Open and Secure: Amending the Security of the BSI Smart Metering Infrastructure to Smart Home Applications via the Smart Meter Gateway

Christian Freudenmann, Dominik Henneke, Christian Kudera, Markus Kammerstetter, Lukasz Wisniewski, Christoph Raquet, Wolfgang Kastner, Jürgen Jasperneite

Open and Secure: Amending the Security of the BSI Smart Metering Infrastructure to Smart Home Applications via the Smart Meter Gateway

Christian Freudenmann[1], Dominik Henneke[2], Christian Kudera[3], Markus Kammerstetter[3], Lukasz Wisniewski[2], Christoph Raquet[1], Wolfgang Kastner[3], Jürgen Jasperneite[2]

[1]Power Plus Communications AG (PPC), Mannheim, Germany
{c.freudenmann, c.raquet}@ppc-ag.de
[2]inIT – Institute Industrial IT, OWL University of Applied Sciences, Lemgo, Germany
{dominik.henneke, lukasz.wisniewski, juergen.jasperneite}@hs-owl.de
[3]Secure Systems Lab, Automation Systems Group, Vienna University of Technology, Vienna, Austria
{ckudera, mk}@seclab.tuwien.ac.at, k@auto.tuwien.ac.at

Abstract. This paper describes an implementation to enable interaction between smart home solutions and Smart Meter Gateways (SMGWs). This is conducted in the example of the approach of the AnyPLACE project to interconnect openHAB with the HAN interface of the SMGW. Furthermore, security issues in the combination of those two realms are addressed, answered and tested so that in addition to the open character of the solution, it is still secure.

1 Smart Home and Smart Metering in Europe

1.1 Challenges for interconnecting Smart Home and Smart Metering

In a time of highly volatile electricity generation, the need for a dynamic energy system and thus Smart Grids is expected [1]. Potentially, also end users with significant load or distributed energy resources can participate in the smart energy distribution by using home energy management systems or smart metering concepts which involve interactions with external market entities. One of two main challenges for interconnecting those components is the demand to support a wide range of different technologies and solutions in the background of proprietary smart home solutions. A second major challenge is the handling of private meter data according to EU requirements on smart metering as well as country specific regulations derived from them. Due to EU requirements being rather high-level, the communication and security requirements differ in each EU member country.

adfa, p. 1, 2011.

1.2 Approach for an interoperable solution

The European research project AnyPLACE is developing a smart metering platform with management and control functionalities. The aim is to create a solution which interconnects in-home appliances, smart meters and also external services, and which can be applied in any European country – in "any place". For making the solution highly interoperable, AnyPLACE is designed to have a common basis as well as adaptable elements. The generic part comprises e.g. a graphical user interface and energy management algorithms. The adaptable elements are realized in the following approach to connect the AnyPLACE core functionalities with other devices and systems.

An existing open-source smart home framework openHAB [2] has been chosen to interconnect a broad variety of different technologies, systems and products. One of its core features is the possibility to amend it with new functionalities e.g. adding the support of new protocols to add new kinds of devices. This can be done by adding optional packages, which can be selected from a wide range of already existing add-ons developed for different smart home appliances and systems. In the AnyPLACE project, additional country specific packages have been designed to connect meters to the smart home system, taking into account respective technological, privacy as well as security requirements which were analyzed for each addressed country. Further details about the requirements which were identified for the different European countries are described in [3].

The present paper focuses on the application environment and thus requirements of the German market and the derived solutions. At first, the regulations for the German smart metering infrastructure as well as possible resulting functionalities are sketched. Afterwards, the implementation of solutions to enable an interaction between this infrastructure and smart home systems is described in details. Finally, the paper gives insights of how those solutions for an interaction between the German smart metering infrastructure and smart home solutions shall be tested regarding security considerations.

2 German Smart Metering Infrastructure Functionalities

2.1 BSI Smart Metering Infrastructure offers platform for connection of subsystems

In Germany, the smart meter rollout has recently been initialized by law and will start in 2017. The Federal Office for Information Security (BSI) prescribes the security architecture for a secure and transparent handling of the end users' private meter data [4], [5], [6]. The Smart Meter Gateway (SMGW) is a core element in this architecture as it is depicted in Figure 1.

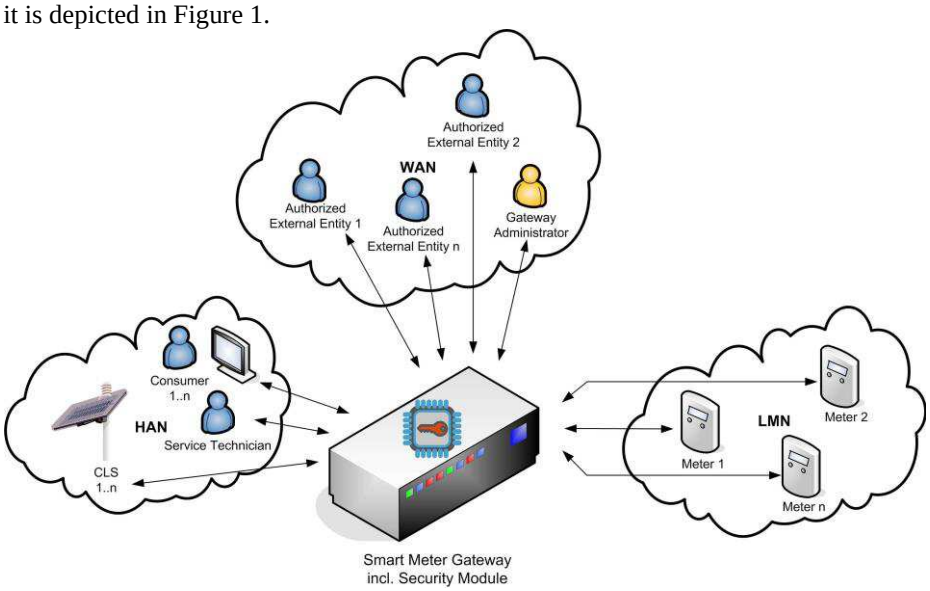

Fig. 1. BSI Smart Metering Infrastructure [6].

Its name suggests that the only purpose of the "Smart Meter Gateway" is to serve as a gateway to transfer meter data from smart meters to the respective energy supplier. But it is not limited to this functionality. It does provide secure communications to meters in the Local Metrological Network (LMN), but also to external service providers (EMT) in the Wide Area Network (WAN) as well as to the Home Area Network (HAN). Due to the communication with those networks, the SMGW serves as a platform to interconnect sub-systems that enable several additional functionalities.

In the LMN it is possible to securely connect several meters to one SMGW. This is not restricted to electricity meters but is also valid for gas, water and heat meters. Further, meters of different households of the same building can be connected to one single SMGW. At the HAN interface of an SMGW, the historic and current meter data are made available specifically to the end user which the respective meters belong to. With the connection to the WAN, an end user can access external services by authorizing specific EMT to access specific meter data. The end user or company can also potentially participate in demand side management and virtual power plants. This

can be done since it is possible to connect controllable local systems (CLS) to the HAN interface and remotely switch them over the secured network by authorized EMT connected to the WAN.

2.2 Functionalities of the HAN interface

In [4] the HAN interface is specified to be divided into three logical interfaces and respective use-cases:

- End user interface (IF_GW_CON)
- Service technician interface (IF_GW_SRV)
- CLS interface (IF_GW_CLS)

The end user interface is a "read-only" access. After authentication via certificate or username and password, the recent and historic meter values as well as tariff levels can be accessed. There are different tariff schemes that are used to store meter data and some of them have load or time variable elements. For those, the end user interface shows the currently active tariff levels, which can be used as information to potentially adapt the house-holds' or industries' prosumption (consumption and production) behavior accordingly. The meter data can be used by the end user to control his or her consumption or energy production results and raise awareness of energy efficiency or alignment of consumption peaks and local energy production. Potentially, this information can also be automatically gathered, used and assessed by local smart home systems. This aspect is described in the following chapter.

The service technician interface can only be accessed by service technicians and provides logs and status information of a SMGW. However, this aspect is not the scope of this paper, since it does not provide functionalities which end users could use in smart home applications.

According to the law [7], the system for measuring, transferring and controlling metering data as well as the secure connection of generation and consumption equipment, must fulfil the requirements specified in the respective protection profiles and technical guidelines. This also involves the SMGW to securely interconnect manageable devices connected to the CLS interface with authorized EMTs. This is done by establishing TLS encrypted connections between the SMGW and CLS devices or EMTs respectively, which are proxied over the SMGW. A single SMGW is designed to connect to several CLS devices. The Gateway Administrator (GWA) configures proxy profiles in the SMGW to define the possible communications between certain CLS devices and EMTs.

The proxy functionality works as a transparent connection that can be used independently of the applied protocols on top of the secure tunnel. In this way, the interface is not restricted to use-cases which are directly associated with energy systems such as switching photovoltaic units or combined heat and power plants, but it can theoretically also be used for any use-case demanding a secured connection between the HAN and the backend. In this sense, examples involving secure banking and sensitive health care data are as relevant as e.g. burglar alarm systems or smart home solutions.

3 Using the BSI concept for Smart Home Applications

3.1 Connecting Smart Home Applications to the HAN interfaces

Among the potential use-cases, also home energy management functionalities of smart home systems can benefit from the connection to an SMGW. They can use the HAN interface to access the readings of all meters that belong to a household and thus derive near real-time information about the energy consumption of a household or building, without the need of installing dedicated sub-meters. Information about the available tariff schemes can be used as an input for energy optimization algorithms that change automated device schedules or derive guidelines that assist users to manually optimize their consumption.

The CLS interface brings further potential to a smart home system. It can be used to access services via the proxy connection, allow external entities to change parameters in the system or make devices available to be controlled by third-parties that originally don't support a CLS communication. The open nature of the connection allows to use it for a wide range of different smart home applications, like mobile access to the smart home system from the users' smartphone or the interconnection with services such as IFTTT ("If This Then That") [8]. Figure 2 summarizes the usage of a smart home system in the BSI framework.

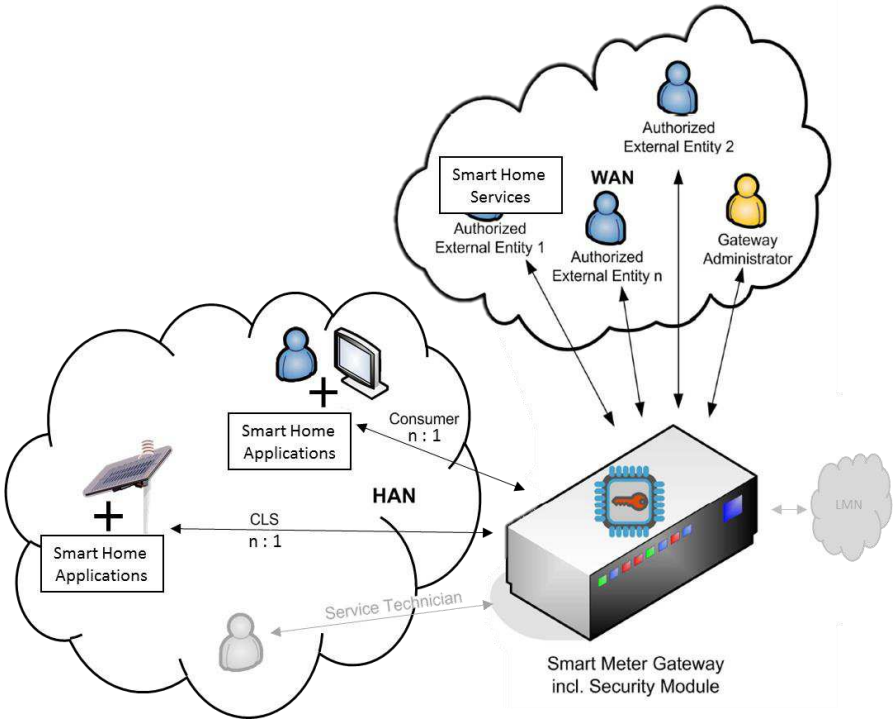

Fig. 2. Integrating Smart Home to the BSI Infrastructure - Adapted from BSI-CC-PP-0077-V2-2015 [6].

In the AnyPLACE approach, both described HAN interfaces are used for the purpose of energy management functionalities of a smart home system. Therefore, a respective system has been enabled to interact with the CLS as well as the end user interface. The approach is described in the following chapter. The implementation in the AnyPLACE project has been realized with the openHAB framework [2] but this concept is also applicable to other smart home systems.

3.2 Implementation HAN end user interface in Smart Home Systems

Regarding the end user interface, the SMGW can be modeled as a gateway that abstracts the access to a number of different meters. A smart home system can connect to the HAN interface to receive meter readings in specified intervals (e.g. 15 minutes; specified by the configuration profiles).

As implementation example, the home automation software openHAB has been extended to support the connection to an SMGW. It uses an information model that abstracts all connected devices as so called things. Each thing is configured by parameters and provides channels that represent information from the devices. Since the gateway concept is also common in many smart home protocols (such as communication bridges to wireless network technologies), the information model can also represent bridges that are used as gateways for the things.

In this context, the SMGW can be implemented as bridge, while all meters are things. Different thing-types for the different meter-types (electricity, heat, water or gas) provide different channels and can be semantically enriched with predefined channel categories. This enables openHAB to read information from the meters as it would from any other connected device. Auto-configuration can also be implemented to automatically create all meters that a user has access to via the SMGW as things. Figure 3 shows the implemented things including the SMGW and meters connected to the SMGW (in this example one electric meter). Figure 4 shows channels of the SMGW and the attached electric meter, which have been realized in the binding.

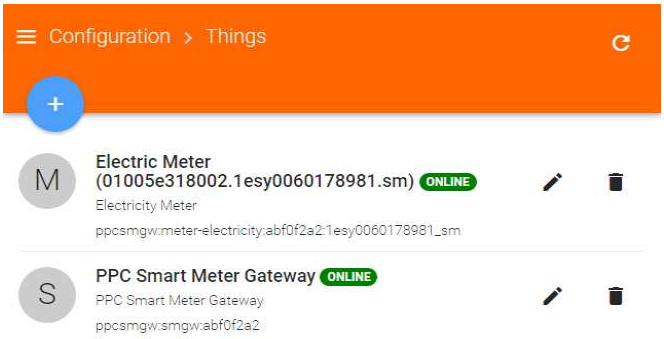

Fig. 3. The SMGW and an electric meter as things in openHAB.

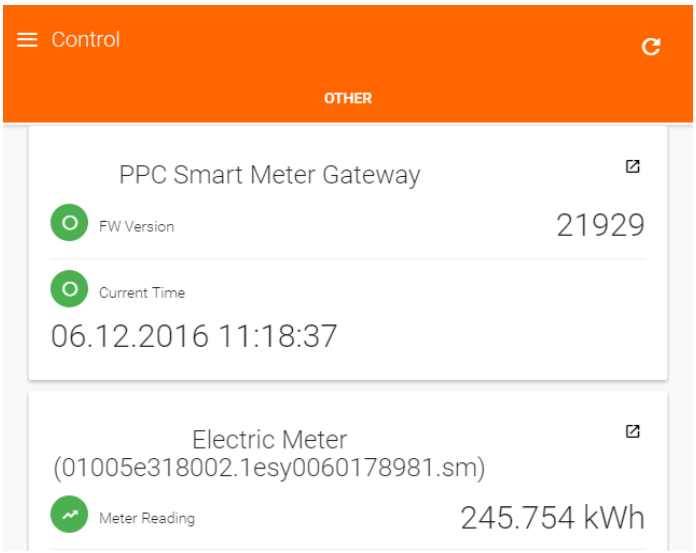

Fig. 4. The channels of the things in openHAB.

3.3 Implementation HAN CLS interface in Smart Home Systems

The connection of smart home systems to the CLS interface provides the possibility to access external services from the system, to publish controls to an external service, or to make selected devices as well as aggregated prosumption available to be controlled and configured by authorized external market entities. The CLS connection demands a client-certificate based connection establishment. Each CLS device is assigned with a client-certificate to connect to the SMGW. The regulatory guideline [5] specifies three communication use cases: CLS-initiated, EMT-initiated, and SMGW-initiated.

The CLS-initiated communication is implemented as SOCKSv5 connection. The CLS establishes the proxy connection and afterwards accesses the EMT service. The SMGW checks if a profile for the tuple <CLS, EMT> is available, forwards the connection establishment, and provides a communication channel between CLS and the EMT.

The EMT-initiated communication starts with a request from the EMT to the GWA for a connection to the CLS. The GWA sends a respective wake-up packet to the SMGW. If a profile for the tuple <CLS, EMT> exists, the SMGW establishes a connection to both the CLS and the EMT. Then, the EMS can send a request to the CLS device.

The SMGW-initiated communication is similar to the EMT-initiated one. But instead of the EMT requesting a connection establishment, this is triggered by an event inside the SMGW (e.g. when a new measurement is available or a tariff has changed).

In the example of openHAB, an extension to support CLS-communication can be implemented in different ways. One possibility is the provision of the RESTful API, that can be used to access and control all connected devices, to the EMT (see fig-

ure 5). A plugin uses the SMGW bridge to establish a CLS channel and to provide an interface that is used to access the API. After an EMT initiates the CLS connection, it is able to control openHAB. For this use case, the smart home system only requires a single CLS certificate to provide the EMT with a full control over the system and its connected devices.

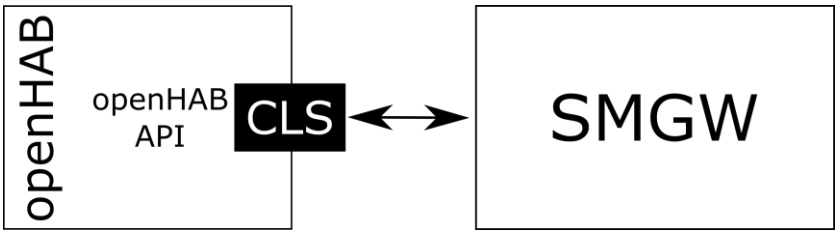

Fig. 5. openHAB serves as a single CLS device

Another possibility is the provision of single items (i.e. channels of a thing) to be accessed and controlled by an EMT (see figure 6). The user can add CLS-things that are assigned with individual items or things. This allows a fine graded permission control and demands an individual CLS certificate for each item or thing. This implementation reflects the same scenario as if all connected devices are CLS-capable by themselves. The advantage over the first possibility is that the user can control which devices are made available to the EMT. Both use cases can be implemented in the EMT-initiated communication scenario.

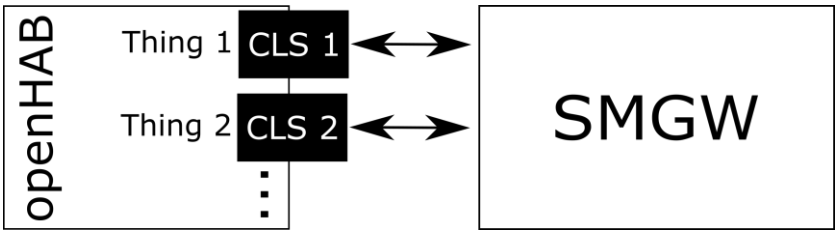

Fig. 6. openHAB serves as multiple CLS devices.

4 Consideration of Security Aspects

4.1 Security test arrangement

In the development of the proposed architecture, security issues need to be considered. Former related work concentrated on the security of the gateway and the overall architecture (e.g. [9]). The focus in the current implementation therefore is on analyzing and addressing the potential existence of security issues in the implementation.

The test arrangement shown in figure 7 is segmented to the LAN (Local Area Network), which is normally operated by the end user and the WAN, which is operated by the grid operator. In the WAN segment the SMGW is connected via the WAN interface to the GWA and an EMT. In the LAN segment the SMGW is connected via the two HAN interfaces End-User and CLS to openHAB, which is part of the AnyPLACE Platform. Based on the BSI Infrastructure standard the openHAB CLS Binding can be controlled by the EMT via the proxy functionality of the SMGW.

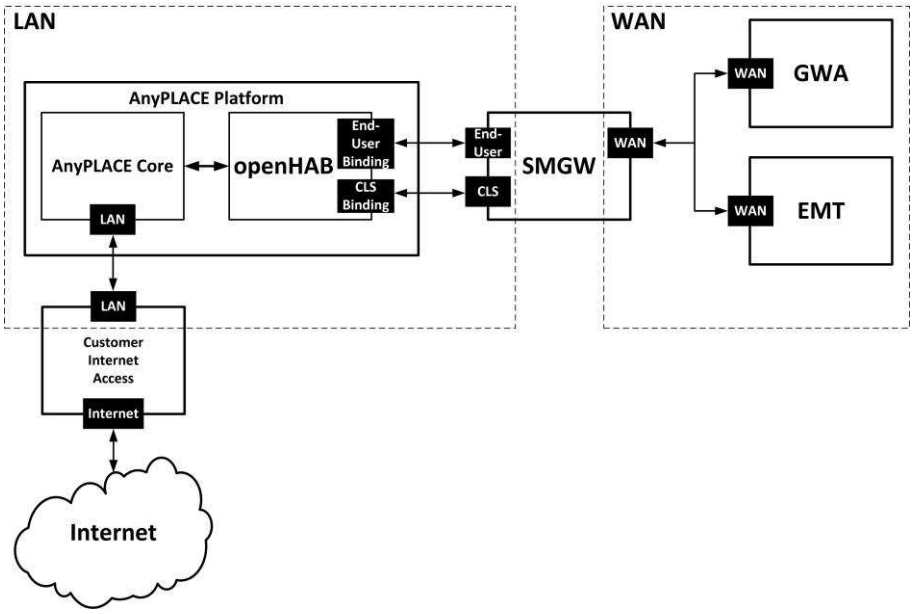

Fig. 7. Test arrangement for the security evaluation.

4.2 Security test scenarios

The test scenarios are divided into the assumption of a compromise of one of the network segments (LAN or WAN) and network components (AnyPLACE Platform, SMGW, EMT or GWA).

In the first scenario the assumption is that the LAN segment is compromised. This enables an attacker to attack the AnyPLACE Platform and the SMGW via the end

user and the CLS interfaces. The attacker has no further information (e.g. network addresses, open ports, certificates, details about encryption, details about authentication, etc.) about the devices in the LAN segment.

As second scenario it is assumed that the WAN segment is compromised. The attacker has no further information about the WAN communication. He can attack the WAN interface, the GWA and the EMT. Since the GWA and the EMT are not a part of the project's implementation, only an attack of the WAN interface is considered.

As a third scenario the compromise of the AnyPLACE Platform is considered. Through the compromise the attacker will receive the certificates for the end user and CLS connection between the AnyPLACE Platform and the SMGW. He can use certificates to generate valid messages, authenticate himself against the SMGW and he can attack the EMT because of the proxy functionality of the SMGW. Since the AnyPLACE Platform is connected to the internet, there is also the possibility that the EMT is attacked from the internet via the path AnyPLACE Core - openHAB - SMGW. This scenario is not in the scope of the tests, since the security means of the EMT are not part of the project's implementation and the EMT must generally make provisions against this scenario.

In the fourth scenario the assumption is that the SMGW is compromised. On the LAN segment the attacker can attack the AnyPLACE Platform, the CLS device and the infrastructure of the retail customer. On the WAN segment the attacker can attack the GWA and the EMT. This scenario is not considered since at this point the whole security infrastructure would be inactive.

In the fifth scenario the attacker manages to compromise the EMT, so he can attack the SMGW on the WAN side or the AnyPLACE Platform and the CLS device due to the proxy functionality of the SMGW. It will be also analyzed if the attacker can attack the network infrastructure of the end user in this scenario.

The sixth scenario is the compromise of the GWA. Through the compromise of the GWA the attacker will get access to the SMGW. This scenario is not considered since at this point the whole security infrastructure would be inactive.

4.3 Security test methodology

For the security evaluation, several suitable methods described in [10] were selected.

Network sniffing: With a network sniffer the network traffic can be recorded and analyzed. Normally an attacker uses network sniffing as first attack to receive some knowledge about the network. The metadata like IP addresses, used protocols or used ports provide information which can be used for further attacks. A limitation of network sniffing is that only services which communicate during the usage of the network sniffer can be identified.

Port scanning: A port scanner is an application to scan a device for open ports (TCP and UDP). Since port scanning is an active method where each port is tested, it is possible to find services which cannot be identified with network sniffing. The information about open ports will be used for further attacks.

Fuzz testing: Fuzz testing is a technique where unexpected or random data is sent to the input of a computer. The aim is to trigger errors like crashes or overflows. In the case of network security, fuzz testing is used to analyze the behavior of services on manipulated messages. Fuzz testing can be a very efficient method to find vulnerabilities on devices. This requires access to debug functionalities in order to determine which kind of error was triggered by the fuzz test.

Replay attacks: This is an attack where a recorded message is repeated maliciously. For example, the message from an EMT to a CLS device to activate some load can be recorded and replayed. If the message is encrypted but has no protection against replay attacks, this attack will also work although the attacker will not know the content of the message.

Man-in-the-middle attacks: This is an attack where an attacker is hooked in a communication between two devices. He can manipulate, alter, delay or generate messages in a malicious way.

Testing of protocols: Often protocols support different standards. For example, the TLS protocol allows a lot of different cipher and some of them are known as insecure. It is important to ensure, that none of this insecure standards are used, otherwise it might be possible to attack the communication between devices or a device itself.

4.4 Security evaluation and result utilization

Each test method will be applied on each scenario to identify security issues at the implementations created in the project. If a vulnerability is identified, the implementation will be overhauled to close the vulnerability. For elements of the overall infrastructure which are not part of the implementations done within the AnyPLACE project and thus not possible to modify, respective recommendations for a potential improvement of security will be formulated.

5 Conclusion and Outlook

The SMGW offers the possibility for end users to access meter data and to securely switch loads and generation in the households via its HAN interface. By connecting smart home systems to the HAN interface an established set of solutions in this area can be connected to the new smart metering infrastructure. In this way, the end user can easily make use of its additional possibilities.

Different implementation scenarios from the scope of the AnyPLACE project has been presented. The connection of the open source home automation framework openHAB shows the possibilities of the interconnection with the SMGW infrastructure. Furthermore, the definition of security tests shows that a thorough implementation and testing is required in order to minimize the added risks that are introduced by establishing this interconnection.

Acknowledgement

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 646580.

References

1. Farhangi, H., "The path of the smart grid," IEEE Power and Energy Magazine, vol. 8, no. 1, January-February 2010, pp.18-28.
2. openHAB UG (haftungsbeschränkt). openHAB. Retrieved November, 15 2016. [Online].
3. Henneke, D., Freudenmann, C., Kammerstetter, M., Rua, D., Wisniewski, L. and Jasperneite, J., "Communications for AnyPLACE: A smart metering platform with management and control functionalities," 2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA), Berlin, Germany, 2016, pp. 1-8.
4. Bundesamt für Sicherheit in der Informationstechnik (BSI). (2014) Protection Profile for the Gateway of a Smart Metering System. Version 1.3, Retrieved November, 15 2016. [Online].
5. Bundesamt für Sicherheit in der Informationstechnik (BSI). (2013) Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems. Technische Richtlinie BSI TR-03109-1, March 2013, Retrieved November, 15 2016. [Online].
6. Bundesamt für Sicherheit in der Informationstechnik (BSI). (2015) Protection Profile for the Security Module of a Smart Metering System (Security Module PP). Version 1.03. Retrieved 15.11.2016. [Online].
7. "Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (Messstellenbetriebsgesetz – MsbG)", Bundesgesetzblatt Jahrgang 2016 Teil I Nr. 43, Bonn, September 1st, 2016.
8. IFTTT – if this than that, IFTTT, Retrieved December, 8 2016.
9. Lunkeit, A., Voss, T. and Pohl, H., "Threat Modeling Smart Metering Gateways," Smart Objects, Systems and Technologies (SmartSysTech), Proceedings of 2013 European Conference on, Erlangen/Nuremberg, Germany, 2013, pp. 1-5.
10. Marc Ruef, "Die Kunst des Penetration Testing", C & L Verlag, 2007.