Trustful Interaction Between Intelligent Building Control and Energy Suppliers of the Smart Power Grid

Michael Massoth and Torsten Wiens
Department of Computer Science
Hochschule Darmstadt — University of Applied Sciences
{michael.massoth | torsten.wiens}@h-da.de

***Abstract*—This paper describes an approach to balance loads in smart power grids using a solution based on Next Generation Network (NGN) components, Smart Home appliances based on the KNX bus, and a secure and trustful interaction between intelligent home control managers and the energy suppliers of the smart power grid. The NGN components are applied as a communication and integration platform between the smartphone of the facility managers, the home automation and building control system, as well as the energy suppliers of the smart power grid. The Session Initiation Protocol (SIP) and the Presence Service are used to build a well performing and scalable system based on open source software. The idea is to publish data of actual power consumption and power reserves of selected Smart Home appliances by use of the Presence Service to the outside world. In a second step, the corresponding energy supplier could subscribe to this data of actual energy consumption and reserves. Based on this data, the energy supplier is enabled to send specialized offers towards the Smart Home owners reflecting possible benefits to the power grid. This solution respects the right to property and the right to self-determination of the Smart Home and facility control managers, because they have to agree to the energy management offer made by the energy supplier. It is a trustful solution because the relevant data could by easily pseudonymized before being published by the Presence Service. An approach to ensure secure communication against attackers from outside is presented and evaluated as well.**

Keywords—Home Automation; Smart Power Grid; Load Balancing, NGN, Presence Service.

I. INTRODUCTION

The current trend is to make the human environment smarter, using ubiquitous IT-technologies. This leads to smart cities, buildings, energy management, cars and phones. Every part of our environment will be connected to each other and can be controlled, with the given rights, from central points.

In such a world, security and trust are of essential importance. Confidentiality, integrity, availability and authenticity have to be given. In this paper, we describe the security of a remotely controllable KNX-based home and building control solution. The owner or facility manager of such a home can remotely monitor and control his house or facility wherever and whenever they like. A Smart Home shall enable interaction with its users, including the ability to monitor the status and control of building appliances and devices remotely from anywhere in the world. Such devices may consist of alarm systems, keyless access control, smoke detectors, light and heat control, medical devices, and all types of sensors (e.g., room, door, window or security surveillance, monitoring and control, statistics and remote metering).

A. Purpose and Relevance

The purpose of this paper is to present a new approach for a well performing, scalable, secure and trustful interaction between intelligent home control managers and the energy suppliers of the smart power grid. The novelty of the presented approach is to make use of an NGN Presence Service for the interaction between the smart home control and the energy supplier, and not only between the smart home and the house owner, as already described in [2,3,4]. The mobile ubiquitous home and facility control solution is based on SIP and the Presence Service. The described solution uses the advantages of a NGN to remotely monitor and control home automation systems via a mobile device using open source software.

The global carrier VoIP and IP Multimedia Subsystem (IMS) market for NGN-based services and infrastructures has reached US$ 658 million in the second quarter of 2012, according to Infonetics Research. Furthermore, the market drivers are intact and the numbers of VoIP and IMS subscribers are growing [1]. This forecast shows the business opportunity and relevance of the proposed solution for ubiquitous home control services.

B. Structure of the Paper

Following the introduction, Section II shows related work and other projects comparable to our solution. In Section III, the general concept is outlined and important use cases are presented. The overall system design is described in Section IV, differentiating three levels of interaction. The components used to build the system are presented in Section V. The security approach is discussed and evaluated in Section VI. Section VII describes the status of our prototype. Section VII concludes the paper and gives an outlook of future work.

II. RELATED WORK

Smart Home is not a new topic. Many companies and institutions are working on solutions for Smart Homes. But only a few are working on a complete solution that relies solely on open standards. Most systems focus on the inside (e.g., KNX) or outside (e.g., IP) system of the building only. This means that their goal is to build a solution either for the

 ISBN: 978-1-61208-282-0

management of actors and sensors, or to develop a communication solution for existing bus systems.

In our previous work [2, 3, 4, 5], we created a signaling gateway between the KNX home automation and building control system [6] and SIP, allowing communication of mobile devices with KNX sensors/actors using existing SIP infrastructure. The idea of our solution was to connect the technology of NGNs to Smart Home Control Systems.

The HomeSIP project is a similar approach, allowing home control only using SIP [7, 8, 9]. The important parts of the system are the SIP proxy and the SIP sensor network gateways. The SIP proxy is the central component for communication. The sensor network gateways are embedded Linux systems, which are used to control the sensor networks and connect them to the SIP proxy. So, SIP is used for communication between the sensor networks, the SIP proxy and the mobile controlling devices, like smartphones. All information from and to the sensor networks is transported via SIP. The paper "Security for KNXnet/IP" [10] evaluates different approaches to grant security in an IP network, which is coupled to KNX. In contrast, we are using SIP as a bridge to the NGN world.

III. USE CASES OF SMART ENERGY MANAGEMENT

In this section, two typical business cases respectively use cases of smart energy management and electric load balancing and regulating are discussed.

A. *Use case (UC1): Surplus or excess of renewable energy*

Let us assume for use case (UC1) that the power consumption and load in the city reaches its lowest level. During the same time frame, the renewable energy is fed into the power grid at maximum because of strong winds or strong sun radiation. This surplus or excess of electric power shall be used by the intelligent buildings of the city. In order to do that, the surplus of energy is signaled by the energy suppliers towards the owners of intelligent buildings in the city by means of usual communication technologies. In our case, a smartphone app is used. The house owners can then react by turning on additional power loads such as domestic appliances (e.g., white goods, air conditioning units or heat pumps), as well as electric cars and vehicles. By that, the energy supply within the city could be balanced in a better way by the swarm behavior of the intelligent consumers by activating additional power loads.

B. *Use case (UC2): Insufficient or lack of renewable energy*

Let us assume for use case (UC2) that the power consumption and load in the city reaches its maximum level. During the same time frame, the feed-in of renewable energy is diminishing at minimum because of wind calm or the lack of sun radiation (e.g., at night). This lack of electric power shall be balanced, at least partly, by the intelligent buildings of the city. In order to do that, the lack of energy is signaled by the power providers towards the owners of intelligent buildings in the city by means of usual communication technologies. The house owners can then react by switching off domestic appliances (e.g., white goods), set air conditioning units, or heat pumps into eco-mode and deactivate charging stations for electric cars and vehicles. Therefore, the energy supply within the city could be balanced in a better way by the swarm behavior of the intelligent consumers by de-activating power loads.

IV. CONCEPT AND OVERALL SYSTEM DESIGN

The core concept is to balance loads in power grids by using KNX-enabled Smart Homes and a communication infrastructure based on NGN technologies and the Presence Service. The essential idea of this approach is to publish data of actual power consumption and power reserves of selected Smart Home appliances by use of the NGN Presence Service to the outside world. In a second step, the corresponding energy supplier could subscribe to this data of actual energy consumption and reserves. Based on this data, the energy supplier is enabled to send specialized offers towards the Smart Home owners in order to manage a surplus or lack of renewable energy, enabling a feedback control and power regulation within the smart grid.

NGN technologies are used to build an integration platform between mobile devices and intelligent buildings with a home automation solution. As depicted in Fig. 1, a Signaling Gateway interconnects the NGN core network and the Smart Home.

To interconnect the two architectures, a special gateway is needed. The gateway manages connections between the SIP-based NGN and the single appliances of the Smart Home solution. In this system, the NGN infrastructure consists of an IMS [11].

The IMS is a control architecture based on the standardized SIP [12] designed by the wireless standards body 3rd Generation Partnership Project (3GPP). It aims to standardize access to different networks. Therefore, all communication is based on the Internet Protocol (IP).

An important functionality of the IMS is the Presence Service, which enables to represent different home automation appliances as users to the outside world. Each appliance can set its own current status. Thus it is possible to register a mobile device at the SIP network, and in this way at the Presence Server. Hence, the status information of the different home automation appliances can be viewed on a mobile device.

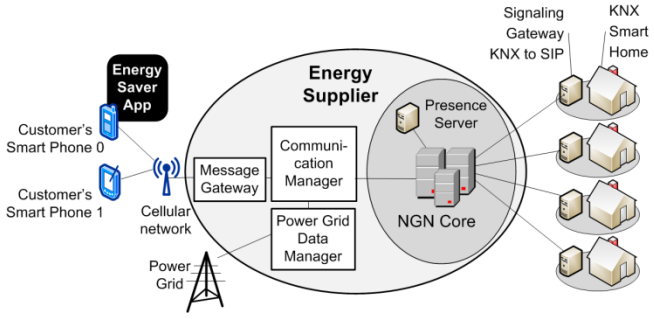

Figure 1. System overview.

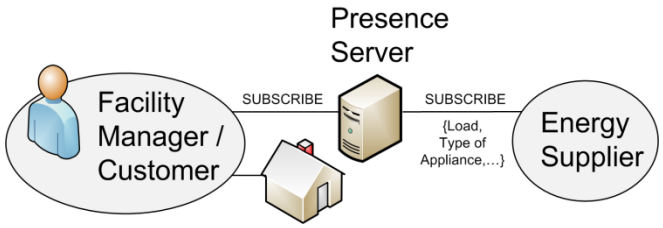

Figure 2. Basic system functionality and interaction between customer, energy supplier and Presence Server.

The Signaling Gateway is responsible for updating the status information at the Presence Server. For example, any time a sensor in the home automation system changes its status, an update has to be sent by the gateway.

At the energy supplier, the software component Communication Manager is the core component that contains all business logic to assess load data from the power grid, organized by the Power Grid Data Manager, and data collected from the Presence Service. A Message Gateway is used to send messages to the Smart Home owner's smartphone.

V. COMPONENTS

In the following section, we describe the components that are used to build our system. The description is divided into three subsections, each presenting different levels of interaction within the whole system.

Basically, this approach extends the core technology mentioned in our previously published work by implementing a push service [2, 3, 4, 5]. Additional components have been integrated to accomplish the task defined in this paper. Subsections A and B describe these new components. Subsection C provides an overview of the core system that has been continually refined.

A. Interaction between Energy Supplier and Smart Home

The corresponding Energy Supplier system registers itself at the Presence Server (see Fig. 2). In a second step, the energy supplier subscribes to the data sets of actual energy consumption and reserves. Status data from all Smart Homes connected to the Presence Server is continuously monitored by the Communication Manager component (see Fig. 1). Status data from the power grid is collected through the Power Grid Data Manager component. Comparing these two data sources, the system is able to detect situations in the power grid as described in use cases UC1 or UC2 (see Section III). Then, offers are calculated that match the specific capabilities of the relevant Smart Homes in a given area and sent out via the Message Gateway component.

B. Interaction between Energy Supplier and Smart Home Manager

At the Energy Supplier, a core component encapsulates the system's business logic (Communication Manager, see Fig. 1). Communication to the Smart Home Customer's smartphone is set up and controlled by the Message Gateway component. At the mobile device, the EnergySaver App is implemented as an extension of our Android SIP client described in Subsection C. A web service is implemented at the Message Gateway that interacts with the smartphone communication component by means of push notification [21].

The EnergySaver App receives and displays messages from the Energy Supplier containing offers to the Smart Home customer as described above. The customer then is able to accept or decline a specific offer. If the offer is accepted, the customer's Smart Home appliances are set up accordingly, communication being done through the infrastructure described in Subsection C. For example, power reserves of specific appliances can be released into the public network after accepting a suitable offer.

C. Interaction between House Manager and Smart Home

In this subsection, the core system that provides interaction between the House Manager and the Smart Home is described.

1) Next Generation Network Core

To set up the NGN Core networks, we evaluated two solutions to guarantee that the signaling gateway is able to work with different NGN platforms.

As a lightweight solution to realize the NGN Core, a SIP server with a Registrar and a Presence Service is used. This common SIP server also provides all the functionality that is needed to set up a SIP-based communication and integration platform. SIP is a signaling protocol for controlling multimedia communication. It can be used to create, modify or terminate a multimedia session, which can exist between two parties or multiple parties.

The Session Description Protocol (SDP) [13] describes properties of multimedia sessions. SDP is used by SIP for negotiation regarding media codecs, transport protocols and transport addresses. SIP for Instant Messaging and Presence Leveraging Extensions (SIMPLE) [14] describes a presence and instant messaging protocol suite based on SIP.

Instant messaging enables users to communicate by text. For the Presence Service, a User Agent (UA) has to register at a Presence Server. The server acts as a Presence Agent. It stores the status of the UA. Other users (subscribers) can subscribe to the UA's presence information. Every time the UA changes its status, the subscribers will be notified by the Presence Agent.

2) Mobile Device

We chose Android 2.2 [15] as the development platform for the mobile device prototype. After we evaluated different SIP APIs for Android, we chose CSipSimple [16], because only CSipSimple is able to send SIP messages conforming to the RFC3428 standard. CSipSimple is an open source VoIP application for Android using SIP. Based on CSipSimple, we built our own Android SIP client prototype including our own GUI and the functionality to display and change presence states.

3) KNX

The KNX system [17] is the only worldwide standard for home automation and intelligent building control.

 ISBN: 978-1-61208-282-0

KNX was invented in response to the following shortcomings: In conventional home installations, the control line and the power line are not independent from each other. For example, lights are controlled by turning their power on or off. Complex control mechanisms are hard to implement, and to change a wire-bound energy-controlled system after its installation is very complex. Therefore, power and control lines in the KNX standard are independent from each other.

The KNX standard supports the following communication media: Twisted pair (TP) wiring, power line (PL) networking, radio frequency (RF) and Internet Protocol over Ethernet (KNX/IP or KNXnet/IP).

4) Signaling Gateway

The signaling gateway, depicted in Fig. 3, is the central component of this concept. This software service connects the KNX bus to the NGN components.

Every sensor and actor that is connected to the KNX bus gets its own address (SIP URI) to log on to the service. Registering each KNX device in the Presence Service, allows storing the current status of the device, like “on” or “off”. Each device update received from KNX is converted to a SIP request and sent to the Presence Server. Now the user of the mobile device can monitor and even change the current status for each KNX device. Every change is then transmitted back to the KNX bus.

With a KNXnet/IP (interface between KNX and Ethernet) device, KNX telegrams can be transferred to the IP network. The whole telegram is transmitted over the network as payload of an IP packet. Thus, one functionality of the signaling gateway is to receive these IP packets sent by the KNXnet/IP device. Furthermore, the information in the telegram has to be extracted. This could consist of sensor values or other status messages of different home automation appliances.

The KNXnet/IP device is also able to receive IP packets sent via the IMS from the IP network and forward the containing telegram to the KNX bus. Thus, in order to control appliances that are associated with the bus installation, the signaling gateway has to have the ability to generate KNX telegrams.

The framework Calimero 2.0 is a collection of Java APIs that form a high level framework for communication with a KNX installation with the use of KNXnet/IP [18].

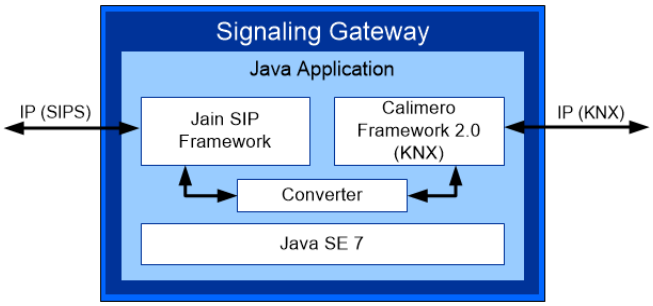

Figure 3. Connection interfaces of the Signaling Gateway

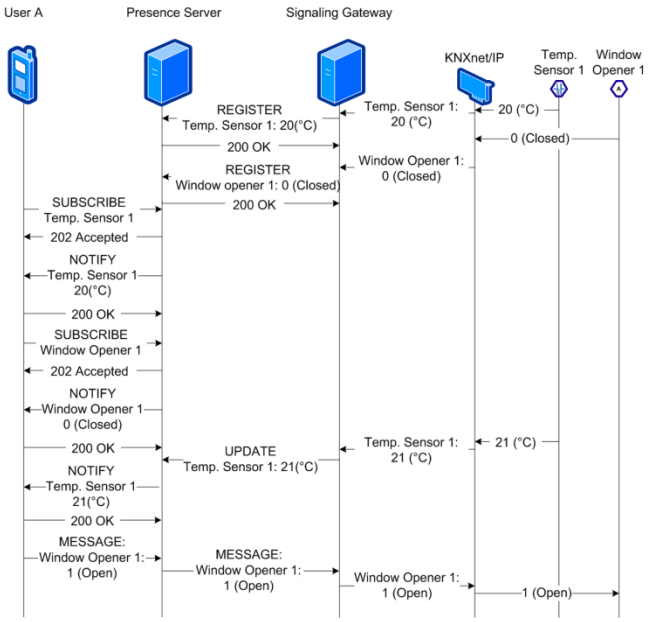

Figure 4. Complete message flow, ranging from registration of the KNX devices to the control of the KNX devices.

The framework aids in building high level applications that need to communicate with the KNX bus system for remote access and control. It can receive and decode KNX messages as well as send and encode its own KNX messages. This framework is used in the signaling gateway to handle communication with the KNX bus.

Once the information of the telegram has been filtered, the status change must be transmitted to the Presence Server located in the IMS. This leads to the second main functionality of the signaling gateway: The connection to the IMS. To accomplish this, the Jain-SIP (JSIP) framework [19] for Java is being used. The signaling gateway registers every appliance of the KNX bus installation as a "user" at the Presence Server. To set the status of a user, a SIP message must be sent through the IMS network. This message flow is depicted in Fig. 3. To view the current status of a part of the home automation system, the mobile device only has to subscribe to the Presence Server.

If a user wants to control an appliance of the home automation system, a SIP message is sent from the mobile device to the signaling gateway. Furthermore, the information in the SIP message body must be converted to a KNX telegram. This body is optional and can include messages written in SDP, SOAP, XML or ASCII.

Furthermore, status data of energy-related appliances in the Smart Home are published to the Presence service. This includes type of appliance (see use case description in Section III), power source/power sink, load characteristics and capacity as well as other parameters. Not every appliance in the Smart Home is reflected in this data set, but only the most important ones with the largest impact on load balancing, e.g., powerful car batteries or freezers.

This data is pseudonymized by means of a hash function, meaning that regular customer identifiers are replaced by other identifiers that only allow the energy supplier to

 ISBN: 978-1-61208-282-0

reconstruct the customer's identity. Therefore, no personal data is transmitted via the Presence Service. Because of this, the proposed system is in accordance to national legal regulations, for example the German "Bundesdatenschutzgesetz" (Federal Data Protection Act) [20].

VI. System Security

Without an implementation of suitable security measures, the system could be compromised by attackers. Therefore, it is necessary to ensure a secure connection to the mobile device and a secure authentication for the user. In this section, a security approach is introduced that will be used to secure the end-to-end network communication of the system as shown in Fig. 1. At the current development stage of the system, only a basic security model is assumed that primarily considers attackers from outside.

A. SIPS Introduction

SIP Security (SIPS) is using Transport Layer Security (TLS) and the Secure Real-Time Transport Protocol (SRTP). SRTP are used for secure Voice- and Video-Data connections, TLS is used for exchanging signaling messages (e.g., authentication and registration).

TLS is a hybrid encryption protocol for secure data connections over the internet. In the OSI reference model (Fig. 4), TLS is acting at the transport layer. In SIPS, TLS takes care of the following security tasks:

- Bidirectional authentication of communication endpoints
- Exchanging a shared secret
- Cryptographic encoding of data to be transferred
- Securing integrity of transferred SIP messages

To prevent possible man in the middle attacks, TLS can be extended with digital certificate authentication [22].

B. Evaluation of system security

We measure the security of the selected approach according to the four pillars of information security [23]:

- Confidentiality
- Integrity
- Availability
- Authenticity

As described above, SIPS is using the protocols TLS and SRTP for secure communication. TLS uses a high security encoding and grants therefore high confidentiality. The TCP/IP protocol ensures integrity by adding a checksum to each message. Authenticity is granted by authentication with credentials. The SIPS availability is given as long as the SIP server is connected to the internet.

Furthermore, software aspects like performance, scalability, manageability and cost have been evaluated.

Compared to an unsecured and connectionless UDP connection, a TLS connection is less performant. The reason for this is that SIPS is based on connection oriented TCP, which needs significantly more resources. Encryption is also costly. This fact also reduces the scalability of such a system. Because of the wide-spread use of SIPS, there are many frameworks and libraries, which make SIPS easily manageable and implementable.

If a certificate is used to ensure the identity of the communication partners, a disadvantage of TLS are the costs to buy trusted certificates from a Certificate Authority [24].

Other security models have also been considered for the system. A Virtual Private Network (VPN) is a possible approach, but would not be feasible [25]. The VPN needs to be set up before using the mobile client and to be closed after using the mobile client. Closing it in between will disconnect the mobile client from the SIP server. An active VPN connection uses additional internet bandwidth and battery power, because it needs to stay active as long as the application is running.

We also don't recommend the use of an ID Token [26], because of the implementation effort, the low performance and the extra cost for an ID Token reader/writer.

We choose SIPS for this system, as it is easy to implement (because TLS is supported by all software used for the prototype) and ensures a high level of security. Still, loss of the mobile device is a security risk to be prevented. This could be done in combination with a password for authentication with the system, or even an ID Token could be used (as a password). Now, after the loss of the device, only the password needs to be changed or disabled, to prevent unauthorized access.

VII. Actual Status of the Prototype

The prototype consists of a fully addressed and configured KNX TP bus system with different kinds of sensors and actors like weather station, dimmers and digital/analog switches for lighting and power outlets. The signaling gateway is implemented as a Java application using the Calimero 2.0 framework and the JSIP framework. The Calimero framework is used for communication with the KNX bus via the KNXnet/IP interface. Every KNX device gets translated as a SIP UA and therefore can be accessed individually.

The Presence server is implemented as a servlet using the Sailfin framework for SIP on a GlassFish-Server. Sailfin offers a full featured Presence service and SIP call control functions.

The mobile client is implemented as an Android application based on a modification of the open source software called CSipSimple for Android. The mobile client can get a list of all UAs for the KNX devices by sending a message to a specialized UA in the signaling gateway, which sends back the SIP URIs for the devices. With this list, the mobile client can subscribe to each device at the Presence server. Direct messages to the KNX devices can change the status of the device. The devices themselves can publish their status to each subscribed user.

The communication between each party is secured by using the TLS protocol. The Sailfin, JSIP and the CSipSimple framework all support TLS and authentication, no own implementation of TLS is needed.

The EnergySaver App has been implemented as a prototype.

 ISBN: 978-1-61208-282-0

VIII. CONCLUSION AND FUTURE WORK

The presented solution enables a secure and trustful interaction between intelligent home control managers and the energy suppliers of the smart power grid.

The interaction between house manager and smart home is implemented as mobile, ubiquitous, two-way home control solution based on SIP and the Presence Service. Hereby, the house manager could control all smart home appliances (e.g., actors and sensors) in real-time via his Android-based smartphone. It is realized as secure TLS connection based on SIP Security from the smartphone towards the signaling gateway, which is typically located inside the smart home.

The interaction between energy supplier and smart home is mainly effected by the Presence Service, which publishes the data of actual power consumption and power reserves of selected smart home appliances to the outside world. The Presence Service is a well performing, scalable, field-proven, near-real-time push-solution of the energy data sets towards the corresponding energy supplier. The described solution is trustful, because data privacy protection could be fulfilled easily by pseudonymization or anonymization of the energy data sets on the presence server side. By that, our solution respects the right to data privacy protection of the smart home owners.

The interaction between energy supplier and smart home manager is characterized by a half-automated energy load management solution. Our solution respects the rights of property and self-determination (autonomy) of the smart home owners, because they have to agree to the energy management offer made by the energy supplier.

It has to be noted that this kind of interaction is limited to day-time use only. Appropriate automatisms should be applied for the time users are sleeping or are “off-line”. This will be addressed in future work. Furthermore, another point is to make the mobile client platform independent and to introduce a security model that exceeds the basic considerations described herein.

ACKNOWLEDGMENT

This work has been performed within the project “Smart Home Control” at Hochschule Darmstadt (University of Applied Sciences). The authors would like to acknowledge the support of Albrecht JUNG GmbH & Co. KG for their contribution of KNX actors, sensors and other KNX home automation devices and kind support.

REFERENCES

[1] Infonetics Research, “IMS equipment and subscribers report”, 10/17/2012.

[2] R. Acker, S. Brandt, N. Buchmann, T. Fugmann, and M. Massoth, “Ubiquitous Home Control based on SIP and Presence Service”. In: Proceedings of the 12th International Conference on Information Integration and Web Based Applications & Services (iiWAS 2010), ACM, 2010, pp. 757–760.

[3] M. Massoth et al., “Ubiquitous Smart Grid Control Solution based on a Next Generation Network as Integration Platform”. In: Proceedings of the 1st International Conference on Smart Grids, Green Communications and IT Energy-aware Technologies (ENERGY 2011), IARIA, 2011.

[4] R. Acker and M. Massoth, “Secure Ubiquitous House and Facility Control Solution”. In: Proceedings of the 5th International Conference on Internet and Web Applications and Services (ICIW 2010), IEEE Computer Society, 2010, pp. 262–267.

[5] M. Massoth et al., “Security Assessment of an Ubiquitous KNX based Home Control Solution using SIP and the Presence Service”. KNX Scientific Conference 2012, University of Las Palmas de Gran Canaria, 2012.

[6] KNX Association, http://www.knx.org/knx-standard/standardisation, [retrieved: April, 2012].

[7] HomeSIP Project, http://www.enseirb.fr/cosynux/HomeSIP/, [retrieved: May, 2013].

[8] B. Bertran, C. Consel, P. Kadionik, and B. Lamer, “A sip-based Home Automation platform: an experimental study”, Proc. 13th International Conference on Intelligence in Next Generation Networks, 2009 (ICIN 2009), IEEE Press, Oct. 2009, pp. 1-6, doi: 10.1109/ICIN.2009.5357075.

[9] C. Bertran, C. Consel, W. Jouve, H. Guan, and P. Kadionik, “SIP as a universal communication bus: a methodology and an experimental study”, Proc. 2010 IEEE International Conference on In Communications (ICC 10), IEEE Press, July 2010, pp. 1-5, doi: 10.1109/ICC.2010.5502591.

[10] D. Lechner, W. Granzer, and W. Kastner, „Security for KNXnet/IP“. In: Proc. KNX Scientific Conference Nov. 2008.

[11] J. Soininen (Ed.), “Transition scenarios for 3gpp networks”, IETF, RFC 3574, Aug. 2003.

[12] H. Schulzrinne et al., “SIP: session initiation protocol”, IETF, RFC 3261, Jun. 2002.

[13] M. Handley, V. Jacobson, and C. Perkins: “SDP: session description protocol”, IETF, RFC 4566, Jul. 2006.

[14] SIP for Instant Messaging and Presence Leveraging Extensions (SIMPLE). IETF Working Group

[15] Android, http://www.android.com, [retrieved: May, 2013].

[16] CSipSimple, http://code.google.com/p/csipsimple, [retrieved: May, 2013].

[17] KNX Association, “KNX logical topology faq”, 2005, [retrieved: May, 2013].

[18] Calimero 2.0, http://calimero.sourceforge.net/, [retrieved: May, 2013].

[19] Jain SIP Framework, http://jsip.java.net/, [retrieved: May, 2013].

[20] Bundesministerium der Justiz, „Bundesdatenschutzgesetz in der Fassung vom 14. Januar 2003, zuletzt geändert am 14. August 2009“, Berlin, 2009.

[21] W3C, “Web Services Description Requirements. W3C Working Draft 28 October 2002”. http://www.w3.org/TR/ws-desc-reqs/, [retrieved: May, 2013].

[22] BSI, „VoIPSEC Studie zur Sicherheit von Voice over Internet Protocol“, https://www.bsi.bund.de/ContentBSI/Publikationen/Studien/VoIP/index_htm.html, [retrieved: May, 2013].

[23] A. Menezes, P. van Oorschot, and S. Vanstone: "Handbook of Applied Cryptography (Discrete Mathematics and Its Applications)”, CRC Press, 1996.

[24] Microsoft, “Digital Certificates”. http://support.microsoft.com/kb/195724, [retrieved: May, 2013].

[25] M. Lewis, "Comparing, Designing, and Deploying VPNs", Chapter 1, Cisco Press, 22.04.2006.

[26] RFC 2808: The SecurID(r) SASL Mechanism. http://www.ietf.org/rfc/rfc2808.txt, [retrieved: May, 2013].

 ISBN: 978-1-61208-282-0