using SSL, this connection is secured. It is unknown how the connection between the servers of Plugwise and a smart device outside of the HAN is set up, and how the app itself is secured.

This leaves a lot of questions for future research concerning the exact methods of communication and verification if indeed the Smile, when set up using the wireless connection, is as insecure as it seems. Although questions remain, the assumption is made that the Smile is insecure when using the wireless connection.

### 5.3.5 Legal compliance of the Smile P1

The Smile P1 HEMS does not completely comply with the legal requirements as the processing of data has not been found within the CBP registry[207] and the protection of the wireless network that the Smile is capable of making is inadequate.

| | | | | | | |
|---|---|---|---|---|---|---|
| grounds | purpose | transparent | CBP | presentation | free | protected |

Table 6: Fulfilment by the Smile P1 HEMS of the legal requirements as described in section 4.6.

Plugwise does have legal grounds for processing (consent and to fulfil the contract with the end-user) and states the purposes for processing in its Privacy and Cookie Policy, both of which are easily obtained from their website although they are in 'legalise'. The documentation provided allows for the transparency of data processing as the identity of the controller and the purpose for processing are stated. The CBP has not informed on the intent to process personal data.[208] The Plugwise app provides understandable interpretations of energy consumption data in understandable format and in a timely manner. Because Plugwise is not an energy supplier, offering this

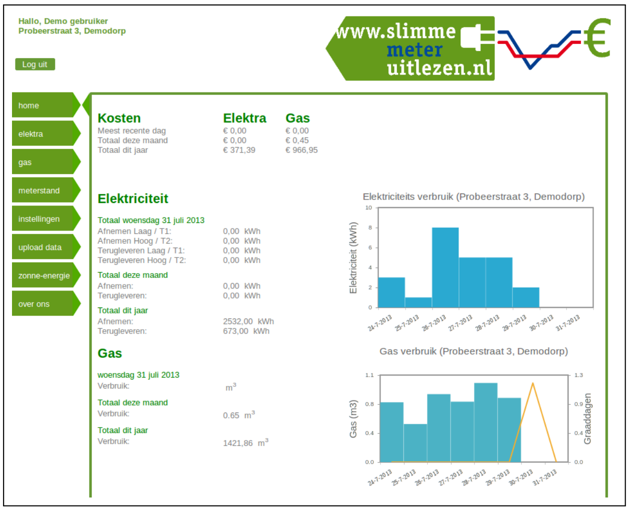
[207] There is no mention of registration within the documentation provided on the website of Plugwise, and no mention of Plugwise can be found within the registry.

[208] Although a mention is found in the CBP registry (notification number 1348099) for Plugwise B.V. this only stipulates the processing of Name and Adress, and not of energy consumption data. https://www.collegebeschermingpersoonsgegevens.nl/asp/ORDetail.asp?moid=8f8b8e8288, last referenced August 10 2013.

service free of charge is not required and thus the colour grey is used in the Table 6. Lastly, the protection of the energy consumption data is doubted as there are issues with the wireless capabilities of the Smile P1.

## 5.4 Slimmemeteruitlezen.nl

Slimmemeteruitlezen.nl (hereafter called ’SMU’) is a website portal by Enepa, an independent energy consultant situated in the Netherlands. On their website, it is possible to register for the service of remote reading of the Smart Meter. Judging by the demonstration environment that is offered, and the basics of smart metering as discussed in section 3.1, the data used to generate the Smart Meter readouts is taken from the P4 port although this is not explicitly mentioned.



Hallo, Demo gebruiker
Probeerstraat 3, Demodorp

| Kosten | Elektra | Gas |
|---|---|---|
| Meest recente dag | € 0,00 | € 0,00 |
| Totaal deze maand | € 0,00 | € 0,45 |
| Totaal dit jaar | € 371,39 | € 966,95 |

Elektriciteit

| Totaal woensdag 31 juli 2013 | |
|---|---|
| Afnemen Laag / T1: | 0,00 kWh |
| Afnemen Hoog / T2: | 0,00 kWh |
| Terugleveren Laag / T1: | 0,00 kWh |
| Terugleveren Hoog / T2: | 0,00 kWh |
| Totaal deze maand | |
| Afnemen: | 0,00 kWh |
| Terugleveren: | 0,00 kWh |
| Totaal dit jaar | |
| Afnemen: | 2532,00 kWh |
| Terugleveren: | 673,00 kWh |

Gas

| woensdag 31 juli 2013 | |
|---|---|
| Verbruik: | $m^3$ |
| Totaal deze maand | |
| Verbruik: | 0.65 $m^3$ |
| Totaal dit jaar | |
| Verbruik: | 1421,86 $m^3$ |

Figure 10: The slimmemeteruitlezen.nl web portal, logged in with the demo account as provided by Enepa.

The site offers very little functionality other than a day by day overview of both gas and electricity consumption of the last seven days, electricity production in this same period, and figures for this month and this year so far. A daily consumption figure can also be requested for days outside of the seven day range. This is also possible outside of the forty day range that the P4 port offers, from which the conclusion is drawn that P4 data is stored on the SMU server and not just collected from EDSN and presented ad hoc.

To prevent unauthorized access, the end-user must log on to the site with a username/password combination. The use of the SMU service has an annual fee of twenty euro’s.

### 5.4.1 Minimal dataflow

Data flows within SMU are limited in that the flow of data from the Smart Meter up to port P4 lies outside of SMU's control, all SMU does is gather the information from EDSN, store it on a server, and make it available to the customer through a web portal.

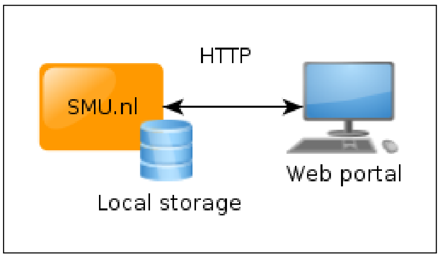


Figure 11: Dataflow within the SMU HEMS.

The only connection that SMU has to secure itself is the connection between its servers and the browser of the customer as the connection between EDSN and SMU is regulated by EDSN. The connection between the servers and the end-user's browser is made through a regular HTTP connection, entailing any data being sent in plaintext. It must be said that this is only with the demo account, as no live account has been used. However, given that the demo account uses a username/password combination such as would also be the case in a live account, it stands to reason that security will be the same.

As to how the servers themselves are secured, it is left unclear as all Enepa is willing to state is that 'the infrastructure and procedures are set up to provide optimal protection of data, with respect to the current state of technological development'.[209]

### 5.4.2 Terms of Service and Privacy Statement

The ToS of SMU are surprising, although they are readily available on the SMU website, the document that is made available is a concept-ToS dating back to October 31st, 2011. That this is a concept is made explicitly clear by the vague overlay of the word 'concept' on each page. The ToS states that it is based on a general ToS-template by the Dutch homeshoppingorganisation ('Nederlandse Thuiswinkelorganisatie') together with the consumer protection organisation ('consumentenbond'), which becomes clear as the ToS describes use cases concerning physical products and delivery where SMU offers only an online service.

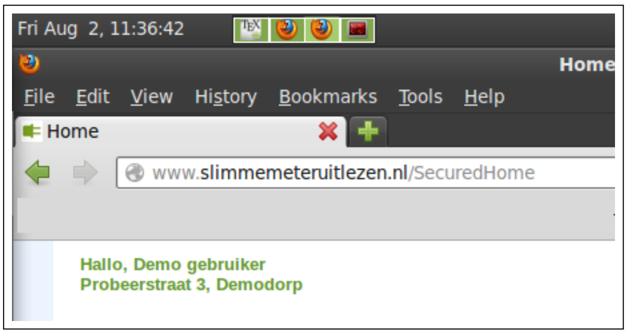
[209] SMU Privacy Statement, available at http://www.slimmemeteruitlezen.nl/Content/info/PrivacyStatement.pdf, last referenced August 11 2013.

Upon contacting Enepa through e-mail about the fact that their ToS was still a concept version the author was supplied with an updated version and the promise that this version would be made available on the website as soon as possible. At last reference on August 9th, 2013, the concept version was still the version being made available though. The version that was supplied through e-mail had slight alterations compared to the concept version, such as the date of modification being changed, yet on the first page it stated 23d of December 2012, whilst on the other pages it stated August 1st, 2013.

In the Privacy Statement, Enepa acknowledges that energy consumption can be seen as personal data and state that they have implemented suitable technical and organizational measures to prevent data loss and illegitimate processing. The purposes for processing of personal data are stated to be the facilitation and increase in energy savings, and $CO_2$ reduction. The exact data to be collected is stated as well, and conforms with what the P4 port makes available.

Lastly, Enepa retains the right to change the Privacy Statement, and suggests that the customer reference the statement on a regular basis to remain informed. The Privacy Statement concludes with a date, although it is unclear as to whether this is the date of the first draft or of the last change as there is no explicit mention of what this date means.

### 5.4.3 Data security


Fri Aug 2, 11:36:42
Home
File Edit View History Bookmarks Tools Help
Home
www.slimmemeteruitlezen.nl/SecuredHome

Hallo, Demo gebruiker
Probeerstraat 3, Demodorp

Figure 12: A detail screenshot of the address field of a Firefox web browser logged into the demo account of slimmemeteruitlezen.nl. Note the globe symbol in front of the address field. If the connection to this website was using HTTPS, a lock would be displayed instead. Clicking the globe yields more information, and ends with the statement: *"**Connection not encrypted:** The website www.slimmemeteruitlezen.nl does not support encryption for the page you are viewing. Information sent over the Internet without encryption can be seen by other people while it is in transit"*.

Up to the servers of Enepa, data security is handled by the regulations concerning the P4 port.[210] As soon as the data is on the servers of Enepa however, they become the data controller and are responsible for the protection of this data. Logging in to the SMU web portal requires a username/password combination, which because of the implementation of a HTTP connection is sent in plaintext to the servers for authentication purposes. Anyone can listen in on this traffic while it is in transit, and use this to log in to the web portal themselves. Because of the implementation of HTTP, and the ensuing possibility of loss of login credentials, confidentiality and authenticity do not exist.

To verify this point, Wireshark was used to sniff for a post request upon attempting to log into the web portal using the demo account. Part of the resulting trace was as follows:

```
[...]
02f0  6e 67 74 68 3a 20 37 38  0d 0a 0d 0a 55 73 65 72   ngth: 78 ....User
0300  4e 61 6d 65 3d 63 6f 6e  73 75 6d 65 6e 74 25 34   Name=con sument%4
0310  30 73 6c 69 6d 6d 65 6d  65 74 65 72 75 69 74 6c   0slimmem eteruitl
0320  65 7a 65 6e 2e 6e 6c 26  50 61 73 73 77 6f 72 64   ezen.nl& Password
0330  3d 65 6e 65 70 61 31 32  33 26 52 65 6d 65 6d 62   =enepa12 3&Rememb
0340  65 72 4d 65 3d 66 61 6c  73 65                     erMe=fal se
```

From this trace, the name and password are almost immediately clear, stating Name=consument%40slimmemeteruitlezen.nl&Password=enepa123. The %40 is the ASCII hex notation for the glyph '@', which is the only small detail not immediately clear but can easily be looked up in an ASCII table, or simply guessed from the format of the rest of the username. Confidentiality is thus compromised.

Data integrity, availability and authenticity can also be compromised as a user is never sure if the website he is visiting is actually SMU, or another site masquerading as SMU, because no certificates are used to authenticate the web portal. Thus, although from the perspective of Enepa data might keep integrity, the user can be viewing a completely different information set, or one that is slightly altered, making his true data unavailable.

This leaves the final goal of non-repudiation. As the login credentials can easily be captured, SMU can never be certain that the person who logs in, is the person whom the login credentials belong to. Any ensuing actions by that person whilst logged in are thus reputable, such as the changing of the password, address data, or the consent to receive the newsletter.

### 5.4.4 Legal Compliance of SMU

The slimmemeteruitlezen.nl HEMS does not completely comply with the legal requirements as data processing has not been registered with the CBP, and protection of personal data is inadequate.

[210] See section 3.3.2 of this thesis.

| | | | | | | |
|---|---|---|---|---|---|---|
| grounds | purpose | transparent | CBP | presentation | free | protected |

Table 7: Fulfilment by the slimmemeteruitlezen.nl HEMS of the legal requirements as described in section 4.6.

Enepa does have legal grounds for processing (consent and to fulfil the contract with the end-user) and states the purposes for processing in its Privacy Statement, which is easily obtained from the SMU website. The documentation provided allows for the transparency of data processing as the identity of the controller and the purpose for processing are stated, although the fact that a concept version of the ToS is made available raises doubts on its validity. The CBP has not informed on the intent to process personal data.[211] The SMU portal provides understandable interpretations of energy consumption data in understandable format and in a timely manner. Because Enepa/SMU is not an energy supplier, offering this service free of charge is not required and thus the colour grey is used in the Table 6. Lastly, the protection of the energy consumption data is virtually non-existent as the communication from and to the browser is done in plain HTTP, allowing anyone full access.

## 5.5 Slimmemeterportal.nl

Like the previously discussed HEMS, slimmemeterporal.nl (hereafter called 'SMP') is a website portal that provides insight into energy consumption data gathered from the P4 port. SMP can be used completely free of charge, as it is used as a way to promote the services offered by energyalert.nl.

Within the settings on the portal, the customer is able to set building type, build year, family size, size of the building, and the current tariffs, as well as having to fill in the mandatory fields of name, address, and e-mail address.

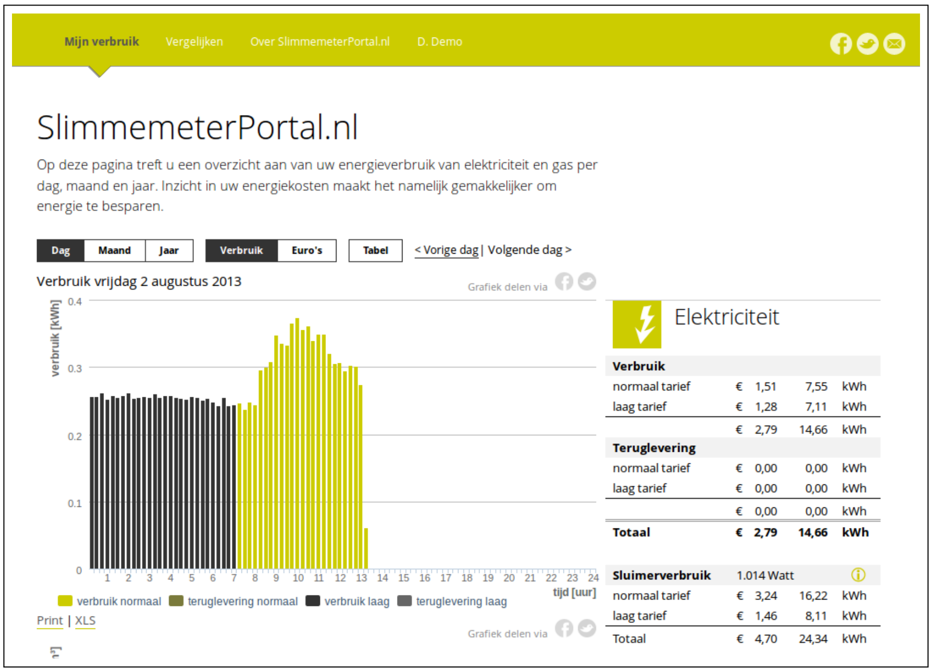
SMP allows for the comparison with the same building type, customers in the neighbourhood, and with all connections known to SMP.[212] Finally, customers can share consumption information and comparison information through Facebook and Twitter.

### 5.5.1 Secured connection

As SMP is a web portal-only service, they retrieve information from the P4 port upon the customer's request (consent). As with SMU, this entails that the connection up to SMP is regulated and its security is out of SMP's hands. Once SMP gains control over the data, they become the data controller and must have adequate security measures in place.

[211] No mention of Enepa or SMU can be found in the registry of the CBP.

[212] If the number of customers in a neighbourhood is small this is a privacy issue.



SlimmemeterPortal.nl

Op deze pagina treft u een overzicht aan van uw energieverbruik van elektriciteit en gas per dag, maand en jaar. Inzicht in uw energiekosten maakt het namelijk gemakkelijker om energie te besparen.

Verbruik vrijdag 2 augustus 2013

Elektriciteit

| | | | | |
|---|---|---|---|---|
| **Verbruik** | | | | |
| normaal tarief | € | 1,51 | 7,55 | kWh |
| laag tarief | € | 1,28 | 7,11 | kWh |
| | € | 2,79 | 14,66 | kWh |
| **Teruglevering** | | | | |
| normaal tarief | € | 0,00 | 0,00 | kWh |
| laag tarief | € | 0,00 | 0,00 | kWh |
| | € | 0,00 | 0,00 | kWh |
| **Totaal** | **€** | **2,79** | **14,66** | **kWh** |
| **Sluimerverbruik** | 1.014 Watt | | | ⓘ |
| normaal tarief | € | 3,24 | 16,22 | kWh |
| laag tarief | € | 1,46 | 8,11 | kWh |
| Totaal | € | 4,70 | 24,34 | kWh |

Figure 13: A screenshot of the SMP web portal whilst logged into the demo account. This particular screen details 15-minute readings.

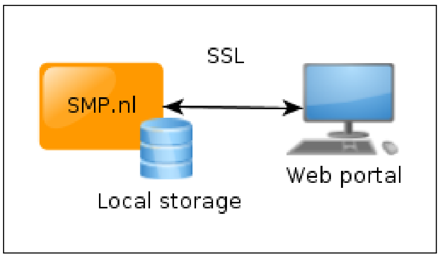


Figure 14: Dataflow within the SMP HEMS.

The connection between the servers and the client's browser is protected using digital certificates (SSL) as can bee seen in Figure 15 and can thus be considered secure.

As to what measures are in place to safeguard the servers themselves against unlawful data processing is unknown.

### 5.5.2 Terms of Service and Privacy Statement

It is unclear as to what ToS is applicable to SMP, as there are no ToS available on the web portal. EnergyAlert does have a ToS on their website, but nowhere on SMP does the client have to accept those ToS, nor does the ToS of EnergyAlert state that it also applies to SMP. Also, in the VAS

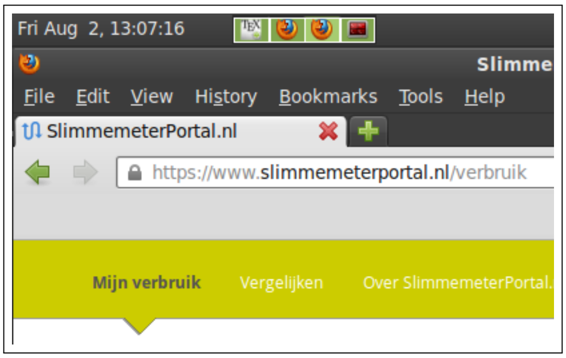


Figure 15: A detail screenshot of the address field of a Firefox web browser logged into the demo account of slimmemeterportal.nl. Note the padlock symbol in front of the address field signifying the use of HTTPS, as opposed to the globe symbol observed in Figure 12. Clicking the lock yields more information, such as details on the CA that signed the certificate, and ends with the statement: *"**Connection encrypted: High Grade Encryption (AES-256, 256 bit keys)**. The page you are viewing was encrypted before it was sent over the Internet. Encryption makes it very difficult for unauthorized people to view information travelling between computers. It is therefore very unlikely that anyone read this page as it travelled across the network"*.

declaration that the customer has to consent to, no mention is made of either EnergyAlert or SMP, but rather of Oblivion B.V. as being the data controller, who are the builders and administrators of the SMP web portal. Oblivion B.V. also does not supply a ToS. It is thus very unclear as to what ToS apply, or even if there are ToS.

As with the ToS, there is no Privacy Statement to be found anywhere on the SMP website. Although there is a 'disclaimer' to be found on the energyalert.nl website, this disclaimer specifically states that it is applicable to energyalert.nl only.[213] An examination of the sitemap[214] of SMP shows that there is no link towards either a ToS or a Privacy Statement.

[213] *"The following statement is applicable to this website. By using this website, you agree with this diclaimer"* Translation from Dutch by the author. https://www.energyalert.nl/articles/bf34558a-982e-11e1-99f1-02bfc765e276/disclaimer, last referenced July 30 2013.

[214] A sitemap is a graph-like overview of all the accessible pages on a website. This is generated by following all links on the homepage, and following all links on subsequent pages until no new pages can be found within the domain. This can also include links to all documents linked to.

### 5.5.3 Data security

Judging the data security of SMP is troublesome there are only two factors that play a role; the servers of Oblivion, and the connection between these servers and the web-browser of the end-user. Although the connection between the server and the end-user is protected using SSL, and thus considered secure, nothing is known about the servers of Oblivion.

SSL however, protects confidentiality, integrity, authenticity and non-repudiation. It does not protect availability, and a DoS against the servers of Oblivion might be successful in making the portal unavailable.

As there is just one line of data communication, and that line is considered secure, the conclusion is drawn that SMP provides adequate data security.

### 5.5.4 Legal compliance of slimmemeterportal.nl

The slimmemeterportal.nl HEMS does not completely comply with the legal requirements as there is no clear purpose for the processing of data, therefore transparency is also not given to the data subject.

| | | | | | | |
|---|---|---|---|---|---|---|
| grounds | purpose | transparent | CBP | presentation | free | protected |

Table 8: Fulfilment by the slimmemeterportal.nl HEMS of the legal requirements as described in section 4.6.

SMP does have legal grounds for processing (consent) but does not state the exact purpose of data processing, it only vaguely hints at it.[215] There is ToS or Privacy Statement document provided, and no clear statement on purpose of data processing, although the identity of the data processor is stated on the website. The CBP has not informed on the intent to process personal data.[216] The SMP website provides understandable interpretations of energy consumption data in understandable format and in a timely manner. Because SMP is not an energy supplier, offering this service free of charge is not required and thus the colour grey is used in the Table 6, although the service is for free. Lastly, the protection of energy consumption data by SMP is not doubted and considered secure.

[215] 'Slimmemeterportal.nl reads the data from your Smart Meter and transforms this into clarifying graphs, giving you insight in your actual energy consumption.' Translation from Dutch by the author. Source: https://www.slimmemeterportal.nl/articles/d1f9346c-d818-11e2-8abb-02bfc77fa6c3/Wat%20is%20het%3F, last referenced August 10 2013.

[216] No mention has been found in the registry for EnergyAlert or for slimmemeterportal.nl

# 6 Conforming to legal requirements

In this chapter, each of the derived legal requirements is discussed as to how they can be fulfilled.

> Have grounds upon which data processing is legitimised.

As described in section 4.4, the grounds for processing are: consent, to fulfil a contract, legal obligation, vital interest of the data subject, public interest, and legitimate interest of the data controller. Consent and to fulfil a contract are most often used in the domain of HEMS, and although care must be taken to obtain prior informed consent and thus provide the data subject with transparency on data processing , such a legal ground suffices for the purpose of energy consumption data processing.

> Process personal data only for a specified purpose.

Purpose limitation entails that processing may be done only for explicitly stated purposes. Thus, to fulfil this requirement, a data controller will have to explicitly state the full purpose of processing, and not just give a vague description. If the only purpose stated is 'for marketing' this is not enough.

> Notify the data subject on this data processing, in for the data subject understandable language.

Transparency of processing entails that the data subject knows who is processing his data, and for what purpose. To accomplish this, it does not suffice to state identity and purpose in a section of a document or a webpage that a typical data subject will not, or can not understand. A regular user will not understand highly technical or legal content. Therefore, a clear and accessible statement on 'The data processor is:', 'The following data will be processed:', and 'The purpose of this processing is:' that offers a concise and simple overview of processing is recommended.

Although the need for legal language in ToS' is clear, there is no need for the HEMS supplier to omit a simplified overview of processed data and on what grounds it is being processed. This overview can be made into a separate webpage that needs to be viewed, and can not be clicked away for a number of seconds, along with the potential customer only being able to sign up after seeing this page and providing positive consent to this page. Included in this page can be a link towards the ToS, the Privacy Statement, and the registration number under which the processing is to be found in the CBP registry. Such a page would leave no doubt as to whether the client is properly informed on what data is being processed and by who.

Also, each time a ToS or Privacy statement is changed, this could be made clear by stating the version number of the document, along with the date on which it was changed. For completeness, a record could be kept of previous documents, along with the changes that have been made, so that the customer knows exactly how things have changed and can take appropriate action if desired. Such an overview of documents might be confusing to customers as they might not know which version applies to them, therefore this should also be communicated clearly.

> Notify the CBP on the intent to process data.

Once the identity, nature, and purpose of processing are described, this can easily be notified towards the CBP. This is something which is a legal requirement, although there are a few exceptions to this processing. With energy consumption data, which is being processed through electronic means however, no exceptions apply and a notification must be made.[217]

> Make detailed consumption data available to the data subject, in an understandable format and in a timely manner, as to facilitate self-regulation by the data subject.

The main service that HEMS provide is insight into energy consumption data in such a way as to facilitate self-regulation, and it is thus in the best interest of the HEMS suppliers (be they energy suppliers, or VAS) to provide their clients with the best possible information to keep the client satisfied. As to what an understandable format is exactly, this is the domain of human-computer interaction and website and graphical design.

> Present such data free of charge.

This legal requirement only applies to energy suppliers. Although the HEMS service, with as much detail and additional services as currently provided by for instance Toon, can not be free due to the costs made by Eneco and Quby, a basic functionality that presents a daily load graph based on P4 data and accessible through for instance a web portal should be offered for free to those end-users that consent to the processing of their P4 data.

The argument can be made that detailed information is made available via the P1 port, thus fulfilling the legal requirement of making detailed information available. However, the form of data (telegrams) that is available, and the means by which it can be accessed prevents regular users at this moment from utilizing this information, certain without making an investment

[217] See http://www.cbpweb.nl/Pages/ind_melden.aspx, last referenced August 10 2013.

in hardware and software to access this port and to process the telegrams in order to produce legible graphs. The current situation however, is that detailed consumption data, with a level of detail on par with the capabilities of the Smart Meter, in a legible form, is not available to the consumer for free from the energy suppliers.

> Implement appropriate technical and organizational measures to protect this personal data.

Regarding organizational measures to protect data, this is not possible to assess without having full access to the organizations processing the data. With regards to information security management, there are ISO standards with detailed recommendations on what measures to implement.[218]

Regarding technical measures, there are some basics that should be kept in mind. If using a web portal, make sure that this is using HTTPS (digital certificates) so that authenticity and confidentiality are protected up to the web browser.[219] If using wireless communications of any sort, implement a strong form of encryption such as AES-128, broadcasting plaintext messages should not take place. Secured connections often require keys, which should be revocable and replaceable if compromised. As with the case of the Smile P1 and its PSK, although the key conforms to the minimal requirements as stated by in the WPA/WPA2 standard of 8 characters, there is no reason not to make this key longer in order to significantly increase the keyspace. Also, such a PSK should be revocable and replaceable.

As a last recommendation, the design of the system and the protocols should not be closed. The more people are allowed to examine a system, the more likely flaws in the design will be noticed and can be disclosed to the designers, who can mitigate such issues.

> *”The design of a system should not require secrecy and compromise of the system should not invoncenieuce the corerspondents”*
> Auguste Kerckhoffs 1883

> *”The enemy knows the system”*
> Claude Elwood Shannon 1940

[218] The ISO 27000 series.

[219] It is possible to gain access to personal data through the accessing of the computer that is accessing the web portal. This is however not the responsibility of the HEMS supplier, but of the data subject as it is his computer that is vulnerable.

# 7 Discussion

The research topic is a difficult one. Although a legal framework can be explored in detail and all legislation is open to anyone who wants to explore it, the HEMS implementations are not. Without resorting to gaining physical access to each device and meticulously reverse engineering it and decompiling the code it contains there is no way to be certain that the system operates as stated. Although assumptions can be made, observations can be done, and questions can be asked to developers, chief technical officers, and customer services, there is no way to be absolutely certain that details are not left out, or are lost in the translation somewhere. Therefore, certainty is unobtainable, yet is strived for vigorously.

The number of HEMS explored is limited to just five, the selection being based on having a variation of protocols used in the data streams. The two main protocols in home automation and HEMS are Zigbee and Z-Wave, warranting their inclusion in this thesis through the exploration of Toon and the E-manager.[220] As not all HEMS employ hardware but rather rely on P4 data and a web portal, these needed to be included as well, as were systems by energy suppliers and strictly VAS.

The field of HEMS is still in its infancy as Smart Meters are only just being introduced. The inclusion of the P1 port on Dutch Smart Meters is unique in the smart metering market, making P1 devices a niche market compared to the overall number of Smart Meters that are being rolled out all over the EU.

Future research in the field of translating legal requirements into technical requirements is needed, as there is precious little research done in this field. Example should be taken from research such as by Cavoukian et al. (2010), on 'embedding privacy into the design of electricity conservation'. With the omnipresence of computer technology and the ever growing amount of connectivity (and cloud computing) and possibilities of data mining and big data, not only the possibilities of these technologies to provide services, but also the possibilities of these technologies to invade the personal life of individuals must be kept in mind. Although legislation is slowly catching up, with the current work in progress on a new Data Protection Regulation, which will replace the current Data Protection Directive, that stipulates data protection by design and by default[221], at this moment, data protection by design is not the focus of information technologies, who would rather have a working system first, and worry about data protection later. Although this is a bold claim, there are ample examples to be found of systems that work, but where data protection was an afterthought, improperly implemented, or systems even being implemented even after a vulnerability

[220] Knight (2006), Galeev (2006).

[221] GDRP, Art. 23.

being discovered.[222]

Of particular interest with the HEMS discussed is the use of the Zigbee and Z-Wave protocols. Both of which are used not only in households, but in hospitals and convention centres as well. It is the hope of the author that these two protocols will be the subject of scrutinization by hardware security experts to find out exactly how they operate, and if there are vulnerabilities that allow the manipulation of networks set up with these protocols.

[222] Consider for instance the use of the MiFare classic chip in the Dutch OV-chipcard after research has shown that this chip was broken, see: Verdult et al. (2008).

# 8 Conclusion

The first three chapters of this thesis served as an introduction of both the research question, and the field of smart metering. In particular, the third chapter detailed the different ports on the Smart Meter, and the type of data that these made available. Of interest for this thesis were the P1 port which supplies real-time energy consumption data with a granularity of ten seconds, and the P4 port which supplies historical energy consumption data, with a granularity of fifteen minutes. The data that these two ports supply was the focal point of the technical aspect of this thesis in that its transmission and storage was examined. In this chapter, the potential exploitation of the data from P1 and P4 was also discussed through examples of what can be learned about a household by examining energy consumption data.

Chapter four consisted of the examination of the legal framework surrounding personal data, which served the purpose of answering the first two sub questions. The first sub question was:

> What is personal data and is energy consumption data personal data?

An answer on the first section of this question was quickly found in the Data Protection Directive, which defines personal data as*”any information relating to an identified or identifiable natural person”*. When applying this definition to energy consumption data, the conclusion was drawn that it is indeed ’information’, because this data contains patterns that indicate that an appliance is being used, or even that a certain appliance is present, both of which are information. Energy consumption data has a relation with a person, for it says something about this person, such as this person being at home because certain appliances are switched on and off, which is related to the behaviour of this person. ’Identified or identifiable’ can be concluded from the information typically containing a unique identification code, which is coupled with a household such that billing is possible. Furthermore, although this number can be removed, the unique patterns within energy consumption data still allow for indirect identification. Lastly, a member of a household is a ’natural person’. Thus, after defining personal data, and holding this definition against energy consumption data, the conclusion was drawn that energy consumption data is personal data.

This gave rise to the second sub question, because if energy consumption data is personal data, there must be requirements to fulfil in order to be legitimately processing this data.

> What are the legal requirements to processing personal data?

Although there are numerous requirements for the processing of personal data as described in the Data Protection Directive, three in particular have been selected.

First, there are the grounds for processing, for without a legal ground, the processing of personal data is illegitimate. These grounds are: a) consent, b) to fulfil a contract, c) legal obligation, d) vital interest of the data subject, e) public interest, and f) legitimate interest of the data controller. Detailing on each of these grounds can be found in section 4.4 of this thesis.

The second requirement is that of data quality, the principles of which are stipulated in the Data Protection Directive in article 6. These principles are: a) fair and lawful processing, b) purpose specification, c) adequate, relevant and not excessive, and d) accurate and up to date. These principles were detailed in section 4.5 of this thesis.

The last requirement to be examined was that of Profile Transparency, which is mentioned in the Data Protection Directive, article 10 and detailed in section 4.6 of this thesis. Profile Transparency entails the obligation to inform the data subject about the processing if his data. This informing should at the very least contain the identity of the data controller, and the purpose for which processing of data is intended.

In summation, the legal requirements for the processing of personal data are the need for a legal grounds upon which processing may take place, the upholding of the data quality principles, and informing the data subject.[223]

Having explored the legal framework, a set of legal requirements was formulated at the conclusion of chapter four. This set of requirements would then be used in the upcoming chapter to examine the compliance of the HEMS with the legal framework. According to the requirements energy suppliers are required to:

1. have grounds upon which data processing is legitimised;
2. process personal data only for a specified purpose;
3. notify the data subject on this data processing, in for the data subject understandable language;
4. notify the CBP on the intent to process data;
5. make detailed consumption data available to the data subject, in an understandable format and in a timely manner, as to facilitate self-regulation by the data subject;
6. present such data free of charge;

[223] This is a very slim and incomplete summation, and serves merely as a rough indication. For details please reference the relevant sections of this thesis, along with all the relevant documents used in writing this thesis.

7. implement appropriate technical and organizational measures to protect this personal data.

Chapter five then explored a set of current implementations of HEMS. Each device was explored using the following two sub questions:

> Where is personal data stored within the HEMS, who are the controllers and processors, and who can access this information?

| HEMS | Storage | Controller | Processor | Access |
|---|---|---|---|---|
| Toon | Local | Eneco | Quby | Eneco, Quby, and *Eve*[224] |
| E-manager | Local and Servers of GR | Nuon | GR | Nuon and GR |
| Smile P1 | Servers of Plugwise | Plugwise | Plugwise | Plugwise and *Eve* |
| SMU.nl | Servers of Enepa | Enepa | Enepa | Enepa and *Eve* |
| SMP.nl | Servers of Oblivion | Oblivion | Oblivion | Oblivion |

This table does not cover the extent of details in the sections dedicated to each device, but it does serve as an overview of the devices, and through the access by 'Eve' to data within three of the HEMS', it is also immediately clear that something is wrong. This brings up the next sub question, concerning the security of the HEMS that were explored:

> What data flows are present in the HEMS, and are these secure?

Regarding the flow of data within each HEMS, please reference the figures mentioned in the table, including them in the conclusion of this thesis would make the conclusion needlessly large. Security of each flow was evaluated considering current technology.

After having answered this final sub question, the main question can be answered.

> Do the HEMS that are currently available in the Netherlands comply with the current legal framework? And if it turns out that there are compliance issues, what can be done to mitigate these compliance issues?

In comparing the five devices to the legal requirements, a table was created, wherein green signifies compliance, red signifies non-compliance, and

| HEMS | Flow | Protocols | Secure |
|---|---|---|---|
| Toon | Figure 4 | Z-Wave<br>SSL<br>VPN | No<br>Yes<br>Yes |
| E-manager | Figure 7 | Zigbee<br>SSL | Yes<br>Yes |
| Smile P1 | Figure 9 | WPA/WPA2 PSK<br>SSL | No<br>Yes |
| SMU.nl | Figure 11 | SSL<br>HTTP | Yes<br>No |
| SMP.nl | Figure 15 | SSL | Yes |

grey signifies non-applicable. The non-applicability of requirement number six comes from the fact that the suppliers of these devices are not energy suppliers and so are not obliged to provide the service free of charge.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Toon | 1 🟩 | 2 🟩 | 3 🟩 | 4 🟩 | 5 🟩 | 6 🟥 | 7 🟥 |
| E-manager | 1 🟩 | 2 🟩 | 3 🟩 | 4 🟩 | 5 🟩 | 6 🟥 | 7 🟩 |
| Smile P1 | 1 🟩 | 2 🟩 | 3 🟩 | 4 🟥 | 5 🟩 | 6 ⬜ | 7 🟥 |
| SMU.nl | 1 🟩 | 2 🟩 | 3 🟩 | 4 🟥 | 5 🟩 | 6 ⬜ | 7 🟥 |
| SMP.np | 1 🟩 | 2 🟥 | 3 🟥 | 4 🟥 | 5 🟩 | 6 ⬜ | 7 🟩 |

Although almost all the devices comply with requirements two and three, it should be noted that purpose and transparency were often stated in the ToS or Privacy Statement. These documents, by their very nature, were all more or less in 'legalese' or at least a bit technical in nature. Nevertheless, almost every company has stipulated explicitly what the purpose of processing is, and what data is being collected.

Having determined the flow of energy consumption data within each HEMS, examining what protocols were used in these flows, and if these protocols were considered secure, each HEMS was then compared to the legal requirements as described above. This resulted in the conclusion that the wireless protocols being used were insecure. This does not mean that all wireless communications are insecure however.

This thesis moves from the legal framework towards the technical implementations that are currently available and ends in a comparison of these implementations with the legal requirements as identified, in the search of an answer to the main research question.

The problem with the Smart Meters as they are currently installed is that the display on these devices is to small to offer proper insight into energy consumption data, although legislation states that there should be a visualization of energy consumption data detailed enough to influence consumer behaviour. As such, the conclusion is drawn that HEMS are an essential part of the Smart Meter and are thus a part of this system, because no default screen is supplied with the meter that fulfils this role in a satisfactory way.

As can be seen in Table 8, none of the HEMS investigated conform to all the requirements, with the most frequent compliance issues being data security, registration of the processing of personal data with the CBP, and in case of the supplier-supplied HEMS, adequate information being available for free.

The most straightforward method of mitigating all issues is supplying Smart Meters with an IHD that is large enough to display detailed consumption data. To prevent eavesdropping of wireless signals, this display should be able to be connected directly to the P1 port using a cable, wherein the length of cable can be easily customized to suit every situation. For those willing to accept the security vulnerabilities, a wireless option should also be available although this option must be turned off by default, and a physical switch is needed to turn it on so there can be no doubt as to whether a wireless signal is being broadcast. Such an IHD should have the option to connect to the HAN, although this should not be needed to perform the basic insight functions. Because this device does not communicate energy consumption data outside of the HAN without the data subject knowing this, his privacy is protected.

However, such a device would have two major drawbacks: First, it would decimate the current market for devices, as far as local availability of energy consumption data is concerned. Second, without setting up an Internet connection with this device in some form, the data would not be available from outside of the home, vastly reducing the usability.

In conclusion, although most HEMS are not for free, download numbers of the various applications and sales numbers suggest that customers are willing to pay for detailed energy consumption data. However, just because most people are unaware of the possible implications of energy consumption data leakage does not mean that companies selling HEMS are exempted from their obligation to provide the best possible data protection in order to secure the personal data of their customers. As it stands, energy consumption data is not secured properly, and although it might take some technical skill and time, the neighbours can listen in.

# Glossary

Authenticity

"In the academic literature on security protocols, authenticity means integrity plus freshness: you have established that you are speaking to a genuine principal, not a replay of previous messages." (Anderson (2008), p14.)

Availability

Availability means that the data and the system resources are available (ready to use) when needed, to those parties which are authorized.

Confidentiality

The obligation to protect a secret, which in computers means that unauthorized access is not possible and eavesdropping is unsuccessful; the data should be kept secret from parties who do not have the legitimate right to access this information.

Data Controller

"The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purpose and means of processing of data" (Directive 95/46/EC, Art 2.d)

Data processing

"any operation or set of operations which is performed upon personal data, where or not Ay automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction". (Directive 95/46/EC, Art. 2.b.)

Data processor

"A natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller." (Directive 95/46/EC, Art. 2.e)

Data subject

"An identified or identifiable natural person' (Directive 95/46/EC, Art. 2.a.) 'to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable." (Ibidem, Recital 26.)

Encryption

The act of making data in a computer unintelligible, governed by an encryption key creating a cyphertext, with the possibility of reversal if the protocol and decryption key are known thus recovering the plaintext. Note that although encryption and decryption can use the same key (symmetric encryption), there are also encryption protocols that require separate keys for encryption and decryption (asymmetric encryption) such that what is encrypted with one key, can only be decrypted with the other.

Home Area Network (HAN)

A local area network that is situated within the household, connecting computers, devices and sensors together.

Home Energy Management System (HEMS)

An electronic devices giving feedback to the end-user on his energy consumption. This device can be a website displaying energy consumption data graphs, an in-home display, a smart device application, or a combination of these.

In-Home Display (IHD)

A physical display that presents data on devices and sensors within the HAN, typical information is energy consumption as measured by the Smart Meter, but other possibilities exist such as temperature readouts, messages from the energy supplier, even traffic information.

Integrity

Integrity is about the verification of data, such that accidental or malicious changes are prevented, yet if changes do take place for whatever reason, they do not go unnoticed.

Low-voltage network manager

Low-voltage network managers are one of the three types of network managers within the Netherlands. At the highest level there is TenneT, who manages the high-voltage network or grid that connects the regional nets together, and connects the Dutch grid to the surrounding countries. At the middle level are the middle-voltage network managers, who manage the regional branches. Finally, the low-voltage network managers form the connection between the regional branches and individual households (meters).

Non-repudiation

The inability to deny an action; if a party undertakes an action it can not, at a later moment in time, deny that it undertook this action, because this action has been logged in some way.

P1 port (P1)

A physical port on the Smart Meter consisting of an RJ11 connector (the same connector as can be found on the end of a telephone wire), also known as the consumer port, that allows for one-way communication with systems to connect to the Smart Meter and request data output on current power consumption, with a high frequency of ten seconds. The output messages of the P1 port are called telegrams.

P2 port (P2)

A physical port on the Smart Meter that allows for two-way communication with the Smart Meter, which is used by other meters such as gas and water meters.

P3 port (P3)

A physical port on the Smart Meter that allows for two-way communication between the Smart Meter and the low-voltage network manager. This port can take various forms, allowing communication using GPRS, PLC, or other technologies.

P4 port (P4)

A virtual port *not* on the Smart Meter that allows for two-way communication between the low-voltage network manager and EDSN. The data from this port is shared by EDSN with VAS, energy suppliers and network operators for, service providence, load balancing, and billing purposes.

Personal data

"'Personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identity number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." (Directive 95/46/EC, Art. 2.a)

Secure Socket Layer (SSL)

A protocol that enables an encrypted link between two computers via the Internet. This protocol prevents interception (eavesdropping) and allows a computer to identify the other computer (usually a server) it is communicating with.

Smart Grid

The Smart Grid is the next generation of the electricity grid that will allow not only for the distribution of electricity towards the consumer, but also for the consumer to supply electricity back to the grid. With the aid of the smart metering system, information on consumption and production will facilitate load balancing and grid management.

Smart Metering system (Smart Meter)
An electronic system that can measure energy consumption, adding more information than a conventional meter, and can transmit and receive data using a form of electronic communication.

Telegram
The high frequency message containing detailed information on energy consumption that is send out through the P1 port upon request by a device connected to this port. An example telegram can be seen on page 9.

Value-added services provider (VAS) Any independent service party that is not an energy supplier, grid operator or network manager that provides services for which they need access to energy consumption data. In the Netherlands these go by the name of Overige Dienst Aanbieders or ODA's. Also known as Energy service company or ESCO.

Virtual Private Networking (VPN)
An implementation of a virtual network that ensures two-way secure communications between the stations. A virtual network is a specified group of computers that can communicate with each other without noticing other computers on the physical network.

Z-Wave
Z-Wave is proprietary wireless communication protocol aimed at the residential control and automation market.

Zigbee
Zigbee is a low power and low data-rate wireless communication protocol with a maximum throughput of 250 Kbps, a small stack of just 120 KB with a range of ten to one hundred meters that builds upon the IEEE 802.15.4 standard.( Baronti et al. (2007))

# References

Anderson, R. (2008). *Security engineering*. Wiley .com.

Anderson, R., & Fuloria, S. (2010). Who controls the off switch? In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, (pp. 96–101). IEEE.

Baronti, P., Pillai, P., Chook, V., Chessa, S., Gotta, A., & Hu, Y. (2007). Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and zigbee standards. *Computer communications*, *30*(7), 1655–1695.

Benders, R., Kok, R., Moll, H., Wiersma, G., & Noorman, K. (2006). New approaches for household energy conservation - in search of personal household energy budgets and energy reduction options. *Energy policy*, *34*(18), 3612–3622.

Benzi, F., Anglani, N., Bassi, E., & Frosini, L. (2011). Electricity smart meters interfacing the households. *IEEE Transactions on Industrial Electronics*, *58*(10), 4487–4494.

Bogdanov, A., Khovratovich, D., & Rechberger, C. (2011). Biclique cryptanalysis of the full aes. In *Advances in Cryptology–ASIACRYPT 2011*, (pp. 344–371). Springer.

Braat, J. (2011). De slimme meter: welke waarden mogen standaard worden opgehaald? *Privacy & Informatie*, (6), 292–298.

Carluccio, D., Brinkhaus, S., Löch, D., & Wegener, C. (2011). Smart hacking for privacy. *Behind Enemy Lines, 28C3*.

Cavoukian, A., Polonetsky, J., & Wolf, C. (2010). Smartprivacy for the smart grid: embedding privacy into the design of electricity conservation. *Identity in the Information Society*, *3*(2), 275–294.

CE Delft, & KEMA (2012). Maatschappelijke kosten en baten van intelligente netten. *Rapport in opdracht van Ministerie van Economische Zaken, Landboud en Innovatie (Delft, maart 30, 2012).*

Cleveland, F. (2008). Cyber security issues for advanced metering infrasttructure (ami). In *Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE*, (pp. 1–5). IEEE.

Cuijpers, C. (2011). Slim kiezen bij slimme meters. *Privacy & Informatie*, (3), 133–144.

Darby, S. (2006). The effectiveness of feedback on energy consumption. *A Review for DEFRA of the Literature on Metering, Billing and direct Displays*, *486*, 2006.

Darby, S. (2010). Smart metering: what potential for householder engagement? *Building Research and Information*, *38*(5), 442–457.

Dini, G., & Tiloca, M. (2010). Considerations on security in zigbee networks. In *Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC), 2010 IEEE International Conference on*, (pp. 58–65). IEEE.

Efthymiou, C., & Kalogridis, G. (2010). Smart grid privacy via anonymization of smart metering data. In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, (pp. 238–243). IEEE.

Farhangi, H. (2010). The path of the smart grid. *Power and Energy Magazine, IEEE*, *8*(1), 18–28.

Galeev, M. (2006). Catching the z-wave. *Embedded Systems Design*, *19*(10), 28.

Garcia, F., & Jacobs, B. (2011). Privacy-friendly energy-metering via homomorphic encryption. In *Security and Trust Management*, (pp. 226–238). Springer.

Greveler, U., Justus, B., & Loehr, D. (2012). Multimedia content identification through smart meter power usage profiles. *Computers, Privacy and Data Protection*.

Gungor, V., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., & Hancke, G. (2011). Smart grid technologies: communication technologies and standards. *andustrial informatics, IEEE transactions on*, *7*(4), 529–539.

Hart, G. (1989). Residential energy monitoring and computerized surveillance via utility power flows. *Technology and Society Magazine, IEEE*, *8*(2), 12–16.

Hart, G. (1992). Nonintrusive appliance load monitoring. *Proceedings of the IEEE*, *80*(12), 1870–1891.

Hildebrandt, M. (2013). Legal protection by design in the smart grid.

Hoenkamp, R., Huitema, G., & de Moor-van Vugt, A. (2011). The neglected consumer: the case of the smart meter rollout in the netherlands. *Renewable Energy Law and Policy (RELP)*, *4*, 269–282.

Inoue, M., Higuma, T., Ito, Y., Kushiro, N., & Kubota, H. (2003). Network architecture for home energy management system. *Consumer Electronics, IEEE Transactions on*, *49*(3), 606–613.

Kahn, D. (1967). *The Codebreakers: The story of secret writing*. Simon and Schuster.

Khurana, H., Hadley, M., Lu, N., & Frincke, D. (2010). Smart-grid security issues. *Security and Privacy, IEEE*, *8*(1), 81–85.

Kirmse, A. (2012). Privacy in smart homes. In *ComSys Seminar: Advanced Internet Technology SS2012*.

Knight, M. (2006). How safe is z-wave?[wireless standards]. *Computing and Control Engineering*, *17*(6), 18–23.

Knyrim, R., & Trieb, G. (2011). Smart metering ander eu data protection law. *International Data Privacy Law*, *1*(2), 121–128.

Koops, E., & Cuijpers, C. (2009). Begluren en besturen door slimme energiemeters: Een ongerechtvaardigde inbreuk op onze privacy. *Privacy & Informatie*, (1), 2–7.

Kotschy, W. (2010). General rules on the lawfulness of the processing of personal data. In T. Dreier, C. Gielen, & R. Hacon (Eds.) *Conside European IT law, second edition*, (pp. 49–64). Kluwer Law International.

Kuner, C. (2007). *European data protection law: corporate compliance and regulation*. Oxford University Press.

Kursawe, K. (2012). Privacy in the smart grid. *Presentation at the PI. Lab launch, Tilburg - 13 april 2012*.

Kursawe, K., Danezis, G., & Kohlweiss, M. (2011). Privacy-friendly aggregation for the smart-grid. In *Privacy Enhancing Technologies*, (pp. 175–191). Springer.

Lam, H., Fung, G., & Lee, W. (2007). A novel method to construct taxonomy electrical appliances based on load signaturesof. *Consumer Electronics, IEEE Transactions on*, *53*(2), 653–660.

Lewis, R., Igic, P., & Zhou, Z. (2009). Assessment of communication methods for smart electricity metering in the uk. In *Sustainable Alternative Energy (SAE), 2009 IEEE PES/IAS Conference on*, (pp. 1–4). IEEE.

McDaniel, P., & McLaughlin, S. (2009). Security and privacy challenges in the smart grid. *Security and Privacy, IEEE*, *7*(3), 75–77.

Metke, A., & Ekl, R. (2010). Security technology for smart grid networks. *Smart Grid, IEEE Transactions on*, *1*(1), 99–107.

Molina-Markham, A., Shenoy, P., Fu, K., Cecchet, E., & Irwin, D. (2010). Private memoirs of a smart meter. In *Proceedings of the 2nd ACM workshop on embedded sensing systems for energy-efficiency in building*, (pp. 61–66). ACM.

Morch, A., Parsons, J., & Kester, J. (2007). Smart electricity metering as an energy efficiency instrument: Comparative analyses of regulation and market c anditions in europe. In *ECEEE-Summer Study*.

Nouwt, S. (2008). Reasonable expectations of geo-privacy. *SCRIPT-ed*, *5*(2), 375–403.

Quinn, E. (2009). Smart metering & privacy: Existing law and competing policies.

Schnabel, C. (2009). Privacy and data protection in ec telecommunications law. In C. Koenig, & A. Bartosch (Eds.) *EC competition and telecommunications law*. Kluwer Law International.

Slootweg, J., Cordova, J., Montes Portela, C., & Morren, J. (2011). Smart grids - intelligence for sustainable electrical power systems. In *Telecommunications Energy Conference (INTELEC), 2011 IEEE 33rd International*, (pp. 1–8). IEEE.

Son, Y., Pulkkinen, T., Moon, K., & Kim, C. (2010). Home energy management system based on power line communication. *Consumer Electronics, IEEE Transactions on*, *56*(3), 1380–1386.

Struik, R. (2005). Formal specification of the ccm* mode of operation. *IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs)*.

te Paske, B., Cuijpers, C., van Eekelen, M., Poll, E., & van Schoonhoven, B. (2012). Risicoanalyse slimme meter keten, privacy en security in het nieuwe marktmodel.

Van De Zande, P. (2001). The day DES died, whitepaper. *SANS Institute, July*.

Verdult, R., Garcia, F., de Koning Gans, G., Muijrers, R., Van Rossum, P., Schreur, R., & Jacobs, B. (2008). Dismantling mifare classic. In *Computer Security-ESORICS 2008*, (pp. 97–114). Springer.

Zigbee Alliance (2007). Zigbee and wireless radio frequency coexistence, zigbee whitepaper. *Document 075026r02. June*.

# Legal References

## Directives

Data Protection Directive
Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

e-Privacy Directive
Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector

Directive 2009/72/EC
Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC Text with EEA relevance

Directive on energy efficiency
Directive 2012/27/EU of the European Parliament and of the Council of 25 October 2012 on energy efficiency, amending Directives 2009/125/EC and 2010/30/EU and repealing Directives 2004/8/EC and 2006/32/EC

## Article 29 Working Party

29WP on RFID technology
Working document on data protection issues related to RFID technology, 19 January 2005.

29WP Opinion 4/2007
Article 29 Working Party, 'Opinion 4/2007 on the concept of personal data', June 20 2007.

29WP Opinion 1/2008
Article 29 Working Party, 'Opinion 1/2008 on data protection issues related to search engines', 4 April 2008.

29WP Opinion 12/2011
Article 29 Working Party, 'Opinion 12/2011 on smart metering', 4 April 2011.

29WP Opinion 15/2011
Article 29 Working Party, 'Opinion 15/2011 Consent', 13 July 2011.

29WP Opinion 03/2013
Article 29 Working Party. 'Opinion 03/2013 on purpose limitation', 2 April 2013.

## Dutch legislation

Wet Bescherming Persoonsgegevens
Wet Bescherming Persoonsgegevens, Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens).