FORSCHUNGSINITIATIVE Zukunft BAU

Securing Device Communication in the Smart Home using the Protection Profile for Smart Meter Gateways

Summary Report

This research report was funded by the research initiative „Zukunft Bau“ of the federal institute for research on building, urban affairs and spatial development.
(Reference number: SWD-10.08.18.7-15.10 / II3-F20-14-1-012)
The author is responsible for the content of the report.

Editors: M.Sc. Hannes Raddatz, M.Sc. Michael Rethfeldt, Dipl.-Inf. Martin Kasparick, M.Sc. Arne Wall

Project leader: Prof. Dr.-Ing. Dirk Timmermann

Universität Rostock Traditio et Innovatio

Motivation

The rapid development of the Internet and the increasing number of networked devices, coupled with not consistently enforced security have led to the problem that almost every user can be monitored by unauthorized third parties. The BSI Protection Profile addresses such problems for the gateway of a Smart Metering system. The project secures communication in the Smart Home using the Smart Meter Gateway.

Subject of the Research Project

As part of the research project, a security framework was developed that allows to secure the communication in a Smart Home, taking into account the BSI Protection Profile for Smart Meter Gateways and the current state of the art. At the beginning of the project, a research of the state of the art was conducted and, in particular, current developments of communication protocols in the area of the Internet of Things (IoT) were investigated. The structures and components of Smart Metering systems as well as the Protection Profile for Smart Meter Gateways and the associated Technical Guidelines TR-03109 were part of this analysis. After examining various solutions for Smart Home systems on the market and in the Open Source community as well as evaluating protocol trends of IoT developers, the first requirements for the security framework could be defined. The basis are RESTful Web Services, realized through the Constraint Application Protocol (CoAP), which represents an innovation compared to the BBSR predecessor projects. Benefits of this protocol include popularity among developers, the ability to decentralize Web Services, and the interest of market participants (IKEA, Ericsson) and consortia (Open Mobile Alliance). In the following, further requirements were derived from the BSI Protection Profile and the Technical Guidelines, whereby the subareas of authentication and authorization were identified as elementary components in addition to securing device communication. While established protocols such as Datagram Transport Layer Security (DTLS) exist for the aspect of communication security, there are hardly any solutions for the two newly identified aspects in the area of IoT. Investigations were carried out, whether there are efforts in the research community to develop solutions for these aspects in the IoT sector. The following protocols, some of which are still in the draft stage of the Internet Engineering Task Force (IETF) standardization process, have been identified as promising candidates for the security framework: Concise Binary Object Representation (CBOR) and CBOR Object Signing and Encryption (COSE) as a binary lightweight data format and subsequent security mechanisms for signing and encrypting messages. The Authentication and Authorization for Constrained Environments (ACE) protocol authorizes device access using so-called Tokens. Lightweight M2M (LwM2M) extends CoAP with data models and enables user-friendly management of the devices. Due to limitations arising from securing CoAP using DTLS, Object Security for Constrained RESTful Environments (OSCORE) has been added to the security framework as a security protocol. The challenge was to combine the protocols in an appropriate way to meet the defined requirements.

After the design of the security framework, the integration of Smart Metering elements into the Smart Home network was considered. The rollout of Smart Metering systems in Germany has just begun, but in the near future Smart Metering devices will be installed in every building and automatically send the consumption values to the energy provider. This requires a communication unit, the so-called Smart Meter Gateway. This gateway is a BSI-certified device that meets high security requirements and has specialized cryptographic hardware. One goal of the research project was to integrate this

device as a secure instance into the Smart Home network and the security framework in such a way that all Smart Home devices can benefit from the security features of the gateway. For this purpose, the security framework was adapted accordingly and the Smart Meter Gateway was upgraded with additional functions (Smart Home Gateway). Finally, prototypes of various Smart Home scenarios were developed and implemented using the security framework. These include, besides others, an audio/video intercom and a user authentication and authorization process using the new German identity card. Furthermore, the report states, how the security framework can be integrated quickly into existing smart home products.

Conclusion

The security framework was used to develop a basis for a Smart Home system, which takes into account the current security requirements of the BSI right from the start and integrates the Smart Meter Gateway into the Smart Home network. The framework can be understood as a kind of foundation of a Smart Home system that manufacturers can use to implement their own Smart Home devices and systems. Using this foundation, extensions were developed, which allow further functionalities. The research carried out at the beginning of the research project was used to develop a concept with protocols that allow a rapid implementation into real products, despite its scientific focus.

Key Data

Short title:	Secure Smart Home
Researcher / Project leader:	M.Sc. Hannes Raddatz, M.Sc. M. Rethfeldt, Dipl.-Inf. M. Kasparick, M.Sc. Arne Wall/ Prof. Dr. Dirk Timmermann
Total costs:	467.813,30 €
Federal subsidy:	327.469,31 €
Project duration:	28 Months

Figures

Figure 1: SecureSmartHomeLogo.png
Caption: Logo of the Secure Smart Home project

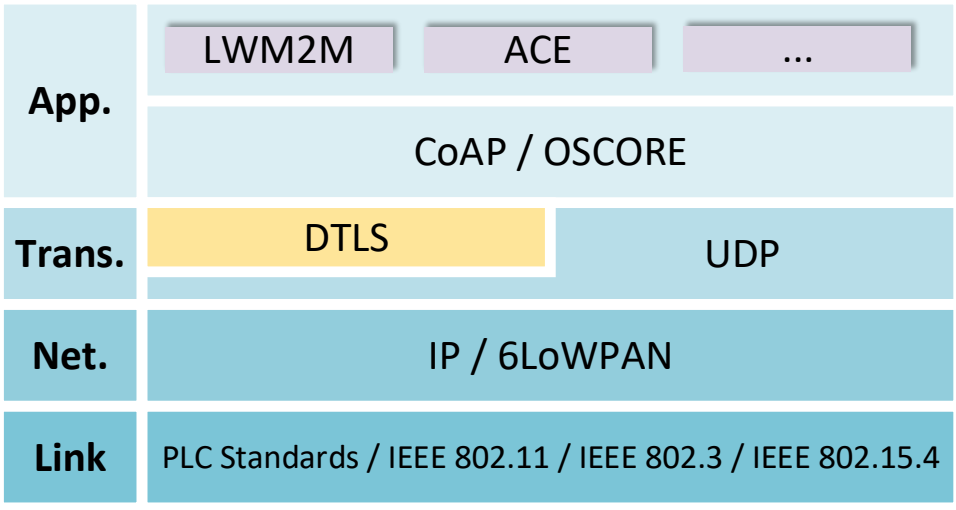

Figure 2: SecureSmartHomeStack.png
Caption: Protocol stack of the security framework

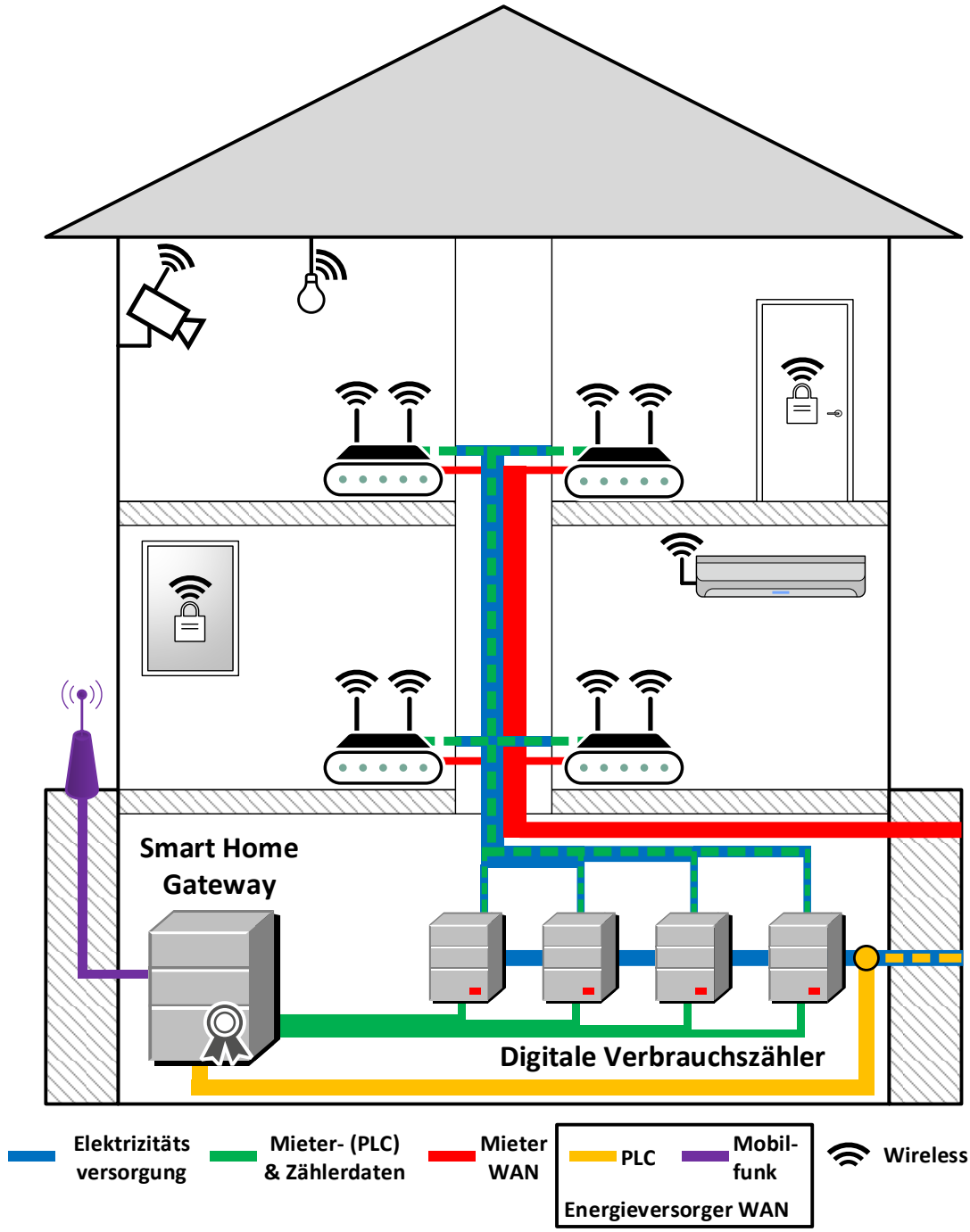

Figure 3: SecureSmartHomeInfrastructure.png
Caption: Infrastructure of the security framework using the example of a building with four residential units equipped with Smart Home devices and Smart Metering system

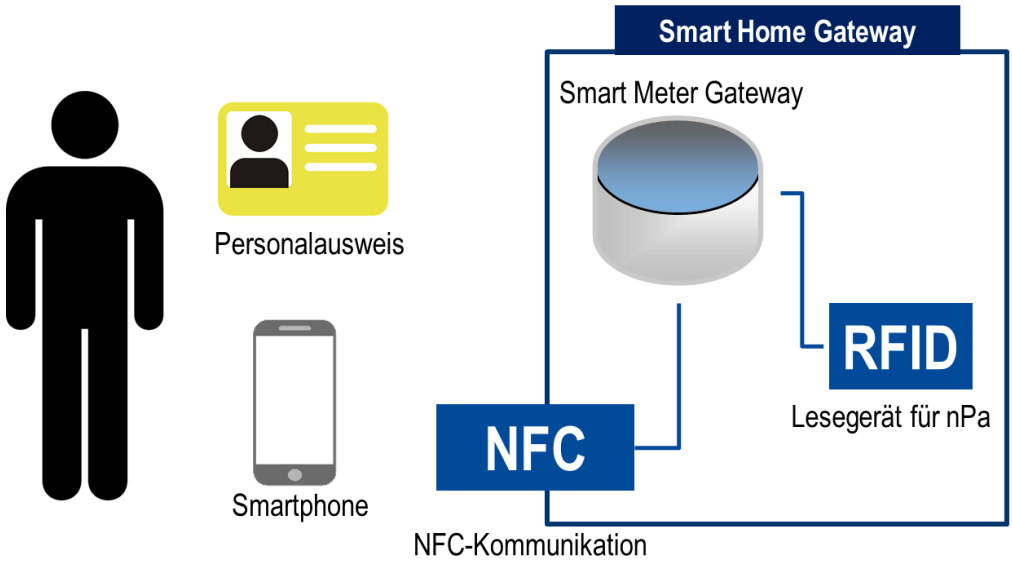

Figure 4: SecureSmartHomeNPA.png
Caption: Registration of new users and authorization of user devices using the new German identity card

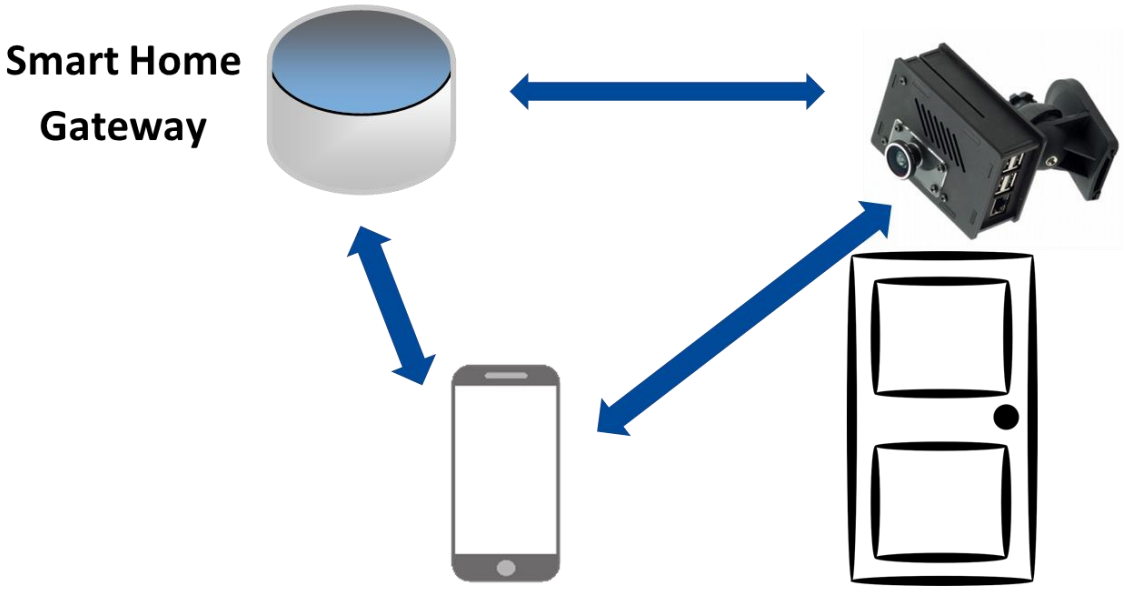

Figure 5: SecureSmartHomeIntercom.png
Caption: Secure communication between intercom and smartphone

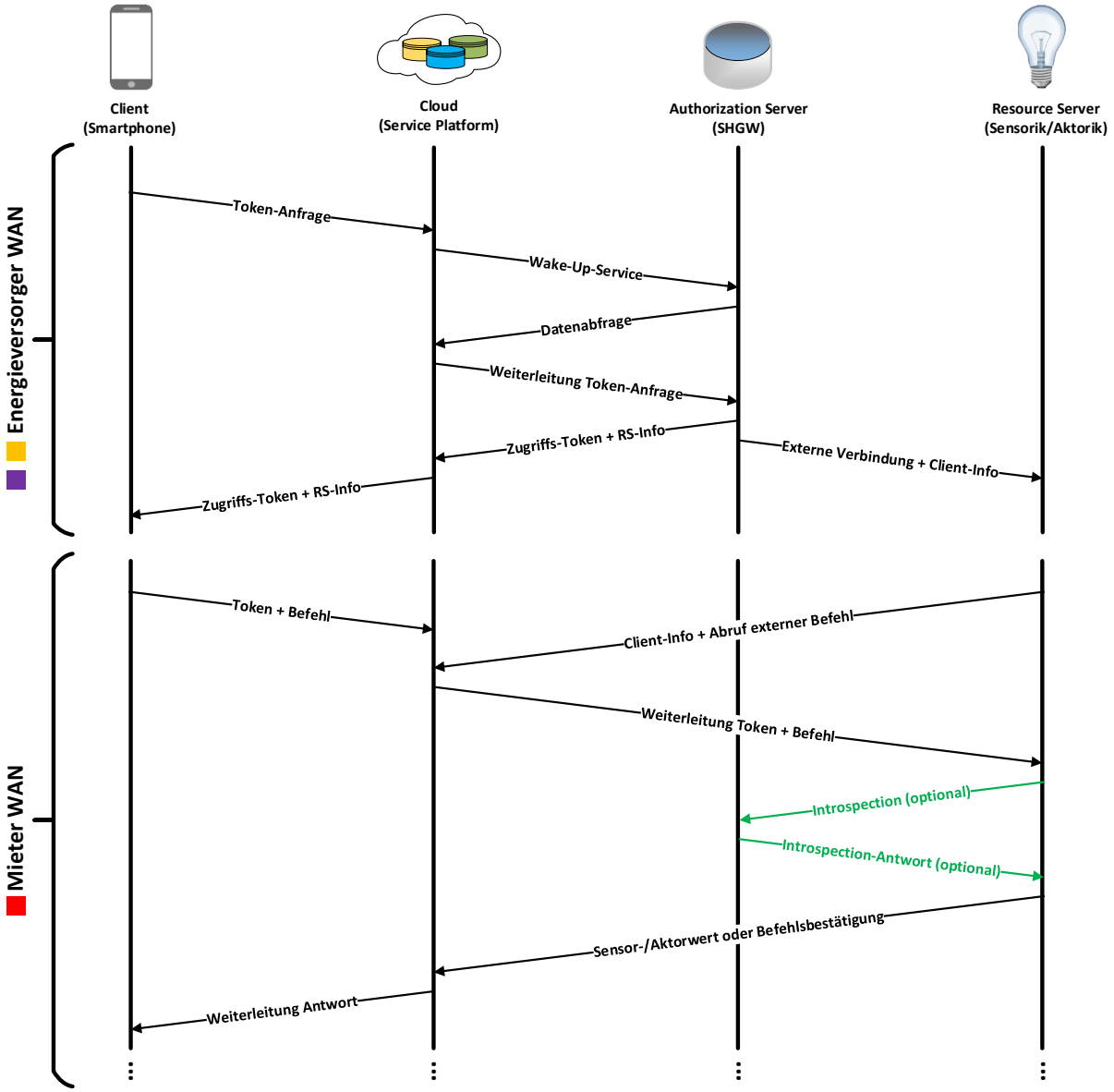

Figure 6: SecureSmartRemoteControl.png
Caption: Secure communication between external user device and a device in the Smart Home

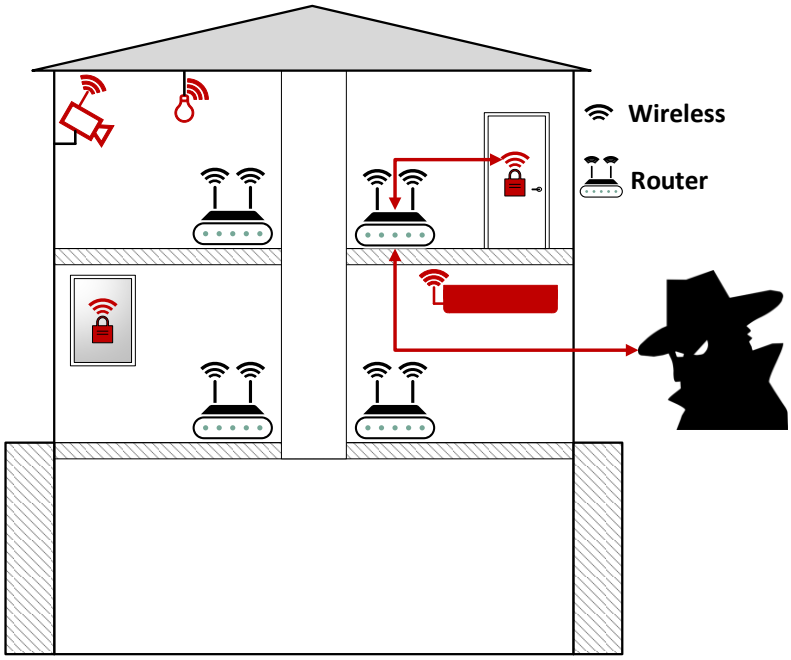

Figure 7: SecureSmartHomeAttackSurface.png
Caption: Attack scenario of a Smart Home network due to misconfiguration

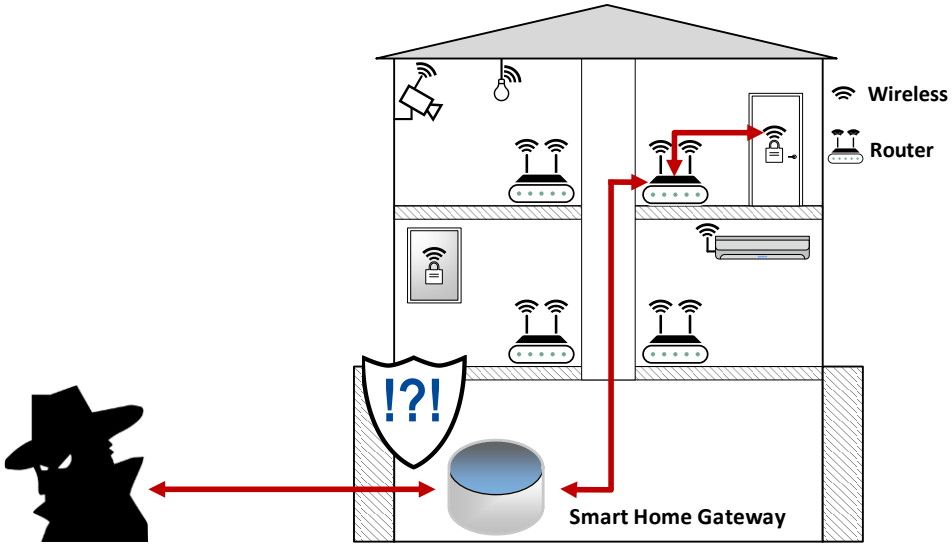

Figure 8: SecureSmartHomeProtected.png
Caption: Attack scenario of a Smart Home network protected by security framework