# Smart metering in the Netherlands: what, how, and why

Pol Van Aubel and Erik Poll
Digital Security group, Institute for Computing and Information Sciences, Radboud University
{pol.vanaubel,erikpoll}@cs.ru.nl

***Abstract*—This paper describes the functionality and realisation of the smart metering infrastructure in the Netherlands, and discusses the changes that have been made in plans in response to privacy and security concerns. We also discuss the rationale for introducing smart meters – which is less clear than one would expect or indeed hope – and ongoing developments in the use of smart metering information in local energy community pilots.**

## I. Introduction

THE advent of smart electricity meters sparked a lot of public debate and media attention in the Netherlands in 2008. The debate has involved grid operators, privacy advocates, politicians, security experts, consumer interest groups such as the Dutch consumers' and homeowners' associations. A decade onwards, the debate still does not seem to be completely settled.

In 2014 the Dutch government decided to go ahead with the roll-put of smart meters to every home [1]. The reported numbers – nearly 3 million households equipped with a smart meter at the end of 2016 [2] – suggests the roll-out is on track to reach the target mentioned in EU Directive 2009/72/EC [3], namely that 80% of households have a smart meter by 2020.

The set-up of a smart metering infrastructure – or Advanced Metering Infrastructure (AMI), to use the technical term – involves many design choices. A global overview of the communication technology and trends of smart metering can be found in [4], [5]. Although the Netherlands is discussed briefly, we feel a more detailed review is warranted. It is interesting to review how and why certain choices have been made in the Netherlands, also to be able to compare different approaches between countries. It is not easy to find this information: it is scattered over many documents, mostly in Dutch, and typically without any discussion of motivation or rationale. This paper aims to give an overview accessible to an international audience.

Section II describes the smart metering infrastructure as deployed in the Netherlands, from both a technical and an organizational point of view. Section III then discusses security and privacy issues that were raised and how they were dealt with, as well as some incididents – data leaks – that happened. Section IV discusses the rationale for smart meters given the current use and Section V discusses more intensive use of smart metering information in pilots with microgrids. We draw our main conclusions in Section VI.

This work is supported by the EU Regional Development Fund (EFRO), as part of the project BES (Betuwse Energie Samenwerking).

## II. The Advanced Metering Infrastructure

This section describes the AMI as is it deployed in the Netherlands: the parties involved, the functionality of the smart meters, which information is collected and exchanged, and how it is exchanged. The main parties involved in the metering infrastructure are illustrated in Fig. 1 and discussed below.

The *Distribution System Operator (DSO)*, or *grid operator* is responsible for the operation of the electrical grid at a regional level. The DSO is typically also responsible for the installation of smart meters and for collecting meter readings. The Dutch DSOs are united in a collaborative industry body called Netbeheer Nederland (literally 'Netherlands Grid Management'). This organization establishes and publishes e.g. the common terms of service for electricity transport and smart meter standards. There are 7 DSOs in the Netherlands, with the 3 biggest – Liander, Enexis, and Stedin – serving the bulk of the country.

The *energy suppliers (energy suppliers)* are the commercial parties that produce or buy electricity and sell it to consumers. They use the infrastructure of the DSO to deliver this electricity. Formerly, a single utility would act as both DSO and ES, but since the liberalization of the energy market in 1998 these roles have been separated, allowing customers to freely choose their energy supplier, while the DSO retains its regional monopoly.

With the introduction of smart meters came a new category of parties: the *Independent Service Providers (ISPs)*[1]. ISPs use meter readings to offer additional services, e.g. providing more detailed insight in electricity, say via a smartphone app, or more generally giving advice on how to save energy. ISP can offer such services to households or businesses. As a concrete example, an ISP can offer a supermarkt chain insight in energy use across all their stores.

To bill a customer, the energy supplier needs the relevant meter readings for the responsible DSO. Rather than broker many-to-many relationships between DSOs and energy suppliers, the Dutch DSOs have set up *Energie Data Services Nederland (EDSN)* as a central organization to smooth the administrative processes. EDSN's responsibilities include providing metering data to energy suppliers and ISPs, irrespective of the DSO responsible for the region where a customer is located. Prior to the introduction of smart meters EDSN already provided one common interface for energy suppliers to get meter readings, which were then still manually collected

[1] In Dutch, Overige Diensten-Aanbieders (ODA's).

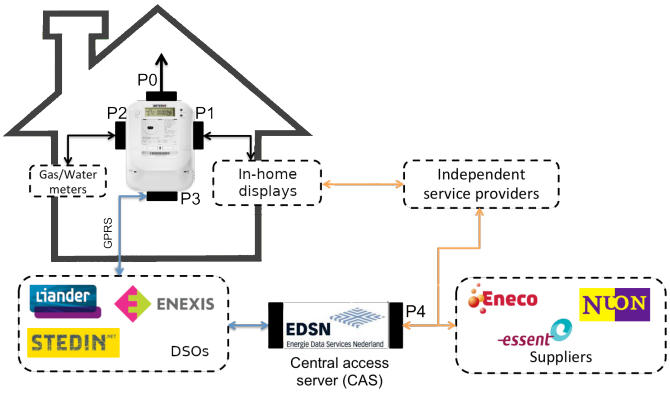


Fig. 1. Standardized smart meter

by the DSOs. EDSN also records for each connection which energy supplier is contracted to deliver electrity.

### A. The Smart Meter

The Dutch Smart Meter Requirements (DSMR) [6] and its companion standards [7] lay down the specifications of smart meters. As most houses in the Netherlands also have a natural gas connection, smart meters meter both gas and electricity. Several versions of the DSMR specs exist; the most recent publicly available version is 4.0.7. Before the introduction of the DSMR, requirements for smart meters were given in a first technical spec NTA 8130 [8], but also in legal documents such as amendments to the Dutch Energy Act [9].

The DSMR specifies that smart meters record and store the following measurements, for the DSO to retrieve them (via port P3, as explained in more detail below):

- daily and monthly aggregate measurements, namely
  - the 40 most recent daily readings;
  - the 13 most recent monthly readings;
- interval measurements for the last 10 days, namely
  - electricity measurements in 15-minute intervals;
  - gas measurements in hourly intervals.

In addition, the following measurements are made available to the consumer (via port P1):

- electricity meter readings every 10 seconds, which are not stored in the meter;
- the most recent gas meter reading;
- equipment status, including tariff information.

The meter can display messages sent by the DSO to the meter. The meter itself can display up to 8 characters. Longer messages of up to 1024 characters can be forwarded for display on consumer equipment.

Besides energy consumption, the meter also measures power quality and outages. It supports time synchronization and shifting between tariffs. The meter has to have some tamper detection, and at least the past 30 attempts to tamper with the meter have to be stored. Here tampering means physical tampering, such as removing the meter's cover, but meters are also required to detect magnetic fields that may interfere with meter.

### B. Physical Communication Infrastructure

The smart meter has 4 communication ports.

*The P0 port* is used for local connection during installation and maintenance work.

*The P1 port*, also called the consumer port, allows for communication with third party equipment locally installed at the consumer's house. The port only supports communication from the meter to this equipment, not the other way around. Via P1 the meter provides real-time measurements, in 10-second intervals, and it can be used to display messages on the connected equipment.

*The P2 port* connects to other local metering equipment. The typical use is that a smart gas meter connects to P2. This port can be wired or – more commonly – wireless. The gas meter sends its measurements to the electricity meter once per hour, which can then store and forward these.

*The P3 port* communicates with the DSO, for sending meter readings (either the stored readings or the current meter readings), status checks, power quality and outage measurements, and remote updates. Unlike P1, P3 supports two-way communication. Generally, communication between P3 and the DSO happens via GPRS, CDMA, or LTE. Earlier meters used a combination of Power Line Communication (PLC) with GPRS, where information was sent via PLC to a data concentrator located in the nearest substation which then forwarded information via GPRS. Since the DSMR version 4 [6], all meters communicate wirelessly, and PLC is no longer considered for use.

The P3 port uses the international standard IEC 62056 DLMS/COSEM [10] as communication protocol. This protocol defines a manufacturer-independent way to identify, retrieve and interpret the information held in any meter.

*The P4 port* is the gateway for energy suppliers and ISPs to obtain P3 measurements. It is a webservice to access the *Central Access Server (CAS)* of EDSN. It allows an energy supplier or ISP to obtain metering data of its customers, irrespective of the responsible DSO. In the current set-up, metering data is not pro-actively collected by EDSN into a central database. Instead, the metering data is only stored in the meter. When an energy supplier or ISP requires metering data of one of its customers, it first has to request the data from EDSN; EDSN forwards this request to the responsible DSO, which in turn retrieves the data from the customer's meter via P3 and sends it to EDSN. EDSN caches the data, and the energy supplier or ISP has to contact EDSN again, the next day, to retrieve the data. Of course, energy suppliers and ISPs then typically will store the data they retrieved in their own databases.

So the difference between P1 and P3 data is not just that P3 data is much less fine-grained (15 minute instead of 10 seconds intervals), but also that P3 data is not available in real-time, as the process of collecting the data via P4 can take up to 24 hours.

### C. Security Overview

The physical communication infrastructure outlined above comes with some technical security measures.

Smart meters have cryptographic keys to secure communication with the DSO via P3: the data sent to the DSO can be authenticated and encrypted. For a short overview of the options this provides, we refer to [11]. Smart meters also have keys to authenticate firmware updates.

However, at least some of the existing options for cryptographic authentication in DLMS/COSEM have shortcomings, as shown in [12], [13]. Moreover, whether these options are used is up to the DSO[2].

Unlike communication between the meters and the DSO, communication between EDSN and an energy supplier or ISP is over the public internet. This communication is secured with TLS using client and server certificates. Note that, even though the current version of DLMS/COSEM supports this in principle, there is no end-to-end security from the meter to the energy supplier or ISP – they have to trust the DSO to supply the correct data.

Unlike P3 data, P1 data cannot be authenticated. This may become an issue if in future evolutions of the grid one would want to use P1 data for grid control, as discussed in Section V

### D. Information Flows

The smart metering infrastructure provides information to DSOs, to energy suppliers and ISPs, and to the customer.

*1) Metering Data for DSOs:* The code of conduct of the Dutch DSOs [14] describes in detail why and when certain metering data is read by DSOs. All DSOs are legally obliged to conform to this code of conduct. It also describes the cases where the DSO reads P3 data in order to send to third parties, so it gives insight into the data flows from the smart meters to ISPs and energy suppliers. As all of this only involves P3 data, it is never more detailed than 15-minute intervals.

The scenarios in the code of conduct are based on the DSO's legal obligations and fall in four main categories:

- grid management, i.e. processing by the DSO itself to perform its legally mandated primary task;
- meter management, incl. communication with the meter to ensure it is functioning correctly;
- experimentation, innovation, and open data, i.e. rules for piloting new projects and providing anonymized data to other parties; and
- market facilitation, i.e. providing metering data to ISPs and energy suppliers.

The scenarios for *grid management* show that DSOs use power quality data for outage detection, analysis, and prediction, and for power quality monitoring. For detecting electricity loss, theft, or fraud, the consumption data is also used. As this is integral part of the DSO's legally mandated task the DSO is not required to get consumer permission for these readings. However, if the consumer has chosen to administratively disable their meter, as explained in Section III-B, it will not be read for these purposes either.

[2] In personal communication, one foreign DSO noted that noise in PLC communication caused loss of a significant, but acceptable, number of messages. When they enabled the 'High-Level Security' (HLS) option for DLMS/COSEM in their smart meters, the authentication data increased the message length to the point beyond which transmission reliability degraded to an unacceptable level. This made it impossible to use HLS.

For *meter management*, the DSO can read all the information for a short period, at most ten days, to verify that a newly installed or updated meter is functioning correctly. Even if the consumer has administratively disabled their meter, the DSO can perform these measurements, as well as communicate with it for performing clock updates, firmware updates, and other maintenance-work.

The clause on *experimentation and innovation* in the code of conduct encompasses the reading of metering data for the purposes of research and pilot projects, as well as reuse of aggregated data read previously. The former is only done with consumer consent, the latter is deemed acceptable regardless since it is aggregated data. To give an example, a research project could be aimed at developing models of the electricity use in a neighbourhood to aid in the planning of the electricity grid in a new neighbourhoods, or revisions to existing grid. The clause on *open data* is a broad clause to enable the publishing of data for the purposes of efficient market operation and enabling new services. This is, again, done either through reuse of aggregated data read in the past, or with new data read after getting user consent.

*2) Metering Data for energy suppliers and ISPs:* The code of conduct for the DSOs also indicates the obligations and restrictions for DSOs to provide data to energy suppliers and ISPs:

- a DSO has to provide meter readings to the energy supplier every two months, as well as incidentally on request from the energy supplier;
- if customers give permission to their energy supplier or ISPs to access the 15-minute interval values, a DSO must provide these upon request from these parties.

Obviously the *energy supplier* need access to metering data for billing. For this they currently do not need detailed readings: billing usually happens annually, or at most monthly, and energy prices for customers do not fluctuate on a daily basis. Therefore, monthly or even annual readings would suffice.

Instead of obtaining the 15-minute interval data via P3 via the DSO and EDSN, an ISP can also obtain data via the P1 port. They then have to a consumer with a device to attach to P1 to send back data, e.g. via that customer's internet connection. This information flow then circumvents the DSO and EDSN.

*3) Feedback to Consumers:* One way in which all consumers receive information from their smart meter is via bi-monthly usage summary from their energy supplier. There is now a legal requirement that the energy suppliers must provide a bi-monthly usage summary to their customers. Research from the Dutch association for home-owners showed that a third of consumers do not receive a bi-monthly summary at all, and that many summaries that are received do not conform to legal requirements and are confusing to consumers [15].

Consumers can obtain additional information via an ISP, or via their energy supplier if it offers services for this. Some ISPs and energy suppliers can provide an in-home display for feedback that obtains data via P1. Such a display can then also stream P1 data back to the ISP or energy supplier via the internet, as mentioned earlier. Alternatively, feedback to customers can be based on P3 data presented via a smartphone

app or website. Advantage of this is it does not involve additional equipment or installation hassle to connect such equipment with the local P1 port. Downside is of course that this cannot provide information about the energy usage in real-time. An annual report by the government agency RVO [2] monitors the adoption of energy management services that use P1 or P3 data, via apps, websites, and in-home displays.

## III. Security and Privacy

Some aspects of the smart meter infrastructure in the Netherlands have changed considerably since the first proposals, partly in response to the public debate about privacy. In the DSMR specs these changes are still visible: each requirement is listed with the year of introduction and source that it is based on. This section discusses the key issues and decisions, and discusses some of the security incidents – all data leaks – to date.

### A. The remote off-switch

A remotely operated off-switch in a smart meter can be convenient: if a household needs to be disconnected, it can be done without having to send out an engineer. However, it is also a security risk [16]: attackers might abuse it to disconnect households or cause serious chaos by disconnecting hospitals and police stations. This was also an important point of contention during the pilot phases in the Netherlands. The DSOs recognized this risk, and the remote off-switch was abolished when the large-scale rollout of smart meters started [1]. Meters installed before that time received a firmware update to disable this functionality permanently. Meters that could not be updated are considered in a periodic risk analysis. Presumably the cost of replacing them was deemed to outweigh the security risk. The requirements that meters should be able to receive firmware updates was already included in NTA 8130 [8]. It is unclear to us how many meters could not be updated to disable the remote off-switch.

### B. Privacy

Meter readings at 10-second intervals reveal a lot of private information. Research shows that this can reveal which TV shows are being watched or whether a newborn child is in the home [17], [18]. But even meter readings at 15-minute intervals provide a detailed view into someone's personal life.

Initial proposals of laws for smart meter roll-outs did not consider consumer privacy beyond complying with the Dutch data protection act, and ran foul of article 8 of the European Convention on Human Rights. Mainly for that reason the First Chamber of Parliament blocked them from passing in their initial form. Only after several amendments did these laws pass. For a detailed account, see [19]. These amendments removed the obligation to have smart meters: people could refuse installation and, if a smart meter had already been installed, they would be able to have it 'administratively turned off'. The amendments also included regulations on the collection, storage, and forwarding of metering data, and required explicit consumer consent for 15-minute and daily measurements, instead of this being the default metering regime.

If a meter is turned off administratively, consumption data and power quality data are no longer read remotely. The DSO can only communicate with the meter to ensure its proper functioning as an electricity meter, and to provide firmware updates. In 2017, around 10% of consumers refused installation of a smart meters and 2% had them turned off administratively [2].

Since the passing of these laws, DSOs, energy suppliers, and ISPs have all deposited codes of conduct with the Dutch data protection authority, in which they confirm this policy of explicit consent [14], [20], [21]. The code of conduct of DSOs makes a distinction between privacy-sensitive metering data and metering data that has no impact on consumer privacy. Only the actual energy usage readings and the power quality (as opposed to voltage quality) readings are privacy-sensitive [14]. Power quality is related to power draw, and therefore to energy usage behaviour. Voltage quality and information about the meter itself, such as low-battery events and reachability, are not considered privacy-sensitive.

Another design decision taken for privacy reasons is the decision not to have a central storage of meter readings by DSOs. Metering data is only stored in the smart meter itself. At the request of an ISP or energy supplier the DSO will retrieve the data, but it will not keep a copy, or proactively collect data from meters to store in a central database.

Note that there is a trade-off between privacy and availability here: downside of the current approach is that should a meter malfunction, the metering data would be lost, including the monthly readings for the past year used for billing. Billing could then be based on best-guess estimates or data kept by the energy supplier for the bi-monthly summary, but the energy supplier is of course not an independent party, like the DSO is, when it comes to billing.

The clauses on open data in the codes of conduct, mentioned in Section II-D, show a very simplified view of the intricacies of data (de-)anonymization and aggregation, which should be adequately considered when publishing (anonymized) personal data for third parties. Publishing anonymized data, when done incorrectly, runs the risk of deanonymization [22].

### C. Procurement, Compliance and Assurance

Taking security into account requires special care in the public tendering process for smart meter. One issue is how security requirements are expressed in tenders. If the description of security requirements is too vague, suppliers may be able to argue that less secure meters meet them, resulting in a race to the bottom. Conversely, if requirements are too detailed or specific, there is the risk that only a single supplier can meet them, who can then set a very high price. Another issue is defining procedures and processes for security testing of meters.

The expert organization ENCS stepped in to help both with specifying security requirements in tenders [23] and with testing smart meters considered for roll-outs [24]. ENCS (European Network for Cyber Security) is a non-profit member

organization that supports the deployment of secure solutions for energy grids and infrastructure by bringing together security expertise and critical infrastructure owners. All the Dutch DSOs are member of ENCS, as are several foreign DSOs. ENCS also help Austrian DSOs in formulating security requirements for tendering, and these have are publicly made available online [25].

A well-known example from outside the Netherlands is the approach taken in Germany here, where a Common Criteria Protection Profile has been defined [26]. Common Criteria security evaluations are notoriously time-consuming and expensive, which may dissuade suppliers from entering the market.

### D. Data leaks so far

A few data leaks have become public in the past years, which point to weak spots in the overall security.

One potential troublespot, already noted in [27], is the authentication of consumers by energy suppliers and ISPs. Any individual can contact an ISP claiming to live at some address to then obtain meter readings of that household via this ISP. An ISP could check the identity for instance by sending a letter by mail with some access code needed for online access to the meter readings, but this is costly and time-consuming. Indeed, in 2015 a journalist demonstrated that some ISPs do not perform any identity check whatsoever [28].

There have also been data leaks where an ISP or energy supplier accidentially or deliberately abused their access to data kept by EDSN. Note that these parties are simply trusted to only request data from their own consumers. In 2016 an employee of an energy supplier deliberately requested large volume of consumer data from EDSN without cause [29]. In 2017 on the website of an energy supplier you could enter an address and postal code to then obtain annual usage figures for that address [30]. In both cases the data stolen or leaked did not include monthly or 15-minute interval readings obtained via P3. Instead, it involved data recorded in central registry of EDSN: standardized yearly consumption, and in the first case also customer names, addresses, current energy suppliers, and end date of contracts.

To counter problems like the ones above, starting 2018 there will be additional access control checks: customer-specific information has to be supplied by an ISP or energy supplier to the DSO as proof that customers have given permission to access their data [31]. This information is either the last three numbers of the customer's bank account, or the year and month of their birthday. This information might be easy to obtain for attacker wishing to impersonate someone, in which case it would not stop the impersonation attack. It would be an obstacle to larger scale data leaks as the accidental and deliberately data leaks mentioned above.

The ISPs and energy suppliers could perform stonger verification of a customer's identity. As mentioned before, sending a letter is costly and slow. However, the smart meter does provide a cheap and effective way to authenticate customers, because the meter can display a message sent by the DSO via the P3 port. So to check the identity of a customer, the smart meter could display a message that the consumer has report back to the ISP or energy supplier. Currently this option is not used, and DSO do not support for Dutch ISP or energy supplier sending such messages. In the UK, this functionality is used to authenticate customers.

## IV. The Rationale for Smart Meters

The debate surrounding smart meters has not only been about security and privacy, but also about whether the costs outweigh the benefits. We do not presume to give any definitive answer to this question, but try to give an overview of the arguments.

The arguments in favour of smart meters can be summarized as follows:

A. giving grid operators better insight in the grid;
B. reducing the cost and hassle of taking meter readings;
C. reducing fraud; and
D. giving consumers better insight in their electricity consumption, in the hope that they will reduce their consumption or shift consumption to off-peak moments.

Leaving aside security and privacy concerns, which we already covered, the main arguments against smart meters are the costs and whether the projected benefits outweigh these costs. A problem here is that it is hard to predict or even quantify some of these benefits, as discussed below.

### A. Better Insight and Control for DSOs

The introduction of smart meters is only a small part of the smart grid. The term 'smart grid' refers to the wider use of IT to connect ever more sensors and actuators in the grid to give better insight and more control. The need to make the grid smarter primarily comes from the growing use of distributed renewable energy sources: instead of a highly centralized electricity supply by a few large and very predictable power stations, electricity is increasingly supplied by a large number of smaller sources, such as solar panels and windmilss, on many locations. This decentralization, along with the inherent variability of solar and wind power, make these energy sources much harder to predict. Controlling supply and demand in such a setting requires more insight and control of what is happening, not just in the central high voltage part of the grid, but also on a more local level, at lower voltage parts of the grid.

DSOs, however, do not seem to need the power consumption measurements from individual households at all [14]. Smart meters do enable a more advanced form of measuring the power supplied back to the grid than the classic single-counter rotating-disk analog meters do, where the disk simply rotates backwards. However, a non-smart digital meter can also easily incorporate multiple counters, which the consumer would simply provide separately to their energy supplier. Smart meters could enable DSOs to directly control whether a given solar installation is allowed to provide power to the grid or not, but the current legal framework does not allow for this and it brings additional security concerns. Similarly, limiting the amount a connection can consume gives more fine-grained control over the grid for the DSO. Again, however, this kind

of dynamic adjustment is not supported by currently rolled out meters, and not possible in the Dutch legal framework. There are some experiments in this field, however, which we expand upon in Section V. Considering this, we are left unsure about the actual impact smart meters have on grid management.

### B. Easier and more frequent meter readings

At first glance, this benefit seems the clearest: with smart meters, it is no longer necessary for a meter reader to go from house to house to take meter readings, as this can be done automatically and remotely. This reduces cost for the grid operator, and hassle for the consumer. Still, the actual benefit in terms of cost saving will vary between countries, and for the Dutch situation it is not so clear. For example, Swedish grid operators have the legal obligation to read meters every month [32], but in the Netherlands consumers without smart meters are typically required to provide their own reading, and only once a year, and the DSOs are only required to verify the meter reading once every three years. Another factor is that meters in the Netherlands are installed inside the house. In countries where meters are fitted at the outside of houses, sending someone around to take meter readings will be faster and cheaper.

Smart meters may make it easier for households to switch energy suppliers, by reducing the hassle for consumers and the cost of having meters read. In that sense smart meters could help with efforts to liberalize the energy market. However, in the Netherlands, reading the meter by the DSO is not a requirement for switching energy suppliers. Many Dutch households already switch yearly between energy suppliers even though they have a traditional meter. Whether the smart meter itself has played or will play a significant role in the liberalization of the energy market remains unclear.

### C. Fraud reduction

Reliable and frequent meter readings that can be carried out remotely can help to reduce certain forms of fraud [14]. One such form of fraud is when energy is being consumed without the consumer having a contract with an energy supplier. It is unclear to us whether this constitutes a significant problem. Another second is where a consumer is passing fraudulent meter readings, though a customer that wishes to defraud the energy supplier in this way could simply have their meter turned administratively off, making the situation no better than before.

Other types of electricity theft, such as tapping of electricity in front of the meter [33] – a common practice to get free electricity for illegal cannabis plantations – may also be detected through comparing aggregate measurements, but this would require a near-100% adoption of smart meters. Power quality measurements may be useful to detect this kind of fraud [14]. We have not found any public figures on the total cost of energy fraud to the Dutch economy, let alone figures about prevention, so the actual benefit remains unclear.

### D. Power savings

Finally, we come to the subject of power saving. Reducing the amount of fossil fuels consumed is a worthwhile goal. However, the smart meter rollout has so far not resulted in the predicted energy savings [2].

The most widely cited cost-benefit analysis of smart meters for the Netherlands [32], commissioned by the Ministry of Economic Affairs, estimates the cost of introducing smart meters at 3.3 billion Euros and the benefits at 4.1 billion, suggesting a clear financial benefit. However, the analysis recognizes that large deviations are possible in benefits, for example if more than 20% of consumers refuses the remote meter reading, or if the energy savings turn out significantly lower than projected. Consumer support is therefore a crucial aspect, but consumer benefits and the broader public interest are not reflected in the standardization process [34]. For the broader EU, research suggests that dynamic tariffs need to be adopted in order to ensure a net positive benefit [35]. The figure of 1.47 billion Euros in savings is based on 3.2% electricity savings and 3.7% natural gas savings [32]. However, more recent numbers show that the actual energy savings fall short of this, and remain at 1% on average [36]–[38].

The main reason for this in the Netherlands seems clear: most consumers do not see any feedback from the smart meter, other than their yearly energy bill or a bi-monthly usage summary. Such an historic overview of the past two months turns out not to be useful for energy saving purposes [36], [37], [39]. Rather, consumers should be informed of their energy use at the moment it happens. Multiple studies performed in the past ten years show that the usage of direct feedback, in the form of in-home displays (IHDs), is effective in achieving permanent energy savings. Research by energy supplier Eneco shows that the usage of their own IHD increases energy savings to 6.1% on natural gas and 3.2% on electricity [40]. In the UK, the smart meter roll-out by DSOs included an IHD, and their pilot projects report significantly higher energy savings [39]. In 2017 only 18% of housholds with a smart meter in the Netherlands used any kind of energy management services – app, website or in-house display; three quarters of these are based on P3 data and do not involve an IHD [2].

In order to improve energy savings, the direct feedback to consumers could be improved. In-home displays are costly, so an alternative such as smartphone apps might be attractive. However, the reports on energy savings imply that even apps are not as effective as IHDs [37].

## V. Ongoing developments

Several pilot projects are experimenting with local energy communities and microgrids are attempting to create a layer below the DSO, where a local neighbourhood does its own load balancing and internal energy trading on a household level. Discussions with DSOs and energy suppliers show that the market is interested in experimenting with dynamic pricing and automated feedback mechanisms, where e.g. household equipment, car chargers, or battery banks automatically switch on and off based on current price.

Such scenarios require real-time measurements of energy usage to ensure grid stability and accurate pricing. We see

a trend where the existing system based on the P3 port is circumvented, and equipment that directly hooks into the P1 port is used to provide these measurements. This brings with it several security and privacy issues.

First, the P1 port does not provide any way to authenticate the data or its origin. Any billing or control process based on data being received from the P1 port can be subverted by simulating the port, which is trivial to do. At best, data obtained via P1 could be cross-checked to see that it is consistent with other data, e.g. P3 data or aggregate measurements taken elsewhere. The former can of course only verify that the 15-minute aggregate of the fine-grained P1 data is correct.

Second, a downside of using P1 rather than P3 is that whereas P3 comes with integrated network support for remote access, for a remote party to access P1 data will require some additional network set-up. For instance, households could forward the P1 data over their internet connections, but this involves a lot of configuration and is likely to fail at times.

Third, on the subject of privacy, we expect similar issues as mentioned in [19] with regards to article 8 of the ECHR, because 10-second interval readings are highly sensitive data. Although the microgrid pilots function on an explicit consent principle, we are skeptical about this being sufficient in the long run. Consumers will be tempted by lower cost, or simply because it is 'the right thing to do'. At some point, it may even become the only option.

With regards to the authenticity and availability of the data, the obvious thing to do would be to make the P1 data available over P3, in real time. However, the capabilities of the communication infrastruction may not be sufficient for this. Also, the prwivacy risks increase with this data passing through the DSO. Another solution would be to authenticate the data coming from the P1 port, and then use a secondary GPRS connection from the third party to directly upload the data to them. Neither solution is ideal.

This discussion on the implications for privacy, but also for grid safety and security, should be had before microgrids become a common occurrence. The design of microgrids should be done practising Privacy-by-Design [41].

## VI. Conclusions

We have given an overview of the Dutch smart metering situation, and explained the policy and design decisions that have been made for privacy and security.

It is not our intention to argue for or against smart meters in general, but there are certain aspects of the Dutch smart meter roll-out that we think are wrong. In our opinion, the relative ineffectiveness in power saving compared to the UK discussed in Section IV-D suggests that the decision to leave the roll-out of in-home displays to market forces may not have been not the right one. We hope that this will be rectified in the future, or that we are proven wrong and that the market will ensure a high penetration of in-home displays in the coming years – or even come up with better alternatives, such as apps that provide concrete suggestions on actions consumers could take to lower energy consumption.

The options for more granular grid management within neighbourhoods and price incentivization described in section V are promising possibilities. Unfortunately the current design of Dutch smart meters does not allow for this to be done securely. This is a consequence of two design decisions: since the P3 port does not provide the required data – and cannot provide data in real-time – the data from the P1 port must be used. However, this data is unauthenticated and must be provided over a separate connection to the ISP. This raises availability and security concerns, which cannot be truly solved without a redesign of the smart meters. Measures such as cross-checking with data from the P3 port might be used to provide at least some basic level of data verification.

There should also be a discussion on the privacy implications of this granular grid management architecture. Data from the P1 port can be used to infer very intimate details about the lives of the consumers. Clear rules should be drawn up for the use of fine-grained meter readings, before this kind of architecture can become commonplace. Related to this, we feel that the clauses on open data in codes of conduct [14], described in section II-D, are potentially too broad. They allow for publication of anonymized data. However, if anonymization is not done correctly, there is the risk of deanonymization. This should be taken into account whenever data is being considered for publication.

Some lessons learnt can be applied to other fields of industry automation, as well as other countries rolling out smart meters. In particular, the problem of drawing up unambiguous security requirements in public tenders discussed in Section III seems to be a more general problem in industry automation. We have also seen this in the related sector of Electric Vehicle charging [42]. Specifying these requirements so that suppliers are forced to meet the spirit of the requirements is hard, and should be handled by security specialists, not by electrical engineers.

## References


[1] "Kamerbrief over besluit grootschalige uitrol slimme meters," Min. EZ, Mar. 2014.

[2] "Marktbarometer aanbieding slimme meters," Netherlands Enterprise Agency (RVO), 2018.

[3] "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," *Official Journal of the European Union*, vol. 211, pp. 55–93, Aug. 2009. [Online]. Available: http://eur-lex.europa.eu/eli/dir/2009/72/oj.

[4] J. Zheng, D. W. Gao, and L. Lin, "Smart meters in smart grid: An overview," in *Green Technologies Conference*, IEEE, 2013, pp. 57–64.

[5] N. Uribe-Pérez, L. Hernández, D. de la Vega, and I. Angulo, "State of the art and trends review of smart metering in electricity grids," *Applied Sciences*, vol. 6, no. 3, p. 68, 2016.

[6] *Dutch Smart Meter Requirements 4.0.7*, Netbeheer NL, 2014.

[7] *P1 companion standard - Dutch Smart Meter Requirements 4.2.2*, Netbeheer NL, Mar. 2014.

[8] *Basisfuncties voor de meetinrichting voor electriciteit, gas en thermische energie voor kleinverbruikers*, NTA 8130, 2007.

[9] "Besluit op afstand uitleesbare meetinrichtingen," Min. EZ, Oct. 2011.

[10] *Electricity metering data exchange - the DLMS/COSEM suite - application layer*, IEC 62056-5-3, 2016.

[11] S. G. Hoffmann, R. Massink, and G. Bumiller, "New security features in dlms/cosem - a comparison to the smart meter gateway," in *Innovative Smart Grid Technologies (ISGT ASIA)*, IEEE, Nov. 2015, pp. 1–6. DOI: 10.1109/ISGT-Asia.2015.7387098.

[12] L. Weith, "DLMS/COSEM protocol security evaluation," Master's thesis, TU/e, Eindhoven, Netherlands, 2014.

[13] J. Choi and I. Shin, "DLMS/COSEM security level enhancement to construct secure advanced metering infrastructure," in *Proc. SEGS*, 2013, pp. 11–16. [Online]. Available: http://doi.acm.org/10.1145/2516930.2516949.

[14] "Gedragscode slimme meters voor netbeheerders," Netbeheer NL, 2017.

[15] *Brief over onderzoeksresultaten VKO*, Vereniging Eigen Huis, Nov. 2016. [Online]. Available: https://www.eigenhuis.nl/docs/default-source/downloads/actueel/lees-de-brief-die-vereniging-eigen-huis-schreef-aan-minister-kamp.pdf.

[16] R. Anderson and S. Fuloria, "Who controls the off switch?" In *SmartGridComm'2010*, IEEE, 2010, pp. 96–101.

[17] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin, "Private memoirs of a smart meter," in *Proc. SenSys*, 2010, pp. 61–66.

[18] U. Greveler, P. Glösekötterz, B. Justusy, and D. Loehr, "Multimedia content identification through smart meter power usage profiles," in *Proc. IKE*, 2012, pp. 383–390.

[19] C. Cuijpers and B.-J. Koops, "Smart metering and privacy in Europe: Lessons from the Dutch case," in *European data protection: coming of age*. Springer, 2013, pp. 269–293.

[20] "Gedragscode verwerking door elektriciteits- en gasleveranciers en door de onder hun verantwoordelijkheid handelende meetbedrijven van op kleinverbruikers betrekking hebbende persoonlijke meetgegevens afkomstig uit slimme meters," Assoc. Energie-Nederland, Nov. 2012. [Online]. Available: https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/gedragscodes/gedragscode-slimme-meters-van-energieleveranciers.

[21] "Gedragscode verwerking door overige diensten aanbieders (ODA's) van op kleinverbruikers betrekking hebbende persoonlijke meetgegevens afkomstig uit slimme meters," VMNED and VEDEK, Jun. 2016. [Online]. Available: https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/gedragscodes/gedragscode-slimme-meters-van-overige-dienstenaanbieders.

[22] A. Narayanan and V. Shmatikov, "How to break anonymity of the Netflix prize dataset," *CoRR*, 2006, http://arxiv.org/abs/cs/0610105.

[23] "ENCS and Enexis: Bringing structure to distribution automation cybersecurity requirements - a case study," ENCS, Oct. 2017. [Online]. Available: https://encs.eu/resources/.

[24] *Dutch smart meters get security tested by ENCS*, NRG Magazine, Dec. 2015. [Online]. Available: http://www.nrgm.nl/news/dutch-smart-meters-get-security-tested-by-encs/.

[25] "Requirements catalog - end-to-end security for smart metering," Österreichs E-Wirtschaft, 2018, Available form https://oesterreichsenergie.at/sicherheitsanforderungen-fuer-smart-meter.html.

[26] "Protection profile for the gateway of a smart metering system," Federal Office for Information Security (BSI), 2011.

[27] B. te Paske, C. Cuijpers, M. van Eekelen, E. Poll, and B. van Schoonhoven, "Risicoanalyse slimme meter keten - privacy en security in het nieuwe marktmodel," TNO, 2012.

[28] J. Meijers, *Slimme meter makkelijk af te lezen voor iedereen*, Jan. 2015. [Online]. Available: http://www.eerlijkemedia.nl/slimme-meter/.

[29] *Gegevens over energieverbruik twee miljoen huishoudens gestolen*, Sep. 2016. [Online]. Available: https://www.nu.nl/internet/4320997/gegevens-energieverbruik-twee-miljoen-huishoudens-gestolen.html.

[30] *Data energieverbruik lagen op straat*, Nov. 2017. [Online]. Available: https://www.bnr.nl/nieuws/technologie/10332399/data-energieverbruik-lagen-op-straat.

[31] *Impressie actieplan dataveiligheid*, NEDU, 2017. [Online]. Available: https://www.youtube.com/watch?v=DslEEi_eIkQ.

[32] R. van Gerwen, F. Koenis, M. Schrijner, and G. Widdershoven, "Intelligente meters in Nederland - herziene financiële analyse en adviezen voor beleid," KEMA, 2010. [Online]. Available: https://www.rijksoverheid.nl/documenten/rapporten/2010/09/03/intelligente-meters-in-nederland-herziene-financiele-analyse-en-adviezen-voor-beleid.

[33] *Energiefraudeur wordt nauwelijks bestraft en is zelfs goedkoper uit*, Stedin, Feb. 2017. [Online]. Available: https://www.stedin.net/over-stedin/pers-en-media/persberichten/energiefraudeur-wordt-nauwelijks-bestraft-en-is-zelfs-goedkoper-uit.

[34] R. Hoenkamp, G. B. Huitema, and A. J. de Moor-van Vugt, "Neglected consumer: The case of the smart meter rollout in the Netherlands," *RELP*, vol. 2, no. 4, pp. 269–282, Nov. 2011.

[35] A. Faruqui, D. Harris, and R. Hledik, "Unlocking the 53 billion savings from smart meters in the eu: How increasing the adoption of dynamic tariffs could make or break the eu's smart grid investment," *Energy Policy*, vol. 38, no. 10, pp. 6222–6231, 2010.

[36] J. Uitzinger and D. Uitdenbogerd, "Monitoring en evaluatie van de slimme meter en het tweemaandelijkse verbruiksoverzicht," IVAM, Mar. 2014.

[37] K. Vringer and T. Dassen, "De slimme meter, uitgelezen energiek," Netherlands Environmental Assessment Agency (PBL), Nov. 2016. [Online]. Available: http://www.pbl.nl/publicaties/de-slimme-meter-uitgelezen-energiek.

[38] ——, "De slimme meter - policy brief," Netherlands Environmental Assessment Agency (PBL), Nov. 2016. [Online]. Available: http://www.pbl.nl/publicaties/de-slimme-meter.

[39] S. Darby, C. Liddell, D. Hills, and D. Drabble, "Smart metering early learning project: Synthesis report," DECC, Mar. 2015. [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/407568/8_Synthesis_FINAL_25feb15.pdf.

[40] K. de Ronde, *Business case slimme meter wankelt*, Energeia, Nov. 2016. [Online]. Available: https://energeia.nl/nieuws/40058986/business-case-slimme-meter-wankelt.

[41] P. V. Aubel, M. Colesky, J.-H. Hoepman, E. Poll, and C. Montes Portela, "Privacy by Design for local energy communities," in *CIRED'18*, 2018.

[42] "EV charging systems - security requirements," ENCS, 2017. [Online]. Available: https://encs.eu/resources/.