Metering Homes: Do Energy Efficiency and Privacy Need to Be in Conflict?

Libor Polčák[1][a] and Petr Matoušek[1][b]
[1]*Brno University of Technnology, Faculty of Information Technology, Božetěchova 2, 612 66 Brno, Czech Republic*
{*polcak,matousp*}*@fit.vut.cz*

Keywords: Data Protection, GDPR, Meters, Wireless M-Bus, Energy Efficiency, Privacy.

Abstract: The European directive on energy efficiency requires that all meters in multi-apartment buildings installed after 25 October 2020 shall be remotely readable devices where technically feasible and cost effective in terms of being proportionate in relation to the potential energy savings. We observed that some manufacturers produce meters that monitor energy consumption in very short intervals, for example, a minute, even though the directive expects to provide billing information to consumers only once a month starting from 2022. This paper reviews privacy and security risks stemming from the high-frequency readouts and provides recommendations for manufacturers and suppliers. The paper focuses on Wireless M-Bus metering devices sold and advertised as a solution to fulfil the directive on energy efficiency requirements. We responsibly disclosed four issues in the metering devices to Common Vulnerability Exposure database; real-world deployments are vulnerable. Many recommendations and observations are also applicable to other protocols or deployments.

1 INTRODUCTION

The European Union has strict law requirements on privacy, personal life, and confidentiality. For example, GDPR defines *personal data* as

> *any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*

GDPR defines a *data controller* as any person (legal or natural) that determines the purposes and means of the processing of personal data. A controller can delegate some processing to a *data processor*.

The Court of Justice of European Union (CJEU), which is the highest European Court that interprets the European legislation, upholds a broad meaning of personal data and the responsibility of controllers in its case-law (e.g., cases C-70/10, 131/12, C-212/13, C-582/14, C-210/16, C-434/16, C40/17, C-623/17, C-673/17, C-311/18, C-511/18).

Metering devices of electricity, water, and heat consumption may reveal information on the private lives of residents (Asghar et al., 2017; Kumar et al., 2019; Brunschwiler, 2013; Chen et al., 2011; Erol-Kantarci and Mouftah, 2013; Lisovich et al., 2010; Wigan, 2014; Orlando and Vandevelde, 2021), for example, about the occupancy or daily life cycles. A household consumption analysis may yield location data and reveal the habits of all members of the household. Furthermore, a person can live alone in a flat. Hence, metering devices can readily produce personal data. The Article 29 Working Party (a European body consisting of European data protection supervising authorities; currently transformed to European Data Protection Board) considers metering data to be personal data (Article 29 Data Protection Working Party, 2011).

The European Commission applied the Article 29 Working Party opinion on smart metering to the Commission Recommendation of 9 March 2012 on preparations for the roll-out of smart metering systems (2012/148/EU). The European Commission also asked European standard bodies to revise and secure standards for smart metering (European Commision, 2011).

Wireless M-Bus is a protocol for metering data

[a] https://orcid.org/0000-0001-9177-3073
[b] https://orcid.org/0000-0003-4589-2041

readouts in the range of tenths or hundreds of meters. The meters always start the communication, so they do not need to consume a battery to listen constantly for incoming communication. As the use cases (including those considered in this paper) cover readouts performed by a person visiting the building, the data transfers must occur frequently. Consequently, the person that remotely reads the meters can go through the building swiftly without unnecessary stops.

(Brunschwiler, 2013) found several security and privacy risks in the Wireless M-Bus standard (EN 13757), including using weak keys and the lack of authentication as the original security mechanisms used shared keys. Consequently, additional security mechanisms were added to the standard, including mechanisms that support authentication and ephemeral keys.

At the end of 2018, the European Parliament and the Council amended the Directive 2012/27/EU on energy efficiency. As a result, all meters in multi-apartment buildings installed after 25 October 2020 shall be remotely readable devices where technically feasible and cost effective in terms of being proportionate in relation to the potential energy savings. We believe that the legislators considered the recent standard updates for metering devices and considered the metering data to be sufficiently protected. Nevertheless, the manufacturers and suppliers seem to sell devices with the original security mechanisms based on shared keys, without appropriate risk analysis and with broken security.

There are several main contributions of this paper:

- We analysed metering solutions by *Enbra* and *Kaden*. During the work, we identified four vulnerabilities that were assigned Common Vulnerability Exposure (CVE) numbers. As the vendors did not cooperate during the disclosure procedure, the metering based on the tested products is vulnerable.
- Additionally, we describe a case study deployment of the meters during which we highlight several other issues causing the deployment likely not to be compliant with data protection laws.
- Finally, we provide recommendations on producing meters and their deployment that are compliant with the data protection law.

This paper is organised as follows. Section 2 provides necessary theoretical background on the European Commission Recommendation of 9 March 2012 on preparations for the roll-out of smart metering systems (2012/148/EU), mainly from the security and privacy perspective, and the key features of Wireless M-Bus, common architectures, and security modes. Section 3 introduces a case study of a metering system that is currently being deployed. The rest of the paper focuses mainly on the case study and the meters deployed in the case study. Section 4 describes our methodology for detecting flaws in the case study metering. Section 5 describes the CVEs and other findings that we reported to the manufacturers. Section 6 provides recommendations for manufacturers and architects of similar systems that focuses on parameters that build trust between the inhabitants of the metered homes and the operators of the metering devices. The paper is concluded in Sect. 7.

2 PRELIMINARIES

This section introduces legal recommendations for smart metering devices in the context of this paper. Subsequently, the section introduces the Wireless M-Bus protocol because we later focus on this protocol in the case study.

2.1 Data Protection

The European Commission Recommendation of 9 March 2012 on preparations for the roll-out of smart metering systems (2012/148/EU) explicitly mentions that *smart metering systems allow processing of data, including predominantly personal data* (see recitals 6–8 of the recommendation).

Furthermore, the recommendation highlights that *particular attention should be paid to security and protection of the personal data processed by smart metering systems* (recital 9).

Moreover, *data protection and information security features should be built into smart metering systems before they are rolled out and used extensively* (recital 10). *The 'security and data protection by design' principle* should be supported *at an early stage in the development of smart grids* (recital 11).

An assessment of the data protection impact carried out by the operator and stakeholders prior to the roll-out of smart metering systems will provide the information necessary in order to take appropriate protective measures. Such measures should be monitored and reviewed throughout the lifetime of the smart meter. (Recital 15)

Article 16 of the recommendation clarifies that *Article 8 of the Charter of Fundamental Rights of the European Union and Article 8(2) of the European Convention on Human Rights require justifying any interference with the right to the protection of personal data. The legitimacy of interference must be assessed on a case-by-case basis in the light of the cumulative criteria of legality, necessity, legitimacy*

and proportionality. Any processing of personal data which interferes with the fundamental right to the protection of personal data within the smart grid and smart metering system therefore has to be necessary and proportional for it to be considered fully in compliance with the Charter.

CJEU considered the necessity and proportionality in cases C-92/09, C-93/09, C-473/12, C-212/13, C-13/16, C-708/18. Briefly, all processed data should be strictly necessary and minimised to the necessary extent.

The Dutch case of a blocked smart meter roll-out due to its incompatibilities with the European Convention on Human Rights is a well-known example of a failed attempt to introduce mandatory smart meters without considering the privacy and data protection law (Cuijpers and Koops, 2012).

Article 18 of the recommendation 2012/148/EU clarifies that the collected, stored, and processed personal data should be appropriate and relevant. According to article 21 of the recommendation, EU *Member States should clearly determine the roles and responsibilities of data controllers and data processors*.

Nevertheless, the Recommendation 2012/148/EU is not legally binding for the manufacturers, owners, and operators of the meters. As the data produced by the meters are typically personal data, GDPR is legally binding. GDPR (Art. 5) requires that personal data are processed lawfully, fairly and transparently in a manner that ensures accuracy, integrity, and confidentiality. In the context of this paper, other articles raise requirements on the necessity of processing without consent (Art. 6), transparency (Articles 12–15), right to portability (Art. 20), responsibilities of controllers and processors (Art. 24–36). We believe that metering data processing following the Recommendation 2012/148/EU is compatible with GDPR. By diverging from the spirit of the Recommendation 2012/148/EU, data controllers and processors might breach GDPR. See Section 6 for our recommendations stemming from GDPR.

2.2 Wireless M-Bus

Wireless M-Bus is a European standard (EN 13757) suitable for remote readouts from the close vicinity of the meter. For example, the person performing the readout does not need to enter the flats, but they need to be close to the building or in its corridors. Wireless M-Bus meters are expected to be powered by batteries so that the protocol is designed to minimise the energy consumption of the meter.

Meters always initiate the Wireless M-Bus data exchange. Each meter regularly (1) wakes up its transmitter, (2) wirelessly transmits data hoping that the data reaches a reading device. The standard presumes either (a) one-way or (b) bidirectional communication. When the meters do not support receiving data, (3a) they immediately switch to a sleep mode after each transmission; (3b) in bidirectional communication, the meters activate the receiver for a limited time during which the reading device can initiate the bidirectional communication. (4b) When the bidirectional communication is finished, the meter falls into the sleep mode.

A reading device can be permanently present and forward read data for further processing, possibly via the Internet. However, the device may be present only occasionally (e.g., once per year or once per month) to gather data required for billing.

Figure 1 shows an example of a Wireless M-Bus meter deployment. The meter transmits data regularly, mostly without the reading device present (dashed lines). Occasionally, a reading device appears in the vicinity (full lines); the reading device either listens only (the first appearance) or continues with bidirectional communication (the second appearance).

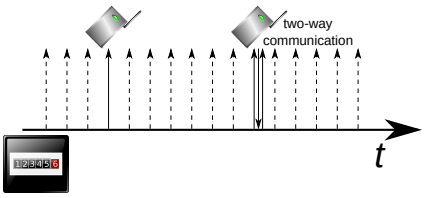

Figure 1: An example of a wireless M-Bus communication between a meter and a reading device that is present occasionally.

As the data transmitted by the one-way communication cannot be negotiated by the reading device, the format of each message (plain text) has to be always the same.

It is possible to buy a Wireless M-Bus receiver for about € 100. The software for Wireless M-Bus parsing is readily available on Internet, e.g., the one produced by (Brunschwiler, 2013). A good antenna and an amplifier are likely to receive the signal hundreds of meters from the building (Rouf et al., 2012). Hence, the meters must implement strong security to comply with the law (e.g., Article 32 of GDPR).

EN 13757-1 mandates deploying a unique key for each meter. Additionally, different sets of keys should be used to authenticate different actors having access to the meter. For example, to increase transparency to household members, they can receive a key that allows them to read the transmitted data (which they can use for their purposes). Another key can be used

to control the meter and access data gathered to prevent meter manipulation and other management tasks.

Initially, the EN 13757 standard family specified several security modes: plain text, DES (now deprecated and (Brunschwiler, 2013) did not observe this cipher to be used in the wild), and AES with a single shared key. However, these security modes guarantee neither integrity nor authentication. Therefore, around 2015, EN 13757 introduced other security modes that ensure authentication and integrity and use ephemeral keys.

3 CASE STUDY

In this paper, we evaluate a Wireless M-Bus solution for water consumption metering deployed to flats of associations of co-owners (condominiums) in multi-apartment buildings to fulfil the amended Directive 2012/27/EU requirements on energy efficiency. We obtained remotely readable Wireless M-Bus meters offered by two vendors, *Enbra* (the radio module is manufactured by *Apator*) and *Kaden*, in an e-shop. Hence, anyone can buy these meters. We selected *Enbra* based on an offer for an association of co-owners that we had seen before starting this research. We bought a reading set offered by *Enbra*. *Kaden* was selected as the first another manufacturer that we found in the offers of Wireless M-Bus meters.

Kaden meters have a built-in module that cannot be detached. *Enbra* meters have a detachable radio module. Although the *Enbra* meter and the radio module have different serial numbers, for simplicity, when we refer to a meter, we mean the meter combined with the radio module. Similarly, the ID of the meter means the ID of the radio module. We explicitly refer to the radio module to distinguish between the meter and the radio module.

The offer of *Enbra* (supplier) to an association of co-owners in multi-apartment buildings mentions that the meters transmit data using one-way Wireless M-Bus. Nevertheless, neither does the offer warn that data processed by the meters will likely process personal data[1], nor does the offer explain the security. Such an offer does not raise red flags to the general public. As all co-owners are typically not specialised in computer security, no one objects.

The supplier offers two types of deployment:

1. No additional permanent infrastructure besides the metering devices. Such deployment requires that a person enters the building and performs readouts for the billing.
2. Wireless M-Bus gateways proxy the messages to the remote server of the supplier. The supplier informed the association that data sent over the Internet are not encrypted. Once on the server, the readouts should be available to the household members and the association of co-owners.

We studied two deployments without permanent infrastructure. As far as we are aware, both associations did not receive the keys, risk analysis prescribed by EN 13757-1, or technical documentation on the transmitted data. One association received information on frequent message transfers following a data subject request.

During our research (see Sect. 5.1), we learnt that the *Enbra* meters are capable of detecting events (like a water leak, unoccupied flats, etc.). As far as we are aware, neither association was informed that the meters can detect events.

4 POSSIBLE RISKS

We decided to evaluate EN 13757 as well as current literature to determine privacy and security threats that might arise in the case study system introduced in the Sect. 3.

4.1 Confidentiality and key management

EN 13757-1, Sect. 4.3.2 anticipates performing a security requirement analysis and threat analysis. One should assess the risks and alternatives according to ISO/IEC 27033 or ISO/IEC 15408 as suggested by EN 13757. As already mentioned in Sect. 3, the associations did not receive any analysis.

EN 13757-1 and EN 13757-7 stress that key management is an important task that needs to be solved to provide confidentiality, integrity, and non-repudiation. According to EN 13757-1, the keys require a high level of protection, and the principle of the *need to know* should be applied. Depending on the deployment and the threat analysis results, the key might need to be changed during the lifetime of the meter. Different sets of keys might be needed for different clients, and unique keys need to be used for each meter. The key cannot be derived from the data like the ID of the meter.

(Chen et al., 2011) successfully detected household activities such as taking a shower, using a washing machine or dishwasher from readouts of 15-

[1]Despite EN 13757-1 (Section 4.3) and EN 13757-7 (Section 9.1) warning that metering data should be treated as private data of the user in most cases

minute periods. Some devices can have a distinct pattern of energy consumption. The pattern could be used to fingerprint such a device (Lisovich et al., 2010; Kelly and Knottenbelt, 2015; van Megen and Mueller, 2010; Hurri et al., 2011). Consequently, an adversary can reveal the manufacturer or even the model of household appliances without ever entering the household. Such information is convenient for burglars, profiling, and marketing.

Hence, we studied the timing between the readouts and the information quality of each readout. We also focused on key management as poor key management might endanger the confidentiality of the measurements (Asghar et al., 2017).

4.2 Zero consumption detection

Subsection 4.1 anticipates that the key of a meter leaks; directly or as a tool able to decrypt and decode the messages. Nevertheless, zero consumption detection may be possible even without a leaked shared key. AES is a block cipher, so the same input (including the initialisation vector — IV) yields the same output. That is the reason why EN 13757-7 explicitly warns against zero consumption detection.

Computer science literature also highlights the risk of zero consumption detection (Erol-Kantarci and Mouftah, 2013; Lisovich et al., 2010). If there is a consumption, typically, there is also a person that uses the water. Vice versa, if the water is not being consumed for some time, there is probably no one in the flat. Long-term observations can reveal the patterns of being away from home (Lisovich et al., 2010). This information can be misused for commercial purposes, criminal activities such as burglaries and stalking.

Consequently, we focused on an analysis of methods to determine zero consumption without the knowledge of the encryption key.

4.3 Integrity

Brunschwiler reported that Wireless M-Bus Security Mode 5 devices are vulnerable to replay attacks — Jam-and-Replay and Shield-and-Replay (Brunschwiler, 2013, Section 4.4.2, 4.4.3). An attacker can intercept messages sent by Wireless M-Bus Security Mode 5 devices at time T. The attacker can replay these messages during readouts at T + several months.

Consequently, we focused on the ability to perform replay attacks against the deployed case study system.

4.4 Identifiability

Enbra claims that it is impossible to identify the flat where a specific meter is being placed. We focused on methods that disprove the claim.

5 FINDINGS

This section focuses on the findings of this paper. We reported issues to CVE database. CVE is a worldwide database used for responsible disclosure. The idea is to confidentially report detected vulnerabilities to the IT manufacturers and vendors and provide them with time to fix the vulnerability or explain more details about the vulnerability. Once the vulnerability is fixed or excessive time passes during which the vendor does not respond or cannot fix the underlying problem, the vulnerability is exposed to anyone in the world so that the customers and users can apply countermeasures to the vulnerabilities such as workarounds or avoid the vulnerable components.

5.1 Preliminary analysis of the meters

After we bought *Enbra* and *Kaden* meters, we observed the messages transmitted by these meters. Data are secured with the original EN 13757 AES mode (Security Mode 5) without the possibility of different roles (e.g., a user authenticates to the meter using a unique AES key). We did not receive any meaningful technical documentation containing the key nor other data necessary to decode deciphered messages although we explicitly asked. We did not receive any risk analysis prescribed by EN 13757-1.

Enbra meters transmit data with a period of 80 seconds for about 12 hours per day — Monday to Friday; and with a period of 300 seconds during Monday to Friday nights, Saturdays, and Sundays. All transmissions produce data of the same length and with the same Wireless M-Bus headers (not encrypted) except an 8-bit access number counter. The meters set the bidirectional bit meaning that they are capable of bidirectional communication. *Apator* website (the manufacturer of the radio module) confirms that the meters are indeed bidirectional. According to *Apator*, it is possible to manage the meters remotely. The meters save historical data on the consumption, provide data on current consumption and meter value, and detect several events such as zero consumption, meter tampering, and water leaks. It is possible to change the key by anyone who knows the old key. Effectively, everyone who knows the key can brick the device by assigning a key that the adversary immediately deletes

(the plain text would not be decryptable, so even if the device would continue transmitting, no one could utilise the readouts).

Kaden meters transmit data with a period of 1 minute for about 10 hours per day and 15 minutes during nights. The meter does not differentiate between workdays and weekends. The meter produces two messages during each transmission interval. One message is shorter and the other longer. The longer message changes at the end of a month; we suppose that it carries historical consumption data. The bidirectional flag is not set, meaning that there is no way to communicate with the meter. We did not find any communication port that could be used to configure the meter.

5.2 Broken key management: CVE-2021-34571

As mentioned in the Sect. 5.1, both *Enbra* and *Kaden* meters are distributed without the encryption key. Even so, both offer a reading device. According to *Enbra*, the security of the system is guaranteed with a proprietary content of the plain text message.

We bought the reading device offered by *Enbra*. The reading device automatically deciphers the consumption reported by meters ordered together with the reading device and meters deployed by both associations of co-owners.

How is the reading device able to decipher the messages? It must have known or computed the key. It seems likely that the encryption depends on a shared key, or, that is possible to derive the key from the serial number of the radio module sent in the plain text part of each message. It is possible that the meters use different keys. However, the observations show that if this was the case, these keys or the algorithm to derive them must had been shared with the reading set. It is not clear who knows the key(s).

As an adversary only needs a compatible reader to read the consumption, the confidentiality of the water metering is endangered. Such security violates EN 13757-1, which mandates unique keys for each meter that cannot be derived from other data like serial numbers. EN 13757-1 expects a key management policy to be developed.

If the EN 13757 is violated, it is likely that also the Article 32 of GDPR is violated as it requires that:

> *Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk [...]*

As the case study system provides data in 5-minutes periods or 80-second periods, the household activities detection should be better than those observed by (Chen et al., 2011).

Moreover, it is possible that the shared keys do not have sufficient strength. In such a case, an adversary can leverage tools like Hashcat to recover the key. We did not try this experiment yet.

If a (shared) key leaks, many consequences can follow, which are hard to enumerate. For example, smart home appliances and gateways vendors can incorporate the leaked keys to gain a marketing advantage for their products. Should the keys be shared, an owner of such a smart home gateway can monitor the activities of the neighbours (possibly without the knowledge that such processing takes place). In the worst-case scenario, such an appliance can be connected to the Internet without sufficient security, and energy consumption details can start to leak to the Internet. As the meter is not in the direct ownership of the households, even a skilled technician is unable to prevent leakage of his or her data. Moreover, if the AES key leaks, one can reconfigure the devices and even change the encryption key. To mitigate the issue, a sound key management policy has to be in place. A shared key between the metering devices and easily guessable keys should not be deployed as both can make the leak worse.

As a countermeasure, we suggest that *Enbra* changes the keys in conformance with EN 13757-1 — the keys must be unique to each meter, and all bits should be randomly generated. As far as we are aware, *Kaden* meters do not provide any way to change the key. The obvious solution is to replace the meters.

5.3 Zero consumption detection without key

The IV used by the AES cipher contains an 8-bit access number counter that is incremented with every transmission. The changing IV indeed prevents the detection of zero consumption in successive readouts. However, once the 8-bit counter overflows (after 256 messages), the ciphertext is the same if the plain text message does not change. Once an adversary detects a repeated message, they know the last consumption that was metered. While the messages repeat, it is clear that the meter value does not change. Later, the adversary can learn when the meter changes again (or something else changes in the payload) — the cipher-

text changes compared to the previous occurrence of the counter value.

The transmission interval of the meters considered in the case study can yield such an overflow after several hours, which means that not only can an adversary detect unoccupied flats, but long-term observations can reveal patterns in daily activities. The standard correctly advises using a timestamp or another counter, but it does not explicitly describe the overflow issue. *Apator* claims:

> *To assure confidentiality of the metering data, the RF transmitted consumption data is secured with the AES-128 + CBC encryption algorithm (which guarantees variation of the transmitted data when no volume changes occur).*

Indeed, EN 13757 mandates using Cipher Block Chaining (CBC) for the applied security mode. However, CBC affects each message separately; the encryption of a message is not chained to the previous message. We reported the issue with zero consumption detection from overflowed access number counter and suggested modifications of the standard text to the European Committee for Standardization (CEN), the standard body behind EN 13757. However, there are no revisions of the standard planned at the moment. Moreover, we found meters vulnerable to zero consumption detection using this method, as further discussed in subsection 5.3.1.

5.3.1 CVE-2021-34576: Zero consumption detection of *Kaden* meters without key

Recall that *Kaden* meters produce two messages every readout period. By observing the messages of *Kaden* meters, we detected that the shorter message of 48 bytes (application payload) seems to hold the current metered value. Each of the short and long messages increment the access number counter value; the counter value overflows every 256 messages. Hence, the IV repeats after 2 hours 8 minutes during day between 9 a.m. and 7 p.m., or 15 hours 12 minutes otherwise.

Suppose there was no metered consumption between the messages with the repeated IV. We observed that the first 32 bytes of the ciphertext of the payload of the shorter message repeat while the final 16 bytes are different. Whenever a consumption occurred between the messages with the repeated IV, the encrypted payload of these two messages with the same IV was completely different. One can deduce that (1) the metered value is located in the starting 16 bytes of the 48-bytes-long message and (2) there seems to be a value that changes frequently located in the final 16 bytes of the message even without any consumption. The employed encryption scheme does not offer full confidentiality in such configuration. Hence, an adversary can observe whether there was water consumption during the overflow time range without the encryption key. Consequently, the attacker can infer information about someone being in the flat or not, daily patterns, and similar information.

Figure 2 shows an example of the vulnerability in *Kaden* devices protected by the original AES mode (Security mode 5).

Meter value 1234.5, counter 100, time 10:00 ⟶ cipher text AAA
Meter value 1234.8, counter 102, time 10:01 ⟶ cipher text BBB
Meter value 1234.8, counter 104, time 10:02 ⟶ cipher text CCC
...
Meter value 1234.8, counter 170, time 10:35 ⟶ cipher text DDD
Meter value 1234.8, counter 172, time 10:36 ⟶ cipher text EEE
...
Meter value 1234.8, counter 100, time 12:08 ⟶ cipher text FFF
Meter value 1234.8, counter 102, time 12:09 ⟶ cipher text BBG
Meter value 1234.8, counter 104, time 12:10 ⟶ cipher text CCH
...
Meter value 1234.8, counter 170, time 12:43 ⟶ cipher text DDI
Meter value 1234.9, counter 172, time 12:44 ⟶ cipher text JJJ

Figure 2: An example of the vulnerability in *Kaden* meters. In the example, an adversary can detect at 12:09 that the meter value has not changed since 10:01 as the beginning of the ciphertext starts to repeat after 12:09. As the beginning of the ciphertext observed at 12:43 is the same as at 10:35 but the following ciphertext changes completely, the adversary can detect that the meter value changed between 12:43 and 12:44.

An adversary can determine if the consumption was zero or non-zero. The adversary cannot detect the metered value if the consumption changes. Because there is a message sent every minute during the day, the attacker can learn the time when the water was metered for the last time (with the delay of 2 hours and 8 minutes during days and 15 hours 12 minutes during nights). The attacker can detect water consumption in the following sent message; the ciphertext differs from the previous message with the same counter number (IV).

5.4 CVE-2021-34572: Vulnerable to replay attacks

Although we lack technical documentation of the radio modules, we think that *Enbra* meters send a timestamp: (1) Wireless M-Bus Security Mode 5 initialisation vectors repeats every 256 messages, or every 5.6 hours during peak hours in the default configuration of *AT-WMBUS-16-2*. As the ciphertext of the observed messages with the same IV changes without consumption, the plain text of the message with the same IV must differ. We suspect that this is due to the

presence of a timestamp. (2) We changed the system data on the reading set. Even so, the reading software by *Enbra* displayed the real date and not the system date. Hence, we conclude that the data was parsed from the message sent by the meter.

A timestamp protects against replay attacks. The reader can compare the time reported by the meter and the system time and detect message replays (of course, the reader should accommodate errors due to clock shifts).

The reading software by *Enbra* provides an export functionality to the CSV format. Exported data can be used for further processing, e.g., to provide billing details. However, exported CSV data does not contain the time observed at the meter but instead provides the system time of the readout. As the software does not notify the user that a readout from the past appeared and it is impossible to check the CSV data for time stamps from the past, replay attacks described by (Brunschwiler, 2013) and similar are likely to remain undetected by the users of the software. Hence, an attacker can replay past data to influence single or multiple meter readouts. Consequently, the integrity of the billing information is affected (the incorrect bill is lower).

As a workaround, persons performing the readout can check the original transmission date in the reading software by *Enbra* before they export data to CSV. However, such a task is time-consuming and error-prone due to the likely fatigue from comparing unaffected data from the majority of the readouts that are expected to happen without an attacker.

5.5 Identifiability of the meter

Enbra claims that it is impossible to identify the flat where a specific meter is being placed. However, this claim is invalid.

- The radio module number is visible on the module. Consequently, every person with physical access to the meter (for example, entering the bathroom where it is installed in the flats of the associations) can easily learn the module number. Note that the very same number can be observed in the unencrypted part of the Wireless M-Bus messages.
- When the supplier replaced old meters with Wireless M-Bus meters, all co-owners needed to sign a protocol about the replacement. The protocol contains the numbers of radio modules and meters and is available to some or all the co-owners depending on the rules of the association.
- The signal strength decreases with distance and the number of obstacles (see Figure 3). Indeed, we were able to experimentally detect the signal of a known radio module (we visually read the number printed on the radio module) outside the building at the place where no other signal was present. We preselected the signal strength measurement location so that the known radio module was the closest and with the least number of obstacles. Moreover, we measured signal strength inside a building. We were able to identify meters in flats from measurement taken from the corridors of the building, see Tab.1. We expect that all meters in a building can be located with one successive message received per flat per meter (about 1–2 minutes per flat for the meters considered in the case study introduced in Sect. 3).
- The zero consumption detection vulnerability (CVE-2021-34576) or access to metered values (CVE-2021-34571) can be leveraged to correlate the persons entering or leaving the building and detected (zero) consumption of the meters.

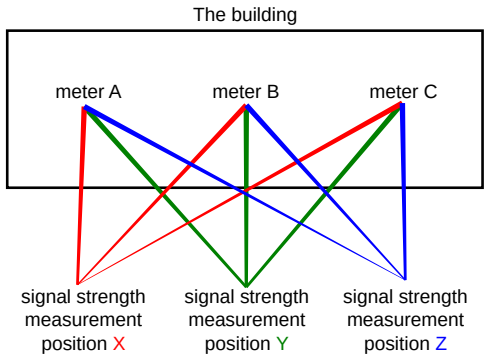

Figure 3: An example of a possible signal strength measurement. The signal of Meter A is strong at X, moderate at Y, and weak at Z. The signal of Meter B is strong at Y, and moderate at X and Z. The signal of meter C is strong at Z, moderate at Y, and weak at X.

5.6 CVE-2021-34573: Misleading event detection

As mentioned in Sect. 3, *Apator* advertise that the meters detect events such as zero consumption, meter tampering, and water leakage. The reading software by *Enbra* seems to be able to read such events and even export them to the CSV format.

One of the events is backflow. We back flowed about 0.015 cubic meters through the meters. The reading software by *Enbra* did not report the backflow event. We are not sure what the issue is: Was the threshold reached? Is it a bug in the meter? Maybe the meter does signal the event, but the reading software by *Enbra* cannot parse the event. Unfortunately,

Table 1: Average signal strength measurements. Note that each flat has two meters. Flat D is located above flat A. Flats B, C, and D are located on the same floor.

Meter 1 in flat A	
50.48 %	corridor in front of flat A
42.90 %	corridor in front of flat D
42.58 %	just below flat A
26.06 %	another place below flat A, several walls
25.59 %	a far away place below flat A
18.71 %	corridor in front of flat B
Meter 2 in flat A	
47.10 %	corridor in front of flat A
34.62 %	corridor in front of flat D
32.26 %	just below flat A
28.39 %	corridor in front of flat B
17.42 %	a far away place below flat A
15.68 %	another place below flat A, several walls
Meter 1 in flat D	
66.29 %	corridor in front of flat D
46.45 %	corridor in front of flat B
25.59 %	just below flat A
25.16 %	corridor in front of flat C
11.81 %	another place below flat A, several walls
2.90 %	a far away place below flat A
Meter 2 in flat D	
72.25 %	corridor in front of flat D
36.94 %	corridor in front of flat B
30.54 %	corridor in front of flat C
9.68 %	just below flat A

the responsible disclosure procedure did not clear the issue.

Additionally, the reading software by *Enbra* reported meter malfunction *Radio module was removed three times* during our first readout. However, there was an *Apator* seal that should indicate if the radio module was removed. The seal was intact on our modules. The meter had not been used for several months before it had been shipped to us, as was visible from historical volumes saved at the end of several preceding months before the readout. We expect that the condition for reporting the event of zero consumption should had been triggered before the readout. The reading software by *Enbra* does not report zero consumption. Even more, when studying the meters in one of the affected associations of co-owners, we noticed that the very same error was also shown but only on a limited number of meters. All the meters that we noticed showed *Radio module was removed three times*. We did not see any other error or number of removals. Is it just a coincidence?

We suspect that the event reporting in the reading software by *Enbra* does not work as it should. The integrity of data can be corrupted without detection. Different events may be represented to the user resulting in confusion. A flat owner can be accused of radio module removal even though the event did not really occur. As a workaround, we suggest ignoring the events or interpret them with a grain of salt.

6 DISCUSSION AND RECOMMENDATIONS

This section discusses recommendations that should be considered by the manufacturers and suppliers of the metering devices. Recall the recital 11 of The European Commission Recommendation of 9 March 2012 on preparations for the roll-out of smart metering systems (2012/148/EU) focusing on security and data protection by design, see Sect. 2.1 for more details. Although we focus on the lessons learned in the previous sections, we believe they can be generalised to other metering devices, even using protocols other than Wireless M-Bus.

6.1 Proportionality, necessity, and data minimisation

European data protection law requires the processed personal data to be proportionate, necessary and minimised. Should the law require yearly readouts, the devices should by default transmit only the yearly balance (Article 29 Data Protection Working Party, 2011). Once the law changes to monthly readouts, the device should provide the data. Of course, one can tolerate a preparation phase during which the devices provide monthly readout earlier than required. The more detailed the readings, the more privacy-sensitive the data becomes (Asghar et al., 2017; Cuijpers and Koops, 2012).

According to an e-shop selling the radio modules of the case study (Sect. 3), they can be configured to change the records being available in the transmitted frames. Hence, it might be possible to alter the behaviour of the meters according to changes in law and signed contracts. Therefore, we recommend that manufacturers implement such configurability into meters that are being designed and those that can be upgraded.

The readouts containing current consumption and flow rate are clearly not needed by the law and should not be transmitted by default (Cuijpers and Koops, 2012; Orlando and Vandevelde, 2021). For successful deployment, the events supported by the radio modules (meter tampering, water leakage, etc.) of the

case study system seem to be a good idea. Suppose the meters are configured not to sent current consumption and flow rate but instead report the events. Such configuration is suitable for the deployment with gateways and the webserver (see the offered type of deployment with gateways in Sect. 3) as the events would detect water leaks, meter tampering, etc. without unnecessarily sacrificing the privacy of the inhabitants. Some events like water leaks could trigger an emergency.

(Orlando and Vandevelde, 2021) focused on gaining trust including the issues of frequent read outs. To increase the trust between the manufacturer, supplier, and household members, we suggests building meters with physical switches to control the frequency of the readouts. In the case of the proxying data to a webserver (or custom readouts mentioned later), someone may be interested in the detailed information about energy consumption (Asghar et al., 2017). The hardware switch could enable such choices. The informed consent can be obtained in the webserver; if the user refuses to consent, the webpage can show instructions about the hardware switch and its current and desired position.

There is also a question if the modules should transmit during nights and weekends. It seems not to be necessary for the deployment without transfers to the webserver. In the use case with a webserver, such transfers are beneficial for event detection.

Sections 4 and 5 show that the meters considered in this paper fulfil the conditions for data protection impact assessment as Article 35(1) of GDPR reads:

> *Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.*

A typical association of co-owners does not have enough knowledge to carry the assessment. Therefore, we believe that the supplier should have the knowledge to perform the assessment.

6.2 Transparency

Previous research shows that consumers need to be adequately informed about the risks and privacy implications of smart meters (Cuijpers and Koops, 2012; Asghar et al., 2017).

The case study system transmits data through the air inside the household. Therefore, it seems straightforward that the household members (data subjects) should be allowed to use that data for their purposes, e.g., to create a smart home (for example, to detect water leaks).

The manufacturers and suppliers should create the meters so that the communication is either one-way only or bidirectional with authentication and support of different roles. The deployment should allow household members to read the data without the possibility to modify the configuration, stored events, and other data outside of the privileges of their role. (Asghar et al., 2017) identified value-added services as an important part of smart metering deployment.

GDPR gives data subjects the right to access personal data even if it was not obtained directly from data subjects. Article 20 gives data subjects rights to data portability if the processing is carried out by automated means and based on consent or contract. By providing the access key for read-only readouts, the controller provides trust through transparency and fulfils the GDPR, Art. 20 requirements.

6.3 Security

Suppose an adversary can deploy Wireless M-Bus readers in the vicinity or inside the building. In that case, encryption is the critical part of the security of the meters. EN 13757 considers the security policy selection a crucial task in terms of confidentiality, integrity, authentication, and non-repudiation. We believe that the standard is correct, and the security analysis of all smart metering systems should take all four requirements seriously.

Hence the key management should be considered a crucial task. The key should not be shared between meters under any circumstance. EN 13757-1 correctly suggests changing the key several times within the lifetime of the meters. See the security analysis (subsection 5.2) for more details on the risks of bad key management.

(Article 29 Data Protection Working Party, 2011) recommends end-to-end encryption of data produced by smart meters. We believe that this recommendation is crucial to ensure the confidentiality of the data to protect the privacy of the household. Hence, both the communication between the meter and a reading device (for example, a gateway) should be encrypted. Also, the transit over the Internet should be encrypted.

6.4 Controllership

Recall that the European Commission Recommendation of 9 March 2012 on preparations for the roll-out of smart metering systems (2012/148/EU) calls for clear determination of responsibilities of data controllers and data processors.

CJEU recently decided in several cases concerning issues in cotrollership, see C-210/16, C-25/17, and C-40/17. For example, Advocate General Mengozzi (Mengozzi, 2018, paragraph 68) considers that it is necessary to rely upon a factual than formal analysis. The European Parliament resolution of 25 March 2021 on the Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application (2020/2717(RSP)) explicitly mentions ICT manufacturers being considered controllers of personal data.

The case study deployment raises uncertainties (see also Sect. 3) about the controllership:

- Is the association of co-owners a sole or joint controller? There are no doubts that the association agreed with the placement of the meters on their premises; hence it determines the means. However, the desired purpose is to provide billing information for co-owners (i.e., it was only interested in yearly or monthly readouts). Consequently, it seems that other controllers jointly determine the means and purposes of the processing. As the buyer (association of co-owners) was misled by the offer that the system is only one way, it could not evaluate risks associated with the bidirectional communication, like the possibility of attacks based on insufficient validation of inputs that can trigger command injections, buffer overflows, and other common vulnerabilities. Moreover, such an association lacks knowledge about the privacy and security issues outlined in Sect. 4. Furthermore, the law should not expect such organisations to gain the expected knowledge of both a skilled technician and a skilled lawyer. Such knowledge is highly specialised and requires extensive training that is, we believe, outside the possibilities of a typical association of co-owners.
- Is the supplier a sole or joint controller? Recall that the supplier likely provided false information in the offer (that the meters are one-way, but according to other information, including the content of each transmitted unencrypted part of the messages sent by the meters, the meters allow bidirectional data transfers). The supplier possesses technical knowledge, albeit it seems that it lacks the knowledge of the law and the content of the standards it explicitly claims to follow.
- Is the manufacturer of the radio module a sole or joint controller? We are not certain about the documentation that was provided to the supplier. Since the supplier offers software tailored for its products and since the meters seem to be configurable in terms of data being sent, the manufacturer probably should not be considered a controller. However, the manufacturer selected the security mode and is possibly the only entity that can update the firmware of the radio module with more suitable encryption schemes.

We believe that the supplier should have the necessary technical knowledge to deploy the metering system and provide the technical expertise to maintain the system and periodically review its security (Article 32 of GDPR), for example, against publicly published attacks (Brunschwiler, 2013). On the other hand, the supplier should not be forced to provide such a service for free.

We believe that the contract between the supplier and the buyers (e.g., an association of co-owners) should clearly determine the roles of the parties. Should the deployed meters transmit data frequently (especially without the presence of the official reading device), the buyer should be clearly notified, and the controllership for frequent data transfers should be clearly determined. The buyer should be (1) notified that the law requires to take security seriously and (2) offered a service to maintain the security of the metering system.

7 CONCLUSION

The European law provides strict guarantees for the data protection of European citizens. The European Commission, the European Parliament, and European Council created data protection laws and recommendations, including GDPR. However, the fast growth of smart gadgets, including smart meters attached without the consent of data subjects in their homes, does not always follow the law and the spirit of the law. We provide a case study and list several uncertainties and possible issues in metering devices currently being deployed in Europe. The ignorance of processing only necessary and minimised data results in privacy risks. The insecure configuration provides data subjects at risk of profiling and burglary. Low transparency does not create trust between the data subjects and the manufacturers and suppliers of the metering devices.

This paper focuses on a case study of a metering system with remote reading capabilities being deployed in associations of co-owners in Europe. As

both the data protection laws and standards expect to carry risk analysis and data protection impact assessments, we analyse the risks of the system. By examining two Wireless M-Bus meters and a reading set, we identified 4 CVEs and several other privacy and security risks in the products. Unfortunately, the affected companies did not react to the responsible disclosure procedure and did not fix the underlying issues. Finally, this paper provides several recommendations in Sect. 6. We believe that the recommendations are generic and valid for any smart metering system, not only those considered in the case study.

According to Art. 58 GDPR, European data protection authorities can, for example, *order the controller or processor to bring processing operations into compliance with the provisions of this Regulation [...]*, *impose a temporary or definitive limitation including a ban on processing*, and *impose an administrative fine*. Schneier expects that *EU enforcement will be harsh* (Schneier, 2018, Chapter 10). Manufacturers of smart gadgets should start to take the law and the risks for data protection seriously if they plan to sell the goods on European markets.

We believe that our recommendations show that privacy and energy efficiency are not in conflict.

ACKNOWLEDGMENTS

This work was supported in part by the Brno University of Technology grant FIT-S-20-6293 (Application of AI methods to cyber security and control systems).

REFERENCES

Article 29 Data Protection Working Party (2011). Opinion 12/2011 on smart metering. Available online at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp183_en.pdf.

Asghar, M. R., Dán, G., Miorandi, D., and Chlamtac, I. (2017). Smart meter data privacy: A survey. *IEEE Communications Surveys Tutorials*, 19(4):2820–2835.

Brunschwiler, C. (2013). Wireless M-Bus Security. *Whitepaper Black Hat USA 2013*. https://www.compass-security.com/fileadmin/Datein/Research/Praesentationen/blackhat_2013_wmbus_security_whitepaper.pdf.

Chen, F., Dai, J., Wang, B., Sahu, S., Naphade, M., and Lu, C.-T. (2011). Activity analysis based on low sample rate smart meters. In *Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pages 240–248, New York, NY, USA. ACM.

Cuijpers, C. and Koops, B.-J. (2012). Smart metering and privacy in Europe: lessons from the Dutch case. In Gutwirth, S., Leenes, R. E., de Hert, P., and Poullet, Y., editors, *European data protection: Coming of age*, pages 269–293. Springer.

Erol-Kantarci, M. and Mouftah, H. T. (2013). Smart grid forensic science: applications, challenges, and open issues. *IEEE Communications Magazine*, 51(1):68–74.

European Commision (2011). M/487 EN: Programming Mandate Addressed to CEN, CENELEC and ETSI to Establish Security Standards. Available online at http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=472#.

Hurri, P., Neuvo, N., Mikkola, T., Bunn, E., Kaakkola, I., and Kivimaa, K. (2011). Smartgrid energy-usage-data storage and presentation systems, devices, protocol, and processes including a visualization, and load fingerprinting process. US Patent US8949050B2 of BASEN CORP.

Kelly, J. and Knottenbelt, W. (2015). The UK-DALE dataset, domestic appliance-level electricity demand and whole-house demand from five UK homes. Master's thesis.

Kumar, P., Lin, Y., Bai, G., Paverd, A., Dong, J. S., and Martin, A. (2019). Smart grid metering networks: A survey on security, privacy and open research issues. *IEEE Communications Surveys Tutorials*, 21(3):2886–2927.

Lisovich, M. A., Mulligan, D. K., and Wicker, S. B. (2010). Inferring personal information from demand-response systems. *IEEE Security Privacy*, 8(1):11–20.

Mengozzi, P. (2018). Opinion of advocate general mengozzi. CJEU Case C-25/17, ECLI:EU:C:2018:57.

Orlando, D. and Vandevelde, W. (2021). Smart meters' roll out, solutions in favour of a trust enhancing law in the eu. *Journal of Law, Technology and Trust*, 2(1).

Rouf, I., Mustafa, H., Xu, M., Xu, W., Miller, R., and Gruteser, M. (2012). Neighborhood watch: Security and privacy analysis of automatic meter reading systems. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, pages 462–473, New York, NY, USA. ACM.

Schneier, B. (2018). *Click here to kill everybody : security and survival in a hyper-connected world*. W.W. Norton & Company Ltd. ISBN 978-0-393-60888-5.

van Megen, F. and Mueller, U. (2010). Classifying devices by fingerprinting voltage and current consumption. US Patent US20110313582A1 of Microsoft Technology Licensing LLC.

Wigan, M. (2014). User issues for smart meter technology. *IEEE Technology and Society Magazine*, 33(1):49–53.