Communications for AnyPLACE: A Smart Metering Platform with Management and Control Functionalities

Dominik Henneke[1], Christian Freudenmann[5], Markus Kammerstetter[2], David Rua[4], Lukasz Wisniewski[1] and Jürgen Jasperneite[1,3]

[1]inIT – Institute Industrial IT, OWL University of Applied Sciences, 32657 Lemgo, Germany
dominik.henneke@hs-owl.de, lukasz.wisniewski@hs-owl.de, juergen.jasperneite@hs-owl.de
[2]Secure Systems Lab, Automation Systems Group, Vienna University of Technology, 1040 Vienna, Austria
[3]Fraunhofer IOSB-INA Application Center Industrial Automation, D-32657 Lemgo, Germany
[4]INESC TEC – INESC Technology and Science, 4200 Porto, Portugal
[5]Power Plus Communications AG, 68167 Mannheim, Germany

***Abstract*—Recent developments under the term Smart Grid change how users consume electricity and interact with the power grid. Smart metering and energy management are developments that transform the yet passive energy consumer to a participant that is actively involved in the energy market by using variable energy tariffs or by demand response services. But such functionality demands a platform that integrates all smart devices in the users property, connects to external services and electricity providers, and has interfaces that provide information and control to the user. AnyPLACE will develop such platform. Based on the latest legislation in the European member states, it will incorporate smart meters and create links to external service providers. Furthermore, it connects the devices in the property of the end-user in order to be able to fully monitor and control the energy consumption. This paper presents the AnyPLACE idea and the problems that are solved on the communications aspect. It provides an in-depth analysis of current European legislation in the context of smart metering and provides the requirements that need to be realized by the platform. Additionally, it proposes a strategy to create a solution that can be used in any place of Europe. The paper also incorporates the security and privacy requirements in different domains. In the end, a solution is sketched and important properties are highlighted.**

I. Introduction

The advent of the Smart Grid concept has been changing the paradigm of the electric industry, the way different stakeholders interact with the electric grid, and how different energy services can be exchanged among them. Included in those stakeholders are the consumers, which are no longer mere passive agents in the system. Instead, they are likely becoming active participants with an important role in using their flexibility in the provision of new services (ex: demand response) which can be exchanged with other stakeholders (ex: retailers or system operators); they are even expected to be capable of optimizing their energy use on their own.

The challenge in having these end-users involved in energy management is multidimensional and involves areas such as awareness, education, and empowerment. The technology has a key role in supporting these areas by providing an energy management platform that can be used in a simple manner and allow end-users to derive benefits from the optimization of energy use. It needs to collect information in a mostly automated fashion, provide easy access to information, and be capable of interacting with devices and systems.

AnyPLACE is a H2020 project that intends to implement a modular, adaptable, and cost-effective solution to support the energy management of households and similar buildings, and integrates smart metering platforms. By using the flexibility of loads and potential microgeneration systems, the objective of the project is to demonstrate the feasibility of implementing advanced monitoring and control schemes that—by including comfort preferences—allow the end-user to better manage the use of energy. To that end, the project intends to design, implement, and test hardware and software modules that when combined will produce different solutions that are capable of being continuously used by end-users in what it is expected to become a "natural" way of managing the energy use. A detailed characterization of the physical, regulatory, and market contexts from five different EU countries was carried out to evaluate the applicability of an energy management solution and how to integrate smart meters. This information was used to establish the definition of the AnyPLACE platform and the interactions between end-users, devices, and systems.

The main contributions of this work are a recent study of smart metering regulations in different European countries as well as the definition of an approach to cover all these in a single modular approach. A service-oriented approach will be presented that provides the basis for a state-of-the-art energy management and smart metering platform. Furthermore, it presents what security aspects need to be taken into account and how these can be implemented in the proposed solution.

The paper is structured as follows: Section II further details the AnyPLACE approach and supporting methodologies. Section III presents existing solutions and section IV focuses on the requirements that are put from the communications perspective—both for communications with external stakeholders as well as with appliances. Section V presents the

architecture that AnyPLACE proposes to fulfill the requirements and to implement a suitable solution. Finally, section VI concludes the paper and provides an outlook about the future activities in the project.

II. The AnyPLACE Approach

The implementation of a solution like AnyPLACE depends on a design that is suitable for controlling loads and microgeneration, integrating smart meters, and engaging end-users in exploring potential advantages in optimizing their energy use. The paradox is that the technology already allows this ambitious implementation, since a significant number of existing solutions already accomplishes parts of these features. However, a cost-effective solution that integrates all these domains is clearly missing.

The AnyPLACE approach has initially been contextualized within the Smart Grid Architecture Model (SGAM) methodology [1], where a business use case was established with interactions among different stakeholders. Different use cases such as Ancillary Services, Retail Market, and Customer Energy Management are provided to end-users, Distribution System Operators (DSOs), Transmission System Operators (TSOs), or manufacturers. Based on these findings, a set of requirements was established as part of the functional specification of the platform. Sets of functionalities were established under the groups of Energy Management, End-user Interaction, Information and Communication Technology (ICT), and Maintenance and Support.

The set of services to be supported by the AnyPLACE platform followed from the definition of high-level use cases in these groups. The energy management group defines the services Data Analytics and Energy Awareness, Tariff Selection Management, Local Energy Management, and Demand Response. Services for the end-user interaction group are Preferences and Configurations, as well as Media Presentation Management. The ICT group defines the services Local Device Management, Interaction with Stakeholders, Metering Management, Systems Integration and Management, Cloud Services, and Secure Access and Exchange. Finally, the maintenance and support group defines the services Maintenance Services, Reporting and Alarms, and Storage Management.

Based on these four types of services, functional requirements were identified which, along with the expected inputs and outputs, helped in bounding the AnyPLACE specification. This creates a component layer according to SGAM guidelines. Concerning ICT—also referred to as communications—a segmentation was introduced in order to cover the multiple interactions that are required. Requirements were defined separately for the vertical interactions with local devices and systems (ex: appliances, sensors, media devices, Heating, Ventilating and Air-Conditioning (HVAC)), meters (ex: legacy, smart), remote systems (ex: web-services, cloud), and transversely through the secure access and data exchange (ex: authentication, authorization, access control, confidentiality, protection). These interactions can be combined into external communications, with meters and remote systems, and internal communications, with local devices and systems.

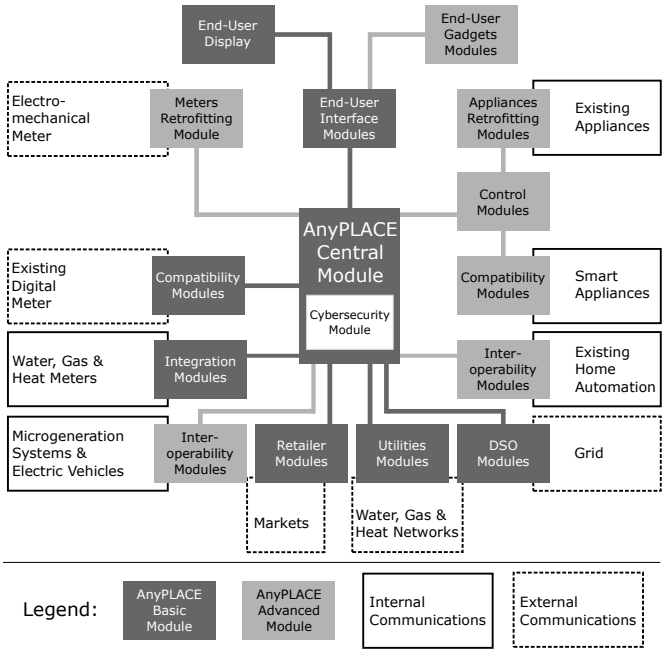

Fig. 1. Initial design of the modular architecture for AnyPLACE

In consequence of this analysis, Fig. 1 shows the proposed modular reference architecture and depicts the different modules that are to be included in the AnyPLACE solution: The AnyPLACE Central Module is the core of the architecture and provides the main functionality of the identified requirements. It is extended with basic and advanced modules, that provide the interaction with different devices and stakeholders, as well as with the end-user. The basic modules are expected to be available in all AnyPLACE installations while the advanced modules can be incorporated depending on the availability of devices in the end-users premises, services provided by independent stakeholders, or available budget for the platform. This approach permits the development of a modular and adaptable infrastructure that is likely to be suited for a large group of different end-users.

III. Related Work

Several projects already covered the areas of energy management, smart meter integration, and end-user engagement. The OPENmeter project addressed the specification of a set of open standards to be used on an Advanced Metering Infrastructure (AMI) supporting electricity, gas, waster, and heat metering [2]. The OpenNode project proposed an architecture that combines smart metering with grid automation to enable a reliable and efficient grid operation [3]. The ADDRESS project studied, developed, and validated solutions to enable an active demand and exploit its benefits [4]. The Smart City Mannheim project integrated an energy mangement tool to households and connected the households via powerline to the smart grid. This enabled customers to react on variable

prices on basis of a market place and thus participate in the stabilization of the distribution grid [5]. Energy@Home targeted the increase of energy efficiency of a house system through the information exchange related to energy usage, energy consumption, and energy tariffs between smart devices and domestic appliances [6]. Smart House/Smart Grid validated an ICT-enabled collaborative technical-commercial aggregation of smart houses to provide higher levels of energy efficiency [7]. However, all these projects either provide outdated information on e.g. smart metering—due to the latest regulations in the EU member states—or do not provide a comparable feature set.

There are already a large number of energy management systems for smart homes in the market. Qivicon, NEST, Miele@home, or Bosch SmartHome are examples for commercial solutions. OpenHAB or Eclipse SmartHome are open source alternatives. However, all these solutions are often limited to support devices of a single vendor, are not able to integrate recent smart metering technologies, and are also often expensive.

The problem of integrating different energy consuming devices to a single platform in order to enable a sophisticated energy management has been reviewed and also solved by a number works. Koß et al. propose the use of a layered Service-oriented Architecture (SoA)-based distributed architecture with open interfaces and support for plug-and-play hardware and software components [8]. They deployed and tested their development in a 'Smart Living Lab'. Irlbeck et al. presented a service-oriented reference architecture for different use-cases in the smart grid scenario [9]. Shrestha et al. proposed a method to integrate different domain-specific applications into a Internet of Things (IoT) [10]. They used the IoT standard Quantum Lifecycle Management (QLM) to abstract different domains such as smart energy, smart building, or smart industry in order to enable a communication between them. They used openHAB as example for the smart building domain and extended it with the proposed interfaces. Granzer and Kastner proposed a mapping between different technologies in the scope of building automation systems and a technological-independent data representation [11]. As example, they mapped KNX, ZigBee, and other protocols to an OPC UA representation.

There are many works and projects that already covered some of the areas that are captured by the project. However, they provide outdated information on the current state of the art in technology or regulations, are not as flexible and extensible as required, or are not directly reusable for the implementation of the project due to missing implementations or support.

IV. Communications Requirements

AnyPLACE communications consists of internal as well as external communications as depicted in Fig. 1. Internal communications is defined as the communications with devices in property of the end-user (ex: electric vehicle charging stations, private submeters). External communications on the other hand concerns the communications with actors, services, and components that are not part of the end-user property (ex: distribution system operator, meters of the meter system operator). The AnyPLACE project identifies, analyzes, and develops solutions for both sectors. As a preparation for this purpose, communications requirements were defined at a technical and technological level.

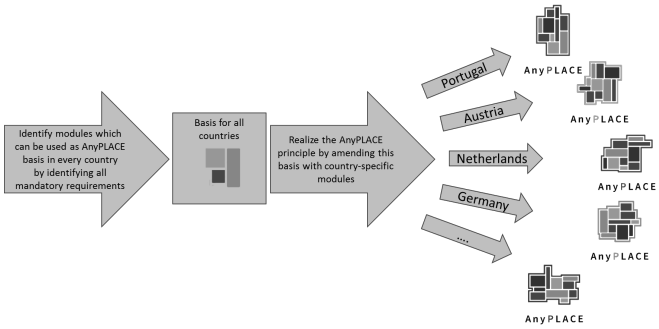

Fig. 2. Approach for the development of a European Solution

The major sources to derive those requirements are: the planned functionality, the physical context, and the regulatory context. Of those sources, the physical and regulatory context may differ from one country to another. However, due to the European context of the project, the developed solution should be able to be situated in any place within Europe. For this purpose, in order to avoid the development of different products from the very beginning, an approach is necessary to identify a common basis that can be situated in any country and may only be adapted depending on country-specific requirements.

In general, there are three approaches to achieve this: The first develops a solution that suits one country that has highly detailed mandatory communications and security requirements. Conflicting requirements of other countries are handled in modifications to derive a solution. The second approach develops a solution for every country separately and derives a common basis afterwards. The third approach combines the advantages of the other approaches and analyzes the mandatory requirements of all countries and derives a common basis from that which is then being developed as a common solution. This approach—which has been chosen for the project—is depicted in Fig. 2.

A. External Communications

Concerning external communications, the regulatory context has very different extents in different European countries. There are several documents issued by the EU that demand general requirements to provide final customers with time-specific information about their energy consumption or to ensure data privacy and data security (e.g. [12]). However, they leave plenty of room for the member countries to further specify the regulations of the technology used for the data transfer. The following section provides details of the country-

specific mandatory communications requirements in Belgium, Portugal, Netherlands, Germany, and Austria.

Belgium has not specified requirements on this topic yet. In Portugal, the EU directive is introduced via Portaria 231/2013 [13]. There are also highly detailed industry-driven standards on smart meters. As far as the requirements of an interaction between smart meters and a platform such as AnyPLACE is concerned, all Portuguese smart meters mandatorily contain an interface to be interconnected with a Home Area Network and a display. The Netherlands Technical Agreement (NTA 8130) [14], [15], as a main part of the Dutch regulations, describes the communications architecture of the Dutch smart meter environment in which the electricity meter has a communications module that serves as a gateway for other meters. This gateway needs to provide an interface where final customers can read meter data from. Additionally, it has an external interface which can only establish a connection to a central system. Authorized external market entities such as the grid operator, suppliers, or independent service providers can use this connection as proxy. This approach is similar to the German regulations [16], [17] that demands a Smart Meter Gateway (SMGW) that is placed on an electricity meter and can be connected to several meters and—among other interfaces—provides an interface to the final customer to read out meter data. Likewise to the Dutch central server, there is the Gateway Administrator (GWA), responsible to provide secure communications between the external interface of the gateway and external market entities (e.g. to provide meter data or to manage controllable devices in the final customer's premises). The communications between the gateway, meters, controllable local systems, and external market entities is specified in technological detail in respective technical guidelines [18]. A special remark can be made on the data log which is specified to enable the final customer to be aware of the data exchanged via the gateway. Austria as a final example, also demands to provide the final customer with detailed information about the usage of his or her data. Likewise to the German approach, secured and encrypted communication is demanded, although—in the Austrian set of regulations—without giving technological specifications.

The AnyPLACE solution includes and controls many critical assets such as metering data or controllable loads. Depending on the type of asset, different security measures are not only necessary but may also be mandated by EU-member states. For instance, for handling smart metering data, both the Netherlands [19] as well as Germany [16], [20] have extensive security requirements for the employed hardware, software, and communications protocols. These include strong cryptographic authentication, end-to-end security, the use of a Public Key Infrastructure (PKI), and key storage on tamper resistant smart cards. While metering data has a strong privacy focus, controllable loads are security critical as they can affect the stability of the power grid at a large scale. If an attacker manages to switch a large number of high current controllable loads (a boiler or building heating) at the same time, the sudden load change can cause critical voltage peaks outside the normal grid operating range. Potentially even amplified by the utilities' protection switches, the result of the attack could be a chain reaction leading to a blackout and physical damages in the worst case. The security design for AnyPLACE is based on a thorough analysis of the hardware, software, and communications security requirements mandated by the EU-member states for smart metering and critical infrastructures in general. Over external interfaces the solution always acts as a network client to reduce the attack surface. Any communications with external services adheres to the extensive smart metering security requirements including certificate based strong mutual authentication, end-to-end security, PKI-usage, and as key storage, key and random number generation, or signature generation and verification on a tamper resistant smart card.

B. Internal Communications

Internal communications covers the connection to devices in the customers premises. These include controllable or uncontrollable devices for power generation or consumption. Under the term 'smart home', an increasing number of devices that enter the market today are equipped with communications interfaces. But due to the diversity of existing (wired and wireless) connection technologies and a large number of competing standards, the devices are not compatible to each other. In fact, the current implementations of many vendors force users into vendor-dependent ecosystems. In order to be able to implement energy management algorithms that can visualize and control the device states, there is a need to access and control all these different technologies and protocols. These include popular wired and wireless protocols such as KNX, Wi-Fi, ZigBee, or Bluetooth, as well as a huge variety of different protocols. The challenge in creating the universal communications modules for all different technologies is to have on the one side the necessary interfaces on the hardware platform and on the other side to provide the implementations to all potential protocols of the devices that need to be supported. However, many communications details are neither publicly available nor intended to be used by a third-party.

For internal communications in AnyPLACE, the solution leverages the concepts of the strong security architecture for external communications interfaces whenever possible. Due to the vendor-specific and proprietary protocols for smart home devices, the full extent of the AnyPLACE security architecture is not applicable. Communications security can then only be realized in a best effort manner by relying on the security measures in the vendor's protocols and the utilized communication technologies. Nevertheless, the hardware and software security mechanisms as well as a user centric authorization scheme within the AnyPLACE solution can still effectively improve the overall security of these smart home devices. In addition, it is important to consider the physical communication technologies. While utilizing an insecure protocol over a wired interface to communicate with a smart home device within the user's premises just a few meters away will typically not have a considerable security impact, using the very same protocol over an unprotected wireless link is a different scenario. In this

case an attacker could easily connect or otherwise interfere with the wireless link, the smart home service, and the linked AnyPLACE services. For wireless interfaces such as Wi-Fi, ZigBee, or Bluetooth the use of integrated link-level security modes is thus highly important as well.

V. Architectual Design

The architectural design follows from the combination of the functional requirements, the regulatory mandates, and the technological properties and limitations. The following sections present different aspects for the implementation of AnyPLACE. An SoA-approach and a security concept are presented and the exemplary analysis of an existing energy management framework is carried out.

A. Service-oriented Architecture

To face the communications requirements of the external and the internal domains, the use of an SoA is aimed. Different connections and interfaces to the domain of external devices and entities are abstracted to weakly coupled services which are consumed by the energy management and user interaction parts of the project. A core aim of AnyPLACE is to achieve a working prototype in a reasonable amount of time and at an affordable price. Section III shows that already a large number of works, projects, and implementations exist that faced these problems before. Therefore, it is highly recommended to think about integrating these existing approaches into the platform.

Thus, assuming existing implementations can be reused, three different strategies were identified to realize the SoA in AnyPLACE (Fig. 3): *greenfield*, *middleware*, and *framework*. The *greenfield* approach implements the energy management platform, as well as the SoA and all required interfaces to support communications with external and internal entities. It releases a fully customized solution that fits to all requirements on the downside of being highly time consuming and lacking reusability. The *middleware* approach implements the energy management platform, but reuses the SoA of an existing (open source) framework. This framework already implements most of the communications requirements and can be extended with missing features. Therefore, the development effort is reduced and—depending on the realized architecture—the framework can be independently updated, changed, or replaced if necessary. The access from the AnyPLACE platform to the SoA of the framework can either be realized by using the Application Programming Interfaces (APIs) that are provided by the framework or are specified and implemented according to the needs of the project. The *framework* approach fully reuses an existing (open source) framework that provides the implementation platform for the energy management as well as the SoA. The framework is extended with all the functionality that is required to realize the intended solution. The main effort will be to ensure that all required functions can be implemented in the platform. As the framework already provides the communication interfaces for a large number of devices—especially from the in-building domain—only yet unsupported devices and services need to be implemented.

TABLE I
Core results of the SWOT-analysis for each approach

	greenfield	middleware	framework
Strength	flexibility	reuse	maturity
Weakness	maturity	integration	limitation
Opportunity	tailor-made	decoupling	effort
Threat	effort	design	dependency

The results of a Strengths, Weaknesses, Opportunities, and Threats (SWOT)-analysis for each approach are provided in TABLE I. While the greenfield approach provides the most flexibility and an opportunity for a tailor-made design, the maturity is limited and effort of such a solution is very high. The framework approach counteracts by providing a mature solution and reduced effort, however, the potential limitations and the introduction of a huge dependency are critical. The middleware approach reuses the advantages of the framework approach but adds additional decoupling, however, this adds an additional interface and software layer. Furthermore, despite the reduced dependence on the existing framework, architectural design changes by the maintainers will still affect this approach.

B. Security

A working security architecture for AnyPLACE relies on a user centric authorization in order to let the user define, which services are allowed to interact with each other. Considering an energy retailer's web service with variable pricing information and a controllable load within the user's premises, the user would thus set up controllable load switching as follows: Initially, the user would sign up to the energy retailer's service to exchange authentication information (i.e. certificates) and to obtain the URL of the pricing information service. The exchange itself is secured with the help of the PKI so that both the user as well as the energy retailer can be sure that each party is who it claims to be. Once the service access URL is set up in the AnyPLACE solution, it can connect to the service over the external communications interface. This connection is secured with security measures such as mutual authentication using certificates or end-to-end security and, since the AnyPLACE solution acts solely as client, the external attack surface is minimized. During setup, the user connects the pricing information service with the controllable load service. During connection setup, the user needs to explicitly authorize the information exchange between those services for the purpose of switching the load. After setup, the solution can thus automatically and securely receive energy pricing information over the external communications interface and react accordingly by controlling the controllable load withing the user's premises.

C. Review of an Existing Framework: openHAB

OpenHAB is a vendor and technology agnostic open source automation software for smart homes [21]. It provides a platform that is on the one side able to connect to various

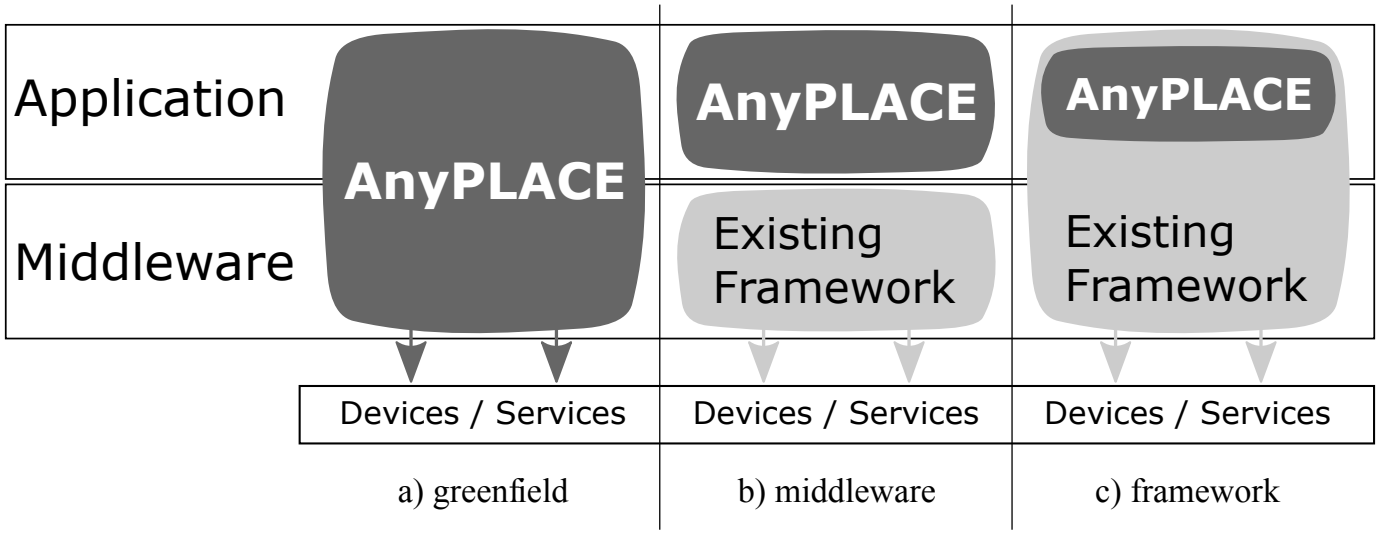

Fig. 3. Three alternatives to realize the SoA: The greenfield approach a) to implement the complete architecture. The middleware approach b) to reuse the implementations of an existing framework. The framework approach c) to extend an existing framework with the needed functionality.

smart devices from diverse manufacturers and on the other side creates automation rules to interconnect these. Its main advantage above other (commercial) smart home solutions is its openness that allows to freely create management solutions without vendor lock-in or restrictions on communication interfaces. openHAB was initially published in 2010, is still actively maintained, is backed by a large community, and is also a core part of the Eclipse SmartHome initiative.

The framework provides programmability by extending the OSGI-based platform with custom modules and also provides Domain-specific Languages (DSLs). The compatibility to external devices is integrated by *bindings* that either directly use the hardware interfaces of the platform or communicate with external gateways that provide access to other technologies. The framework already provides more than 100 bindings, including KNX, EnOcean, or Modbus. Additionally, the software provides a RESTful API that can be used to access the devices and all parameters.

Regarding the security concept of the framework: The communications security architecture for internal and external communications interfaces needs to be implemented in the openHAB protocol bindings. For each protocol, the protocol binding implementation is responsible to include the security measures in that protocol. Similar to Figure 3, a user centric authorization core could either be implemented within or on top of openHAB. In addition internal services can be used to interact with the tamper resistant smart card for functions such as key management or signature generation and verification. The solution thus leverages several internal services that can be efficiently combined to obtain a solid service oriented framework. Depending on the security configuration, protocol binding drivers could thus transparently access smart card functions to exchange and validate certificate information within their specific protocol implementation. The separation into internal services would further improve the overall software security of the solution as a successful attack on a single service does not automatically compromise the security of the entire solution. Internal services are protected from external access through conventional security measures such as firewalls and operating system security functions including permission and access control. In that regard, the solution can rely on established and widely used security mechanisms.

VI. Conclusion and Outlook

Smart metering and energy management are important topics in future energy systems. The AnyPLACE solution provides insights into a platform that integrates the domains home energy management and smart metering. This paper provides information about the current legislation in the European member states concerning smart metering—or external communications in general. There are different approaches in the communications architecture and security requirements. While Netherlands and Germany require the use of a secured intermediate gateway that collects data from connected smart meters and communicates them to the external service, other countries demand less secured and standardized approaches. Reasons for these differences are the rather superficial EU specifications that apply to such smart metering platform with control and management functionalities. While main contents such as the provision of an interface to the user and the ensured data privacy and data security are defined, the specification of technology and data transfer is left open. The development of a platform such as AnyPLACE that should be usable in all European countries is therefore challenging. However, the presented approach on how to tackle these differences shows that only slight modifications are required if the initial design considered this situation.

A lack of universal standards is also highlighted in the internal communications with devices in the end-users property. There is a large amount of communications technologies and

protocols that make it hard to build a solution that can be interconnected with all existing devices. However, there is much work already carried out to solve this problem. The paper presents an approach on how to incorporate this work in AnyPLACE. In the end, a solution is sketched, that fulfills all of the defined requirements from the communications perspective. Also, the openHAB framework has been identified as a suitable candidate to use in the implementation.

In future, the information that were gained by the analysis that was carried out and presented in this paper will be used to implement the proposed platform. A realization and test trial in real households in the rural area of Germany will show the influence on energy consumption and use of end-users while using the platform.

ACKNOWLEDGMENT

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

REFERENCES

[1] Smart Grid Coordination Group (SGCG), "Smart Grid Reference Architecture," CEN-CENELEC-ETSI, Report, November 2012.

[2] European Commission. (2008) OPEN meter – Open Public Extended Network metering. Retrieved April, 15 2016. [Online]. Available: http://cordis.europa.eu/project/rcn/101038_en.html

[3] OpenNode. (2012) The OpenNode Project. Retrieved April, 15 2016. [Online]. Available: http://opennode.atosresearch.eu/

[4] ADDRESS. (2008) ADDRESS – Active Distribution networks with full integration of Demand and distributed energy RESourceS. Retrieved April, 15 2016. [Online]. Available: http://www.addressfp7.org/

[5] MVV Energie. (2013) Modellstadt Mannheim (moma). Retrieved April, 17 2016. [Online]. Available: http://www.modellstadt-mannheim.de/

[6] Energy@home. (2016) Energy@Home. Retrieved April, 15 2016. [Online]. Available: http://www.energy-home.it/

[7] Smarthouse-Smartgrid Consortium. (2008) SmartHouse/SmartGrid. Retrieved April, 15 2016. [Online]. Available: http://www.smarthouse-smartgrid.eu/

[8] D. Koß, D. Bytschkow, P. K. Gupta, B. Schätz, F. Sellmayr, and S. Bauereiß, "Establishing a smart grid node architecture and demonstrator in an office environment using the soa approach," in *2012 International Workshop on Software Engineering for the Smart Grid (SE4SG)*, June 2012, pp. 8–14.

[9] M. Irlbeck, D. Bytschkow, G. Hackenberg, and V. Koutsoumpas, "Towards a bottom-up development of reference architectures for smart energy systems," in *2013 2nd International Workshop on Software Engineering Challenges for the Smart Grid (SE4SG)*, May 2013, pp. 9–16.

[10] N. Shrestha, S. Kubler, and K. Främling, "Standardized framework for integrating domain-specific applications into the iot," in *Future Internet of Things and Cloud (FiCloud), 2014 International Conference on*, Aug 2014, pp. 124–131.

[11] W. Granzer and W. Kastner, "Information modeling in heterogeneous building automation systems," in *Factory Communication Systems (WFCS), 2012 9th IEEE International Workshop on*, May 2012, pp. 291–300.

[12] The European Parliament and the Council of the European Union, "Directive 2012/27/eu of the european parliament and of the council," *Official Journal of the European Union*, no. 315, pp. 1–56, November 2012.

[13] Ministério da economia e do emprego, "Portaria n.º 231/2013," Ministério da economia e do emprego, Tech. Rep., 2013.

[14] Netbeheer Nederland WG DSMR, "Dutch smart meter requirements – P1 companion standard," Netbeheer Nederland, Tech. Rep., June 2015, version 5.0.1 Final.

[15] ——, "Dutch smart meter requirements – main document," Netbeheer Nederland, Tech. Rep., Mar 2014, version 4.2.2 Final.

[16] Bundesamt für Sicherheit in der Informationstechnik (BSI). (2014) Protection Profile for the Gateway of a Smart Metering System. Retrieved April, 14 2016. [Online]. Available: https://www.commoncriteriaportal.org/files/ppfiles/pp0073b_pdf.pdf

[17] Cabinet of Germany, "Entwurf eines Gesetzes zur Digitalisierung der Energiewende," Bundesregierung, Gesetzentwurf der Bundesregierung, 2015.

[18] Bundesamt für Sicherheit in der Informationstechnik (BSI), "Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems," BSI, Technische Richtlinie BSI TR-03109-1, March 2013, retrieved April, 14 2016. [Online]. Available: https://www.commoncriteriaportal.org/files/ppfiles/pp0073b_pdf.pdf

[19] Netbeheer Nederland, Privacy & Security Working Group. (2010) Privacy and security of the advanced metering infrastructure. Retrieved April, 14 2016. [Online]. Available: http://hes-standards.org/doc/SC25_WG1_N1538.pdf

[20] Bundesamt für Sicherheit in der Informationstechnik (BSI). (2013) Protection Profile for the Security Module of a Smart Metering System (Security Module PP). Retrieved April, 14 2016. [Online]. Available: https://www.commoncriteriaportal.org/files/ppfiles/pp0077b_pdf.pdf

[21] openHAB UG (haftungsbeschränkt. openhab. Retrieved April, 13 2016. [Online]. Available: http://www.openhab.org/