Security Aspects of Smart Meter Infrastructures

Ivan Rigoev and Axel Sikora

1 Introduction

One of the most important questions about smart metering systems for the end users is their data privacy and security. Indeed, smart metering systems provide a lot of advantages for distribution system operators (DSO), but functionalities offered to users of existing smart meters are still limited and society is becoming increasingly critical. Smart metering systems are accused of interfering with personal rights and privacy, providing unclear tariff regulations which not sufficiently encourage households to manage their electricity consumption in advance. In the specific field of smart grids, data security appears to be a necessary condition for consumer confidence without which they will not be able to give their consent to the collection and use of personal data concerning them.

From the personal data privacy and security side several articles are showing that with advanced power signature analysis tools such as Nonintrusive Appliance Load Monitoring (NIALM), attackers can determine the types and times of electrical appliances in a home, as well as learn detailed information about a resident's daily activities. Batra et al. (2014) have developed methods for determining the use of electrical appliances using "consumer profiling". Murrill et al. (2012) showed that analyzing energy consumption data over 15 min can determine the types and quantities of appliances used in a home. Molina-Markham et al. (2010) describe how a consumer can be "profiled" using only generic statistics, without detailed network signatures for electrical appliances, and without prior training. Greveler et al. (2012) showed that it is possible to identify which channel is watched on TV only by analyzing consumption data from smart meters. Also, some smart metering devices contain vulnerabilities that could be used by hackers. For example, security

I. Rigoev (✉) · A. Sikora
Institut für Verlässliche Embedded Systems und Kommunikationselektronik (ivESK), Hochschule Offenburg, Badstraße 24, 77652 Offenburg, Germany
e-mail: ivan.rigoev@hs-offenburg.de

D. Ould Abdeslam (ed.), *Smart Meters*, Lecture Notes in Energy 97,
https://doi.org/10.1007/978-3-031-27556-2_5

engineers in Spain discovered that local electricity company smart meters used the same key for AES128 encryption on all devices (Higgins 2014). Or discovering that no security measures are being used because of wrong settings (Carracedo 2019). Due to the significant development of intelligent networks and the data exchanged, hacking into networks or taking control of electrical infrastructures remotely could have dreadful consequences such as the paralysis of the electrical network.

To better understand the current state of French, German, and Swiss smart metering systems were made a comparative security analysis of these systems and it is presented in this chapter.

In Sect. 2 we will consider smart metering supervisory authorities, their requirements, and common smart metering solutions and compare them with reference smart metering infrastructure architecture model.

In Sect. 4, we will describe our methodology and provide more a detailed description of DLMS/COSEM protocol, its security, protocol and common implementations vulnerabilities, a comparison of DLMS/COSEM with TLS with BSI restrictions, and make a theoretical comparison of considered SMI systems.

In Sect. 6 we will present some parts of the penetration testing analysis of two BSI-certificated SMGW devices.

The last section contains some recommendations for future developments and already used smart metering systems.

2 Security Architectures—A Comparative Overview

In this section, we will summarize French, German, and Swiss legal acts and other available documentation related to smart metering. The objective is to describe their architectures and compare them with Smart Metering Coordination Group reference architecture for smart metering communications, which is described in the framework of the smart grids M/490 mandate (Sánchez Jiménez 2011) and smart meters M/441 mandate (CEN/CLC/ETSI/TR 50572, 2011).

2.1 French Case

In France, the protection of personal data confidentiality is guaranteed by the "Data Protection Act" 78-17 of 6 January 1978 "On Data Processing, Data Files, and Individual Liberties" (French National Assembly and the Senate 1978). This act has a wide scope of application, since all information relating to an identified or identifiable natural person, directly or indirectly, is considered as personal data. This act covers all the processing of this data and also gives a broad definition of the processing. Thus, the mere collection of personal information constitutes the processing of these data within the meaning of the law, as well as data conservation. Terms of the areas covered by this act—are very similar to the GDPR. Compliance with this act must

be carried out under the control of the "National Commission of data processing and freedoms" (Commission Nationale de l'informatique et des libertés, CNIL).

In addition to a guarantee of data confidentiality, ensuring the absence of communication without consent by users, the securing of this data against malicious actions and piracy is provided by the regulations. The Data Protection Act required processing of personal data to "take all useful precautions, with regard to the nature of the data and the risks presented by the processing, to preserve the security of the data and, in particular, prevent them from being distorted, damaged, or from unauthorized third parties having access to them". This general obligation of security applies to all categories of personal data subject to processing.

Specifically, regarding electricity metering systems, Decree 2001-630 of 16 July 2001 (Légifrance 2001) [Decree 2004-183 of 18th February 2004 for gas (Légifrance 2004)] requires system operators to keep confidential commercially sensitive data (information whose disclosure could undermine the rules of free and fair competition and non-discrimination). Metering data are commercially sensitive. Since 2010, work has been carried out in France between the CNIL and the Energy Regulatory Commission (Commission de régulation de l'énergie, CRE) on the implementation of smart meters, focusing in particular on the question of data collected by this equipment processing.

In the European Commission recommendation from 9 March 2012 (EUR-Lex 2012) "on preparations for the roll-out of smart metering systems", European Commission has recommended that data protection should be integrated into the functionalities of equipment from their design and that their default settings should be as protective as possible of the security and confidentiality of personal information. For its part, intending to protect privacy, the CNIL has prohibited the collection of data that relates to consumption with a time step of fewer than 10 min for communicating electricity meters, which required avoiding too precise electricity consumption knowledge. General functionalities of French smart meters have been defined in the application of these CNIL recommendations.

Thus, the order of 4 January 2012 (Légifrance 2012a) defining the functionalities of smart electricity meters provides that consumption readings are taken at a time step that cannot be less than 10 min. However, this limitation only concerns installations connected at low voltage for power less than or equal to 36 kVA, which mainly corresponds to private installations, while installations connected at higher power may give rise to more regular readings. In response to the need for security, this order requires that the metering devices comply with safety standards approved by the Minister for Energy, this compliance being subject to verification and certification by the ANSSI. Concerning electricity metering, the order of 4th January 2012 (Légifrance 2012a) requires system operators to have their metering system certified under Decree 2002-535 of 18 April 2002 (Légifrance 2002).

The National Cybersecurity Agency of France (The Agence Nationale de la sécurité des systèmes d'information, ANSSI) is a French service created on 7 July 2009 with responsibility for cybersecurity (https://www.ssi.gouv.fr/en/mission/word-from-director-general/). ANSSI replaced the Central Directorate of Computer Security, which on July 31, 2001, replaced the Service central de la sécurité des

systèmes d'informations (SCSSI Eng. Central Service for Information System Security). By Decree No. 2009-834 of 7 July 2009 (Légifrance 2009) as amended by Decree No. 2011-170 of 11 February 2011 (Légifrance 2011), the agency has responsibility at the national level concerning the defense and security of information systems. It is attached to the Secretariat-General for National Defence and Security (Secrétaire général de la défense et de la sécurité nationale) under the authority of the Prime Minister. ANSSI is responsible for proposing rules for the protection of state information systems and verifying the implementation of measures adopted. In the field of cyber defense, it provides a monitor, detects, alerts, and reactions to computer attacks, especially on state networks.

ANSII considers a certification scheme called CSPN (Certification de Sécurité de Premier Niveau; https://www.ssi.gouv.fr/administration/produits-certifies/cspn/), aims to provide a first-level security certification for IT security products. CSPN set up by ANSSI in 2008 consists of "black box" tests carried out under tight deadlines. Its scope is similar to the vulnerability analysis performed within Common Criteria, with the following specificities:

- The assurance process is simplified
- The evaluation is focused on vulnerability analysis
- The actors are committed to a given evaluation duration and cost.

IT products can currently apply to CSPN if they belong to a specific list of domains (e.g. data deletion, firewalls, secure communication, etc.). This list is regularly updated to address new needs. It should be noted that standard CSPN excludes products too complex to be evaluated in an expected duration and cost and products including non-standard cryptography. The organization and evaluation methodology process is similar to the Common Criteria process. Instead of applying CC security and assurance requirements, the developer uses guidelines described in CSPN. CSPN also has common features with CPA, especially the domain-specific approach. CSPN is used for meters and data concentrator security certification.

On 15 November 2012 (Légifrance 2012b), the CNIL adopted a recommendation that sets the framework and conditions under which consumption data from smart electricity meters may be collected and processed. CNIL recalled that the implementation of smart meters presents risks concerning privacy and recommended the introduction of strong technical measures guaranteeing data security. Beyond IT security, the CNIL has recommended that all players processing data collected by the network operator implement additional security measures because the increase in the level of detail of the data leads to an increase in the risk of invasion of privacy. In this recommendation, the CNIL recalls that the future deployment of smart meters will lead to a very large amount of data collected. In particular data relating to the quality of the electricity supplied to the subscriber or consumption indices, which are already used and processed data. Above all, smart meters offer a new functionality by making it possible to collect information relating to the load curve, consisting of reading at regular intervals of the subscriber's electricity consumption which, according to the CNIL, would make it possible to have information about people lifestyle details (identification of wake up and bedtime, periods of absence, even the

volume of hot water consumed per day or the number of people present in the accommodation). The CNIL, therefore, wanted to regulate the conditions for collecting and use of this load curve by smart meters, recalling that these operations are subject to the Data Protection Act. On the other hand, the storage of the load curve by the meters, without the feedback of the information to the network manager, complied with the requirements of the Data Protection Act.

In general, the Data Protection Act requires the prior consent of the person concerned to be obtained before any processing of personal data, except under certain specific conditions (when the processing of this data is subject to a legal obligation, execution of a public service mission or a contract, for example). Data subjects have the right to access and rectify data concerning them and may object, for legitimate reasons, to the processing of their data. The Data Protection Act also requires that the automated processing of personal data being the subject of a declaration to the CNIL, or even of authorization from this commission for certain categories of data (biometric data, relating to offenses, etc.). The Data Protection Act subjects those responsible for processing personal data to several obligations in terms of informing the persons whose data is processed and regulating the duration of data retention which must be proportionate to the purpose for which the data is collected.

The Data Protection Act fully applies to data from smart grids and no additional legal instrument had to be adopted to guarantee the confidentiality of this data. However, since actors in the energy sector are less familiar with this regulation than in other sectors where data management is already well known problem, the CNIL specified in Deliberation 2012-404 of 15 November 2012 (Légifrance 2012b) how this is applied to the specific area of smart grids, primarily on data collected (consent and limiting load curve sampling period), the duration of data retention (no conservation beyond the time required), the recipients of the data (habilitation) and security measures (assessment and regular updating).

The CNIL has indicated that the processing of the load curve can only be implemented for three purposes:

- maintenance and development of the network (by the DSOs)
- establishment of tariffs adapted to household consumption (by energy suppliers)
- provision of complementary services (by third-party companies).

Taking up the general obligation provided in Article 6 of the Data Protection Act, the CNIL recommended limiting the data retention period to the time necessary to achieve the purpose for which these data are collected. Compliance with this obligation is monitored by the CNIL, which can impose pecuniary sanctions after formal notice to the persons concerned. Penal sanctions are also incurred, ranging up to five years of imprisonment and a fine of 300,000 euros.

In addition, it specifies that the framework for the collection and use of the load curve must be defined according to the recipient of this collection:

- when the recipient is the network manager, the collection of the load curve must be carried out only when power supply problems are detected and not systematically;

- when the recipients are suppliers and service providers, and the load curve is used to set tariffs adapted to household consumption and the supply of additional services, it is necessary to collect the load curve beforehand. Express consent of the persons concerned, which must be free, informed, and specific.

CNIL has developed, within the framework of a partnership with the Fédération des Industries Electriques, Electroniques et de Communication (FIEEC), a "Compliance pack for communicating meters" (Pack de conformité compteurs communicants) (CNIL 2014) which is presented as a guide to good practice intended for manufacturers giving concrete indications on how to comply with the texts relating to the protection of personal data, and specific operating methods.

This compliance pack provides recommendations on how to handle data collected by smart devices based on three scenarios:

- the "IN-IN" scenario, which concerns the management of data collected in the home without communication with the outside (for example, communication mechanisms between the thermostat and the heating or smartphone applications that only send information to the user). This scenario does not impose any formalities before data collection but requires security measures to ensure that no unauthorized person has access to the data;
- the "IN-OUT" scenario, which applies to the management of data collected in the dwelling and transmitted outside (for example, electricity consumption data transmitted to a third party for a thermal renovation service). The service provider must make a declaration to the CNIL and must obtain the prior consent of the person concerned;
- the "IN-OUT-IN" scenario, which concerns the management of data collected in the dwelling and transmitted outside to allow remote control of certain equipment in the dwelling (for example, remote production control system domestic hot water). As for the previous scenario, the service provider must make a declaration to the CNIL and must obtain the prior consent of the person concerned.

Regarding data security technical aspects the Compliance pack has only very abstract requirements which are not so much different for different scenarios. For example, the security part from CNIL Scenario 2 "IN–OUT" contains such requirements as:

- The service provider shall put in place measures to ensure the security and confidentiality of the data processed by the devices provided to the person and shall take all appropriate precautions to prevent being taken over by an unauthorized person, in particular by:
- Providing encrypted data exchanges with state-of-the-art algorithms, protecting the encryption keys from any accidental disclosure, authenticating the devices receiving the data, and making access to the control functions of the installation conditional on authentication of a reliable user (password, electronic certificate, etc.).
- Thus, the measures put in place must be adapted to the level of sensitivity of the data. Regarding the measures to be put in place at the level of infrastructures

external to the housing, the service provider must carry out a study of the risks generated by the treatment to determine and implement the measures necessary to protect the privacy of individuals.

Thus, the application to the energy sector of the regulations relating to data protection should make it possible to prevent the breaches of privacy that the development of the digitalization of networks could have risked causing. Although the documentation produced by the CNIL (recommendations and compliance pack) does not in itself have a binding legal force, it helps guiding professionals by illustrating the concrete application to smart networks of the Data Protection Act.

Because in France smart grids are considered as specific Industrial Control Systems—the most appropriate document with requirements from ANSII is "Cybersecurity for Industrial Control Systems—Detailed Measures" from January 2014 (ANSSI 2014). Requirements from this document theoretically should be applicable for smart metering systems because the working group was not interested in a particular industry and the elements contained in this document are therefore intended to apply to all sectors. Security requirements in this document are more concrete, but it is not fully clear which of these requirements should be applied for smart metering systems.

The importance and usefulness of carrying out impact studies before the deployment of smart grid equipment, following the European recommendations which are described above, was affirmed by CRE in the deliberation of 12 June 2014 (CRE 2014) providing recommendations on the development of low voltage electrical networks, although this is not a legal obligation.

One more important document is the French "Energy Code" (Code de l'énergie). The Energy Code is an official French legal code bringing together various provisions relating to energy law. Energy Code is a very large document, but the most important parts of the document are:

- DSOs are responsible for Energy Individual Data Protection.
- DSOs must ensure access to individual customers to their own energy data via a secured web portal.
- Individual customers must also be able to share—or authorize DSOs to share their data with any authorized third party (through express customer consent).

However, the consent process for individual customers is not yet fully defined (in particular roles and responsibilities of DSOs and Providers/Third Parties). Only in some specific cases, such as for "Flexibility aggregators" and "Energy Providers", there are clear indications of the need of collecting customer consent before getting any data from DSOs. There is no clear indication concerning the process of controlling consents collected on the provider side by the DSO and this is perceived as a weakness because there is no clear guarantee that customer data is properly used.

Enedis and GRDF

All documentation described above does not contain architecture or communication protocol requirements for smart metering systems. There are about 144 distribution

system operators in France (Rullaud and Gruber 2020), but Enedis and GRDF dominate the electricity and gas DSO market. The problem with the lack of information in French documentation for comparison is partly solved because both Enedis and GRDF have only one possible solution for smart metering—Linky smart meter for electricity and Gazpar for gas. The following materials about French smart metering solutions in this document will refer to these systems.

Gaz Réseau Distribution France (GRDF) is a French gas distribution company founded on January 1, 2008. It is the main distributor of natural gas in France and Europe. It is a 100% subsidiary of Engie. GRDF took over the activities previously carried out by EDF Gaz de France Distribution, which operated as a directorate of Gaz de France with independent management (https://www.grdf.fr/english/leading-natural-gas-distribution-operator). Widespread deployment of the advanced Gazpar meter was approved by a decision of the Minister of Ecology, Sustainable Development and Energy and the Minister of Economy, Industry, and Digital on 23 September 2014 (Ministère de l'Écologie DDDEDL 2014). Gazpar should be deployed in 11 million homes by 2022 (https://www.grdf.fr/institutionnel/actualite/dossiers/compteur-communicant-gazpar). As a Linky meter, Gazpar allows remote reading and transmission of actual consumption indices.

Enedis, formerly ERDF (for Électricité Réseau Distribution France), is a public limited company with a supervisory board and management board, a wholly-owned subsidiary of EDF responsible for managing and developing 95% of the electricity distribution network in mainland France (https://www.enedis.fr/qui-sommes-nous). Enedis was created on 1 January 2008, under the name ERDF, by splitting EDF's electricity distribution activities into electricity generation, transmission, and marketing activities.

The first brick in the rollout of smart grids in the French electricity sector was the deployment of the Linky smart electricity meter which was decided by Law 2005-781 of 13 July 2005 (Légifrance 2005) on the orientations of the energy policy. This communication meter can collect consumption data (quantity consumed per hourly interval or power requested by the consumer) and can provide information to the customer himself, in particular to equipment inside the household, or third parties such as energy service providers (via Solenn). The download of daily data from the Enedis portal is possible at any time for customers in a simple standard file format. However, Enedis is working on an alternative file format, based on the IEC international data model CIM, which could be used as a starting base for the next steps in this ad hoc group to build a common interoperable standard. Collecting half-hourly data is possible only for customers that have provided their consent. Enedis may have access to half-hourly data without collecting consent only for operating needs, in a limited timeframe, and in a specific area. Besides, consumers can also directly access their consumption data in near real-time via special adapter devices connected to the Linky meter.

Sharing data through the Enedis data exchange platform with a third party is currently possible only with energy providers, and it is not generalized yet. Separate consent is requested for data transmission and use but is not necessarily collected by the Enedis. The consent mechanism works as follows: customers equipped with

a Linky smart meter are invited to connect to the Enedis web portal where they can consent to the collection of their half-hourly data, storing in the information system, and downloading. Customers can easily opt-out of this process and so far, the web portal does not include the possibility to provide consent to share data with third parties. Providers can send requests to Enedis for starting load curve data collection (monthly to daily data and if available half-hourly data) and accessing customer data. There is no requirement to show the customer consent upfront, but the provider must be able to provide it if asked, to get access to daily and infra-daily data.

To limit the risk of intrusion into privacy, CNIL has strictly supervised data collection. Linky smart meters only report information concerning the consumer's total consumption and do not allow specific uses to be distinguished. The Linky meter can measure three main types of data (UFC-Que Choisir 2017):

- Consumption indexes. Before, they were estimated or transmitted either by the distributor to the supplier, or by the consumer, to establish the invoicing. Now they can be reassembled automatically. No more than before, this information will not allow the distributor and suppliers to know consumption habits.
- The load curve, i.e. the graphic representation of the evolution of energy consumption over a given period. It consists of reading the subscriber's electricity consumption at regular intervals (the time step). This data could pose a problem because it would then be possible to determine at what time of day consumption is more or less important. To stem this risk, the CNIL has imposed that the transmission of the load curve is explicitly consented to by the consumer. In addition, if agreed, the interval at which data is uploaded to Enedis cannot be less than 10 min. Below this period, it is indeed possible to identify the uses that the consumer makes of his devices.
- Data relating to meter quality and security. These data are not personal. They allow Enedis to check the quality of the power supply, power cuts, or even check the openings of the meter cover to prevent fraudulent acts. The collection of this data does not make it possible to know the consumption habits of the consumer.

Refusing to allow Enedis access to its meter to replace it with Linky is illegal (https://www.fournisseurs-electricite.com/guides/compteur/linky/refuser) insofar as electricity metering devices are the property of the local authorities, which grant Enedis management of them, as provided for in Article L322-8 of the Energy Code. The same article also specifies that the DSO is responsible for intervening on the meters for operations such as connection, commissioning, and shutdown of meters or power changes.

Electricity distribution in France is a public service. In accordance with the provisions of concession contracts concluded between local authorities and the network manager, the latter is responsible for the execution of this public service, which he must ensure in compliance with the law and the regulation. However, the law requires the implementation of counting devices. By opposing the installation of Linky meters, clients take the risk of opposing the execution of a public service mission.

In addition, when clients conclude an electricity supply contract, they join the general provisions relating to the access and use of the public distribution network

(GRD contract). In its 2016 version, this contract indicates that (UFC-Que Choisir 2017):

- The customer must commit to "taking any provision to allow DSO to carry out the installation, modification, maintenance, and verification of counting equipment" (art. 2.3).
- The Customer is responsible for "direct damage and some caused in DSO in the event of non-compliance with one or more of the obligations charged to him for access and use of the RPD [Public Network for the Distribution of Distribution electricity, editor's note]" (art. 6.2).
- DSO may make the suspension or refuse access to the RPD, in particular in the event of "non-justification of the compliance of the installations to the regulations and the standards in force" (art. 5-5, point 5).

However, the law requires the implementation of smart meters. Concretely, this means that:

- If a consumer will not allow DSO to make the installation or modification of the counting equipment, DSO will be deprived of the possibility of carrying out a remote meter statement and will therefore be founded to invoice the consumer a special statement.
- By refusing DSO the installation of the meter, the consumer would refuse to bring it up to standards and therefore be exposed to the suspension of access and use of the RPD.

If the installation of the meter has been refused by the consumer, CRE admits that the succession of the meters is billed by the network manager thus causing additional costs for the user (CRE 2016).

Enedis Smart Metering Architecture

Enedis smart metering architecture and used protocols could be founded in the document Linky PLC profile specifications (ERDF-CPT-Linky-SPEC-FONC-CPL) which for some reason currently unavailable on the Enedis website, and only version 1.0 from the year 2009 possible to find on the internet (EDRF 2009). This document describes a stack of protocols that should be used for the Linky system including the application layer protocols. On top of PLC should be used Logical Link Control protocol (LLC) IEC 61334-4-32, IEC 61334-4-41:1996 Distribution automation using distribution line carrier systems—Part 4: Data communication protocols—Section 41: Application protocol—Device Language Message Specification (DLMS), and COSEM from Blue and green "Coloured Books". The objects associated with PLC network management are defined by the COSEM class instances ID 50, 51, 52, 53, and 56 described in the Blue Book. The encoding rules are described in the A-XDR standardization document—Distribution automation using distribution line carrier systems—Part 6: A-XDR encoding rules. The objects accessed via the COSEM application layer are identified according to the rules specified in IEC62056-61 Electricity metering—Data exchange for meter reading, tariff, and load control—Part 61: OBIS Object identification.

Document IDIS (Interoperable Device Interface Specification) White Paper points out that Linky smart meter meets IDIS specifications, and ERDF has issued the LINKY companion specifications describing how these standards are used and which options are chosen (but we were not able to find this document). IDIS specifications will be considered more precise in Sect. 4.3.

Enedis smart metering architecture includes a Linky meter that is commonly installed inside a private territory, a data concentrator installed at non-private territory, and supervisory control servers (Fig. 1). Data concentrator units are used to interrogate meters, to process and store the information it receives, and to send this data to a centralized Information System. Enedis concentrators do not decrypt data (only resend it to a backend system). Every Linky meter connected to a Data concentrator device via PLC (power line carrier). By default, data concentrators are connected to Enedis servers via a cellular network. Common Enedis protocols stack has no other options for these connections.

PLC—is a protocol that uses the possibility to transfer data using common power grid communications by adding high-frequency electrical signals over main 50 Hz (Chauvenet 2016). The main advantage of this technology is that additional communication wires of telecom infrastructure do not require, and that allows to be independent of telecom operators. The most significant shortcoming of PLC technology is that PLC can produce a good signal only at approximately 100 m. To solve this problem—every Linky meter works like a mesh node (after receiving a signal Linky repeats it). On average Enedis use one concentrator per 60 Linky meters, but 1 concentrator can cover up to 1000 smart meters with PLC-G3.

Additionally, the Linky system provides a list of useful features, such as:

- Recording and remote transmission of supply-quality data
- Remote home appliance control
- Energy box management

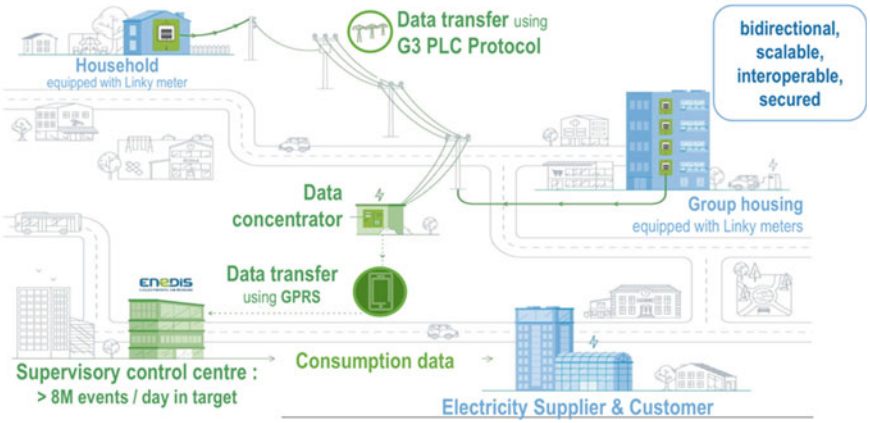


Fig. 1 Enedis DSO smart metering architecture (SMARTER TOGETHER 2019)

- Remote control of the data concentrator and diagnostic
- Remote interrogation of a meter group (Grouped Meter Ping)
- Power outage detection
- Analysis of the loss of power supply on the data concentrator
- Loss of phase alarms on triphased meters
- Reverse voltage detection alarm on the data concentrator
- Remote transmissions of fault detectors connected to the data concentrator
- Analysis of PLC connection between meters and their data concentrator
- "Predictive Maintenance" tools such as CartoLine.

One of the Linky system features is the ability to manage the power consumption of certain appliances in the home. Enedis does not have direct access to the power of home appliances and can only give a binary signal to the "advice" to turn off some of the 7 virtual ports. Physically Linky has only one port—dry contact (French name "Contact sec") (enedis.fr Notice d'utilisation du compteur communicant Linky).

Energy box is a battery device that allows storing energy that could be used in a time when energy cost is high. Linky can count both consumed energy and generated energy (e.g., by private solar panels). When solar panels generate more energy than consumed energy, it can be returned to the energy system to make a profit.

CartoLine is a "Predictive Maintenance" tool for Enedis LV networks. The question answered by CartoLine can simply be summed up as: does the observed voltage data require the intervention of a field technician to avoid a breakdown? The CartoLine tool, developed by Enedis R&D, uses the mass of data relating to the voltages observed by Linky meters to significantly improve the management of predictive maintenance on the low-voltage network. For experts, it offers a Dataviz interface facilitating data analysis. Above all, artificial intelligence runs these analyses in "supervised learning" first and then can conduct them autonomously. These analyses aim to identify situations reflecting a voltage anomaly or a future incident that could lead to a power outage on the LV network.

About security—Enedis mentioned that the security of the Linky system builds on a chain that goes from the meter itself to the Enedis data centers, via the thousands of concentrators deployed throughout France. At each stage, different points of attention were addressed (Marcellin 2018).

About the Linky system field part—each meter is CSPN certified. It has a key to encrypt (in AES standard, symmetric) the retrieved data locally and send it to the concentrator (each of these groups together 10–10,000 m, depending on the concerned area). A concentrator was designed as a digital safe device and it also CSPN and "Common Criteria" certified on behalf of the hardware. The data concentrator deletes the received data in the event of an intrusion detection or even abnormal operation. Another encryption (asymmetric based on elliptic curves) is used between the concentrator and the information system (IS) dedicated to Linky from Enedis. The dedicated IS is based on a DMZ (demilitarized zone), i.e. a sub-network isolated from others and the Internet, closed to business players and accessible only by workstations that are not themselves disconnected from the intranet and the Internet (e.g., no emails). All of the provisions described systems are part of a dedicated PKI

(Public Key Infrastructure) to ensure the trust and durability of the system's security certificates. Finally, at the end of the chain, data that could be used by other Enedis information systems, is passed through controlled interfaces as encrypted flow towards the IS of other companies (RSA following the general ANSSI security reference).

Every household should have its own Linky meter. By 2021, Enedis has already deployed 35 million Linky meters, 770,000 data concentrators, 110,000 remotely controlled devices, replacing about 90% of old meters with a Linky meter. More information about the Linky meter rollout can be found in the documents "Le déploiement du compteur Linky" from the French Ministry of Ecology contains (Ministère de l'Écologie 2017) and "Report on the deployment of Linky smart power meters in the area" from 01 July 2019 (SMARTER TOGETHER 2019).

2.2 German Case

Protection of personal data from smart networks, in particular smart meters, is guaranteed at the legislative level by the Act on Electricity and Gas Supply (Gesetz über die Elektrizitäts- und Gasversorgung—Energiewirtschaftsgesetz, EnWG), which was published 7 July 2005. EnWG requires consumers consent before data collection and limits the data retention period.

The legal basis for smart metering rollout in Germany is described in "Act on the Digitization of the Energy Transition" (Gesetz zur Digitalisierung der Energiewende—GDEW). In February 2015, the Federal Ministry for Economic Affairs and Climate Action (Bundesministerium für Wirtschaft und Klimaschutz BMWK was BMWi) presented the key points for a regulatory package that was intended to promote the use of intelligent measurement systems security and cost-effectiveness. The measures required for the transition of the electricity supply to a decentralized system with bidirectional power and information flows includes:

- Avoidance of disproportionate costs for end consumers, producers as well as metering point and network operators in the conversion of 80% of end consumers to intelligent metering systems Smart Metering, which is required by EU Directives 2009/72/EG and 2009/73/EG.
- Minimal technical requirements to maximize the overall economic benefit from energy savings and load shifting.
- Provision of data protection and data security.

For the roll-out of the intelligent measuring systems (iMSys) in accordance with the law on the GDEW, a display of consumption and generation data that is protected against manipulation and conforms to calibration law is required for invoice verification purposes. End consumers should be able to carry out evidence-proof checks of bills from energy supply companies. In addition, the end consumer should be allowed to call up their current consumption values. More precisely this is described in the document Application Rule AR2418-6.

Moreover, the introduction of intelligent metering systems is tied to the compliance with a staggering price cap for annual costs to protect the end consumers from an extensive cost increase. Consumers have the option to choose an independent third-party metering operator if they are not satisfied with the solution offered by the Distribution System Operator (DSO), who in most cases is defined as the default metering operator if the consumer is not choosing a different operator.

On 2 September 2016, GDEW entered into force (Landis+Gyr 2020). The law also introduces specific and detailed requirements, both for the design of smart meter devices and for the transmission of data. GDEW's goal is to open the German energy market to digitization while ensuring a high standard regarding data protection and ICT security. GDEW's key feature is the introduction of smart meter gateways (SMGW). The gateways will provide each of the actors involved in supplying electricity with all of the information on generation and consumption that they need—from the grid operator or electricity supplier to the consumer. At the same time, smart meter gateways should provide the highest level of data privacy and data security.

The central element of GDEW is the Measuring Point Operating Act (Messstellenbetriebsgesetz, MsBG) which entered into force in September 2016 and regulates the metering points operation market and the equipment of the grid-bound energy supply with modern measuring devices and intelligent measuring systems. MsBG is divided into 4 parts:

- Part 1 regulates the scope and the terms used.
- Part 2 (§§ 3-48) regulates the operation of the measuring points, including the equipment of the measuring points with modern measuring devices and intelligent measuring systems, staggered over time and according to annual consumption.
- Part 3 (§§ 49-75) contains specific data protection regulations.
- Part 4 (§§ 76-77) determines the supervision by the Federal Network Agency (Bundesnetzagentur, BNetzA).

MsBG defines meter operation and measurement as a separate area of network operation that creates new market roles and has abolished electricity billing fees. It prescribes the comprehensive installation of modern measuring devices and intelligent measuring systems by the so-called "basically responsible metering point operator for modern measuring devices and intelligent measuring systems" (§2 No. 6 MsbG) by 2032. The norm addressees of the law are the German distribution system operators/supply grid operators (Versorgungsnetzbetreiber), considering that meter operation is dogmatically separated from network operation. As the basic metering point operators (gMSB), DSO's initially responsible for the rollout and administration of modern metering systems. As a result, the scope of tasks has expanded (previously metering device operation, measurement, and billing). Using a special public procurement procedure, they can however transfer this position to a third-party service provider.

MsBG defines extensive technical requirements for the technologies involved, particularly regarding the reliability and security of energy measurement and data transmission. Compliance with the new rules is controlled and supervised by

both the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik) and the Federal Network Agency (Bundesnetzagentur).

One more important document is the "intelligent metering systems rollout plan". This roadmap describes how gateways should be developed into a comprehensive digital communication platform for the energy transition ("Standardisierungsstrategie and zur sektorübergreifenden Digitalisierung nach dem Gesetz zur Digitalisierung der Energiewende Roadmap für die Weiterentwicklung der technischen BSI-Standards in Form von Schutzprofilen und Technischen Richtlinien"). The process comprises different rollout periods for different types of end consumers and plant operators, depending on the amount of energy they consume. For small consumers—whose annual consumption is less than 6000 kWh/a and/or feed-in systems < 7.5 kW peak, ca. 85% of the market or small producers of renewable energy or cogeneration—whose capacity is less than 7 kW, the installation of a smart meter remains optional because considered that the achieved energy savings would not return the invest of a SMGW installation. Customers with higher consumption and/or bigger renewable energy feed-in systems should install SMGW (ca. 15% of the market).

In Germany, the situation with DSO is different from France, because in the electricity sector exist 883 distribution network operators of varying sizes (Rullaud and Gruber 2020). The general rollout of intelligent metering systems began when BSI certified smart meter gateways (SMGW) from three manufacturers and issued a corresponding market declaration.

The Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, abbreviated as BSI) is the German upper-level federal agency in charge of managing computer and communication security for the German government. BSI is responsible for the security of computer applications, critical infrastructure protection, cybersecurity, cryptography, counter eavesdropping, certification of security products, and the accreditation of security test laboratories. The BSI's scope of duties is defined by the German Federal Office for Information Security Act (BSI Act). The aim of the BSI is the preventive promotion of information and cybersecurity to enable and promote the secure use of information and communication technology in the state, economy, and society. As an example, the BSI develops practice-oriented minimum standards and target group-specific recommendations for action on IT and cybersecurity to support users in avoiding risks. BSI is also responsible for protecting the IT systems of the federal government. This involves defending against cyber-attacks and other technical threats to the IT systems and networks of the federal administration.

According to the requirements set by the "Metering Point Operating Act", the smart meter gateways must meet the security architecture defined by the BSI with regard to communication data protection and interoperability. These uniform technical and organizational specifications were written down in so-called protection profiles ("PP") and technical guidelines ("TR"), on which the BSI carries out the certification. The BSI has an extensive and well-structured documentation for the German smart metering infrastructure which describes at most every aspect of smart metering system work including

requirements both for the architecture and the protocols used for deploying smart metering system. A full list of documentation is publicly available on the BSI website (https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Smart-metering/smart-metering_node.html).

One of the most important BSI documents about SMGW is Common Criteria Protection Profile BSI-CC-PP-0073-2014. The Common Criteria (CC) for Information Technology Security Evaluation is an international standard (ISO/IEC 15408) for testing and evaluating the security characteristics of IT products. The protection profile describes possible threats to a smart meter gateway in its operational environment and defines the minimum requirements for appropriate security measures. The protection profile for the smart meter gateway focuses on the security performance to be met by a gateway and defines security requirements for the interfaces to the three networks (LMN, HAN, and WAN) that each gateway must provide.

Other important documents included the Technical Guideline BSI-TR-03109, which encapsulates requirements for functionality, interoperability, and security that the individual components in an intelligent metering system must meet. It specifies the security requirements and assumptions from protection profiles. The BSI-TR-03109 is divided into several parts:

- BSI-TR-03109-1 “Smart-Meter-Gateway”
- BSI-TR-03109-2 “Security module”
- BSI-TR-03109-3 “Cryptographic Specifications”
- BSI-TR-03109-4 “Public Key Infrastructure”
- BSI-TR-03109-5 “Other system units”
- BSI-TR-03109-6 “Smart Meter Gateway Administration”.

After passing the Common Criteria Protection Profile certification a SMGW model gets a BSI-DSZ-CC-* type certificate. In case a SMGW passes the test specification “Testkonzept zu BSI TR-03109-TS-1” the SMGW model gets a BSI-K-TR-* type certificate. The TR-03109-1 certification includes not only hardware tests—but also software, and because of it, this certificate includes information about the software versions.

The market analysis was firstly published by the BSI on 31 January 2019. On 31 January 2020, the BSI updated the market analysis and published the administrative act to determine the technical possibility of installing intelligent metering systems. Currently, already 4 smart meter gateway models are certified by BSI rules (https://icube.ch/Security/security1.html).

With an urgent decision of March 4, 2021, the Higher Administrative Court of Münster (Oberverwaltungsgericht, OVG) in procedure 21 B 1162/20 has the suspensive effect of the main action pending before the Köln Administrative Court (Verwaltungsgericht, VG) against the general ruling of the Federal Office for Information Security (BSI) according to § 30 MsbG. The decision of the Higher Administrative Court in Münster was made in the form of provisional legal protection. The main decision by the Administrative Court in Köln is still pending. The BSI will therefore examine the OVG’s reasons for the decision in detail and hopes

to be able to comprehensively refute the OVG's concerns in the main proceedings (https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/Stellungnahme-OVG-Muenster-Smart-Meter_080321.html).

The Federal Network Agency (BNetzA) was not and is not involved in the proceedings before the administrative courts. However, as the supervisory authority for the MsbG, the Federal Network Agency must decide how to proceed with supervisory measures in the future. Due to the large number and complexity of the questions associated with the urgent decision, a final assessment is not yet possible. The BNetzA is currently also in close contact with the BMWK and the BSI on the consequences of the decision (https://www.bundesnetzagentur.de/DE/Beschlusskammern/BK08/BK8_09_MsbG/BK8_MsbG_Basepage.html).

BSI Smart Metering Architecture

The BSI smart metering architecture and protocols are strictly defined in BSI-TR-03109. A central element in the German smart metering system is SMGW (smart meter gateway). SMGW manages connections between 3 networks, stores, and checks consumption data (Fig. 2). The network formed by connecting electricity, gas, water, and heat meters to a smart meter getaway forms an LMN (Local Metrological Network). In HAN (Home Area Network) a SMGW communicates with the controllable energy consumers or energy producers (Controllable Local Systems, CLS, e.g. intelligent household appliances, heat, power, or photovoltaic systems, circuit breakers). The SMGW also provides data for the end consumer or the service technician in a HAN. Via a WAN (Wide Area Network) interface, external market participants and gateway administrators can access, configure and monitor the SMGW. The main functionality of the SMGW includes storing the measured consumption values received from the LMN, processing them according to configured rules, and sending the processed measured values to authorized market participants in the WAN (such as consumption and network status data). A SMGW fulfills the tasks of a firewall system and separates the connected networks from each other. As a decentralized storage of personal measured values, which are only sent to authorized parties under contractual regulations, the SMGW ensures data protection and data security for the end consumer.

A SMGW administrator is the most important actor in the German SMGW system. A SMGW administrator performs the following list of tasks:

- device management. Devices (meters, CLS, display units) must be registered by the SMGW administrator and assigned to an end user.
- client management. The SMGW administrator must create, edit, assign or delete assigned certificates or user ID/passwords.
- profile management. The SMGW administrator must have the opportunity to install and change meter, communication, and evaluation ACP (access control profiles) e.g. activate and delete tariffing and network status reporting.
- key/certificate management. The SMGW administrator must insert, activate, deactivate or delete keys and certificates for communication with meters, CLS, and external market participants.

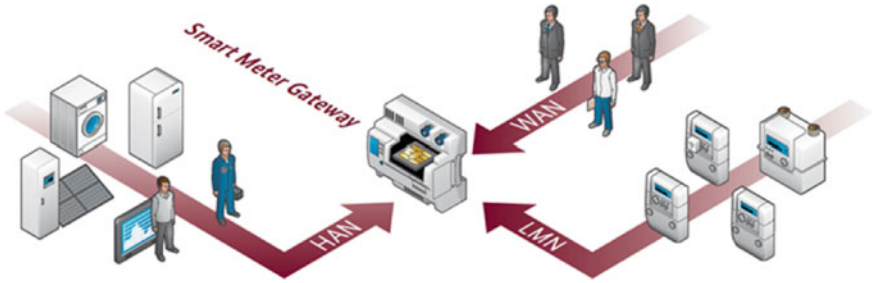


Fig. 2 German SMGW networks (https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Smart-metering/Smart-Meter-Gateway/smart-meter-gateway_node.html)

- firmware update. The SMGW must allow the SMGW administrator to install, verify and activate new firmware in the SMGW. The SMGW admin must have mechanisms to verify the integrity before the activation of a SMGW can take place.
- configures, monitors, and controls an SMGW. The SMGW must allow the SMGW administrator to query the status of the SMGW and to read log entries from the system and calibration log. The GWA is not allowed to access privacy-relevant data, such as billing or meter data. The GWA can read a log with records of local attacks on SMGW.
- wake-up configuration. The SMGW must allow the SMGW administrator to configure the address of the wake-up service.
- can perform the GW operator role (delete CMS signature to pseudonymize data)

The German smart metering system uses two types of user data. Identifiable data used for billing purposes and pseudonymized data. Pseudonymized data is used by a grid operator to control the functioning of the energy network. By using pseudonymized data an operator cannot know who exactly consumed the reported amount of electricity because instead of a user name used an impersonal ID number and a grid operator gets this data integrally. That means that only the area in which the user is located is known. Since high-resolution energy consumption profiles can be used maliciously, the SMGW offers the possibility to calculate the total electricity cost locally at the SMGW and send it to the energy service provider once per month. By BSI requirements metering data must be stored directly in the SMGW. Data for up to 24 months can be downloaded at any time by the customer and shared with third parties. The supplier, who has the right to use the data, is obliged to delete all person-related metering data after the completion of his tasks.

Only SMGW administrators can install and change ACPs. An ACP defines which and how often data should be sent to external market participants and which cryptographic keys should be used for symmetric encryption and asymmetric data signing on the content layer. There are 3 types of profiles that determine how the SMGW collects and processes measurements from meters:

- Meter Profile: The Meter Profiles specify how a SMGW interacts with a Smart Meter. Among others, it configures the unique meter identifier, which protocol to use, which measurement registers to collect, information regarding encryption, and whether the communication is unidirectional or bidirectional. It also configures the time interval in which a SMGW must receive or request the measurements and update the internally saved latest meter reading.
- Evaluation Profile: The Evaluation Profiles specify which data need to be derived from the meter measurements. This is done by configuring a tariff use case and the respective parameters. Each examination profile contains a list of Communication Profiles determining the recipient of the generated data.
- Communication Profiles: There are different Communication Profiles for the HAN and the WAN. In both cases, the profiles define connection details that specify how to reach a communication partner based on uniform resource identifiers (URIs). For each of the three profile types, multiple instances may be configured, e.g., multiple Meter Profiles to collect measurements from multiple meters.

All secure keys and certificate materials (such as a private key for TLS authentication) must be stored in an SMGW hardware security module—HSM, which is a CC-certified (BSI-CC-PP-0077) subcomponent that is used for providing cryptographic operations. The smart meter gateway internally communicates with a security module via APDU commands (which are commonly used in smart cards such as SIM cards). More information about this can be found in BSI TR-03109-2. Full functional requirements for all three SMGW networks are presented in BSI TR-03109-1 paragraphs 2.3.1–2.3.4.

A SMGW communicates with meters only in the local metrological network—LMN. Locally connected meters have been made known to the SMGW by the SMGW administrator in the form of meter profiles. According to the TR, the LMN interface can be designed either as a short-range radio interface (wireless Mbus) or as a serial interface. Wireless connections have two variants—uni- and bi-directional communication. A uni-direction type of connection is required because a lot of smart meters could work only in uni-directional mode.

In cases of wired and wireless bi-directional communication connections are secured by the TLS protocol. In case of a uni-directional communication connections are secured by using AES-CBC+CMAC. The BSI TR-03116-3 (3.3.4) states that SMGW must be able to implement the role of the TLS server as well as the role of the TLS client to secure the communication links in the LMN. A SMGW must use HSM (hardware security module) for TLS handshakes and other cryptographic operations. For mutual authentication between a SMGW and meters in the LMN, LMN certificates which are X.509 self-signed certificates must be used.

The data transmitted by the connected meters in the LMN can be consumption values as well as information on energy quantities fed into the grid (e.g., in case of photovoltaic systems, combined heat, and power plants). Also, further parameters relevant to grid operation such as grid voltage, frequency, and phase angle, which may be provided by a meter, can be recorded by the SMGW. The following processing steps are performed by the SMGW at the LMN interface:

1. The SMGW receives or retrieves the measured values of the locally connected meters at regular intervals. The SMGW receives the measured values in an encrypted form and securely integrates them.
2. After successful decryption and integrity check of the measured values, the SMGW provides them with a timestamp provided by the system clock of the SMGW and stores them in measured value lists.
3. The SMGW determines derived value from certain measured values using a set of rules and sends these processed values to authorized external market participants.

For reasons of data protection, BSI has precisely defined how the software must process the measured values according to the respective evaluation profiles in the gateway. There are various tariff use cases (TAF) for tariffing, balancing, and network status data collection, which must be implemented as a minimum requirement of SMGW through regulations.

According to the BSI's standardization strategy, the conformity of Generation 1 smart meter gateways with calibration law is evaluated based on application rule 50.8 defined by the National Metrology Institute of Germany (Physikalisch-Technische Bundesanstalt or in short PTB). Currently, there exist 14 tariff use cases, but Generation 1 smart meter gateways support only TAF 1, 2, 6, and 7.

After collecting data from a smart meter the SMGW should check it, and send it to external market participants (EMP or EMT in German) in Wide Area Network (WAN). The WAN interface is designed as an IP interface. Usually, the SMGW uses a cellular network to connect to external market participants (Fig. 3). There also exist solutions that use Ethernet as a WAN port, but in practice, they are less common.

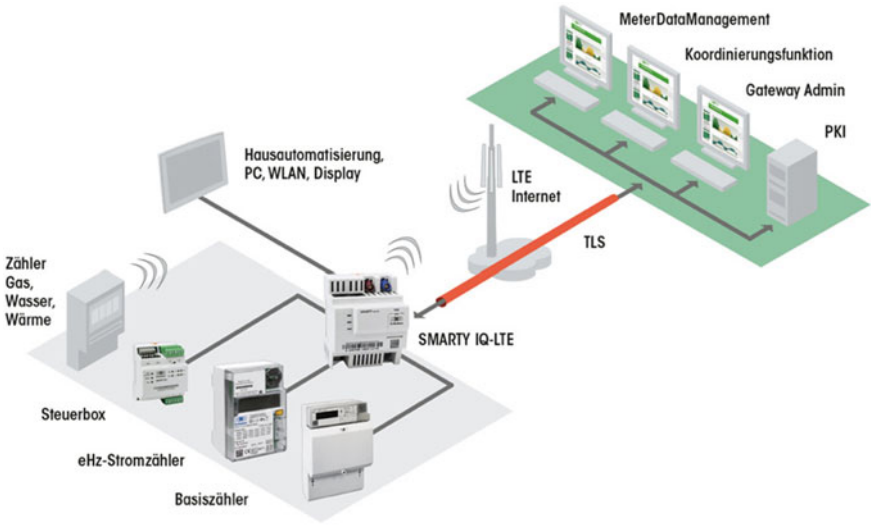


Fig. 3 German smart metering architecture (Siconia® SMARTY IQ-LTE | Sagemcom)

The Smart Meter Gateway is integrated into a public key infrastructure via the WAN interface and all communication is encrypted with TLS. A WAN connection must always be established as a mutually authenticated TLS channel based on certificates. The used certificates must be issued by the Smart Metering Public Key Infrastructure (BSI 2017). In cryptology, a public key infrastructure (PKI) is a system that can issue, distribute and check digital certificates.

All WAN use cases and communication scenarios are described in BSI TR-03109-1 chapters 3.2.2–3.2.3. For the communication with participants in the WAN, the SMGW must always implement the role of the TLS client and the remote terminal the role of the TLS server—which means that all communication connections must always originate from the Smart Meter Gateway. WAN connections can be established by the gateway at specified times (e.g., by a timer trigger), or by spontaneous events. The ability to react to spontaneous events requires the use of a SMGW wake-up service (WAF 7)—which is the only way to establish a connection with a SMGW from outside. Only SMGW administrators can get access to this service using valid cryptographically signed messages because a SMGW should not respond to any other connection attempts. A more complete description of the wake-up service could be found in BSI TR-03109-1 chapter 3.2.5.

Data in WAN SMGW communications are not always transmitted via a direct transport channel between a sender and an end recipient, but sometimes via third parties (e.g., the gateway administrator). This type of data exchange between communication partners in the WAN takes place within a TLS channel based on messages encrypted and signed at the content level for the end recipient via CMS (Cryptographic Message Syntax). CMS is a special set of data types each of which can be represented as a box performing a certain action, for example—encryption. CMS types Signed-data Content-Type and Authenticated-Enveloped-Data Type are used to sign and encrypt data. More information can be found in the document "Technische Richtlinie BSI TR-03109-1 Anlage I: CMS-Datenformat für die Inhaltsdatenverschlüsselung und -signatur". CMS is used for data pseudonymization. A SMGW replaces the client identification number with a pseudonym, encrypts, and signs the data at the content level. Only the energy service provider has the key to decrypt this data. In the case of pseudonymized transmission of measured values (network status data), the SMGW must replace the canonical device ID of the SMGW and the canonical device ID of the logical device from which the measured values originate with a pseudonym. The pseudonymization of network status data during transmission from the SMGW to an external market participant must be ensured by the following steps:

1. The SMGW removes the unique canonical device ID from measured values that are to be transmitted pseudonymized following an evaluation profile and replaces it with a pseudonym stored in the evaluation profile.
2. Data prepared in this way are then encrypted by the SMGW for the recipient (EMT), signed, and transmitted to the SMGW administrator.
3. SMGW administrator checks the signature of the SMGW, thus verifies the authenticity of the received data and forwards it to the recipient after removing the SMGW signature.
4. The recipient decrypts the message.

Tracing the final consumer based on the signature of the sending SMGW is much more difficult for the recipient (in the example: EMT-A) because the SMGW signature has been removed by the SMGW administrator. Tracing the final consumer via a canonical device ID is considerably more difficult for the recipient since the data contains a pseudonym instead of the canonical device ID.

For metering and gateway administration used COSEM IEC 62056-6-2 with OBIS (Object Identification System). COSEM (Companion Specification for Energy Metering)—is a specification that reflects an interface model of the metering devices to represent their functionality. The interface model uses an object-oriented approach.

Home area networks (HAN) are networks that ensure the networking of computers and their peripheral devices in smart homes and home offices. For authorized end-users, a SMGW provides the possibility to retrieve information stored in the SMGW through the end-user interface in HAN. This scenario is implemented by HAF1: End-user data provision. This data can only be accessed in read-only mode and only after successful authentication. The reading and visualization of the data at this interface, requires a dedicated cryptographically secured display, local PC, or another (CLS) device that can process the cryptographically secured data stream. Other SMGW functions in the HAN interface include:

- HAF2: Service technician data provision.
- HAF3: Transparent communication channel between CLS and active EMT.
- HAF4: Establishing GWA communication by a service technician.
- HAF5: Triggering of self-test functions by a service technician.

There are 5 HKS (HAN communication scenarios) for SMGW in HAN (Home Area Network):

- HKS1: Bidirectional communication in HAN with authentication using HAN certificates.
- HKS2: Bidirectional communication in the HAN with authentication using a unique identifier and Password.
- HKS3: Transparent communication channel initiated by CLS.
- HKS4: Transparent communication channel initiated by active EMT.
- HKS5: Transparent communication channel initiated by SMGW.

As shown, a connection can be initialized by an EMT, the SMGW, or the CLS initiative, but it previously requires a registration by the SMGW administrator. HKS1 can be used by the end-user to retrieve consumption data or by a service technician to obtain technical data. In HKS1 the SMGW implements the role of the TLS server and the participant implements the role of the TLS client. When establishing the TLS connection between the HAN participant and the SMGW, client–server authentication is performed in the TLS handshake using the GW_HAN_TLS_CRT and CON_HAN_TLS_CRT certificates and their associated keys. The certificate CON_HAN_TLS_CRT is uniquely assigned to an end-user or service technician known to the SMGW.

In HKS2 the SMGW implements the TLS server role and the end-user implements the TLS client role. A service technician must not use the communication scenario

HKS2 and should use a special certificate for authorization. As mentioned before, the SMGW also supports the remote control of CLS (controllable local systems) by EMP (external market participants). For this purpose, the SMGW provides HKS3, HKS4, and HKS5 using communication channels secured by TLS within which an EMP can communicate with a CLS using any protocol that works over TLS.

To be able to use HKS3 CLS should support the draft RFC "Secure Sockets Layer for SOCKS Version 5". By default, SOCKS5 does not encrypt traffic and for security purposes, this draft RFC requires establishing a TLS channel before the main connection establishing. In the case of HKS3 CLS initiates the communication by connecting to a SMGW SOCKS5 port. The SMGW answers by indicating the support of the X'86' authentication method only. The CLS in the role of TLS client initiates the TLS connection. The SOCKS5 protocol in this case is required to redirect data from the SMGW specified in Socks5 message EMP. Before establishing this connection, the SMGW should check if the SMGW administrator allows the connection of this CLS to the requested EMP by checking the communication profiles. Because direct connections from the WAN to SMGWs are forbidden, in HKS4 the EMP must first set up the backend system TLS server port and send a connection request to the SMGW administrator with the necessary CLS information (proxy profile ID and connection profile ID). Then SMGW administrator wake-up SMGW and use these IDs to establish a connection to an EMP. In this case CLS should be able to implement a TLS server role. The SMGW implements the role of the TLS client both in the HAN and the WAN. In HKS5 a connection is initialized by a SMGW trigger which could be some timer or event. As in HKS4, in HKS5 the SMGW implements a TLS client role in HAN and WAN and the CLS implements a TLS server role.

In all 3 scenarios of communication with an EMP the SMGW acts like a proxy server for controllable local systems (CLS) connected to the HAN. It means that TLS-protected communication channels in the direction of the CLS and the external market participant are terminated in the SMGW and the SMGW takes over the transparent forwarding of the received data. The current version of the TR requires the implementation of HKS1, HKS2, and HKS3 only. The implementation of HKS4 and HKS5 is optional. HAN use cases, communication scenarios, and profiles are described more precisely in BSI TR-03109-1 chapters 3.4.2.1–3.4.2.3, 3.4.3.1–3.4.3.5, 3.4.6.2.

Also, the HAN interface is used by the service technician to view configuration profiles and the system log that supports error diagnosing. The SMGW logs all actions in three different log levels, the system log, the end-user log, and the calibration log. Every important event (e.g., error messages, failure of the WAN connection, security-relevant events, activities of the SMGW administrator, etc.) in the SMGW is logged in the system log. This log can only be viewed by the authorized SMGW administrator and the authorized service technician on site. The information is used to identify the current status of the SMGW and to identify possible sources of errors or malfunctions.

All SMGW transactions (e.g., the sending of measured values and activities of the SMGW administrator) are recorded in a final consumer log. An authenticated and authorized end user can call up the relevant information from the SMGW via the logical HAN interface for display units and thus keep track of who has received which data, when or whether user-related data (e.g., profiles) have been changed, added, or removed. To maintain the confidentiality and integrity of the personal log data, an SMGW administrator is not allowed access to the end-user log.

The calibration log stores events relevant to calibration (e.g., detected falsifications of measurements or failed time synchronization). Besides, changes to parameters that are relevant to calibration technology are registered here (e.g., setting of the device clock). This log can only be viewed by the authorized SMGW administrator and verified by the SMGW administrator authorities if it is required.

Authentication for getting logs is also important because the SMGW must be able to record and save the measured values from meters of various final consumers (for example in multi-family houses). For this purpose, the SMGW has implemented mechanisms to support multi-client capability and the associated authentication requirements from GW_PP chapter 1.4.6.6.

2.3 Swiss Case

Due to the heterogeneity of network operators in Switzerland, implementation of the standards varies depending on the size of the network operator. Currently, there is a parallelism between federal and cantonal law in the area of data protection in Switzerland. In particular, federal data protection legislation, which also regulates data security, does not contain sector-specific rules, but general rules whose application in a specific case may leave considerable room for interpretation. In addition to the Federal Data Protection Act, which applies to private individuals and federal authorities, the cantons also have their data protection laws that apply to cantonal authorities. Since the vast majority of network operators are part of the cantonal administration in the broader sense (cantonal utilities), such network operators are affected by cantonal laws. This parallelism of federal and cantonal law leads to legal uncertainty, particularly in the operation of smart metering systems. This legal fragmentation, particularly concerning granularity and the use of load profile data, can impair the benefits of smart metering systems (UVEK 2015).

The core document about Swiss smart metering was provided by Federal Council (Schweizerische Bundesrat) and named Stromversorgungsverordnung (StromVV, Electricity Supply Ordinance). Articles from Art. 8a to Art. 8d contain information about (Schweizerische Bundesrat 2008):

(a) Smart metering systems
(b) Data security check
(c) Intelligent control and regulation systems for network operation
(d) Handling of data from intelligent measurement, control, and regulation systems.

From the technical point of view, these articles contain very mild limitations, such as:

- The smart meter should have a physical display on the smart meter case.
- The smart meter must have local data storage. This storage is necessary to store information in case there is no connection to the server, SMGW, or data concentrator. Also, this storage should be enough to store load profiles with a 15 min period for at least sixty days.
- The smart meter should have interfaces for bidirectional communication with a data processing system and enable the possibility to get measured values at the moment of their acquisition as well as the load profiles to the end-user, producer, or storage operator.
- Manipulations and other external influences on the smart meter should be detected, recorded, and reported.
- Other digital measuring equipment, as well as intelligent control and regulation systems of the network operator can be integrated with a smart meter.

Also, this document contains customer data management restrictions. The personal data and personality profiles should be destroyed after 12 months unless they are relevant to billing or have been anonymized. The network operator shall retrieve the data from intelligent metering systems a maximum of once a day unless network operation requires more frequent retrieval.

Network operators may process data from the use of measurement and control systems without the consent of the data subject for the following purposes:

(a) personality profiles and personal data in pseudonymized form, including load profiles of 15 min or more: for measurement, control, and regulation, for the use of tariff systems and secure, efficient, and effective network operation, network balancing, and network planning;
(b) personality profiles and personal data in non-pseudonymized form, including load profile values of 15 min and more: for the billing of energy supply, grid usage charges, and remuneration for the use of control and regulation systems.

Network operators may pass on the data from the use of measurement systems to the following persons without the consent of the person concerned:

(a) personality profiles and personal data in pseudonymized or suitably aggregated form: to the parties involved by Article 8 paragraph 3;
(b) the information needed to decipher the pseudonyms: the energy supplier of the final consumer concerned.

Requirements from StromVV were checked and supplemented by DETEC and VSE at the next steps. DETEC—Federal Department of Environment, Transport, Energy and Communications (Generalsekretariat des UVEK). DETEC is one of the seven departments of the Swiss federal government, headed by a member of the Swiss Federal Council. This department is responsible for issues related to environmental policy, management and development of transport, management, and monitoring of energy sources (electricity, gas, oil, etc.), and mass media (including television).

VSE (Verband Schweizerischer Elektrizitätsunternehmen) is the main organization, educational institution, and political mouthpiece for the Swiss electricity industry. Its members ensure over 90% of Switzerland's electricity supply. VSE creates industry recommendations, manuals and also develops future scenarios, basics, and positions in the electricity field. The most important VSE documents about smart metering are "Smart Metering System Data Security Guidelines" (VSE 2018) and "Intelligent measuring systems. The use of intelligent measuring systems in Switzerland" (VSE 2019). VSE recommendations are more concrete compared with StromVV. As an example:

3.4.1 Firmware—operating system and applications in all major components are subject to version control; are installed upon delivery and secured against unauthorized commissioning. The integrity of this data is a prerequisite for proper and trustworthy operation. Firmware update—operating system and applications in the main components are subject to version control; are installed and put into operation in the main components according to the version control by authorized users in the role of administrator. The integrity of this data is a prerequisite for proper and trustworthy operation.

6.2.5 Customer interface. The customer interface should be located on the meter. The communication should be encrypted according to the data security check. Protocol and interface are designed manufacturer-specific (e.g. DLMS via RS485). Visualization systems that can be used also depend on the manufacturer and it is not standardized. To be able to offer customer support in the selection of third-party products, it is recommended to consult the supplier of the iMS for possible references.

Swiss Smart Metering Architecture

Possible smart metering architectures are considered in "Smart Metering System Data Security Guidelines" (VSE 2018) in article 2.5 and "Intelligent measuring systems" (VSE 2019) in 6.3.2.

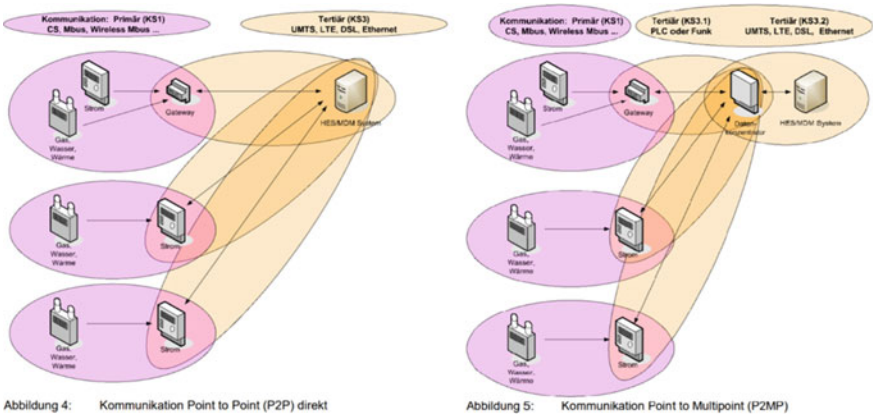


Fig. 4 Swiss smart metering architecture (VSE 2019)

As we could see from Fig. 4, using of smart meter gateway or data concentrator is optional. Gas and water meters can transmit data through an electricity meter. Possible options for the in-home architecture from [Richtlinien für die Datensicherheit von intelligenten Messsystemen, Anhang 1] includes:

1. Smart meter devices connected in parallel (without data concentrator)
2. Smart meter device with LMN
3. Smart meter device with cascaded LMN
4. Gateway with LMN
5. Gateway with cascaded LMN.

In the document "Basics of designing an introduction of intelligent measuring systems at the end consumer in Switzerland Minimum technical requirements and introduction modalities" (UVEK 2014) the Swiss Federal Office of Energy evaluated the appropriateness of different smart metering approaches by defining minimum national requirements and comparing them with implementations in other countries, resulting in a large overlap between the Swiss requirements and the German approach.

To be officially used in Switzerland smart metering system should obtain a certificate from the METAS-Cert (Eidgenössisches Institut für Metrologie Konformitätsbewertungsstelle; https://www.metas.ch/ds) In accordance with the provisions of Electricity Supply Ordinance Article 8, it must be proven for all elements used that they meet the data security requirements resulting from the Swiss protection requirements analysis. Certification proof methodology could be found in the document "Prüfmethodologie zur Durchführung der Datensicherheitsprüfung für Smart Metering Komponenten in der Schweiz" (swissmig 2019). This document contains concrete security testing requirements divided by one section per type of smart metering system element:

- Section 5.1—General requirements—apply to all main components (Hauptkomponenten, HK) of an intelligent measuring system (iMS) include four sheets numbered with Roman numerals in this representation
- Section 5.2—Requirements for the intelligent measuring device (iMG)
- Section 5.3—Requirements for the gateway (GW) as a communication system (KS)
- Section 5.4—Requirements for the data concentrator (DC) as a communication system (KS)
- Section 5.5—Requirements for the head end system (HES)
- Section 5.6—Requirements for key management (KM).

For example, requirements for intelligent measuring device interface KS2 from chapter 5.2.2.3 include:

(a) At least the user role prosumer is available to access this interface according to the corresponding access rights.
(b) Authentication takes place at least via user name and password.
(c) The interface allows the prosumer role to have read-only access to the count data intended for visualization.

(d) No connection to other interfaces of the iMG is possible via the interface.
(e) The interface is hardened against attacks such as denial of service, replay, buffer overflow, etc.
(f) A failure of the interface does not affect the metrological part or the other interfaces.
(g) Unauthorized access attempts and other disruptions trigger an alarm to the MDM system and these events are included in the log data.

As we can see, these requirements are close to the requirements from BSI protection profile BSI-CC-PP-0073-2014, but compared to German requirements from TR-03109-1 still more abstract because of the lack of predefined communication scenarios, running services, etc. Because these important elements are not defined—it is complicated to produce more concrete requirements than requirements that are currently defined in the "Test methodology" document.

In differ from the French situation with Enedis, the Swiss Federal Electricity Commission counts over 630 active DSOs for the 8.6 million Switzerland population in the year 2020 (Rullaud and Gruber 2020). In this document, we will compare the smart metering systems of two major manufacturers—Landis+Gyr and Siemens—that are used in Switzerland due to the large number of DSOs and relatively abstract supervisory requirements.

Landis+Gyr Smart Metering Infrastructure

The following sections considers a Landis+Gyr E450 smart meter and the DC450 data concentrator configuration. Landis+Gyr was the first supplier to receive data security certification from the Federal Institute for Metrology (METAS) for a G3-PLC data concentrator on 16th March 2021. A few weeks later Landis+Gyr's E450 smart meter and Head-End-System HES were equally certified resulting in Landis+Gyr now covering the complete chain of a smart metering system in an end-to-end certified solution. Landis+Gyr entrusted CCLab in 2019 to evaluate three components by the Swiss Smart Metering protection requirements (https://www.cclab.com/news/landis-gyr-metas-certificate):

- E450 is a residential advanced meter with an integrated PLC modem,
- DC450 is a new generation intelligent data concentrator for a large-scale meter reading and controlling applications and
- the HES which is an interoperable head end system that provides a communication and data collection layer between the smart meter infrastructure and the utility.

This architecture looks very similar to French Linky system architecture. It does not have smart meter gateways (smart meter already plays the role of meter and communicating unit in one box), has a data concentrator, uses PLC at the physical layer, and has the ability to connect household appliances to manage power (Fig. 5).

To secure data Landis+Gyr E450 smart meters use DLMS/COSEM security suite 0 with High security level. DLMS security is always used independently of the lower communications and security layers, which means that data concentrators just resend data without decrypting it. To prevent interception or falsification of messages

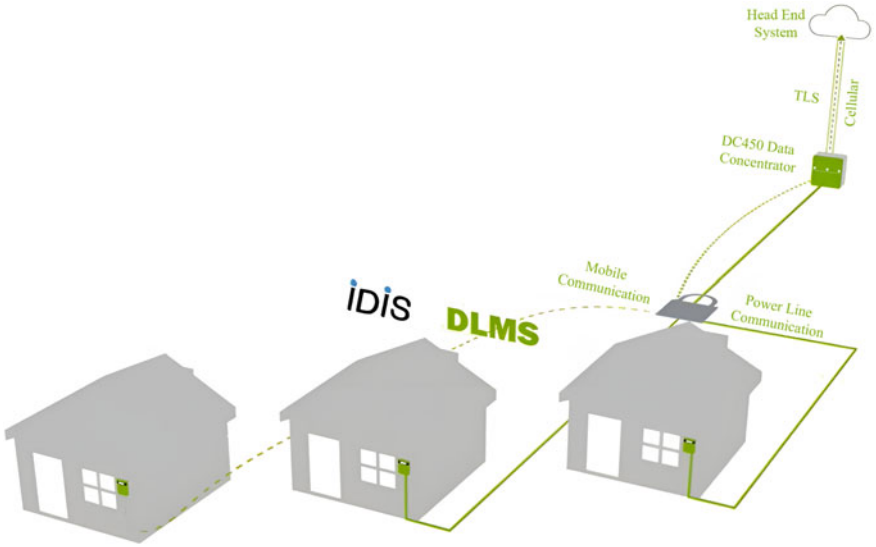


Fig. 5 Landis+Gyr smart metering solution architecture (https://www.landisgyr.de/product/landisgyr-concentrateur-dc450-2/)

and feed unauthorized commands between the HES (head-end system, in German SMI terms, is one of EMP), data concentrator, and smart meters used DLMS or TLS encrypted and authenticated data (Landis+Gyr 2020). Communication security based on the IDIS DLMS/COSEM standard which includes:

- Symmetric encryption and keys for meter communication with previously exchanged keys are used to enable good communication performance with embedded devices.
- 4-stage client-server authentication with GMAC.
- Recognized and proven AES encryption, 128-bit key.

In case to implement secure communication key management:

- Secure keys are created and stored in an encrypted format on devices at the time of manufacturing.
- The key material is encryptedly sent to the customer's HES system.
- The keys are stored in Landis+Gyr's HES Secure Key Manager.
- Once communication is established, the keys can be exchanged regularly or on-demand.

Most of the Landis+Gyr smart meters have from at least one to several control outputs to switch loads. There is also the demand for supervision in the meter which means if the demand/used current reaches a pre-defined limit, loads can be switched off/on (depending on the parametrization and load connected). The control output can also be controlled from the system side, reacting to information not available at

the meter point. User access to functions and data is securely controlled based on the user's role M-Bus (authentication, authorization). Future security upgrades can be securely distributed, stored, and activated. Connection via local interfaces such as CII (Customer Information Interface), M-Bus, or wireless M-Bus, and optical interfaces can also be encrypted if required.

Only the utility has access to the smart meter data. Other parties can get their data from a central data hub in the cloud or do not get smart meter data at all (depending on concrete place laws). Landis+Gyr smart meters currently do not support multiple users of one device—every consumer needs their own smart meter to measure consumption. The data coming from a smart meter is only related to the serial number of the meter. Only the utility can make the connection between the meter serial number and consumer identity. Currently, data pseudonymization was not necessary because the utility is allowed to use the data for billing and also for grid stability checking (e.g., 15 min PQ values). Data is typically sent one or two times per day. Locally smart meters measure data at 1-s intervals. It is possible to push these data every 5 s over a consumer port into the consumer's home. Smart meters usually store data in meters from 10 days up to 1 year, depending on the kind of data. Data can be sent every 15 min or more often. The most significant limitation is the used communication technology and the cost for the utility to data transfer, but modern smart meters are flexible in this regard and can be parametrized towards the use case.

In order to get an insight in Landis+Gyrs security, the Gridstream (Landis+Gyr 2020, 2014) solution which is usually integrated in the above described devices is considered in the following. Gridstream is a powerful energy management service based on two-way data communication, which enables a wide range of applications, such as remote meter reading, customer relationship management, and demand-side management. Gridstream provides functions to assist utilities with load control, reporting power outages, and monitoring power quality. The data flowing through the Gridstream system is exposed to various risks, such as intrusions in the field network, the data center, or even at a system level. The security architecture for Gridstream ensures system and network availability, while at the same time meeting critical security objectives, such as confidentiality, integrity, and authentication of data. The key elements of the Gridstream security approach include:

- PKI environment for managing security certificates. This infrastructure forms the basis for the management of secure communication, also on the LAN and WAN level.
- HSM module—The HSM serves as the root of trust where the utility ECC private key is vaulted. The private key is used to generate digital signatures to downstream commands sent by the HES. The HSM also features FIPS 140-2 and Common Criteria Level 4 certifications, providing strong protection for one of the critical elements in the advanced security architecture.
- Role-Based Access Control—The HES enforces access controls through a Role-Based Access Control (RBAC) functionality. RBAC allows the security administrator within a utility to manage user credentials and privileges assignment. In

this way, the utility can manage which employees have access to commands and features related to the devices in the network.

- Meter Tamper Alarms—Landis+Gyr meters offer tamper alarms such as reverse energy flow, tilt/tamper, and outage notifications in case a meter is removed from the socket. The alarms are transmitted to the HES upon occurrence and logged by the head end, displayed on the GUI, and optionally emailed to appropriate users. In the case of the network gateway or network bridge cover removal, an alarm will be immediately sent to the head end, displayed on the GUI, and optionally emailed to the appropriate users.
- Firmware Integrity—All firmware images released by Landis+Gyr are digitally signed utilizing the Landis+Gyr asymmetric private key (ECC). Each endpoint within the network will validate the digital signature using the Landis+Gyr public key. If the key doesn't match the Landis+Gyr signature, the device will not upgrade that firmware version. This is a strong prevention mechanism to avoid the injection of rogue code into the network.
- From the factory, all Landis+Gyr IDIS devices are produced with a security key set in an ISO27001 certified environment. These are stored in encrypted form in the meter and stored in a hardware security module at Landis+Gyr. Later, as part of the activation of the communication security process, these keys are transmitted to the certified customer as a file using a secure procedure.

The servers in the head-end system platform are all protected using hierarchical access control mechanisms based on access rights (roles). The internal network of AIM system platform servers is typically protected from external access using firewalls and multiple levels of network access control mechanisms. All users of external connections should be authenticated inside a secure data connection protocol. This is especially important for protection against signals from an unauthorized meter or a computer that emulates a meter. The authenticity of a meter that is sending data is ensured using the DLMS-COSEM high level security authentication protocol. The DLMS-COSEM protocol ensures secure access to the electricity meter's data. Data access security is based on assigning different access rights (Fig. 6).

Remote reading of metering values from a point-to-point metering device (e.g., a device that communicates with the head end system using a mobile network) by the data collection system is typically protected using a virtual private network (VPN) tunnel between the internal Gridstream network and security enforced by the communication service provider and network-provider. In the case of a local area network (LAN) connected meter, a VPN with a firewall may be enforced between the LAN meter and the AIM internal network.

Field tools and data collection system applications—for operating the AIM site manager application, the site manager typically runs on a server in a de-militarized zone (DMZ) and is connected via a VPN tunnel to the telecom operator network with an optional HTTPS connection between the field tool device application and the site manager server. For AIM dashboard, it is advisable to run the dashboard server in the DMZ, and those HTTPS connections are enforced between the user terminal and

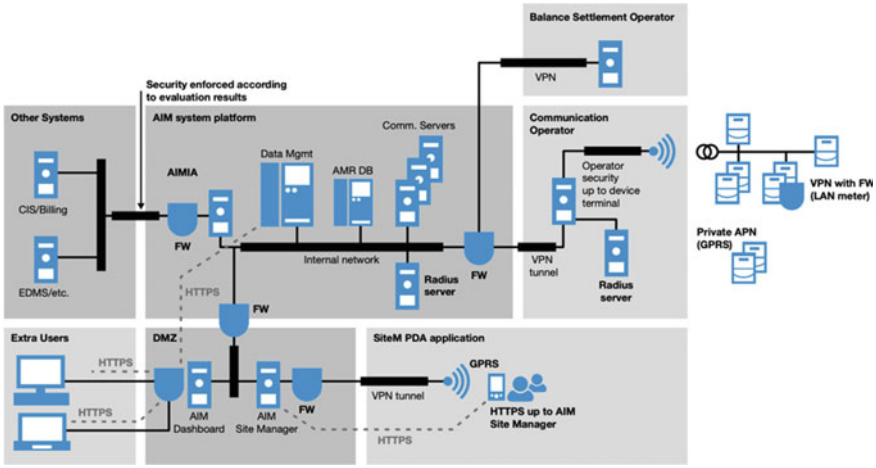


Fig. 6 Example Gridstream AIM infrastructure using sub-networks and zones (Landis+Gyr 2014)

the dashboard server. The data transfer between the AIM Dashboard server and the AIM system platform server may also use the HTTPS protocol.

Gridstream includes automatic repeat functions at different system levels to enable smooth recovery and to solve any possible communication problems. The communication protocols used have automated control and correction functions. Communication between the measurement, display device, and data collection system is typically implemented via a cellular network or power line communication (PLC). Message security over the mobile telephony network is typically provided by the wide-area networking VPN functionality of the network provider, in conjunction with the use of HTTPS on the transport layer. Providing message security over power line communications has been a subject of work in the IDIS consortium and DLMS-COSEM standardization. Confidentiality, integrity, and authentication are provided by using AES encryption and key distribution services throughout the measurement, switching, and display system itself, and at the interfaces to the data collection system. Communication within a meter is done by using an internal bus. For instance, meter values are read directly from the meter's measurement integrated circuits by using the meter's internal bus. The internal bus is only accessible by breaking the meter cover seal, which sends a system alarm to the data collection system, making such security attacks easy to detect and locate.

In addition to securing communication, Gridstream ensures that all data is safely stored and transferred. Each metering value coming from the meter has a status indication with the assured time of measurement, to show whether the user can trust the value or not. It shows, for example, if there were power cuts or if the device's time was adjusted during the measuring period. This information helps the user to locate the details of the device in question, if necessary. The Gridstream logging and auditing functions ensure that all modifications to the system data are carefully traced in the system.

Siemens Smart Metering Infrastructure

The Siemens architecture with IM150 or IM350 Smart Meters and smart meter gateway SGW1050 is very close to the Landis+Gyr architecture, but instead of "data concentrator" it uses a "gateway". Whereas traditional "data concentrators" include intermediate storage of the meter data, due to security reasons the Siemens SGW1050 gateway transparently and securely tunnels the meter data on their way to the HES. There is no decryption/re-encryption or insight into meter data on the gateway. The smart meter gateway SGW1050 can work not only with Siemens smart meters and can handle up to 2000 smart meters.

A smart meter measures electricity and communicates with the central system. For this reason, a communication module is used which can be either integrated or replaceable that allows the use of different communication technologies like G3-PLC, mobile, or some other. Since both parts have to go through separate certification processes, the firmware for both parts is split which allows updating communication relevant device logic without touching the measurement-related part of the device firmware.

Each smart meter can manage up to 4 m connected via wired or wireless M-BUS (OMS and IDIS Standard). The Siemens IM350 Smart Meter is using a wired MBUS interface to allow suppliers of secondary meters to connect their own wireless adapters to communicate with their meters. This concept works particularly well in regions where the smart meter is housed in a closed outdoor box with limited wireless connectivity. The smart meter collects consumption data, stores it internally, and sends it to the HES via a communication channel. On the HES level, those 4 m are independent and the orchestration is maintained. After transferring the data to an MDMS they will be interpreted as different channels (electricity, gas, water, heat, district heat) coming from the same SDP (service delivery point). A SDP describes a specific connection point in the field.

The master data system (billing system) can choose a measurement profile (data that the meters have to collect and should be stored in HES/MDMS for information purposes) and a billing profile (data that shall be sent further to the billing system for accounting). Both types of data are transmitted in pseudonymized form. There are register-based data (daily) profiles, interval-based data profiles (on 15 min schedule), or both. The kind of selected profiles depends on the purpose of the meter. Residential meters need to be billed on a monthly period but can collect 15 min values as well (to receive an in-depth network load picture per 15 min). Small industrial and industrial meters have to follow a specific schedule and need to be billed daily. After running a plausibility check and if necessary, a substitute value creation process, this data will be exported to an Energy Date Management system like BELVIS. Whichever profile has been set, all meters will send their data daily to the central system.

If a meter couldn't be reached on a specific day, the HES will request all missed data as soon as the device is reachable again. Due to network interferences and interferers, it's quite common by using PLC technology to receive on one daily readout roughly 80% of the installed smart meters. After 2–3 days the central system receives missed data as well until it has collected around 95% of the total data for a

specific day. The smart meter stores its data for a minimum period of 60 days locally. The head-end system tries to read out each meter per day and can collect missed data as long as the meter has been stored locally. If a meter is not communicative for a longer period, a service technician has to care about this specific device. Instantaneous energy consumption is always counted and never deleted (counter reading). Register-based or interval data will be stored out of the instantaneous values according to their defined schedule (daily at midnight and interval per each 15 min). This allows all data to be collected in the aftermath, even when the meter was powered off in the meantime.

Electrical data is stored in the OBIS Code registers form. Such a register refers to a specific value and its metadata. All these registers can be stored on four different tariffs. Most of the utilities in Switzerland use just two of them (High- and Low Tariff). In the future, there will be no tariff-based storage on the smart meters anymore because the MDMS can deviate it directly into the central system (necessary for dynamic tariffing/pricing). Siemens IM350 can store 64 different energy-related registers. Most of the customers are using profiles containing 4–17 registers.

Since the gateway only transmits information but does not decrypt it the security features of the DLMS/COSEM protocol are used in conjunction with TLS. The customer interface uses IDIS CII standard encryption for transmitting information securely using AES-128 encryption. To secure communication channels RSA TLS with at least 4096-bit key lengths is used. Asynchronous encryption is ensured by certificates issued for a specific key usage ran under a dedicated Public-Key Infrastructure. To secure meter encrypted data 48 role-based meter keys are used. A role-based access concept ensured by individual keys and certificates is implemented for each device and application.

Siemens makes use of HLS with DLMS/COSEM Security Suite 0 and 1. NLS is not used at all. The DLMS/COSEM Standard belongs to this kind of standard which leaves open quite a big amount of interpretation. For this reason, Smart Meter suppliers in Switzerland implemented the IDIS Standard (Package 1-3) which is, in fact, a tight definition of how the DLMS/COSEM standard has to be implemented. This allows smart meters of different vendors to act interoperable.

Besides, Siemens is using dedicated appliances such as a hardware security module. This module is responsible for the whole meter data decryption and is the only system on which clear text meter keys are present. Meter keys never leave the tamper-resistant foil-coated CPU or its cache. This ensures a physical protection layer to the smart meter data security.

3 Comparison with Reference Architecture

As a base for architectures and used protocols comparison a reference architecture for smart metering communications of the Smart Metering Coordination Group was defined in the framework of the smart grids M/490 mandate and that for smart meters M/441 mandate (CEN/CLC/ETSI/TR 50572, 2011) which includes (Fig. 7):

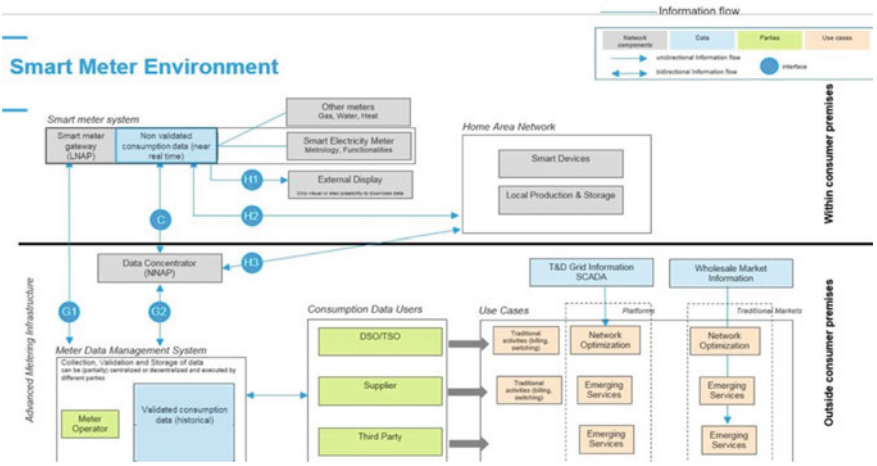


Fig. 7 Reference architecture with protocol labels (European Commission DG Energy 2019)

- Interface **H1** connects the smart meter system to an external display, via one-way communication. The external display is not uniquely designed. For instance, information may be provided only visually, or be available for download. In BSI terms interface **H1** is used in HAF1 for the end-user data provision in the Home Area Network (HAN).
- Interface **H2** connects the smart meter system with the Home Area Network (HAN). The HAN interconnects smart home devices for energy management purposes. Interface **H2** provides two-way communication, i.e. the HAN can send information on individual devices back to the smart meter system. In BSI terms interface **H2** is required to communicate with Controllable Local Systems (CLS).
- Data from the smart meter is shared externally with the meter data management system (a central communication system). This system communicates with meters either directly through the Wide Area Network (WAN) and enabled by interface **G1**, or via a data concentrator where information from several meters in a neighborhood is concentrated (Neighbourhood Network Access Points, NNAP) and enabled by interface **G2**.
- Interface **C** is used to connect LNAP (Local Network Access Point) and/or metering end devices to an NNAP.
- The **M** interface is between this communications function of the meter and the LNAP or between metering end devices. The interface defines the access of external devices to internal data on the meter. The interface profile has to offer services that enable the meter to provide access via the LNAP to the functions implemented in the MID part of the meter or outside it. In BSI terms interface **M** implements a Local Metrological Network (LMN).

Interface	French Linky system	Swiss Landis+Gyr (E450 and DC450)
Interface C	• DLMS/COSEM • UDP or TCP • IPv6 • IETF 6LoWPAN • IEEE 802.15.4 MAC • Mesh ITU-T G3 PLC (power line communication, France's name CPL). PLC-G1 CENELEC A (3–95 kHz). In the future, PLC-G1 will be replaced by PLC-G3 CENELEC A (10–90 kHz)	• DLMS/COSEM + security IEC 62056-5-3 • TCP, UDP • IPv4, IPv6 S-FSK PLC, G3 OFDM PLC, Ethernet, GPRS, UMTS, RF-Mesh
Interface G1	–	–
Interface G2	• DLMS/COSEM • TCP • IP • GSM/GPRS	• DLMS/COSEM • TLS • IPv4, IPv6 RJ45 Ethernet (existing modification with GSM/GPRS/UMTS/LTS)
Interface H1	LAN interface: Euridis (utility interface) 2-way 9600 bps interface. Linky has a physical screen and a remote customer information port. Through this port, users can get various information from the meter (current consumption, apparent power, and tariff period)	An optional integrated wireless interface (ZigBee) enables bi-directional communication with our ecoMeter in-home display. A local port on the smart meter enables consumer access to consumption data. The local port can be implemented by any smart meter physical port e.g. optical port, M-Bus port, IP port (G3 PLC)
Interface H2	Mono-directional line for energy management (7 virtual contacts)—Dry contact (French name "Contact sec") or TIC interface 1-way, 9600 Baud. Exist an option to install on the Linky meter ERL module (Emetteur Radio Linky). This will provide an opportunity to use KNX RF Multi (868 MHz) and ZigBee (2.4 GHz) protocols with the MQTT protocol on the application level. At the meeting, experts from Enedis said that with a special dongle any communication protocol could be used for this purpose	The IDIS CII establishes the foundation for any future consumer HAN services outside the meter. Consumer Interface (open HAN Interface) optical and M-Bus wired + wireless M-Bus (868 MHz). E450 has 1 digital output with a 90 mA relay option and 1 Bistable relay 8A. Also, optionally possible to add 1 Bistable relay 8 A and 1 latching relay 5 A
Interface M		The E450 meter can act as a gateway for collecting data and interacting with other energy meters, like gas, water, or heat. E450 supports DSMR 2.2+ and OMS 4.03. Default E450 has a wireless M-Bus (868 MHz). Wired M-Bus can be used with an additional dongle and use RS485
Interface	German BSI SMGW system	Swiss Siemens (IM150 and SGW1050)

(continued)

(continued)

Interface	French Linky system	Swiss Landis+Gyr (E450 and DC450)
Interface C		• DLMS/COSEM (IEC 62056) • TCP • IPv4, IPv6 • G3-PLC CENELEC A (35–91 kHz) or FCC (150–490 kHz). With external module can be used RS-232 with RJ45 connector, GSM/GPRS/UMTS/LTS
Interface G1	• DLMS/COSEM-IC IEC 62056-6-2 (only COSEM part) • OBIS IEC 62056-6-1 • XML Transfer syntax for COSEM/OBIS objects (optional) • CMS (Cryptographic Message Syntax) IETF RFC 5652 • RESTful COSEM web services (optional) • HTTP 1.1 RFC 7230-7235 • TLS 1.2 RFC 5246 • TCP • IPv4/IPv6 GPRS/EDGE/UMTS/LTE, DSL/Ethernet	• DLMS/COSEM (IEC 62056) • TLS • TCP • IPv4, IPv6 • GSM/GPRS/UMTS/LTS
Interface G2	–	–
Interface H1	• TLS 1.2 RFC 5246 • TCP • IPv4, IPv6 Ethernet > 10 Mbit/s IEEE 802.3i	DSMR P1 interface (RJ12)
Interface H2	• SOCKSv5. Draft RFC “Secure Sockets Layer for SOCKS Version 5” (only for HKS3) • TLS 1.2 RFC 5246 • TCP • IPv4, IPv6 Ethernet > 10 Mbit/s IEEE 802.3i	DSMR P1 interface (RJ12)

(continued)

(continued)

Interface	French Linky system	Swiss Landis+Gyr (E450 and DC450)
Interface M	(a) Wireless bidirectional connection • M-BUS EN 13757-3:2011 • TLS RFC 5246 (M-BUS mode 13) • AFL (Authentication and Fragmentation Level) • Wireless M-Bus EN 13757-4:2011 (b) Wireless unidirectional connection • M-BUS EN 13757-3:2011 • Encryption Mode-7 AES-CBC + CMAC • AFL (Authentication and Fragmentation Level) • Wireless M-Bus EN 13757-4:2011 (c) Wired connection • OBIS IEC 62056-6-1 + DIN EN 13757-1 (OBIS) DLMS/COSEM IEC 62056-6-2 • SML IEC 62056-5-3-8 • TLS 1.2 RFC 5246 • HDLC ISO/IEC 13239 (Format Type 3, CRC according to IEC 62056-46) • EIA/RS-485	Wired and wireless M-Bus (EN13757)

4 Security Analysis

Based on the information provided, it appears that the architecture of French Linky and the Swiss solutions from Landis+Gyr and Siemens are similar from a smart metering systems perspective. Both use the DLMS/COSEM stack of protocols, commonly use PLC G3 on the physical layer, and have a data concentrator in their architectures. The Interoperable Device Interface Specification White Paper (Landis+Gyr White Paper) even points out that Linky smart meters meet IDIS specifications.

In differ to the French and Swiss systems that are considered in this work, the German BSI system uses TLS as the main protocol to secure all 3 SMGW networks. That means to make a comparison from a security protocols point of view for comparison of French, German, and Swiss (Landis+Gyr and Siemens) systems we should compare DLMS/COSEM and TLS (with BSI requirements) protected architectures. We will not describe the TLS protocol in detail because TLS is very widespread and there are lots of materials that describe the main principles of TLS in simplified form.

4.1 DLMS/COSEM Protocol Description

To be more precise, the DLMS/COSEM stack of protocols and vulnerabilities should be considered in more detail. Device Language Message Specification (DLMS) is a server-client protocol that is used for retrieving consumption data from smart meters and for transmission of this data to the energy supplier's Meter Data Management System (MDMS). DLMS works with Companion Specification for Energy Metering (COSEM) and uses OBIS codes (Object Identification System) for meter identification.

COSEM interface classes and their instantiations (objects) are used for modeling energy management use cases including metering. Object modeling is a powerful tool to formally represent simple or complex data. Each aspect of the data is modeled with an attribute. Objects may have several attributes and also methods to perform operations on the attributes. Objects can be used in combinations, to model simple use cases such as register reading, or more complex ones such as tariff and billing schemes or load management. At the moment there are 89 specified interface classes.

OBIS is the naming system of COSEM objects. OBIS codes are specified for electricity, gas, water, heat cost allocators (HCAs), and thermal energy metering, as well as for abstract data that are not related to the energy kind measured. The hierarchical structure of OBIS allows classifying the characteristics of the data e.g., electrical energy, active power, integration, tariff, and billing period.

The DLMS concept was standardized as an international standard by the International Electrotechnical Commission as IEC 62056. IEC 62056 is a set of standards for electricity metering, data exchange for meter reading, tariff, and load control established by the International Electrotechnical Commission (IEC). This series includes the following list of standards:

- IEC 62056-21: Direct local data exchange
- IEC 62056-42: Physical layer services and procedures for connection-oriented asynchronous data exchange
- IEC 62056-46: Data link layer using HDLC protocol
- IEC 62056-47: COSEM transport layers for IPv4 networks
- IEC 62056-53: COSEM Application layer
- IEC 62056-61: Object identification system (OBIS)
- IEC 62056-62: Interface classes.

IEC 62056 standards are focused on electricity metering while DLMS/COSEM is more general and applied to any energy metering. Communication standards differ, e.g., IEC 62056-21 is ASCII-based communication while DLMS is a binary protocol. These standards have been adopted by a large number of manufacturers and service providers making them one of the most widely implemented in smart meters. In the interaction, DLMS/COSEM forms an object model for the monitoring, communication, and transmission of meter readings.

The DLMS/COSEM provides different interface classes to represent real smart metering infrastructure objects and their functionalities. Through the instantiation of

these classes, the status and functionality of the measurement equipment are represented, to expose it through the communication network. Physical devices modeled in the protocol contain one or several logical devices that are responsible for modeling the specific functionalities of each device. These objects, as in the object-oriented programming paradigm, are nothing more than a grouping of attributes and methods. Gauges act as servers, which are queried by client applications that retrieve data, provide control information, or perform actions on the gauge through the attributes and methods exposed on the objects defined in the gauge.

To define a meter it is required to define a physical device with its logical devices and instantiate the desired interface classes. The standard defines 70 interface classes that can be used, each with different attributes and available methods. For example, to define an energy measurement, a register class is provided, which will be instantiated by each of the types of measurements that the meter maintains. Taking as an example a meter that is responsible for measuring the consumption of electricity, gas, and water, will be defined as a device containing three logical devices one for each type of energy, and within each one of them will have an instance of the register class, which will contain an attribute with the value of the energy consumption measurement.

The server role is commonly implemented in smart meter devices and the client role on the energy service provider side. To be able to access the objects in a DLMS/COSEM server, it is necessary to establish an Application Association (AA) with the client to identify the participants and establish the context in which the communication will take place, that provides e.g., which authentication mechanism should be used. Servers always have an instance of a special kind of class called an Association, which contains this information and also contains a list of all the objects that are accessible on that particular server so that a client application can know what to do, what information allowed to access, and how to do it.

The protocol provides two ways to access objects, by Logical Name (LN) or by Short Name (SN). Each object always has a LN. In general, manufacturers use the same values in their devices, so that the same application in charge of collecting data from meters can do it regardless of the manufacturer. The LN is the first attribute of a COSEM object and together with the id of the interface class defines the meaning of the object. The LN is defined as a 6-byte OBIS (Object Identification System) code, for example, the association object code is always 0.0.40.0.0.255, and within each object, the attributes and methods are identified with a numeric id.

In the form of access by LN, the methods and attributes are accessed through the id of the interface class, the value of the LN, and the index of the attribute or method which needs to be accessed (class id | logical name | id attribute or method.) In contrast to the SN access form, each object is mapped to just one SN. This is a simplified form of access, indicated to be used by simple devices. In this case, each attribute and method of the objects is identified with a 13-bit integer. Through these two forms, the client can access the objects, read or modify the values of their attributes or trigger actions through their methods. COSEM objects can be accessible by using the address of the client to define which objects that particular client can have access to and of what type (read or write).

For managing the connection between a client and a DLMS/COSEM server, using the services provided by the Association Control Service Element (ACSE). When starting a connection, the client sends an AARQ message to the server, indicating some of its data and what encryption and authentication method it wishes to use, plus additional information such as which version of the protocol to use. In response to this message, the server sends an AARE message, accepting or rejecting the connection attempt, or if HLS is used as the authentication method, partially accepting the connection, waiting for it to complete the extra step of mutual authentication. This extra step consists of the response to a challenge presented by the counterpart. The server sends the client a nonce, whereupon the client sends the server its response based on this nonce, and vice versa. In the case of using MD5 or SHA1, HLS responses are computed based on a nonce and shared secret. When using GMAC to compute the challenge-response, GMAC is applied to the concatenation of a control byte 0x10, the authentication key, and the nonce.

After the connection is established, the client can send requests to the server, both to obtain data and to invoke methods, for which it will receive responses from the server. The messages have a header that indicates the type of message it is and the type of communication. For the termination of the connection, the client sends a server an RLRQ message requesting termination and then the server responds with an RLRE message confirming the conclusion of the communication between them.

In the ISO OSI model, DLMS communicates over L4-L5 (transport and session layer), and COSEM forms the presentation layer (L6) (Matoušek 2017; Table 1):

The DLMS/COSEM protocol allows communication over both TCP or UDP over IP and HDLC networks. In the case of TCP-UDP/IP networks, COSEM services are supported by the COSEM transport layer, which consists of a wrapper over the TCP or UDP protocol that adds an 8-byte header before the message, indicating the version. The protocol used, the source and destination ports, and the length of the message sent. This ensures that the entire message is received before being processed. For DLMS/COSEM, IANA registers port numbers 4059/TCP and 4059/UDP.

Table 1 DLMS/COSEM OSI model layers (European Commission DG Energy 2019)

Layer	Function	DLMS/COSEM
Application	Network process to application	Application
Presentation	Data representation, encryption and decryption, convert machine dependent data to machine independent data	COSEM
Session	Interhost communication, managing sessions between applications	DLMS
Transport	End-to-end connections, reliability and flow control	DLMS
Network	Path determination and logical addressing	DLMS
Data link	Physical addressing	HDLC, IEC 62056-47
Physical	Media, signal and binary transmission	Serial media, cable, radio

4.2 DLMS/COSEM Security

DLMS/COSEM protocol provides two "types" of security—access security and transport security. Access security concerns the rights of a client (for example an application running on a PC) to access data stored on a given server (for example an electricity meter). Transport security concerns the "ciphering" applied to the information exchanged between the server and the client.

DLMS/COSEM protocol defines three authentication security levels:

- Lowest Security Level (NLS)—Neither the client or the server is authenticated.
- Low Level Security (LLS)—Only the client is authenticated by presenting a password to the server. This type of authentication should only be used when the communication is carried out over a secure channel, in order to avoid eavesdropping and message replay.
- High Level Security (HLS)—mutual authentication both client and server authenticate against each other is used. This is the recommended authentication method since in general the security of the communication channel cannot be guaranteed. Possible options—HLS-MD5 (Message Digest 5), HLS-SHA1 (Secure Hash Algorithm), or HLS GMAC (Galois Message Authentication Code).

For transport security DLMS-COSEM defines the concept of 4 different available security policies:

1. Security is not imposed.
2. All messages are authenticated.
3. All messages are encrypted.
4. All messages are authenticated and encrypted.

Moreover, several security suites specify the cryptographic algorithm that is used for message security, such as Security suite 0 which employs AES-GCM-128 for authentication, encryption, and key-wrapping. The major difference between security suite 0 and suites 1 or 2 is that methods of asymmetric cryptography are not available so an offline key agreement is necessary. Security suites 1 and 2 presented in Green Book both use elliptic curve-based digital signatures (ECDSA) and Diffie-Hellman key agreement (ECDH). Additionally, compression can be used (Fig. 8).

DLMS/COSEM defines 3 security suites where AES key wrap (RFC-3394) used for key update (Table 2):

For message encryption, the protocol uses the Galois Counter Mode (GCM) and AES-128 block. Each block in the keystream is calculated using AES-128 based on the 128-bit AES key, a unique initialization vector (IV), and the block counter, which is expressed as a 32-bit unsigned integer that starts with the value 1. It is very important to have a unique IV, since repeating the keystream can have serious consequences, compromising the confidentiality of the communication. The IV in theory can be of any length, but IVs less than 96 bits long are considered unsafe (Dworkin 2007). DLMS/COSEM follows this recommendation and uses as IV the concatenation of the AP Title, a 64-bit value that identifies each device and is exchanged during connection establishment, followed by the 32-bit frame counter.

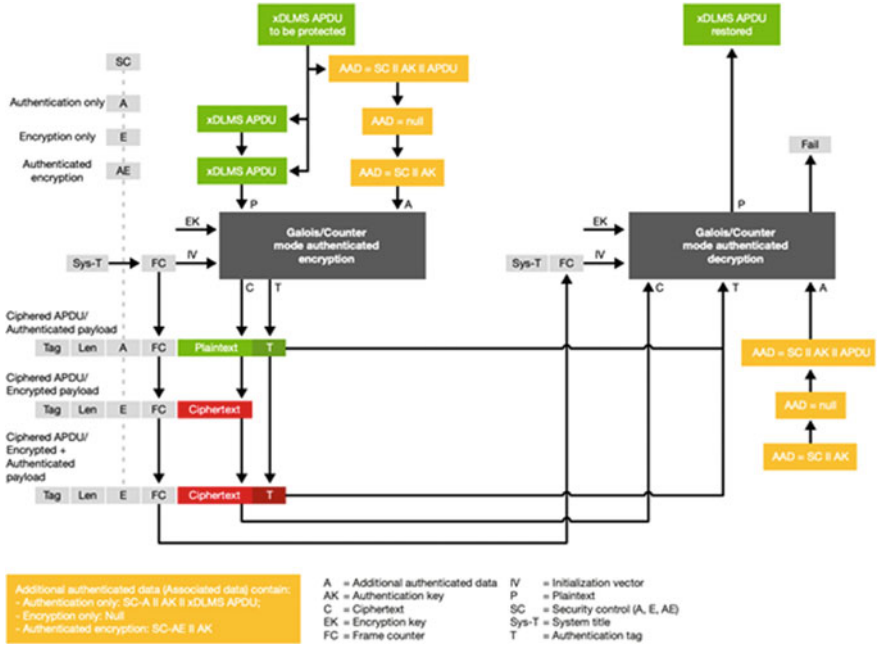


Fig. 8 DLMS-COSEM message cryptography architecture (Landis+Gyr 2014)

Table 2 DLMS/COSEM security suites

Security suite	Authenticated encryption	Digital signature	Key agreement
0	AES-GCM-128	–	–
1	AES-GCM-128	ECDSA with P-256	ECDH with P-256
2	AES-GCM-256	ECDSA with P-384	ECDH with P-384
Security suite	Hash	Key transport	Compression
0	–	AES-Wrap with 128 bit key	–
1	SHA-256	AES-Wrap with 128 bit key	V.44
2	SHA-384	AES-Wrap with 256 bit key	V.44

Transport security is achieved by using ciphered COSEM services (glo_…services) instead of plain COSEM services. All the plain COSEM services (ReadRequest, GetRequest, ReadResponse, WriteResponse, etc.) have a matching ciphered variant (glo_ReadRequest, glo_GetRequest, glo_ReadResponse, glo_WriteResponse, etc.). Ciphered services can only be used within a ciphered application context established by an AssociationRequest “’with ciphering”. More concrete info can be found in the source (https://icube.ch/Security/security1.html).

4.3 IDIS Specifications

As Landis+Gyr and Siemens solutions, Linky smart meters (at least some of them) which were described in this document meet IDIS specifications (Landis+Gyr White Paper). IDIS—is Interoperable Device Interface Specification. IDIS in fact, is a tight definition of how the DLMS/COSEM standard has to be implemented. This allows smart meters of different vendors to act interoperable. The IDIS association develops, maintains, and promotes publicly available technical interoperability specifications, based on open standards and supports their implementation in interoperable products. The association manages, administers, and protects the IDIS quality label and supports rigorous interoperability testing to ensure high-quality standards. IDIS is an association for smart metering companies which are committed to providing interoperable products based on open standards. IDIS membership is open to any legal entity providing IDIS conformance-tested equipment. IDIS members include Iskraemeco, Itron, and Landis+Gyr.

The specification team of the IDIS association is currently completing the detailed specifications for IDIS package 1 (based on secured S-FSK PLC communication according to IEC 61334-5-1 considering the latest extensions of the DLMS User Association), supporting the following smart metering use cases:

- Automatic meter registration and system integration
- Remote tariff programming
- On-demand and scheduled meter readings for electricity, gas, heat, and water meters
- Disconnection and reconnection of electricity and gas supply
- System-wide clock synchronization
- Quality of supply supervision at end nodes of the distribution network
- Demand/load management
- Remote firmware update
- Restricted data access to authenticated users
- Secure data exchange by enciphering sensitive information and by authenticating the source of data.

Communication security based on the IDIS DLMS/COSEM standard requires:

- use HLS for authentication security
- use security policy 4 (all messages are authenticated and encrypted)
- Recognized and proven AES encryption, 128-bit key
- 4-stage client-server authentication with GMAC
- Symmetric encryption and keys for meter communication with previously exchanged keys are used to enable good communication performance with embedded devices.

The IDIS security specification references the key scheme of DLMS-COSEM, which is based on a single set of unique symmetric keys per meter. Each key type has

a specific purpose (e.g., key encryption, authentication, message encryption) within the DLMS-COSEM communication protocol:

- Master key—is an AES key, programmed into the meter's firmware at the time of manufacturing. It is required to change the encryption method and encryption and authentication keys.
- Encryption key—128 or 256-bit key, used for encryption of DLMS/COSEM messages.

Authentication key—It is a key of the same length as the encryption key. It is used to calculate the authentication tag of the messages sent, this authentication tag serves as proof of the integrity of the message and demonstrates the knowledge of the authentication key by the sender of the message (Table 3).

Table 3 DLMS/COSEM key types (Landis+Gyr 2014)

Key type	Use	Generation
Master key (MK)	Key encryption key for global keys	Landis+Gyr production system
Global unicast encryption key (GUK)	Global encryption of unicast xDLMS APDUs	HES
Global broadcast encryption key (GBEK)	Global encryption of broadcast xDLMS APDUs	HES
Global broadcast authentication key (GAK)	Authentication of xDLMS APDUs	HES
Dedicated unicast encryption key (DUEK)		
Key type	Delivery	Location
Master key (MK)	From Landis+Gyr production system to HES using signed messaging	• Production system • HES • Meter
Global unicast encryption key (GUK)	Wrapped with master key, invocation of global_key_transfer method by HES or the DC	• HES • DC • Meter
Global broadcast encryption key (GBEK)	Wrapped with master key, invocation of global_key_transfer method by HES or the DC	• HES • DC • Meter
Global broadcast authentication key (GAK)	Wrapped with master key, invocation of global_key_transfer method by HES or the DC	• HES • DC • Meter
Dedicated unicast encryption key (DUEK)	Transported as part of the xDLMS Initiate Request APDU, which is encrypted and authenticated using the AES-GCM-128 algorithm, the global unicast encryption key and the authentication key	

To gain a deeper understanding of the security key generation and management possible to consider the Gridstream IDIS process (Landis+Gyr 2014):

1. The Landis+Gyr manufacturing facility uses secure key management software and secure key storage hardware to generate an initial unique key set for each meter consisting of a master key (encryption key) and initial global keys (GUK, GBEK, and GUEK). It is important to note that the DLMS term "global" means valid over multiple communication associations, and not system-wide.
2. The global keys are then encrypted using the master key and written to the meter.
3. The Landis+Gyr production system sends a copy of the key material to the utility AIM system using signed secure based on the Landis+Gyr public key infrastructure.
4. The utility AIM system stores and manages the key material using its local secure key manager and secure key storage hardware.
5. As each meter is registered to the AIM system as part of the installation process, AIM securely distributes the key material to the appropriate data concentrator (using TLS over mobile communications) and initiates communication with the meter.
6. As a part of the communication initialization process, AIM renews the meter's global keys and distributes them to the data concentrator and meter.

All communication from the head end system to the meter via the data collection system is authenticated and encrypted using the renewed meter-specific keys.

4.4 DLMS/COSEM Vulnerabilities

The DLMS/COSEM protocol is not free of vulnerabilities, both the protocol itself and particular to its different implementations. Below listed some of the known DLMS protocol vulnerabilities (Lüring et al. 2018; https://research.tue.nl/en/studentTheses/dlms-cosem-protocol-security-evaluation):

- Optional authentication—The use of authentication is optional according to the definition of the protocol, and it is independent of the encryption of the messages. An attacker can manipulate the security byte of messages and truncate the message in such a way as to remove the authentication byte and thus maintain an unauthenticated communication, without the receiver knowing if this was the case, the original intention of the issuer.
- Information leaking—each message contains a header indicating the type of message and communication mode used. This is unnecessary since the type of message is revealed even when it is an encrypted communication, making it possible for attackers to know what information is being transmitted. This could be replaced by simply indicating whether the communication is encrypted using the global key or a dedicated key and the indicated message type encrypted with the rest of the message. Devices do not require this additional information in order

to decrypt the message. But even in this case, because each service has a fixed, well-known, preamble and message structure an attacker may be able to perform a known plaintext attack.

- Vulnerable Authentication Methods—In HLS, the method used to authenticate the client and the server are the same. Given the right circumstances, an attacker could impersonate a valid server by replaying the AP title, nonce, and the response to the authentication challenge. A rogue server may reply to the client CtoS and f(CtoS) to trick the client that he knows the secret key. Since the f(CtoS) and f(StoC) are exchanged using the execute service, the attack requires that the APDUs are exchanged in plain text. To prevent it—the client must reject association responses if StoC is equal to CtoS.
- When HLS association is performed using MD5 or SHA1, offline dictionary attacks are possible, since the nonce (sent in plain text), the challenge-response, and the authentication function are known. With this information, given enough time and resources, the key used can be calculated. If an adversary acquires a valid HLS response and its corresponding nonce (e.g., via server impersonation or by sniffing traffic) he can then try to find out the shared secret. An attacker has nonce and h = f (nonce ‖ password). Offline he can try several passwords until he obtains h. To prevent this, the use of MD5 or SHA1 mechanisms should be forbidden, and required to use of randomly generated secrets.
- Possibility of injecting answers to the client—The responses are not linked to the requests, that is, given a request sent by the client, the responses can be replaced by another message and as long as it contains the expected data type, it will be taken as a valid response.
- Security downgrade—even with high security mode using of authentication mechanism is non obligatorily. XOR keystream model ciphers are vulnerable to bit-flip attacks, which makes it possible to remove message authentication tags. This vulnerability of DLMS/COSEM protocol leads to the possibility of acquiring ciphertexts by known parts of plaintext, authentication mechanism disables, and message replacement.

DLMS/COSEM implementations are also not free of bugs. Some vulnerabilities that may be present in particular implementations of the DLMS/COSEM protocol are listed below (https://research.tue.nl/en/studentTheses/dlms-cosem-protocol-security-evaluation):

- Invocation Counters Unenforced—the server accepts messages whose frame counter is less than or equal to the counter of the last encrypted message received from a device. This results in a lack of adequate protection against replay attacks.
- Predictable Association Challenges/Nonces—If predictable nonces are used, an attacker could calculate the necessary HLS responses to be able to authenticate with the server or client. Highly unpredictable nonces shall be used (e.g. using a CSPRNG or a TRNG). As a solution—implementations should not use a linear congruential generator.

- Identical AP Titles Allowed—If communication between two devices with the same AP title is allowed, a client or server can allow communication with a DLMS/COSEM device with the same AP title. This could allow replay attacks.
- Arbitrary System Titles Accepted—For each different ST the last used IC shall be remembered. If arbitrary ST are accepted, an attacker may attempt a Denial of Service (DoS) attack by filling the IC database. If a ring buffer is used, an attacker may attempt to reset one counter by filling up the buffer and eventually proceed with a replay attack.
- The messages are processed only based on the header that indicates the type of message, without verifying their content—If messages are processed only taking into account the header indicating the type of message, an attacker could send a message whose type indicates that it is an encrypted message, but with the encryption and authentication bits disabled in the byte of security, potentially tricking the server into processing a malicious message sent in plain text.
- Encrypted AARE messages are sent in response to plaintext AARQ—This may allow this information to be used to obtain the keystream since the values of the AARE messages are known based on the AARQ sent.
- Possibility of online dictionary attacks—Multiple authentication attempts are allowed, allowing online dictionary attacks. After N connection attempts, the error messages should be the same.
- Messages with an invalid authentication tag are allowed—If messages are processed without checking the authentication tag, the messages are vulnerable to integrity violations.
- Encrypted messages without authentication are allowed—Encrypted messages without authentication are susceptible to manipulation, so it is desirable that they are not processed.
- Insecure authentication methods are allowed—LLS should not be used as the password is sent in plain text. In addition, proprietary authentication methods, and the MD5 and SHA1 versions of HLS are vulnerable to man-in-the-middle attacks.
- Ciphered APDU Type Ignored—when in the security header the tag leaks information about the secured message type (e.g. Get), the contained plain text message type shall be consistent. Some devices ignore this and accept the message.
- Plain Text APDU Accepted—some implementations that are supposed to accept only secured messages can be fooled to accept plain text messages by simply using the security header with both the crypto/auth bits turned off.
- Message authentication code (MAC) not enforced—Messages with invalid MAC are accepted. Invocation Counter Reset After Reboot On power loss, some implementations reset the IC to zero.
- Premature Session Termination—HLS Associations shall terminate with an encrypted termination message. Some implementations accept plain text termination messages, thus allowing an attacker to disconnect legitimate sessions.
- Default keys on production—Meters on the field are occasionally left with their manufacturer default keys. The keys are not only equal between user profiles, but also between several hundreds of meters.

- Client Skips HLS Authentication Check—some clients do not check rogue servers and just ignore the received f(CtoS) response.

Covering all of the considered vulnerabilities is possible via adding additional restrictions to DLMS/COSEM software implementation. As an example—possible to make the implementation force reject a message if this message does not use an authentication mechanism. By information that we have from SMI project meetings and direct responses—Landis+Gyr, Siemens SMI, and Linky solutions should be resilient to described vulnerabilities because they are implemented according to the IDIS specifications.

4.5 TLS with BSI Restrictions and DLMS/COSEM Comparison

Transport Layer Security (TLS, formerly Secure Sockets Layer or SSL), is a cryptographic protocol designed to provide secure communications over computer networks. TLS could be represented as the special shell that provides encryption and integrity (to prevent eavesdropping and tampering) of higher-level data protocols such as email, instant messaging, voice over IP, or HTTP. TLS was proposed by Internet Engineering Task Force (IETF) as a standard and was first defined in 1999 on the earlier SSL protocol specifications (1994, 1995, 1996) developed by Netscape for adding secure HTTP protocol to their Navigator web browser. The modern TLS version 1.3 was defined in August 2018, but BSI SMGW documentation requires to use of TLS version 1.2 whose implementations are currently much better tested compared to version 1.3. The TLS protocol includes two main parts—the TLS record and the TLS handshake protocol. When a TLS server and a TLS client have agreed to use TLS, they use a handshake with asymmetric cryptography to establish cipher settings and create a session-specific shared key which is later used for symmetrically encrypted communication. The handshake protocol is responsible for choosing parameters that will be used to establish the secured connection.

Comparing TLS and DLMS/COSEM stack of protocols, they have similar cryptographic security levels. Both use PKI (Public Key Infrastructure), modern security primitives, and cipher suites. The difference between DLMS/COSEM and BSI SMGW TLS PKI is that in the SMGW PKI uses a state-controlled root-CA which means that the signature should be legally standardized and issued certificates have demanded lifetime periods for all three network interfaces in TR (Table 4).

The main difference between these two protocols is that DLMS/COSEM is less complex compared to TLS. TLS can be regarded as a “wrapper” protocol that is used to secure application-level data, whereas DLMS/COSEM is a more specialized protocol which theoretically should reduce the chance of vulnerability appearance. TLS is a more complicated protocol which means that TLS has more points that potentially could be vulnerable to an attack. The TLS protocol is designed to be

Table 4 TLS and DLMS comparison (Lüring et al. 2018)

	DLMS/COSEM	BSI SMGW TLS
PKI	+	+
Authenticated encryption	AES-GSM-128 AES-GSM-256	AES-GSM-128 AES-GSM-256 AES-CBC-128 AES-CBC-256
Elliptic curves	NIST P-256 NIST P-384	NIST P-256 NIST P-384 BrainpoolP256r1 BrainpoolP384r1 BrainpoolP512r1
Digital signature	ECDSA	ECDSA
Key agreement	ECDH	ECDHE
Key transport	AES key wrap	AES key wrap
Hash function	SHA-256 SHA-384	SHA-256 SHA-384
Message authentication code	GMAC	CMAC

flexible and adaptable, allowing for the easy addition or removal of security primitives and algorithms as needed, such as in the case of a discovered vulnerability. The TLS protocol is also designed to be independent of any specific security primitive or algorithm, and there are currently over 442 cipher suites registered with the IANA that can be used with TLS implementations. In the case of DLMS/COSEM implementations changing the algorithm will be more complicated in comparison with TLS, because currently DLMS/COSEM supports only 3 security suites. Also, because DLMS/COSEM supports only 3 Security Suites—implementations are more lightweight, which is essential for embedded systems.

One more advantage of the TLS protocol is its widely carried out research for potential vulnerabilities. The reason for this lies in the widespread use (e.g., in banking and shopping businesses areas where secure Internet connections are very important). There are significantly more known vulnerabilities in the TLS protocol compared to DLMS/COSEM, with 781 reported for TLS compared to just 2 CVEs for DLMS/COSEM. CVE (Common Vulnerabilities and Exposures) is a system for publicly known information-security vulnerabilities. However, there appears to be significantly more research and testing conducted on TLS, as indicated by the higher number of papers on the topic in Google Scholar, with over 25,000 papers published on TLS compared to just 862 for DLMS. DLMS has info only about 2 CVEs and both in free open source software Gurux.

Two more differences are the used random number generation mechanisms and secure key storage. In the case of BSI SMGW, TLS TR requires a certain number of generator classes that can be used and cryptographic materials should be stored in a special SMGW security module. In the case of DLMS/COSEM the specification

just requires the use of a "strong random number generator" and does not have any requirements for special cryptographic materials storage.

5 Theoretical SMI Systems Security Comparison

To compare French, German, and Swiss smart metering infrastructure we start with a comparison of the supervisory authority's requirements for smart metering infrastructure solutions. France had very concrete legal data protection since 1978 (French National Assembly and the Senate 1978), but technical requirements for smart metering systems are the most abstract compared to German and Swiss supervisory authority's requirements. Due to Enedis energy distribution market dominance, the problem with lack of technical requirements is partially solved. Because Enedis managed to create a great system with a lot of useful smart metering features and for comparison purposes, we use a Linky system as the only French smart metering solution for comparison. One of the cons of the Enedis documentation is that most Linky features are only described in marketing materials (such as Enedis presentations/brochures; https://www.enedis.fr/documents?term_node_tid_depth%5B106%5D=106) and we did not find much publicly available technical documentation (such complete as German TR-03109-1). Some information about the Linky system was received from Enedis speakers at project meetings, but unfortunately, we were not able to find some documentation proof and should make conclusions based only on the speaker's words and marketing materials. In the document "Linky PLC profile functional specifications" [ERDF-CPT-Linky-SPEC-FONC-CPL (EDRF 2009)] Enedis refers to DLMS/COSEM (IEC 62056) protocol from "Coloured books", in which authentication and encryption are used as the main Linky system security mechanisms. From a security point of view, the Enedis energy market-dominating has some advantages. Using only one device type for a smart metering solution means that the algorithm for making any device settings is also the same. The probability that service technicians will do incorrect settings that could lead to a system vulnerability is lower than in the case of multiple solutions from different models.

BSI creates a complete documentation system that fully describes an architecture, protocols, access rights, and other requirements for a smart metering infrastructure. All documentation is publicly available on the BSI website (https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Smart-metering/Smart-Meter-Gateway/smart-meter-gateway_node.html). In contrast to France, in the German distribution network exist about 883 distribution companies of various sizes. It is likely that the decision to have a longer process for developing the requirements and documentation structure for the German BSI smart metering system contributed to the fact that it was implemented later than the systems in France and Switzerland. BSI documentation gives the impression of transparency and a comprehensive elaboration in comparison with Swiss and French SMI supervisory authorities' requirements.

But different from the German system, Swiss supervisory restrictions in the field of architecture and used protocols are very low. Theoretically, that can lead to an increase in the probability of vulnerability presence because of the large number of used protocols and device variations. From another point of view, if a significant vulnerability is found in one system, for example in Landis+Gyr, that will not mean that the Siemens system will have the same problems, and the probability that all smart metering solutions in the country will be vulnerable in one moment is lower than in French system. Landis+Gyr and Siemens provide answers to most of our questions about their systems but were careful in questions about the security part.

Based on information from the previous sections it is possible to say that from the smart metering systems architecture point of view French Linky and Swiss solutions from Landis+Gyr and Siemens are very similar. These systems include several points that theoretically could be attacked:

1. Energy service provider backend system
2. WAN connection from an energy service provider to a data concentrator
3. Data concentrator device
4. PLC connection from a data concentrator to a smart meter
5. Smart meter device
6. Connection from smart meter device to controllable local devices
7. Controllable local devices.

German BSI SMGW system smart metering architecture is slightly different from the solutions described above. Describing the points on which it is theoretically possible to make an attack, possible to distinguish:

1. Energy service provider backend system
2. Smart meter gateway administrator system
3. Smart meter gateway operator system
4. WAN connection from SMGW to external market participants
5. SMGW device
6. LMN connection from SMGW to meter devices
7. Connection from smart meter device to controllable local devices
8. Controllable local devices.

To make the analysis more correct it is important to divide the attackers into two groups—internal attackers and external attackers. Internal attackers are household owners who are interested in energy consumption data tampering to reduce their costs. They are not interested in controllable local device hacks because they already have physical access to them. The role of outside attackers can perform as malefactors which want to gain profit or potential adversary services interested in causing damage to destabilize the local situation.

Because of very soft restrictions for Swiss smart metering systems, both German and French SMI systems potentially can be used in Switzerland. All systems considered in this report use the OBIS model, which means that theoretically, they could use the same software in the backend system.

From the point of view of an outside attacker, the most interesting aim is the energy service providers backend system. We do not have the permission to make energy service provides backend systems scanning or penetration testing in this project. Therefore, we do not have information about services and software running on the energy providers servers, but we are sure that at least it should have a service to receive consumption data and control home appliances on the energy consumer side (in the case of France and Germany). Enedis has a web API that can be used by users to collect consumption data (https://data.enedis.fr/api/v2/console). The probability that the same company network will run web, FTP, SSH, or some other common services that could be vulnerable and used as entering points is higher than the probability of finding a vulnerability in other elements of smart metering architecture because all devices considered in this work are relatively simple in terms of operating logic compared to the backend part and have a small number of "influence points" which are possible to test.

Also, the hacking of backend servers provides a large list of opportunities that cause the most damage to the system such as:

- Accessing the consumption data of a large number of users.
- Gaining access to smart metering devices control (such as data concentrators or smart meters) which, for example, can be used to create a botnet or simple devices deny of service.
- Make a "blackout" by getting remote access to power substations.

Some artificial intelligence and predictive maintenance tools such as Enedis Carto-Line theoretically can be used to make some harm to the systems. Knowledge about calculations algorithms and access to manipulating smart metering device consumption data or data concentrator should be possible to use for transmitting incorrect data to HES, which will lead to the incorrect settings on electricity substation and can therefore cause a blackout or overvoltage which could in turn lead to a system running out of order. Also, stopping all the meters at the same time could create an energy excess and a break in the network.

To make a botnet it is important to have the ability to upgrade firmware or install additional software. At the SMI project meeting, the speaker from Enedis said that a Linky meter can produce a remote and local firmware upgrade. In open sources, there was no concrete information about how the Linky, Landis+Gyr, or Siemens devices firmware upgrade process is organized (how to transfer a new firmware image to the device and how to secure this process). But there exists information about how the firmware upgrade process could be done with smart meters that use DLMS protocol in the documentation of open-source software for DLMS-based smart meter managing—Gurux (https://www.gurux.fi/front-page). Based on the information from the Gurux documentation, it is required to use the "highest" security mode of the DLMS connection (with ciphering, authentication, and encryption) to perform a firmware upgrade.

In contrast to the French and Swiss Landis+Gyr and Siemens solutions, in the case a hacker gets access to the German BSI energy provider backend system—a hacker will only get access to the store on this server energy consumption data and to

the controllable local devices, which were previously confirmed by the smart meter gateway administrator. Only SMGW administrators can install firmware updates or add a new controllable local system devices. The SMGW administrators should check for firmware updates from SMGW producers' resources and only after successful verification install updates on SMGWs.

One other important aspect is the SMGW's "wake up" service—which is described in the "German smart metering infrastructure" section. Because of the "wake up" service hackers will not even be able to scan a SMGW from the WAN side even if a SMGW will have a public IP address in the WAN and therefore the task to hack a SMGW from the WAN side looks close to be impossible. Even if an attacker will be able to bypass the wake-up service, the SMGW will initiate a TLS connection to the SMGW administrator, which will be protected by TLS and also requires to be hacked to make some harm. In case of DLMS/COSEM based devices, there is no information about such things as BSI "wake-up" service, and because of that in the systems where smart metering devices implement the DLMS/COSEM server role, an attacker can perform any scan or attack attempt if he is able to get access to the required network.

Linky does not have an additional protection by TLS on a connection from the data concentrator to the Energy service provider backend system and only uses the PLC protocol at the physical layer (EDRF 2009). Was found the source which mentions the use of TLS in the context of the Linky system—"The Linky system uses more traditional protocols, not specific to the IoT world, such as https, the ins, and outs of which are better understood. It was thus possible to rely on TLS to secure exchanges" (Marcellin 2018). But in this case, the speaker probably means some Enedis website, because none of the documentation or some promotion materials contains info about TLS.

The PLC G3, which is used in the French Linky, Swiss Landis+Gyr, and Siemens systems to connect a smart meter to a data concentrator, uses AES128-CCM encryption for Data Link (OSI layer 2) security (Genest et al.). For the German BSI SMGW system, the most common WAN type is a cellular network LTE connection. In the case of LTE data encryption exists 4 possible options (https://www.sharetechnote.com/html/Handbook_LTE_EEA.html.; Bartock et al.):

1. 0000—Null ciphering algorithm
2. 0001—SNOW 3G—stream cipher designed by Lund University (Sweden)
3. 0002—AES128—Block cipher standardized by NIST (USA)
4. 0003—ZUC—stream cipher designed by the Chinese Academy of Sciences (China).

As we can see, both options are equally protected at the data link level, but the LTE solution has more possible options.

One more possible direction of comparison is the use of HSMs (Hardware Security Modules). In the case of the Linky system, there is not much information about HSM. It is just one time mentioned in the source (Marcellin 2018), where said that HSM "allows data to be stored" and on page 9 of the source (Nguyen) is shown that HSM is used in the data concentrator device.

German BSI Hardware security module is a different physical device, which allows to divide security and measuring functionalities. BSI TR-03109-1 strictly defines how HSMs should be used. A BSI SMGW must use a HSM for the TLS handshake and other cryptographic operations. For mutual authentication between a SMGW and meters in the LMN, LMN certificates which are X.509 self-signed certificates must be used.

Landis+Gyr Gridstream solutions include the next information about the HSM module (Landis+Gyr 2020)—the HSM serves as the root of trust where the utility ECC private key is vaulted. The private key is used to generate digital signatures to downstream commands sent by the HES. The HSM also features FIPS 140-2 and Common Criteria Level 4 certifications, providing strong protection for one of the critical elements in the advanced security architecture.

In the case of Siemens solutions were found such information as (Jöbstl 2019)—Siemens is using dedicated appliances such as the Hardware Security Module. This module is responsible for the whole meter data decryption and is the only system on which clear text meter keys are present. Meter keys never leave the tamper-resistant foil-coated CPU or its cache. This ensures a physical protection layer to the smart meter data security.

Regarding other architectural aspects, commonly data concentrators (which are used in Landis+Gyr, Siemens, and French SMI systems) are installed in the public territory and have an Ethernet interface with a web server to make settings. Because this element is installed outside the household, compared to the German system, this adds an additional potential vulnerable point to the system, which theoretically can be attacked if the malefactor has physical access from the smart meter to the data concentrator side (for example adding noise to PLC connection in the case to organize DOS attack) and from WAN side.

The German BSI SMGW is commonly installed inside a household. In case a wired connection is used for the LAN and the HAN network is not connected to the home internet router, then the only way to get access to this system from the outside is the WAN (which is well protected as described above). Theoretically, a malefactor can try to attack a SMGW administrator, but due to the limited number of tasks and complicated certification conditions success probability of this attack is quite low compared to an attack on an energy service provider network or data concentrator in French and Swiss Landis+Gyr and Siemens systems. An implementation of passive data sniffing (e.g., if a malefactor will get access to the mobile network base station), will be more complicated in case of the German BSI SMGW, because the consumption data is additionally protected by TLS on the CMS level. Even SMGW administrators could not read energy consumption data, because only the energy distribution service has a key to decrypt the data on the CMS layer.

From an architectural point of view, French and Swiss architectures are theoretically more vulnerable to outside attackers compared to German systems, but less vulnerable to the inside attacker, because the electricity meter module is placed in the same case as the communication unit. In Germany, it is allowed for the meter and SMGW modules to be placed in the same box “SMGW-PP 1.4.5.3 Possible TOE Design: One Box Solution”, but there are no known devices on the market that use

this architecture. Both German and French SMI systems may potentially be used in Switzerland due to the relatively lenient regulations for Swiss smart metering systems.

Comparison of smart metering systems parts installed inside the household is complicated. In the case of French and Swiss systems, by information that we got from Enedis, Landis+Gyr and Siemens any communication protocol could be used by connecting an additional dongle to the main smart meter system. There are no restrictions in documentation from supervisory authorities on this part. Based on this information, the only conclusion that we could do is that potentially these systems could not be protected at all (for example in the case with wrong settings) and are very vulnerable because of this. From a security point of view—one more advantage of Landis+Gyr and Siemens and French Linky system is that the energy meter and communication module are placed at the same device—which makes internal attacker's actions more complicated because there are fewer entry points in comparison to the SMGW system.

In case of the German BSI SMGW, an attack on the local metrological network (that connects meters and SMGW) will be problematic to an outside attacker, because the SMGW is commonly installed inside the household and in case of a wired LMN connection the SMGW device and energy meter device are installed in the same box. BSI allows several protocol variations for LMN and WAN, it increases the chance of misconfigurations. As we know from our partner the local DSO configuration settings process of Ethernet, mobile network for WAN connections, wireless M-Bus or wired connection for LAN differ a lot. Wireless M-Bus short connection range makes the possibility of a massive SMGW devices DoS (denial of service) attack on LMN extremely difficult for an outside attacker and the probability that an outside attacker will be interested in LMN data tampering or DoS attack only on one device is very low.

6 Use Case: Secure Smart Meter Gateway

As we can see from previous sections, the German BSI SMGW has a very well elaborated security system. Currently, BSI has certified 4 SMGWs (SMARTY IQ, CASA 1.0, PPC LTE, CONEXA 3.0), and 5 more SMGWs are currently under the certification process. Even SMGW device acquisition is a complicated task.

One of the possible alternatives is to use some virtual SMGW. But the only project that was found is jOSEF (A Java-Based Open-Source Smart Meter Gateway Experimentation Framework). Unfortunately, the jOSEF project does not implement SMGW security features responsible for encryption and authentication (TLS, PKI, etc.).

To acquire a real SMGW device, it is required to register as a system operator (Anlagenbetreiber) at German Federal Network Agency (BNetzA) website www.marktstammdatenregister.de/MaStR/. IvESK got a license MaStR-Nummer: ABR931965228164. After that, we get the permission from the local DSO company

to test two SMGW devices CONEXA 3.0 from Theben and smart meter gateway PPC LTE from Power Plus Communications AG. But there are a number of limitations to testing these devices:

1. We should not try to test SMGW admin and EMP infrastructure.
2. We should not do any physical harm to devices (including device disassembly to try to download the firmware or affect some interfaces).

In general, it means that we were only able to test SMGW device interfaces in form of a "black box" testing, because we do not have some shell running on the device or even device firmware. During the information gathering and reconnaissance phase the SMGW firmware of PPC was found on their website (https://gwafirmware.ppc-ag.de/). But the download from the website requires authorization.

Device Scanning and Information Gathering

First, we needed to find a way to communicate or interfere with the testing devices and to find SMGW ports available for interaction. For this purpose, the Netdiscover software was used for active/passive address reconnaissance by actively sending ARP requests.

The Theben CONEXA 3.0 SMGW box has three Ethernet ports (Table 5). The WAN-1 Ethernet port is probably turned off because Netdiscover shows nothing on this port. Even when the Ethernet port is connected to the adapter port the LEDs do not start to blink. It is most probable that this port has been completely disabled by the administrator because the SMGW uses a cellular network for a WAN connection.

The CONEXA 3.0 SMGW and PPC SMGW show different MAC addresses in CLS and HAN Ethernet ports. However, the IP address is static and in both ports and set to192.168.100.100. The CLS Ethernet port does not respond to ping requests. Only the HAN Ethernet port on PPC SMGW can be reached.

Finding the IP addresses in the HAN for both SMGWs was successful. Both SMGWs have static IP addresses, but all other parameters are different. In the case of the CONEXA 3.0 SMGW, it has an IP address 192.168.0.1 on both HAN Ethernet ports that have the same MAC address (one on the device corpse and one in the

Table 5 Available SMGW's interfaces

CONEXA 3.0 SMGW	SMGW PPC LTE
• 1 WAN Ethernet port (RJ45) • 1 WAN LTE antenna port (FAKRA SMB connector) • 1 SIM card slot • 1 CLS (HAN) over Ethernet port (RJ45) • 1 HAN over Ethernet port (RJ45 on MTG Mehrwert Konnektor module) • 1 LMN over RS485 (RJ12) port • 1 LMN Wireless M-Bus (OMS) antenna port (FAKRA SMB connector) • Power supply connector	• 1 WAN LTE antenna port (FAKRA SMB connector) • SIM card slot • 1 CLS (HAN) over Ethernet port (RJ45) • 1 (HAN) over Ethernet port (RJ45) • 1 LMN over RS485 (RJ12) port • 1 LMN Wireless M-Bus (OMS) antenna port (FAKRA SMB connector) • Power supply connecter

Mehrwert module), which means that probably the Mehrwert module works as a simple switch. In case of the SMGW PPC the LTE HAN Ethernet port and CLS (HAN) port have the same IP address 192.168.100.100, but different MAC addresses which differ only in the last bit.

For finding running services the zenmap port scanner software was used. Zenmap is the official Nmap Security Scanner GUI.

List 1 SMGW Conexa 3.0 HAN zenmap scan

```
PORT    STATE SERVICE    VERSION
443/tcp open  ssl/https?
| ssl-cert: Subject: common-
Name=ETHE03XXX.SMGW/organizationName=SMGW/countryName=DE
| Subject Alternative Name: DNS:ethe03XXX.sm
| Issuer: common-
Name=ETHE03XXX.SMGW/organizationName=SMGW/countryName=DE
| Public Key type: unknown
| Public Key bits: 384
| Signature Algorithm: ecdsa-with-SHA256
| Not valid before: 2021-01-22T09:08:00
| Not valid after:  2026-01-22T09:08:00
| MD5:   e31e e6eb 1089 4991 46b0 f839 6d85 5781
|_SHA-1: f94f 7a10 6716 8102 fcbf 4cb2 05b6 501e 6d6e 63d9

1080/tcp open  socks?

MAC Address: 5C:CA:32:XX:XX:XX (Theben AG)

Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port

Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.10 - 4.11, Linux 3.2 - 4.9
```

As presented in the list above, the default zenmap scanner only shows two open ports in the Conexa SMGW HAN. It is a TLS server that runs on default port 443 which fulfills the requirements of BSI TR-03109-1 interface realization IF_GW_CON CON for HAF1—end-user data provision and, probably, HAF2: Service technician data provision. This TLS server uses a fairly reliable signature algorithm mechanism ecdsa-with-SHA256. The fingerprinting NSE script cannot define the CONEXA SMGW HAN TLS server version.

The second open port is 1080, which zenmap defines as socks. This port is responsible for the implementation of HKS3 (home communication scenario 3—transparent channel initiated by CLS). One more interesting observation is that sometimes

this socks port just disappears even when the scan was done exactly with the same parameters. Unfortunately, we did not find a reason for this behavior.

Another important moment is defined by zenmap in the OS details section Linux version, but it will be described later.

List 2 SMGW PPC LTE HAN zenmap scan

```
PORT     STATE  SERVICE       VERSION
443/tcp  open   ssl/http      lighttpd
| ssl-cert: Subject: commonName=EPPC02XXX/organizationName=OpenLimit-
PPC/countryName=DE
| Subject Alternative Name: othername:<unsupported>
| Issuer: commonName=EPPC02XXX/organizationName=OpenLimit-
PPC/countryName=DE
| Public Key type: unknown
| Public Key bits: 256
| Signature Algorithm: ecdsa-with-SHA256
| Not valid before: 2020-03-04T10:47:53
| Not valid after:  2027-03-04T10:47:53
| MD5:   0421 1112 0256 bcf5 6ab9 c7cc 185a 9ae7
|_SHA-1: 1f53 f675 84e9 9351 e6b2 6d38 8d50 4d78 1bf6 63d1
2222/tcp open   ssh           Dropbear sshd 2017.75 (protocol 2.0)
8001/tcp closed vcom-tunnel
8002/tcp closed teradataordbms
8003/tcp closed mcreport

MAC Address: 00:25:18:XX:XX:XX (Power Plus Communications AG)

Aggressive OS guesses: Linux 3.10 - 4.11 (98%), Linux 3.2 - 4.9 (94%), Asus RT-
AC66U WAP (93%), Linux 4.4 (92%), Linux 4.1 (92%), HP P2000 G3 NAS device
(91%), Linux 3.16 - 4.6 (91%), Linux 2.6.32 - 3.13 (91%), OpenWrt Chaos Calmer
15.05 (Linux 3.18) or Designated Driver (Linux 4.1 or 4.4) (90%), Android 5.1 (90%)

No exact OS matches for host (test conditions non-ideal).
```

Default zenmap monitor shows 2 open ports in PPC SMGW LTE HAN. Regarding TLS port 443 it implements the same like with CONEXA 3.0 SMGW, but in this case zenmap was able to fingerprint web server software—lighttpd. Other open port is SSH server which listen port 2222. Zenmap was also able to fingerprint version of SSH server—is Dropbear sshd 2017.75.

Also, zenmap define ports 8001, 8002 and 8003 as closed. In zenmap is some port is marked as closed this means that the port is accessible (it receives and responds to Nmap probe packets), but there is no application listening on it (Nguyen). During our research we did not find any information regarding purpose of this ports.

Possible Attack Directions

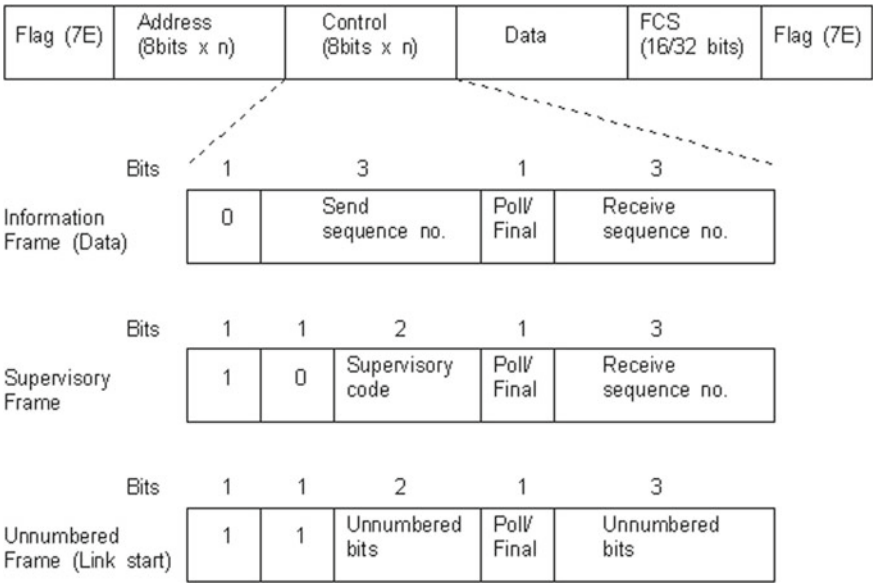
After the analysis of our theoretical comparison section and the scanning of real devices, we define a list of possible SMGWs testing directions:

1. The direct attack to the energy service provider network
2. The direct attack on the SMGW administrator network
3. SMGW manufacturer website firmware modification
4. Use registered by SMGW administrator CLS certificate to penetrate the energy service provider network via TLS tunnel
5. WAN PKI attacks
6. WAN Wake-Up service fuzzing
7. Manual Wake-Up package overflows of header identification, recipient, and timestamp fields
8. WAN port DDOS. Because in PP 1.4.6.5 step 1.d check wake-up message has not been received before, and only after that check the signature of the wake-up message. If the number of these wrong messages will be big enough, before SMGW will check the real SMGW admin wake-up package, the timestamp of this package already will be outdated
9. "Received before" packages logs overflow
10. LMN AFL tests
11. LMN consumption data tampering (TLS attacks)
12. Internal logs overflow (consumption, actions, etc.)
13. HAN TLS server common vulnerabilities testing
14. HAN TLS server fuzzing
15. HAN username/password sniffing
16. HAN Web servers testing
17. CONEXA SMGW HAN socks server testing
18. PPC SMGW HAN SSH server testing.

Testing of 1–4 was unavailable for us because of the testing agreement conditions and lack connected to SMGW CLS devices to be able to test it. 5–9 requires to have an access to the SMGW WAN port. Because the wired WAN option was disabled, we attempt to interact with SMGW using a Wideband Radio Communication Tester R&S CMW500 and create a MITM connection. For this purpose, we use a spectrum analyzer to find the LTE Band which the SMGW uses to communicate via the cellular network, change the SIM card to a special one and wirelessly connect the SMGW to the CMW500. We succeeded in LTE-level traffic sniffing but were unable to decode it into IP-level data because of a lack of a special license. After some time it was decided to concentrate on other testing directions because even in case of success all planned attacks analysis will be too complicated because of the lack of access to SMGW administrator software and even the lack of possibilities to run the SMGW software locally on some other device.

For testing the cases 10 and 12 a communicate with the SMGW in the LMN network is required. For this purpose, we firstly use a RS-485 to UART adapter module based on the MAX485 board. After getting the possibility to analyze SMGW

RS485 data we found that none of the tested by us software (4 python lib's including scapy, 2 c++ lib's, and Wireshark text2pcap) can parse this HDLC data, and was decided to analyze it manually.



Picture Common HDLC frame structure

As we can see from the picture above—common HDLC implementations include frame start flag 7E field, address field, control field, information field, frame check sequence (FCS), and frame end flag 7E as presented in the picture below. In case of observed data, this sequence differs:

List 3 SMGW CONEXA LMN data

```
7e a0 09 fe03 0203 13 842a 7e
7e a0 2b 0203 b803 131cb6 5c 00
0a01454d4800005ec1f6000000000a01454d4800005ec1f6000000000000 4cec 7e
7e a0 09 b803 0203 53 3a92 7e
7e a0 09 0203 b803 1f 46f1 7e
7e a0 2b fe05 0205 13f8b8 5c 01
0a01454d4800005ec1f6000000000a01454d4800005ec1f6000000000000 7829 7e
7e a0 2b 0205 b805 1356a9 5c 01
0a01454d4800005ec1f6000000000a01454d4800005ec1f6000000000000 7829 7e
7e a0 09 b803 0203 93 3654 7e
7e a0 09 0203 b803 73 2c58 7e
7e a0 09 b803 0203 11 2cf3 7e
7e a0 09 0203 b803 11 3818 7e
7e a0 7a b803 0203 10d92b
160303006a0100006603036140f3c77fed3a4d19f8f9305b67e356222a0e625fdf7c27f00
c6c0bf3f8546000000ac02bc02cc023c02400ff01000033000d000800060403050306030
00a000c000a00170018001a001b001c000b000201000001000103001600000017000000
0230000 31d3 7e
7e a0 09 0203 b803 35 1e7f 7e
7e a0 2b fe03 0203 13b2a7 5c
000a01454d4800005ec1f6000000000a01454d4800005ec1f6000000000000 4cec  7e
7e a0 09 b803 0203 11 2cf3 7e
7e  a2  4d  0203  b803  30750d
160303006402000060030366 1e9440e22e15479217cdd6c62142d2fXXX
```

Where:

7e—frame start/end flag

a0—some control data OR first part of a frame length field

09—frame length (including this and first byte)

fe03 b803—HDLC address (destination). fe03—is a broadcast address

0203 b803—HDLC address (source). 0203 is probably SMGW address that is always the same in the case of PPC and 0a01454d—some individual smart meter number string that includes EMH (name of smart meter producer) in utf8 form

842a—FCS, frame check sequence

13—some unknown payload parts

160303006aXXX—TLS client_hello payload

1603030064XXX—TLS server_hello payload

As we can see, the flag and address frame fields are the same with a common HDLC, but FCS (frame check sequence) calculates differently. We tried different FCS algorithms with special calculators but were not able to find the correct one. The TLS messages look normal and we can analyze them in hex form, but using some external testing software required additional modification. Because of all described problems was decided to concentrate on HAN attacks for several reasons:

- It is likely that the same implementation of TLS is used across all SMGW networks.

- TCP layer attacks should have the same effect in every network because commonly TCP implementation work on the kernel level.
- It is just more convenient to communicate with SMGW via Ethernet.

SSH Server Testing

The first priority was testing of the SSH server that was found on the SMGW PPC LTE because getting access to it (even in non-root mode) will make testing much more effective because it will allow to understand processes running in the device. It was surprising to discover this SSH server, as the only source of information about it was (https://stg-tud.github.io/sep/projects/2017/eMobilityTeam/site/#technologies). This source also has a few important pieces of information about the testing system:

> As developers, we can access the system via Secure Shell (SSH) with root rights. It is an embedded PTXDist Linux that PPC already uses in the same form for the SMGW. The hardware is an ARMv5 board. Much of the memory (except for /usr/ local/) is persistent. When the system starts, the script /usr/local/bin/custom.sh is called. This can be adapted by the developer in order to generate a certain behavior after a restart. Package management is available with Open Package Management (OPKG) so that the software can be packed into a Debian package and installed.
>
> Due to the low computing power (ARM926EJ-S with ~ 226 BogoMIPS), the limited memory (~ 250 MB main memory, ~ 200 MB free permanent memory) and the hardware-related requirements, the SEI software will consist almost exclusively of C and C++ components.

Manual connection to the PPC SMGW HAN SSH server shows that the server accepts username/password authentication (not only certificate). Authentication log:

List 4 PPC SMGW HAN SSH server manual connection log and common SSH connection log

```
ssh root@192.168.100.100 -p 2222
root@192.168.100.100's password:
Permission denied, please try again.
root@192.168.100.100's password:
Permission denied, please try again.
root@192.168.100.100's password:
root@192.168.100.100: Permission denied (publickey,password).
```

The technician from the company which provides us with SMGW devices told us that by their information SMGW testing firmware is the same as the production one, and they don't know about such difference. It is possible that SSH may be used by service technicians, but the likelihood is low because SSH provides too wide access capabilities and it is difficult to restrict all prohibited functionality. Moreover, "HAF2: Service technician data provision" requires the use of certificate based authentication instead of password based. We assume that the SSH server is presented only in testing firmware, but even in this case, it can be very useful for our testing.

Because the SSH password authentication method is available—one of the methods to get the password is to use the brute force technique. The most effective SSH brute force can be done if at least the list of machine users is known. Fortunately, used on SMGW Dropbear SSH version 2017.75 is vulnerable to CVE-2018-15599. In Dropbear through 2018.76 function recv_msg_userauth_request in svr-auth.c is prone to a user enumeration vulnerability because username validity affects how fields in SSH_MSG_USERAUTH messages are handled. This is an issue similar to CVE-2018-15473.

The first way to exploit this vulnerability is to compare SSH server response time with different usernames. To check this was created test bench—raspberry pi with the same version of Dropbear SSH 2017.75 and was created Paramiko lib based python script. Because the list of users available via SSH in a raspberry pi test bench is known—the testing approach includes SSH username request-response timing comparing different usernames with the same big-length password. On the test bench USB-Ethernet PC connection ping time is an average of 0.57 ms. Via direct PC PCI-Ethernet to SMGW HAN Ethernet average ping time was 0.47 ms. But even with this timing on the test bench it was impossible to distinguish available and absent SSH users, probably because the used python library is too slow for this purpose.

An alternative way to test this vulnerability is to use the Metasploit auxiliary/scanner/ssh/ssh_enumusers module. This Metasploit module includes two options—"Timing Attack" and "Malformed Packet Attack". The timing attack option is close to the previous method and is based on the fact, that some versions of SSH will return a "permission denied" error for an invalid user faster than for a valid user. With the Malformed Packet option, Metasploit sends a malformed (corrupted) SSH_MSG_USERAUTH_REQUEST packet using public key authentication (that must be enabled) to enumerate users.

As in the case of using the python SSH timing script—The Metasploit ssh_enumusers module with the "Timing Attack" option does not lead to any results even in the raspberry pi test bench. But Metasploit Malformed Packet Attack gives results and we got a list of usernames for which SSH authentication is enabled and in the case of the raspberry pi test bench and on PPC SMGW. The received list of users did not allow speed up brute-force or make any assumptions about the operating system or other software running on the SMGW because these user names are present in most Linux-based systems.

The next brute-force step is to try to find a password for found usernames. There exist a lot of instruments for SSH credentials brute force attacks. The most popular are Metasploit ssh_login module with PASS_FILE option, Nmap NSE ssh-brute script, Patator, Medusa, and Hydra. Metasploit and Nmap options are the slowest in comparison with the other software because they can do brute force only with one thread. Hydra has the advantages to include the possibility to use several threads to improve the brute force speed and the possibility to continue from the point of word list after a brute force stop. Developers recommend using only 4 threads with low-performance devices to not cause a device DOS. With 4 threads speed of SSH brute force in PPC SMGW is only about 150 tries/min. Hydra PPC SMGW SSH brute

force tests show that it is also possible to use 5 threads. When was used 6 threads or more we got server responses "Connection reset by peer" on some of the requests.

At the moment, no password was found for any of the users. Perhaps the password is not present in the dictionary. Due to the low speed of password brute force, likely, it will not be possible to find the correct password until the end of the project. There are number of known vulnerabilities in Dropbear 2017.75, but none of them allows to bypass authentication or leads to remote core execution. Password sniffing is not important in our case because we do not have a client who knows the password to intercept it.

Web Servers Testing

Conexa SMGW allows to end-user consumption data retrieve only using special software such as TRuDI from PTB. TRuDI (Transparenz-und Displaysoftware) is a manufacturer-independent, standardized visualization solution that meets the requirements of the MsbG (especially §35, §62), the PTB-A50.8, and within the framework of the BSI specifications. TRuDI offers a display function with which the measured values that are available in the SMGW are displayed for the end consumer. In addition, a so-called transparency function is available. As part of this functional feature, the end consumer is able to use the software to locally understand tariff calculations that have been carried out on the basis of the measured values of the SMGW in the supplier's system landscape and thus to check his invoice.

For authentication, TRuDI allows using certificates (HKS1) or Username-Password pair (HKS2). Also, establishing a TRuDI connection requires a SMGW identification number, IP address, and port number. An identification number is required to determine the SMGW model and version in order to select the correct API (the location of this information may vary depending on the company that manufactures a SMGW).

On the HAN TLS port, Conexa SMGW provides a web page on the address https://192.168.0.1/smgw/cust/con-9910634000006-1273.sm/ where cust—probably means customer, con-9910634000006-1273—is user number and, sm—is a part from SMGW DNS. This web page includes only two tabs—the home page and the self-test. Access to this web page is protected via the same username-password as in TRuDI. We were not able to determine which framework or programming language was used via exploring web page code and based on other information. The home page just shows information about the SMGW such as the firmware version, SMGW ID, status, and system time. The self-test page includes only one button to run the self-test. After finishing the SMGW self-test for some reason the are results commonly not showing. Multiple calling self-test functions in a short time range (e.g., by python GET script) does not lead to any harm such as denial of service (DOS). Because the Conexa SMGW web server does not have any fields to enter some data—common SQL injections were tested only in the login and password fields.

PPC SMGW web server includes more possibilities for penetration testing compared with Conexa SMGW. It is accessible on URL /cgi-bin/hanservice.cgi, which means that CGI or common gateway interface technology was used on top of the Lighttpd service.

Common Gateway Interface (CGI) is a web server interface that enables standardized data exchange between external applications and servers. It is one of the first Internet interface technologies which is still widely used nowadays. In the case of using CGI, HTML pages are dynamically generated after the user requests a website and as an advantage, this means that HTML pages do not need to be stored on a server. This means that a CGI script cannot execute directly from a browser. To use a CGI script, it must be located on the same machine where a server is located.

When a user requests a server, this data is first processed by a CGI script. Then, the data is transferred via a standardized CGI interface, which can display the newly generated information in HTML form. CGI scripts are usually stored in a special folder on the web server. A CGI script can be implemented by a wide variety of programming languages. The Common Gateway Interface ensures that the web server and script can communicate with each other, independently of the used programming language. This programming language independency is based on a web server and CGI script interaction—because commonly it uses standard console output.

CGI also has some disadvantages, such as increased performance requirements of the webserver. Every time the CGI application is accessed, a new process is spawned with all the resulting overheads. If the application is buggy, it can loop for example. The browser will terminate the connection when the timeout expires, but the server-side process will continue until the administrator forcibly removes it.

Another problem is even with a low server load the response time of the CGI application is sometimes quite long because a script has to be restarted for each new input. Especially for websites with high traffic, it can become a problem that servers often only support a certain number of CGI applications and further incoming requests are then put into a queue or rejected—but for SMGW is not a big problem because conception assumes a low number of users. But even without a DOS attack, the PPC SMGW web server works slowly, from 2 to 10 s to open just 1 page. Commonly it required 5 s before getting the login form and about 5 more seconds to open a web page. Taking all the above disadvantages into account, we assume that PPC uses CGI—because it is a widespread and free standard.

SMGWs web server testing is not so different from common web server testing. The main difference is that the number of fields and points which possible to test is minimal. PPC SMGW web server includes more fields and forms to test compared with Conexa SMGW. PPC SMGW web server includes logs, counter, evaluation profile, communication profile, self-test, and software version pages. Logs and counter pages include fields that allow entering dates, and the evaluation profile page includes a drop-down menu. All these fields were tested for common SQL injections and successfully bypass this testing. Testing both SMGWs via Greenbone OpenVAS, Nikto, Burp suite (incl. spider and burp intruder testing), and OWASP ZAP does not allow us to find any vulnerabilities.

Also, because zenmap was able to fingerprint that PPC SMGW use Lighttpd, but was not able to fingerprint the exact version, was tested a few exploits for such CVEs as 2010-0295, 2011-4362, and FastCGI Header Overflow. None of the tested exploits were successful.

TLS Servers Testing

One of SMGWs penetration testing directions is TLS server testing. First, parameters such as TLS server version, cipher suites, or extensions supported by the SMGW are checked. For this purpose, it is possible to use instruments such as sslscan or sslyze. Both SMGWs support only TLS version 1.2 and use ECDHE-ECDSA-AES256-GCM-SHA384, ECDHE-ECDSA-AES128-GCM-SHA256, ECDHE-ECDSA-AES256-SHA384, ECDHE-ECDSA-AES128-SHA256 cipher suites as required by BSI-TR-03109-1. The difference between SMGW's TLS servers—server key exchange group in the case of Conexa SMGW uses 192 bits secp384r1 (NIST P-384) and SSL Certificate ECC Curve secp384r1. PPC SMGW uses 128 bits secp256r1 (NIST P-256) and SSL Certificate ECC Curve prime256v1.

Next, common TLS protocol vulnerabilities were checked. These vulnerabilities can lead to DoS or acceptance by TLS server parameters, which should not be accepted in normal circumstances (for example some weak cipher suites). This testing in HAN is important because as it was mentioned before, LMN and WAN SMGW networks probably use the same TLS implementation. For checking common TLS server vulnerabilities, Java-based TLS-attacker and tlsfuzzer software was used.

TLS-attacker was used to check the following list of common TLS vulnerabilities: Bleichenbacher attack, PSK bruteforcer, invalid curves, heartbleed, lucky13, padding oracle, tls poodle, CVE-2016-2107, early ccs, early finished, and Drown. All tests from this list were successfully bypassed by both SMGW's.

Also, old versions of TLS-Attacker (versions below or equal to 1.2) support TLS server fuzzing instrument. Fuzzing is a special technique for the automated detection of code errors. The fuzzer software sends the known incorrect (invalid, unexpected, or randomized) data to software under test and then analyses software response or monitoring for exceptions such as crashes, failing built-in code assertions, or memory leaks. Effective fuzzing software can generate semi-valid input data which can be accepted by the software parsing part and lead to some unexpected behavior. TLS-Attacker allows the execution of TLS communication with a required number of variable random modifications (mutations) or specially constructed invalid messages. As an example, during integers mutation TLS-Attacker can apply the following list of modifications—the original integer value can be XORed with random bits, shifted left or right, and increased or decreased by a random value. In addition, specific values can be returned based on a dictionary consisting of a zero value and values causing overflows in specific number representations. Similar strategies are employed by modification of further numeric data types. Byte arrays are modified by applying additional strategies. TLS-Attacker automatically generates modifications that duplicate arrays, remove or insert specific bytes, or shuffle the given byte array. The design of modifiable variables allows TLS-Attacker to make a chain of generated modifications.

To detect buffer boundary violations, integer overflows, or other memory corruptions, the runtime behavior of the TLS library has to be observed. For this purpose, the authors use AddressSanitizer (ASan). ASan is a memory error detector that can be enabled during compilation in recent versions of LLVM or GCC compilers. It

is typically used while fuzzing C and C++ applications. If a fuzzer finds a memory error in an application compiled with ASan, the application crashes, prints an error message, and exits with a non-zero code.

In the case of SMGW testing, this method does not work, since we do not have access to the TLS server source code or SMGW operating system. Hence, we should produce tests using the "black-box" testing method. For TLS applications, unlike C++ programming languages (like Java) and "black-box" testing cases, TLS-attacker produces a method to analyze the protocol flows with a TLS context analyzer. The TLS context analyzer checks whether a TLS protocol messages flow has been executed correctly contains an invalid protocol flow with an additional protocol message, or a message in a valid protocol flow is modified by a specific modification. In case of a runtime error or an invalid protocol flow, TLS-Attacker stores the protocol flow in an XML file format. This file can later be used for future analysis and TLS messages workflow repeating.

The TLS-attacker fuzzing process occurs in three phases. The starting point for each phase is a set of known TLS protocol flows that includes correct TLS protocol flows and several invalid TLS protocol flows (by default project has 19 workflows). At the beginning of the fuzzing process, TLS-Attacker attempts to execute these protocol flows and stores correctly executed, complete protocol flows for further executions in the next phases.

During the use of TLS-attacker software against Conexa SMGW we observe unusual behavior—SMGW stops responding even at standard TRuDI connection with correct credentials. Also, during the Zenmap scan at the first full cycle of the intense scan, all TCP ports finish normally. But after the second run of intense scans, the SMGW HAN TLS server stops responding. Even after 48 h, the TLS server not came back to working mode. Only device reboot helps to get SMGW back to normal condition.

Zenmap shows that the TLS server port is open and still working normally, but the port state changes to tcpwrapped.

List 5 CONEXA SMGW HAN zenmap analyze

```
Not shown: 999 filtered ports
PORT STATE SERVICE VERSION
443/tcp open tcpwrapped
```

TCP Wrapper is a client-side software solution for Linux/BSD machines that provides firewall features. It monitors all machine incoming packets and if an external node attempts to connect, the software checks if this node is authorized or not based on various criteria that are possible to specify. TCP Wrapper was originally written to protect TCP and UDP-accepting services, but it is also possible to use it to filter certain ICMP packets. When Nmap labels something tcpwrapped, it means that the behavior of the port is consistent with one that is protected by TCP Wrapper. Specifically, it means that a full TCP handshake was completed, but the remote

host closed the connection without receiving any data—flag 0x014 (RST, ACK) in Wireshark. It is important to note that TCP Wrapper protects programs (not ports). This means that a valid (not false-positive) tcpwrapped response indicates a real network service is available, but the client is not on a server allowed list of hosts. When a very large number of ports are shown as tcpwrapped, it is unlikely that they represent real services, so the behavior probably means something else like a load balancer or firewall is intercepting the connection requests.

To find parameters that lead Conexa SMGW TLS server to TCP-wrapped condition was created a python script that allows sending TRuDI-like ClientHello TLS messages with some delay pattern. This test shows that for the Conexa SMGW HAN TLS server matters only a number of requests (about 25) and the delay between these requests is not mattered (tested even with 20 min delay). Also, if TLS workflow includes a full TLS connection messages cycle, which means:

1. ClientHello
2. ServerHello, ServerCertificate
3. ServerKeyExchange, ClientCertificateRequest, ServerHelloDone
4. ClientCertificate (empty, contain only Handshake Type: Certificate and Length fields)
5. ClientKey Exchange
6. ClientChange Cipher Spec
7. ClientEncrypted Handshake Message
8. ServerChangeCipherSpec, ServerEncryptedHandshakeMessage.

In this case, the Conexa SMGW HAN TLS server does not stop responding even after 600 full TLS connection messages cycles with 5 s delay. Based on the described information we could conclude that the Conexa SMGW HAN TLS server has additional protection, which is activated on the following conditions:

- If the ClientHello TLS message contains some parameters that do not fit the TLS server settings. The TLS server will not even send a ServerHello message as a response to the ClientHello message.
- Even if the ClientHello parameters are correct, when the TLS connection workflow is not full, the SMGW TLS server will be blocked after 25 incorrect connection attempts.
- Mixing connections with correct and incorrect parameters are not helping. If the counter of incorrect connection reaches 25, the SMGW HAN TLS server will be blocked.
- Changing of Client IP/MAC address did not help to bypass TCPwrapped protection. To check this, an attempt to connect to the SMGW via TRuDI from another machine (with different IP and mac address) in the same local network was done. But theoretically, TCPwrapper software should accept data from an unblocked IP address.

This additional protection was a problem for testing software such as fuzzer in the case of Conexa SMGW because making reboots in the required time gap is not a common task. In the case of PPC SMGW, it also has a similar protection, but SMGW

is back to normal condition without a reboot after some timeout (about 300 s), which allows us to simply increase all timeout settings in testing software to use it. TLS-attacker fuzzer does not allow us to find some vulnerabilities in the case of PPC SMGW, and because of the reboot requirement, we were not able to use it correctly against Conexa SMGW.

Another TLS server testing software that was used is TLSfuzzer. TLSfuzzer is not a fuzzing software in common sense—because it is a python library for convenient interaction with TLS protocol messages, which repository includes a list of tlsfuzzer lib-based testing scripts (at current moment 145). Some of these testing scripts such as test-record-size-limit test or test-cve-2016-2107, and 5 scripts for fuzzing TLS plaintext, MAC, padding, ciphertext, and finished messages. The main disadvantage of tlsfuzzer fuzzing scripts—is that scripts have a finite (and comparatively small) set of tests. For example, the padding fuzzing script produces only 11 tests. Ciphertext fuzzing script only 40 tests. But because of a large number of testing scripts for TLS and clear source codes makes this tool useful for the project. In the case of tlsfuzzer testing—all tlsfuzzer tests were successfully passed or show indefinite conditions for both SMGWs.

Because of the SMGW's TCPwrapper protection problem for Conexa SMGW and the small number of reference workflows in the TLS-fuzzer software, it was decided to make our own SMGW fuzzing software based on TLS Response-Guided Differential Fuzzing approach which was presented in the paper "Maximizing and Leveraging Behavioral Discrepancies in TLS Implementations using Response-Guided Differential Fuzzing" (Walz and Sikora 2018) from Andreas Walz and Axel Sikora.

Differential fuzzing is a technique used to find vulnerabilities in software by sending inputs to multiple implementations of the same software and comparing the responses. The assumption behind differential fuzzing is that if two different implementations of the same software behave differently when given the same input, there may be a vulnerability in one of the implementations. This technique can be particularly useful for testing implementations of protocols like TLS, where it can be difficult to determine whether an implementation is correct or not. To use differential fuzzing, it is important to first set up the environment with multiple implementations of the software which will be tested. You can then use a fuzzing tool to generate a large number of random inputs and send them to each of the implementations. Next possible to compare the responses from each implementation. If some of the response is not the same, probability of vulnerability in the place of TLS implementation which was activated by this request is much higher.

It is important to note that differential fuzzing is not a foolproof method and should be used in conjunction with other testing techniques to ensure the most thorough testing possible. However, as shown on paper, this approach allows us to get better testing and TLS server source code "covering" compared to TLS-attacker or NEZHA (Walz and Sikora 2020). Also, for Conexa SMGW we added electricity smart plug software control support for our fuzzing software which allowed us to automatize fuzzing process.

To determine if anything goes wrong during fuzzing without access to the device shell, we have checked the following list of cases:

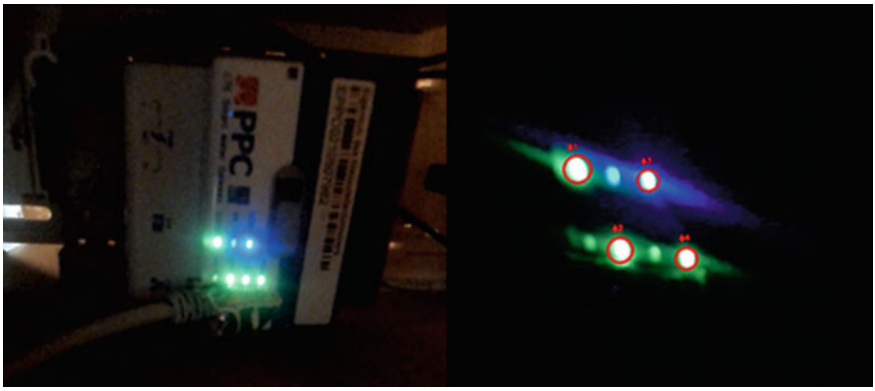


Fig. 9 Watch-dog software example

1. The device Web server does not respond.
2. The device TLS server acts differently in comparison with other TLS servers.
3. The device TLS server does not respond.
4. The device does not respond on the TCP layer.
5. Physical—the interface is down/non-standard LEDs blinking.

Devices LEDs blinking are described in the user manual. We use python OpenCV script to automatize led blinking analysis (Fig. 9). It takes a picture of the device as its input and applies few filters. It then analyses the resulting image (by knowing the comparative LED's position), and returns a list where every element describes the current LED state. But even after that we still don't have a full understanding of what is going on inside the device because we have no shell, and the testing speed was comparatively low, as the tested devices were not so powerful.

As a result of testing, using our fuzzing software against SMGW at the current stage—we were able to observe different behavior of SMGW's HAN TLS servers compared with reference TLS implementations but did not find a way to use it to make some harm.

Another possible direction of TLS server testing is using some TLS certificate vulnerabilities such as CVE-2019-3829 which allows making memory corruption (double free) during the certificate verification (NVD—CVE-2019-3829). Any client or server application that verifies X.509 certificates with GnuTLS 3.5.8 or later should be affected. There are even a number of publicly available exploits for such vulnerabilities (as an example, https://www.exploit-db.com/exploits/46626) but without the knowledge of TLS server version and implementation, this testing is problematic due to a big number of variations.

Because of that, our next work was focused on developing a TLS server fingerprinting software which is based on the same "Response-Guided Differential Fuzzing" approach. This software requires SMGW's TLS implementation and version. Knowing TLS server implementation and version will allow to run tests on a local PC, which is important to increase testing speed and allows to use of

address sanitizer for software memory analysis. Unfortunately, during work on this software, we faced several problems that would require more than the expected time to get resolved. Hence, our TLS fingerprinting approach will be described more precisely later in a different paper.

Other Testing Directions

Another possible way to influence Conexa SMGW is to use open the Socks5 port, which is required to implement HKS3—A transparent communication channel initiated by CLS. In the case of the HKS3, the connection must be established using SOCKSv5 [RFC1928] and "TLS for SOCKSv5" [DRAFT-IETF-AFT-SOCKS-SSL-00], which requires establishing of TLS connection before creating SOCKS5 proxy channel. Different Socks5 server authentication methods were tested—and it was observed that Conexa SMGW Socks5 accepts only authentication method 0x86 described in the draft RFC Secure Sockets Layer for SOCKS Version 5. Multiple connection attempts to the Socks5 server do not lead to Conexa SMGW denial of service (which was tested using a python script).

Because of the small number of running on the device services probably the most potentially effective SMGW testing direction is TCP-layer attacks. In most Linux-based systems, the TCP/IP stack is integrated into the kernel, which means that even if some tested port is in a close state or it is implementing a "Wake-Up" service (because, by our knowledge, it is implemented as a listening port on some host system as it shown on page 15 in Detken et al. 2016), it could be vulnerable to TCP-layer attacks. One more advantage is that if the HAN interface is vulnerable to a TCP-layer attack, it is highly probable that LMN and WAN will also be vulnerable to this attack (because of TCP stack kernel integration).

An example of a TCP-Layer attack is the CVE-2019-11815—Remote code execution in Linux kernel TCP/IP implementation. The vulnerability exists due to a race condition that leads to a use-after-free error when TCP packets in rds_tcp_kill_sock() function in net/rds/tcp.c. A remote unauthenticated attacker can specially craft TCP packets to the affected system, trigger a use-after-free error, and execute arbitrary code on the target system. Successful exploitation of the vulnerability may allow an attacker to compromise a vulnerable system (https://www.cybersecurity-help.cz/vdb/SB2019051302). By the data from source (NVD—CVE-2019-11815) vulnerable should be all Linux systems with kernel version lower than 5.0.8, which is true for tested SMGWs by the zenmap data (which can be wrong).

Another example of TCP-layer attacks is Remote DoS in TCP/IP implementation in Linux kernel (https://www.cybersecurity-help.cz/vdb/SB2019061702) (CVE-2019-11477, CVE-2019-11478, and CVE-2019-11479). In the TCP protocol, each segment has a sequence number that indicates the position of the data contained in the packet within the overall stream of data being transmitted. When two systems establish a TCP connection, they exchange initial sequence numbers (ISNs) and use them to initialize a sequence number counter. The sequence number of each subsequent packet is then determined by adding the length of the data in the packet to the previous sequence number. If an attacker sends packets with sequence numbers that are out of order, it can cause problems for the recipient. For example, if an attacker

sends segments 3, 4, and 5 before segment 2, the recipient will not be able to properly reassemble the data stream.

To help mitigate this problem, the TCP protocol includes a feature called Selective Acknowledgment (SACK). When SACK is enabled, the recipient of a TCP connection can send a special type of acknowledgment (ACK) packet that includes a list of the sequence numbers of the packets it has received. This allows the sender to identify which packets have been received and which ones have been lost or are out of order, and to retransmit the missing packets as needed.

If an attacker sends segments 3, 4, and 5 before sending segment 2, and SACK is enabled on the recipients end, the recipient will buffer segments 3, 4, and 5 and send duplicate ACKs for them when they arrive. However, it will not be able to fully reassemble the data stream until it receives segment 2, so it may lead to a buffer overflow.

There are no publicly available exploits to test these CVEs, but from the point of view of security, it is good. In the public access, only one exploit for CVE-2019-11477 was found (GitHub—sasqwatch/cve-2019-11477-poc), and even that was not working properly on the local system (with the required exploit parameters).

7 Recommendations

The BSI SMGW has a great protection level because even in case of a small number of points of entrance and great elaboration (which is shown by the "Wake-Up" service), it has additional security mechanisms such as "TCP Wrapper" which makes penetration testing even more difficult. Both SMGW devices have minimalistic web servers. Forms/APIs which allow user input was protected (escaped) against tested injections. PPC SMGW SSH server is vulnerable to the information-disclosure vulnerability, but to our knowledge, this SSH service is preserved only in testing SMGW firmware. As we can see testing of such devices requires not an "in-wide" approach as in the common penetration testing but an "in-depth" approach, because the number of possibilities to test are low. Such tasks require much more effort and knowledge from the tester.

Based on materials from this chapter it is possible to give some recommendations because even taking into account all the reviewed systems and their differences, the most likely successful attack vectors are the same:

- A good practice is to apply security control at all stages of the development—design, implementation, product decommissioning, and maintenance.
- Always make security updates/patching in time. Currently, there is no information about any vulnerabilities in the reviewed systems parts. But this does not mean that they will not appear in the future. For example, the source (Marcellin 2018) mentioned that Enedis hubs use the Java programming language. The author pointed out that Java has suffered for years from chronic vulnerabilities, which Java publisher Oracle—patches month after month. In December 2021 has been

discovered a serious vulnerability in a very widespread Java library for logging service Log4J (CVE-2021-44228), which theoretically can exist in some Enedis software.

- Make hardware upgrades in time. Theoretically old Linky meters can be vulnerable because in document PLC profile specifications (ERDF-CPT-Linky-SPEC-FONC-CPL) from the year 2009 (but it is the newest founded version) refers to Green Book Cosem DLMS UA 1000-2:2008 edition 7, which does not contain such important DLMS/COSEM features as asymmetric cryptography that allow producing digital signatures and a secure key establishment and management.
- It is a good practice to use common protocols such as TLS or DLMS/COSEM and the most well-known implementations of these protocols to secure a system. Because these implementations have been tested many times and are guaranteed to provide a high security level if they are used with the correct settings. TLS and DLMS/COSEM protocols offer approximately same level of security in smart metering solutions. Both use PKI, modern security primitives, and cipher suites. DLMS/COSEM is comparatively more lightweight. The advantage of TLS is that this protocol is more widely researched for potential vulnerabilities because it is more widespread (for example, in banking and shopping business areas where secure Internet connections are very important).
- Users should be entrusted to solve as few security related issues as possible. A professional trained certified operators such as SMGW administrators in the BSI SMGW system are less likely to make some wrong settings which could lead to vulnerability. In conjunction with wide logging and system analysis, suspicious activity can be quickly identified. It is also easier to pinpoint who acted, when, which actions were performed, and the results of this activity.
- It is important to supervise employees legitimate access to systems. To protect against the malicious activity of authorized employees, it is necessary to implement strong auditing, reporting processes and capabilities that can capture user activity.
- Organize staff cyber security/social engineering training more frequently. In most cases, hackers intrude inside a secure system using attacks involving a human factor (Positive technologies 2018), like in the case of the Ukrainian power station in December 2015, where hackers used email with spear-phishing Microsoft office document (CVE-2014-4114) containing malicious macros to turn off power substations (Macola 2020).
- Check HES/SMGW admin/EMP networks perimeter or use a special intrusion detection system periodically. This is potentially the most interesting part for hackers because they have the highest probability of making profit in the case of a successful hack. They also have potentially more system entry points here.
- Tamper resistance is very important to protect the system from an internal attacker. The mechanisms such as encrypted communication, signed and verified firmware, disabled debug communications interface (such as JTAG), encrypted flash memory, configurable locked optical ports, meter tamper detection, backhaul protection, and other physical and system-level security features should be used.

- Devices should have as few services/interfaces as possible because it will decrease the number of possible entry points. If devices need to use a web server, it is important to try to reduce the number of forms/APIs that allow user input into the system. Those forms/APIs that will be present on the web server must be carefully escaped (most important on the server side) in order to eliminate the possibility to perform SQL/XSS injection. In the case of SMGW penetration testing, these were the main factors that made testing difficult.
- Decrease information about names and versions of services running on the device. As in the case of SMGW penetration testing—getting information about services allows a hacker to switch from a "black-box" type of testing to testing a service on the local machine—which significantly speeds up the testing process and the probability of vulnerability finding.
- If a device like in the case with SMGW HAN is able to connect to the home internet router—check the home internet router security (firewall should be enabled, and all accessible from WAN services should be sufficiently protected).

References

Agence nationale de la sécurité des systèmes d'information. A word from the Director-General. https://www.ssi.gouv.fr/en/mission/word-from-director-general/. Accessed 5 Dec 2022

Agence nationale de la sécurité des systèmes d'information Certification CSPN. https://www.ssi.gouv.fr/administration/produits-certifies/cspn/. Accessed 5 Dec 2022

ANSSI (2014) Detailed measures cybersecurity for industrial control systems

Bartock M, Cichonski J, Franklin J. LTE security—how good is it?

Batra N, Kelly J, Parson O, Dutta H, Knottenbelt W, Rogers A, Singh A, Srivastava M (2014) NILMTK: an open source toolkit for non-intrusive load monitoring. In: E-energy 2014—proceedings of the 5th ACM international conference on future energy systems. Association for Computing Machinery, pp 265–276

BSI (2017) BSI TR-03109-4—Smart Metering PKI—Public Key Infrastruktur für Smart Meter Gateways

BSI Smart Meter Gateway. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Smart-metering/Smart-Meter-Gateway/smart-meter-gateway_node.html. Accessed 6 Dec 2022

BSI Smart Meter: Stellungnahme des BSI zum Eilbeschluss des Oberverwaltungsgerichts Münster. https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/Stellungnahme-OVG-Muenster-Smart-Meter_080321.html. Accessed 6 Dec 2022

BSI Smart Metering Systems. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Smart-metering/smart-metering_node.html. Accessed 6 Dec 2022

Carracedo G (2019) Smart meters in Spain—telemanagement system | Tarlogic. https://www.tarlogic.com/blog/smart-meters-spanish-scenario-telemanagement/. Accessed 4 Dec 2022

CEN/CLC/ETSI/TR 50572 (2011) Functional reference architecture for communications in smart metering systems

Chauvenet C (2016) G3-PLC, the standard of the LINKY roll-out and beyond

CNIL (2014) Pack de conformité sur les compteurs communicant

Compteur Linky Obligatoire : comment refuser la pose et date limite. https://www.fournisseurs-electricite.com/guides/compteur/linky/refuser. Accessed 5 Dec 2022

CRE (2014) Délibération de la Commission de régulation de l'énergie du 12 juin 2014 portant recommandations sur le développement des réseaux électriques intelligents en basse tension
CRE (2016) Délibération de la Commission de régulation de l'énergie du 3 mars 2016 portant décision sur la tarification des prestations annexes réalisées à titre exclusif par les gestionnaires de réseaux de distribution d'électricité
Detken K-O, Jahnke M, Humann M (2016) Integritätsmessung von Smart Meter Gateways
DLMS/COSEM protocol security evaluation. https://research.tue.nl/en/studentTheses/dlms-cosem-protocol-security-evaluation. Accessed 5 Dec 2022
Dworkin M (2007) Recommendation for block cipher modes of operation: Galois/Counter Mode (GCM) and GMAC. https://doi.org/10.6028/NIST.SP.800-38d
EDRF (2009) Linky PLC profile functional specifications—ERDF-CPT-Linky-SPEC-FONC-CPL
enedis API—Enedis Open Data. https://data.enedis.fr/api/v2/console. Accessed 5 Dec 2022
Enedis Documentation de référence. https://www.enedis.fr/documents?term_node_tid_depth%5B106%5D=106. Accessed 5 Dec 2022
enedis.fr Enedis company profile. https://www.enedis.fr/qui-sommes-nous. Accessed 5 Dec 2022
enedis.fr Notice d'utilisation du compteur communicant Linky
EUR-Lex (2012) 2012/148/EU: Commission Recommendation of 9 March 2012 on preparations for the roll-out of smart metering systems—EN. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32012H0148&qid=1650551228719. Accessed 5 Dec 2022
European Commission DG Energy (2019) European smart metering benchmark
French National Assembly and the Senate (1978) ACT 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties
Genest O, Maury V, Huc Y. Technical overview of G3-PLC. Trialog. https://www.trialog.com/en/technical-overview-of-g3-plc/. Accessed 5 Dec 2022
GitHub—sasqwatch/cve-2019-11477-poc. https://github.com/sasqwatch/cve-2019-11477-poc. Accessed 8 Dec 2022
gnutls 3.6.6—"verify_crt()" Use-After-Free—Linux dos Exploit. https://www.exploit-db.com/exploits/46626. Accessed 8 Dec 2022
GRDF.FR GRDF: France's leading natural gas distribution operator. https://www.grdf.fr/english/leading-natural-gas-distribution-operator. Accessed 5 Dec 2022
GRDF.FR Le compteur communicant gaz par GRDF. https://www.grdf.fr/institutionnel/actualite/dossiers/compteur-communicant-gazpar. Accessed 5 Dec 2022
Greveler U, Rhein-Waal H, Glösekötter P, Justus B, Loehr D (2012) Multimedia content identification through smart meter power usage profiles
Gurux for DLMS smart meters. https://www.gurux.fi/front-page. Accessed 5 Dec 2022
Higgins KJ (2014) Smart meter hack shuts off the lights. https://www.darkreading.com/perimeter/smart-meter-hack-shuts-off-the-lights. Accessed 4 Dec 2022
Hoffmann SG, Massink R, Bumiller G (2016) New security features in DLMS/COSEM—a comparison to the smart meter gateway. In: Proceedings of the 2015 IEEE innovative smart grid technologies—Asia, ISGT ASIA 2015. https://doi.org/10.1109/ISGT-ASIA.2015.7387098
i-cube software DLMS security basics. https://icube.ch/Security/security1.html. Accessed 5 Dec 2022
Jöbstl W (2019) Innovations beyond smart metering
Landis+Gyr (2014) Gridstream solution security overview—white paper
Landis+Gyr (2020) Gridstream solution Landis+Gyr HES product description
Landis+Gyr Landis+Gyr DC450. https://www.landisgyr.de/product/landisgyr-concentrateur-dc450-2/. Accessed 5 Dec 2022
Landis+Gyr METAS certificate. https://www.cclab.com/news/landis-gyr-metas-certificate. Accessed 20 Dec 2022
Landis+Gyr White Paper. IDIS interoperability—securing long-term investments with interoperable solutions
Landis+Gyr White Paper. IDIS (Interoperable Device Interface Specification)

Légifrance (2001) Décret n°2001-630 du 16 juillet 2001 relatif à la confidentialité des informations détenues par les gestionnaires de réseaux publics de transport ou de distribution d'électricité, pris pour l'application des articles 16 et 20 de la loi n° 2000-108 du 10 février 2000 relative à la modernisation et au développement du service public de l'électricité
Légifrance (2002) Décret n°2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information
Légifrance (2004) Décret n°2004-183 du 18 février 2004 relatif à la confidentialité des informations détenues par les opérateurs exploitant des ouvrages de transport, de distribution ou de stockage de gaz naturel ou des installations de gaz naturel liquéfié
Légifrance (2005) Loi n° 2005-781 du 13 juillet 2005 de programme fixant les orientations de la politique énergétique
Légifrance (2009) Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information »
Légifrance (2011) Décret n° 2011-170 du 11 février 2011 modifiant le décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information »
Légifrance (2012a) Arrêté du 4 janvier 2012 pris en application de l'article 4 du décret n° 2010-1022 du 31 août 2010 relatif aux dispositifs de comptage sur les réseaux publics d'électricité
Légifrance (2012b) Délibération 2012-404 du 15 novembre 2012
Légifrance Code de l'énergie
Lüring N, Szameitat D, Hoffmann S, Bumiller G (2018) Analysis of security features in DLMS/COSEM: vulnerabilities and countermeasures. In: 2018 IEEE power and energy society innovative smart grid technologies conference, ISGT 2018, pp 1–5. https://doi.org/10.1109/ISGT.2018.8403340
Macola IG (2020) The five worst cyberattacks against the power industry since 2014. https://www.power-technology.com/analysis/the-five-worst-cyberattacks-against-the-power-industry-since2014. Accessed 5 Dec 2022
Marcellin D (2018) Cybersécurité : Linky, un système IIoT atypique | Alliancy. https://www.alliancy.fr/cybersecurite-linky-un-systeme-iiot-atypique. Accessed 6 Dec 2022
Matoušek P (2017) Analysis of DLMS protocol. Technical Report no. FIT-TR-2017-13
Bundesnetzagentur Messstellenbetriebsgesetz (MsbG). https://www.bundesnetzagentur.de/DE/Beschlusskammern/BK08/BK8_09_MsbG/BK8_MsbG_Basepage.html. Accessed 6 Dec 2022
METAS Datensicherheitsprüfungen durch METAS-Cert. https://www.metas.ch/ds. Accessed 7 Dec 2022
Ministère de l'Écologie (2017) Le déploiement du compteur Linky
Ministère de l'Écologie DDDEDL (2014) Décision du 23 septembre 2014 relative à la généralisation du projet de compteurs communicants en gaz naturel
Molina-Markham A, Shenoy P, Fu K, Cecchet E, Irwin D (2010) Private memoirs of a smart meter. In: BuildSys'10—proceedings of the 2nd ACM workshop on embedded sensing systems for energy-efficiency in buildings, pp 61–66
Murrill BJ, Liu EC, Thompson RM (2012) CRS report for congress smart meter data: privacy and cybersecurity
Nguyen PB. Protection des données et compteur intelligent
NVD-CVE-2019-11815. https://nvd.nist.gov/vuln/detail/CVE-2019-11815. Accessed 8 Dec 2022
Port Scanning Basics | Nmap Network Scanning. https://nmap.org/book/man-port-scanning-basics.html. Accessed 8 Dec 2022
Positive technologies (2018) Positive research 2018. J Inf Secur
PPC Power Plus Communications firmware. https://gwafirmware.ppc-ag.de/. Accessed 8 Dec 2022
Remote code execution in Linux kernel TCP/IP implementation. https://www.cybersecurity-help.cz/vdb/SB2019051302. Accessed 8 Dec 2022
Remote DoS in TCP/IP implementation in Linux kernel. https://www.cybersecurity-help.cz/vdb/SB2019061702. Accessed 8 Dec 2022
RS485 sniffer. http://jheyman.github.io/blog/pages/RS485Sniffer/. Accessed 8 Dec 2022

Rullaud L, Gruber C (2020) Distribution grids in Europe
Siconia® SMARTY IQ-LTE | Sagemcom. https://www.sagemcom.com/V02/de/smart-city/dr-neuhaus/smart-metering/siconiatm-smarty-iq-lte/. Accessed 5 Dec 2022
Sánchez Jiménez M (2011) M/490 EN. Standardization mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployment
Schweizerische Bundesrat (2008) SR 734.71—Stromversorgungsverordnung (StromVV). Schweizerische Bundesrat
SEP eMobility Team Der Smart Energy Identifier. https://stg-tud.github.io/sep/projects/2017/eMobilityTeam/site/#technologies. Accessed 8 Dec 2022
ShareTechnote 4G/LTE—NAS. https://www.sharetechnote.com/html/Handbook_LTE_EEA.html. Accessed 8 Dec 2022
SMARTER TOGETHER (2019) Report on deployment of Linky smart power meters in the area
BSI Standardisierungsstrategie zur sektorübergreifenden Digitalisierung nach dem Gesetz zur Digitalisierung der Energiewende Roadmap für die Weiterentwicklung der technischen BSI-Standards in Form von Schutzprofilen und Technischen Richtlinien
swissmig (2019) Prüfmethodologie zur Durchführung der Datensicherheitsprüfung für Smart Metering Komponenten in der Schweiz
UFC-Que Choisir (2017) Compteur Linky—Le vrai du faux. https://www.quechoisir.org/action-ufc-que-choisir-compteur-linky-le-vrai-du-faux-n11627/. Accessed 5 Dec 2022
UVEK (2014) Grundlagen der Ausgestaltung einer Einführung intelligenter Messsysteme beim Endverbraucher in der Schweiz Technische Mindestanforderungen und Einführungsmodalitäten
UVEK (2015) Smart Grid Roadmap Schweiz Wege in die Zukunft der Schweizer Elektrizitätsnetze
VSE (2018) Richtlinien für die Datensicherheit von intelligenten Messsystemen
VSE (2019) Intelligente Messsysteme Der Einsatz von intelligenten Messsystemen in der Schweiz
Walz A, Sikora A (2018) Maximizing and leveraging behavioral discrepancies in TLS implementations using response-guided differential fuzzing. In: Proceedings—international Carnahan conference on security technology, Oct 2018. https://doi.org/10.1109/CCST.2018.8585565
Walz A, Sikora A (2020) Exploiting dissent: towards fuzzing-based differential black-box testing of TLS implementations. IEEE Trans Depend Secure Comput 17:278–291. https://doi.org/10.1109/TDSC.2017.2763947
NVD—CVE-2019-3829. https://nvd.nist.gov/vuln/detail/CVE-2019-3829. Accessed 8 Dec 2022