Privacy in Smart Metering Ecosystems

Peter Ebinger, José Luis Hernández Ramos, Panayotis Kikiras, Mario Lischka, and Alexander Wiesmaier

AGT Group (R&D), Darmstadt, Germany
{pebinger,jramos,pkikiras,mlischka,
awiesmaier}@agtinternational.com

Abstract. While smart metering is a key technology for reaching a sustainable consumption of resources, smart buildings are on their way to provide ubiquitous home automation. These technologies combine to frame a smart metering ecosystem with corresponding services and business models introducing new security challenges including privacy protection. This paper outlines a novel approach to provide customers of smart metering ecosystems with full control over their data in all areas of data collection, processing and exchange. The approach keeps the privilege model simple enough for regular users to understand how to configure their desired level of privacy. More concrete, we provide a simple, easy to use privacy dashboard that translates user input into XACML policies based on privilege modeling for this scenario. Generated XACML policies are evaluated upon receiving access requests to sensor data or actuators. Using the proposed model greatly improves user understanding and implementation of privacy rights related to smart metering ecosystems.

1 Smart Metering Ecosystem

Deployment of smart meters in many parts of the world has changed the interaction between consumers and electricity providers and enables the development of new business models [1, 23]. Smart meters communicate consumption information back to the utility for monitoring and billing purposes and may also be shipped with a gateway that communicates to local devices via an ad hoc network enabling communication for household devices with Internet services. The integration of smart meters, home automation systems, and an Internet connection enable new technological solutions. The resulting *smart metering ecosystem* may facilitate a multitude of applications and value added services (VAS). Security and privacy are a major concern in this context as these applications and services directly affect users' everyday life and may collect a substantial amount of sensitive data.

An abstract view of the stakeholders contributing to a smart metering ecosystem and their interactions is shown in Fig. 1. There are three groups of stakeholders involved in the smart metering system: *consumer*, *smart grid* and *valued added services*. In the following, we take a closer look at the stakeholders involved in the three groups.

J. Cuellar (Ed.): SmartGridSec 2012, LNCS 7823, pp. 120–131, 2013.

The *consumer* group is the link between the smart grid and value added services. The consumer is on the top of the ecosystem – consuming electricity but also value added services. They provide the most important asset of the future to the other stakeholders: user data. This includes metering data which is, for example, used for billing by the electricity provider but also additional sensor data that can be used by value added services.

The *smart grid*'s primary function is to provide electricity to the consumer. There are several players involved in this process – from the electricity producer via transmission and distribution networks to the consumer. Increasingly a number of microgeneration plants and local storage add new capabilities to the electricity grid.

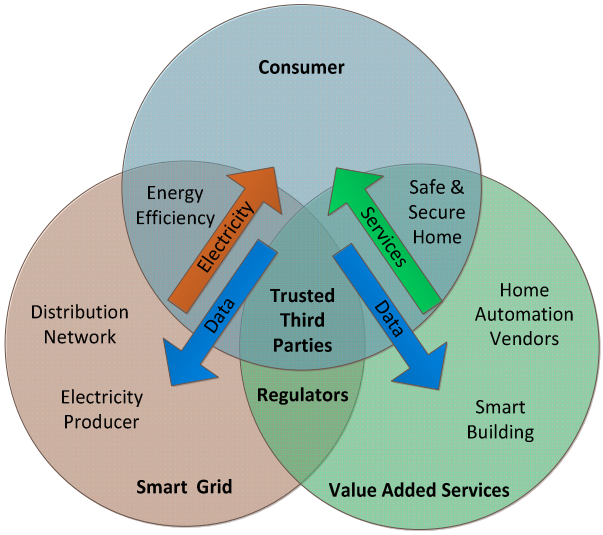

Fig. 1. Stakeholders of a Smart Metering Ecosystem

A new group of stakeholders providing *value added services* to the consumer is emerging into the ecosystem. This goes hand in hand with the evolution of homes into smart buildings where vendors of home automation systems provide the infrastructure that enables new applications. New business models are required to address the new challenges and enable new application scenarios and trusted third parties are required in such an open ecosystem to enable the trustworthy interaction of the different parties. Regulators may set the legal basis to assure that the privacy of users is sufficiently protected.

Value added services may provide an analysis of energy consumption and guidance to save energy. Such kind of services get a detailed insight on the users' behavior, thus there is an increasing interest to guideline the usage of their private data has to be addressed. While the expressiveness of existing policy language can model the required privileges, a common user could hardly specify them. Thus we have to enable the user to model the privileges in an easy way and transform them into concrete policies which are evaluated to decide on access requests.

2 Challenges and Problems Regarding Security and Privacy

This new ecosystem poses unique problems for all stakeholders. Some risks are induced by mixing Information and Communication Technology (ICT) with the existing physical infrastructure, which brings vulnerabilities from the ICT world to this field ranging from cyber-attacks on the infrastructure devices to the inappropriate use of the data collected by the smart meters.

Smart meters are expected to attract malicious hackers due to the fact that the exploitation of their vulnerabilities can immediately produce significant gains to those that employ them (e.g. by minimizing energy costs). This type of fraud already exists in this area, called meter inversion [14], but it is expected to bloom with the further adaptation of smart metering devices. Other threats deriving from the ICT world are meter bots, distributed denial-of-service attacks, usage loggers, smart meter rootkits, meter-based viruses, and other malware that will target both individuals and energy providers [17]. Threats to the VAS portion of the ecosystem are expected to follow threat patterns of cloud services, therefore risks of data loss or leakage of data, account or service hijacking and service outage must be expected and mitigations for this kind of threats must be considered.

The ability of various stakeholders of the ecosystem to collect data linkable to consumers can have significant impact to customer privacy. Energy use information can reveal users' habits and behavior (e.g. TV program you are watching [9]). Additionally, data collected by other sensors such as presence, motion, light, contact and so on can further reveal consumer's activities [18]. By performing analysis on the collected data it is possible to infer attributes such as presence or absence of an individual in the household which in turn might induce further risks. Furthermore, data collection, aggregation and storage should be visible to the user and access to the collected data must be allowed only with her or his consent to avoid conflicts with the basic rights and privacy of individuals.

In order to enable these services *new security and privacy solutions* are required. The user needs simple-to-use mechanisms that provide a transparent view on all data that is collected and processed within such an ecosystem. The user should be in perfect control of which data is collected, how it is processed and which data is exchanged with which third parties (e.g. for providing value added services).

3 Abstract Architecture

We define an abstract architecture to describe the dependencies and interactions between the components based on our experiences in the PeerEnergyCloud[1] project. The layered structure of a smart metering ecosystem is shown in Fig. 2. The device tier consists of devices that passively or actively interact with the target area (usually a building) that they are distributed across. Examples are electricity meters, motion

[1] www.peerenergycloud.de

detectors, and gas valves. The management tier consists of devices managing and coordinating the information flow from and to the device tier. While the smart metering gateway manages legal-for-trade data, the home portal manages other data and commands. The service tier consists of applications that make use of smart meters, sensors, or actuators via a gateway or portal. Examples are local power consumption analysis and neighborhood watch applications. The user tier consists of entities that make use of the services provided by the service tier. Example users are home owners and power suppliers.

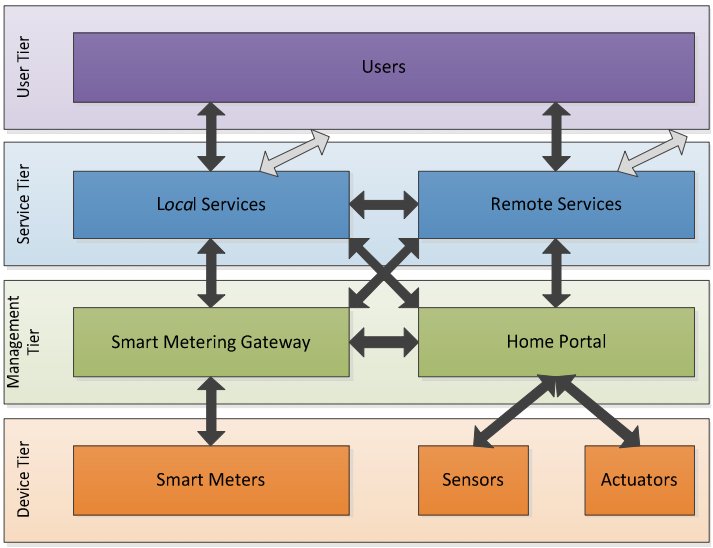

Fig. 2. Smart Metering Ecosystem Architecture

We now explain how the wireless sensor network value chain roles defined in [11] map to the architecture shown in Fig. 2 and to the stakeholders outlined in Fig. 1. An infrastructure owner owns (parts of) the deployed metering, sensor, or actuator infrastructure including any required networking infrastructure. The role *infrastructure owner*, located in the device tier (Fig. 2), maps to stakeholders in the smart grid group (Fig. 1). A content provider is located in the management tier and is the mediator between data sources and data sinks. As it provides the smart metering gateway or the home portal, it overlaps with the role infrastructure owner and also maps to stakeholders in the smart grid group. Service providers supply users with services based on content compiled by content providers. They are located in the service tier and map to stakeholders in the value added services group. The user is an entity that consumes information (ranging from raw over processed to enhanced data). Users are located in the user tier and map to stakeholders in the consumer group. Trusted third parties have access to (portions of) data for regulatory purposes or other legal uses. They are considered part of the smart metering ecosystem, but are not part

of the previously introduced tiers. Trusted third parties can be mapped to stakeholders in the consumer, smart grid, or value added services groups. Other actors in the service chain such as infrastructure equipment vendors also exist, but are out of scope of the work at hand as they never come in contact with user data. Thus, they are not reflected in the architecture and are not mapped to stakeholders.

4 User-Controlled Access to Private Sensor Data

The home portal allows us to provide data for additional services ranging from assistant living to trading energy. While these services require sampling data at a specific frequency to fulfill their service, the tendency is to get the data as detailed as possible, impacting the inhabitants' privacy. There have been approaches to extract this kind of information from the smart metering data through disaggregation of activities. It has been shown in [6] that a lower sampling rate will diminish the accuracy of the disaggregation[2]. In order to address these privacy issues we have to enable the house owner to model his privacy preferences in an easily defined manner. Under this scenario local and remote services could utilize the home portal to access data provided by sensors or to trigger actuators. It is eminent that this interface will require tight controls and granted access must be aligned with the interests of the owner or tenant of the house or apartment (called *user* in the following). While specifying complex access rights is not feasible, the main constraint is to enable a layperson, uneducated in policy language, to express the privileges regarding usage of sensor data collected in her or his household[3]. Thus an intuitive interface which enables a user to specify privileges to the desired level of detail is required. There already exists a few approaches to model policies more intuitively, but as discussed in Section 5, they are not applicable to this scenario, as they are utilizing proprietary policy languages or cryptographic approaches allowing only a limited granularity of information.

As indicated in Fig. 3 user input from the privacy dashboard is transformed into statements in a given policy language. These policy statements are then used to evaluate access requests from various applications. Actual details of this transformation are discussed in section 4.2. Generated policies are stored and utilized by the policy decision point to decide on access requests. These requests are based on intercepted data requests regarding all forms of information handled through the home portal.

In order to make our approach as open as possible XACML [21] is used as the policy decision language, as its expressiveness allows full coverage of all necessary aspects for our application scenarios.

---

[2] While the study has been done on water consumption, the underlying technology allows a transfer to electric consumption and disaggregation.

[3] At this stage we do not differentiate between different family members and their rights.

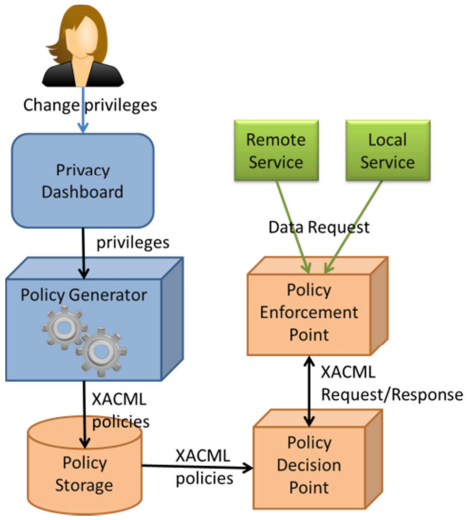

Fig. 3. Privilege Modeling

4.1 Privilege Modeling

In the current version of the privacy dashboard shown in Fig. 4 deployed sensors and devices are presented to the user in a hierarchical fashion grouped first by the sensor type (motion, temperature, etc.) and within this group according to actual sensor location. While this layout reflects logical structure according to types of information requested from each application, it can easily be modified or adapted. Future adaptation might include information regarding the requested sampling rate of the service, or the sampling rate required for a particular service level[4].

In case we have more specific settings by the user (e.g. temperature reading from the living room) the more general privileges (i.e. general temperature or any sensor) are overridden. An application may ask for current values (labeled anytime) or for the averages with a particular granularity (i.e. during the last hour, day week or month). It is implied that when access is granted for one specific granularity, access to coarser granularity is granted as well. In the above example weekly access is explicitly granted, but access to monthly overviews is also given, as the application can already calculate this value based on existing privileges.

For any registered applications the user may define exceptions to general privileges, enabling more detailed access to trustworthy ones, or restricting access to a minimum for those the user is in doubt of.

[4] The current framework does not include the exchange of these details between the home portal and the services.

4.2 Transformation into XACML Policies

According to previously defined *Privilege Modeling* the *Policy Generator* is responsible for transformation of user-defined privileges into XACML policies. In this section we describe how this entity establishes a mechanism that allows users to define access control policies in a simplistic manner without suffering any loss of expressivity provided by XACML.

Under the XACML data model [21] the definition of access control policies is based on three elements: *PolicySet*, *Policy* and *Rule*. A *PolicySet* may contain other *PolicySets* and *Policy's*, whereas a *Policy* includes a set of *Rules*, specifying an *Effect* (*Permit* or *Deny*), as a result of applying that *Rule* for a particular request. Because different *Rules* might be applicable to a certain authorization request, XACML defines *Combining Algorithms* in order to reconcile multiple decisions. The *Target* sections of these elements defines the set of *resources*, *subjects*, *actions* and *environment* to which the *PolicySet*, *Policy* or *Rule* are intended to be applied.

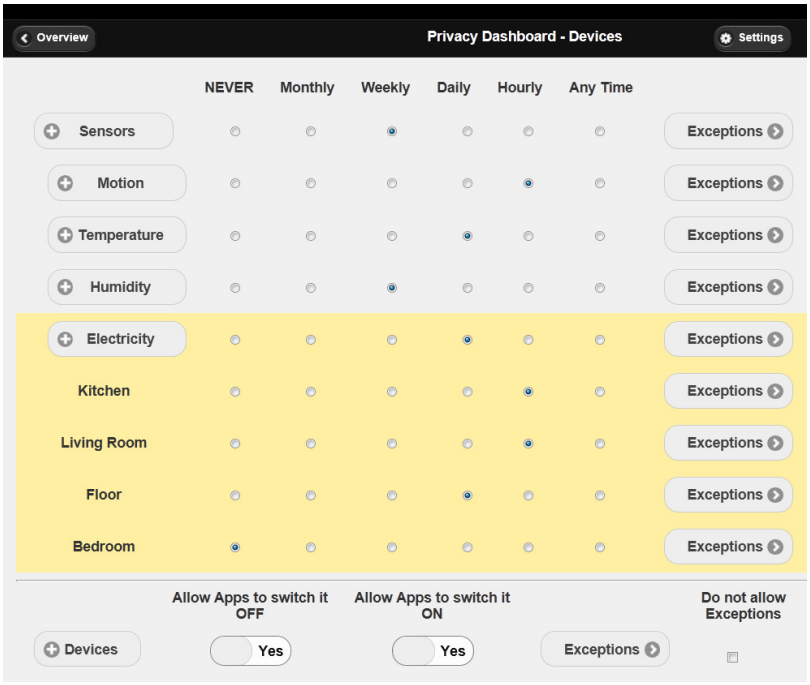

Fig. 4. Privacy Dashboard

The definition of the *Privacy Dashboard* together with the specified structure of XACML policies, favors a direct translation of the privileges model displayed to users into a machine-readable specification as sketched in Fig. 5. For the translation we assume that the set of sensors (their specific type and location) are currently fixed, but could be extended with additional or more fine grained location information at any

time. The granularity regarding the aggregated information is predefined as discussed in the previous section.

The definition of the *Privacy Dashboard* together with the specified structure of XACML policies, favors a direct translation of the privileges model displayed to users into a machine-readable specification as sketched in Fig. 5. For the translation we assume that the set of sensors (their specific type and location) are currently fixed, but could be extended with additional or more fine grained location information at any time. The granularity regarding the aggregated information is predefined as discussed in the previous section.

```
(1) PolicySet
(2)   Target: Action: sensorQuery
(3)     PolicySet
(4)     Target: Resource:  temperature/.*
(5)     Policy
(6)       Target: Resource: temperature/kitchen/.*
(7)       Rule (Effect: Permit)
(8)         Target: Subject: app1, Resource: temperature/kitchen/daily
(9)       Rule (Effect: Permit)
(10)        Target: Resource: temperature/kitchen/weekly
(11)      Rule (Effect: Deny)
(12)    Policy
(13)      Target: Resource: temperature/.*/.*
(14)      Rule (Effect: Permit
(15)        Target: Subject: app3, Resource: temperature/.*/daily
(16)      Rule (Effect: Permit)
(17)        Target: Resource: temperature/.*/monthly
(18)      Rule (Effect: Deny)
(19) PolicySet
(20)    Target: Resource:  motion/.*
(21) PolicySet
(22)    Target: Resource:  humidity/.*
(23) PolicySet
(24)    Target: Resource:  electricity/.*
(25) Policy
(26)    Target: Resource: .*/.*/.*
(27)    Rule (Effect: Permit)
(28)      Target: Subject: app1, Resource: .*/.*/monthly
(29)    Rule (Effect: Permit)
(30)      Target: Resource: .*/.*/hourly
(31)    Rule (Effect: Deny)
(32)PolicySet
```

Fig. 5. Sketch of an XACML Policy

While the top-level XACML *PolicySet* distinguishes between the different access *Action*(s), the next level distinguishes between different types of sensors modeled as resources (line 4, 10, 22, 24) and identified through regular expressions. For, a *Policy* element (line 5) is specified for each pair (sensor type, location), as well as a default *Policy* (line 12ff) in order to add or remove privileges to all sensors of the same type or in general (line 25ff). Due to the usage of the *first-applicable combining* algorithm the default Policy is only evaluated in case the previously listed detailed policy does

not match. The level of detail to which information on a specific sensor type and location is provided is expressed through *Rule* elements as well as exceptions for particular applications (line14f).

The privacy of sensor data is determined by the privileges defined by the users via the *Privacy Dashboard*. The way we have specified the XACML policy, facilitates an effective management of the access control model. In particular, when a user tries to add or remove privileges on sensor data, the schema will only be modified at the *Rule* level. As we use the *first-applicable* combining algorithm exceptions are added at the beginning of the appropriate *Policy*, and for the general privileges, new rules are put just below the exceptions.

According to the XACML structure sketched in Fig. 5, in order to consider not explicitly stated sensor types and locations, default policies have been defined. For example the default policies for temperature (line 12-18) and for all sensors (line 25-31) are shown. In cases where users want to indicate privileges for a new particular sensor type or location, no substantial changes on the schema are required. These situations can be addressed by specifying new *PolicySet* and *Policy* elements on the predefined model.

5 Related Work

In this section we give an overview on related work describing smart metering ecosystems and on authorization mechanisms proposed in the literature that may be used in such scenarios.

The European Network and Information Security Agency (ENISA) provides in [7] ten recommendations on smart grid cyber security. The recommendations are directed to the European Commission, the EU member states, and the private sector and aim at "improving current initiatives, enhancing co-operation, raising awareness, developing new measures and good practices, and reducing barriers to information sharing".

The German Federal Office for Information Security (BSI) is working on a family of technical directives on smart energy [3]. The documents define the requirements on the functionality, interoperability, and security which the components of smart metering systems have to fulfill. Additionally, the BSI works on respective Common Criteria Protection Profiles for the "Gateway of a Smart Metering System" [4] and for the "Security Module of a Smart Metering System" [5].

The conceptual reference model for smart grid information networks provided by NIST [20] covers a broader scope than this work but also pictures the *customer* (consumer), the end user of electricity, as the corner stone of the ecosystem. Several smart grid domains and actors are distinguished. The consumer interacts with the other actors of the ecosystem using two interfaces: a direct connection to the *smart grid* electricity provider and an additional interface via the Internet or some other e-Business platform to *service providers (value added services)*.

The role of smart meters, the architecture of smart meter ecosystems and related security and business implications is analyzed in [10]. Their focus is on the interaction of energy consumers and producers and how smart metering

infrastructures enable proactive and quick reaction and adaption. They describe the ecosystem as a highly distributed service oriented infrastructure where providers and consumers heavily interact.

An advanced metering ecosystem is described in [19] connecting smart appliances locally in a wireless HAN (Home Area Network) and communicating to the utility through a smart metering gateway via a WAN (Wide Area Network), e.g. the Internet. However, they focus on smart grid aspects only (energy consumption, micro-generation and demand side management) and do not consider the integration with value added services such as advanced home automation systems.

A framework which enables the user to enforce her or his privacy obligations is presented in [13], but is limited to general metering information, not including additional sensors. Additionally the authors utilize a proprietary language [14] to express the privileges. In [16] the metering information is encrypted asymmetrically in multiple time granularities and access is granted by providing the responding key. Another cryptographic approach to control the access to smart metering is presented in [2], which controls the access to the data, but could not include further obligations. The proposal presented in [80] introduces an approach to improve the usability of XACML; the user specifies different diagrams which are converted into XACML policies. The same issue is also discussed in [22], but focuses on a usable definition of conditions. The Smart Home is also controlled via XACML in [12] as well, but they limited themselves to the members and guests of the household controlling particular devices and do not really consider external services.

6 Conclusion and Future Work

This paper presents a smart grid ecosystem which already exists today. Our analysis identifies privacy as one of the major concerns for the wide adaptation of a smart grid by users. To further this direction a framework for enabling privacy based on XACML is presented. Our approach is based on the belief that these kinds of devices are soon going to be considered as an integral part of everyday life for each and every household and therefore must provide an easy to use and understand interface; even for those which happen to be not computer literate. Future research in this area will address automated mechanisms for transitioning privacy between similar applications, methods for handling privacy rules in the presence of multiple inhabitants in a home and automated recommendation mechanisms of privacy policies for new applications based on a user's decision input history. First experiences with the described *Privacy Dashboard* will be gathered during a field trial in the upcoming month, which will provide us with data regarding the actual energy usage and the information provided to applications. In addition home owners' settings regarding their privacy can be analyzed.

Acknowledgement. This work was partially funded by the BMWi (Federal Ministry of Economics and Technology) based on a decision of the German Bundestag (the national parliament of the Federal Republic of Germany).

References

1. Altmann, M., Schmidt, P., Landinger, H., Michalski, J., Brenninkmeijer, A., Buscke, I., Trucco, P., Barquín, J.: Effect of smart metering on electricity prices. Study for the European Parliament (2011)
2. Bohli, J.-M., Sorge, C., Ugus, O.: A Privacy Model for Smart Metering. In: 2010 IEEE International Conference on Communications Workshops, pp. 1–5 (2010)
3. BSI, TR-03109 Smart Energy, https://www.bsi.bund.de/DE/Themen/SmartMeter/TechnRichtlinie/TR_node.html
4. BSI, Protection Profile for the Gateway of a Smart Metering System, https://www.bsi.bund.de/DE/Themen/SmartMeter/Schutzprofil_Gateway/schutzprofil_smart_meter_gateway_node.html
5. BSI, Protection Profile for the Security Module of a Smart Metering System, https://www.bsi.bund.de/DE/Themen/SmartMeter/Schutzprofil_Security/security_module_node.html
6. Chen, F., Dai, J., Wang, B., Sahu, S., Naphade, M., Lu, C.-T.: Activity analysis based on low sample rate smart meters. In: Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, KDD 2011, pp. 240–248 (2011)
7. ENISA, Smart Grid Security, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ENISA-smart-grid-security-recommendations
8. Giordano, M., Polese, G., Scanniello, G., Tortora, G.: A System For Visual Role-Based Policy Modelling. In: International Journal of Visual Languages & Computing, vol. 20(1), pp. 41–64. Elsevier (February 2010), doi:10.1016/j.jvlc.2009.11.002
9. Greveler, U., Justus, B.: Multimedia Content Identification Through Smart Meter Power Usage Profiles. In: Computers, Privacy & Data Protection CPDP, Brussels, Belgium (2012)
10. Karnouskos, S., Terzidis, O., Karnouskos, P.: An Advanced Metering Infrastructure for Future Energy Networks. In: Proceedings of International Conference on New Technologies, Mobility and Security, pp. 597–606. Springer, Paris (2007)
11. Kikiras, P.K., Drakoulis, D.K., Dres, D.A., Stamoulis, G.I.: Wireless Sensor Networks: Business Models and Market Issues. In: 6th Conference on Telecommunication Techno-Economics, June 14-15, pp. 1–5 (2007)
12. Kim, J.E., Boulos, G., Yackovich, J., Barth, T., Beckel, C., Mosse, D.: Seamless Integration of Heterogeneous Devices and Access Control in Smart Homes. In: Eighth International Conference on Intelligent Environments, pp. 206–213 (June 2012)
13. Kumari, P., Kelbert, F., Pretschner, A.: Data protection in heterogeneous distributed systems: A smart meter example. In: Dependable Software for Critical Infrastructure (2011)
14. Kumari, P., Pretschner, A., Peschla, J., Kuhn, J.-M.: Distributed data usage control for web applications: a social network implementation. In: ACM Conference on Data and Application Security and Privacy (CODASPY), pp. 85–96 (2011)
15. Khurana, H., Hadley, M., Lu, N., Frincke, D.: Smart-Grid Security Issues. IEEE Security and Privacy (January/February 2010)
16. Lin, H.-Y., Shen, S.-T., Lin, B.-S.P.: A Privacy Preserving Smart Metering System Supporting Multiple Time Granularities. In: IEEE Sixth International Conference on Software Security and Reliability Companion, pp. 119–126 (June 2012)

17. McDaniel, P., McLaughlin, S.: Security and Privacy Challenges in the Smart Grid. IEEE Security and Privacy (May/June 2009)
18. Molina-Markham, A., Shenoy, P., Fu, K., Cecchet, E., Irwin, D.: Private memoirs of a smart meter. In: Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building, BuildSys 2010 (2012)
19. Mohit, A.: Advanced Metering: ecosystem, security threats and counter measures. In: Proceedings of International Conference on Roadmap for Smart Grid, Bangalore, India (2010)
20. NIST, Office of the National Coordinator for Smart Grid Interoperability, Engineering Laboratory in collaboration with Physical Measurement Laboratory and Information Technology Laboratory. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0. National Institute of Standards and Technology (2012)
21. Moses, T. (ed.): OASIS, eXtensible Access Control Markup Language 2 (XACML) (February 2005)
22. Stepien, B., Felty, A., Matwin, S.: A Non-technical User-Oriented Display Notation for XACML Conditions. In: Babin, G., Kropf, P., Weiss, M. (eds.) MCETECH 2009. LNBIP, vol. 26, pp. 53–64. Springer, Heidelberg (2009)
23. Torriti, J.: Price-based demand side management: Assessing the impacts of time-of-use tariffs on residential electricity demand and peak shifting in Northern Italy. In: Energy, pp. 576–583. Elsevier (2012)