Chapter 3
Computer Security Anchors in Smart Grids: The Smart Metering Scenario and Challenges

Alessandro Barenghi, Luca Breveglieri, Mariagrazia Fugini, and Gerardo Pelosi

Abstract The modern energy distribution grid is increasingly responsible for extensive self-monitoring and load balancing, together with prompt failure response and small energy producer integration. In this scenario, where the grid doubles as a data transmission grid, commonly named smart grid, new information security challenges arise. In particular, providing confidential data transmission, privacy preserving metering and authentication for the metering software, emerge as key issues. In this chapter we will provide an overview of the security challenges of the smart metering scenario, highlighting both the security services to be guaranteed and their actors, and the ongoing standardization activities.

3.1 Introduction

In the latest years, social and policy changes have been driving the need for a reconfiguration of the current power grid, leading towards the integration of information and communication technologies (ICT) within the traditional energy distribution systems. The transformation of the power grid from a mostly unidirectional, centralized and hierarchical organization, to a distributed, networked and automated energy value chain, in turn spurred the need to integrate its management across a broad spectrum of heterogeneous business and operation domains, involving multiple enterprises and customers coming from different industries.

Smart meters, sensors, and analytics tools enable users to manage and control the energy usage in individual networked appliances as well as to automatically monitor the health state of the power grid, pinpoint outages as quickly as possible, and remotely assess the entity of eventual damages to grid assets, thus providing the grounds to locate and isolate the failure while maintenance teams are dispatched. Moreover, the integration of ICT enables energy and utility companies to better

A. Barenghi (✉) • L. Breveglieri • M. Fugini • G. Pelosi
Politecnico di Milano, Dipartimento di Elettronica, Informazione e Bioingegneria (DEIB), Piazza L. da Vinci, 32, 20133, Milan, Italy
e-mail: alessandro.barenghi@polimi.it; luca.breveglieri@polimi.it; mariagrazia.fugini@polimi.it; gerardo.pelosi@polimi.it

B. Candaele et al. (eds.), *Trusted Computing for Embedded Systems*,
DOI 10.1007/978-3-319-09420-5_3

evaluate the entity of power demand, possibly in near real-time, so that the delivery and independent production integration strategies may yield higher efficiencies altogether [12]. Beyond the application of traditional information-technology (IT) security mechanisms (such as authentication, secure protocols, and intrusion detection/response systems) together with proper security engineering processes, cyber-security in the smart-grid also faces novel challenges. In fact, the IT security approaches have to be reconciled with the traditional plant safety methodologies found in industrial control systems. This requires guaranteeing the stability of control systems, which may be disturbed by malicious activities. At the same time, IT security must take into account the real-time and analog nature of the grid and adapt the risk management by providing graceful degradation as opposed to a sudden, disastrous failure when under attack. The interconnection with other systems such as buildings and home networks also poses significant challenges in terms of consumer trust and the utilities' ability to manage encryption keys as well as the compliance with authorization policies satisfying the requirements of involved parties.

3.2 The Smart Metering Scenario

Smart meters are among the core components supposed to help transforming the energy delivery network into a two-way information system. They automatically measure the electric energy consumption of any end-consumer system (e.g., a single house, an enterprise, or even a whole urban block), and transmit the collected data to the utility provider, which in turn will automatically bill the consumer. They also take care of measuring a few technical parameters for the provider to balance the load in the power grid, and they disconnect and reconnect the consumer for either contract-related reasons (i.e., unfulfilled bill payments) or technical safety reasons (such as large power surges on the grid). Moreover, the same information can be used to manage emergencies and cope with grid faults, as well as to generate reports and statistics. Finally, as the main component of a two-way information system, a smart meter can notify pricing changes to final customers; they in turn will be able to automate the use of that heavy-load appliances such as cars and dishwashers work when the energy is cheapest. The automatic management of the utilities can be extended by means of smart metering and accounting, also to other commodity goods such as gas and water, through employing intelligent meters provided with a convenient data line to transmit the collected information.

Among different data connections, the one most suited for smart meters is performed via power line communications. A power line connection distributes electric power and data together, using the existing electric power grid to this purpose. It is characterized by having a reliability higher than that of the recent wireless communication technologies like the WiMAX [13] and GPRS/UMTS protocols, as well as by providing capillary access to all the households in a manner very similar to the common public switched telephone network or the local area network technologies.

Typically, a group of power meters, acting as data gateways, are connected to a concentrator, which can be conveniently placed within a mid to low voltage step-down substation. A low data rate, and an energy efficient wireless connection, most likely based on ZigBee [28], can be used to provide connectivity locally among nearby meters (e.g., those placed in a home or a building), which do not have a direct power line connection, such as the ones measuring non-electric goods like gas and water. For all such meters, the electric power meter works as a gateway to the power line connection.

At an intermediate level, the concentrators are connected to both the power grid and to an IP-based network (e.g., the global internet) in order to act as a data bridge to and from power lines. The electric power meter is able to communicate with the concentrator via the power line connection, and eventually the concentrator can communicate with the provider via a data network. Groups of distributors and providers can work in a Virtual Organization mode, e.g., they may share services and customers.

3.2.1 Architectural Reference: Actors and Services

Smart Metering involves four different actors: provider, distributor, consumer and meter. The first three roles, shown in Fig. 3.1, are identified through the following labels [8]: Energy Service Provider (ESP), Distribution Service Operator (DSO), and Final Customer (FC).

The ESP generates electricity from renewable and non-renewable energy sources in bulk quantities, and supplies it to the power distribution network. These sources are usually classified as: *renewable, variable sources*, such as solar and wind; or

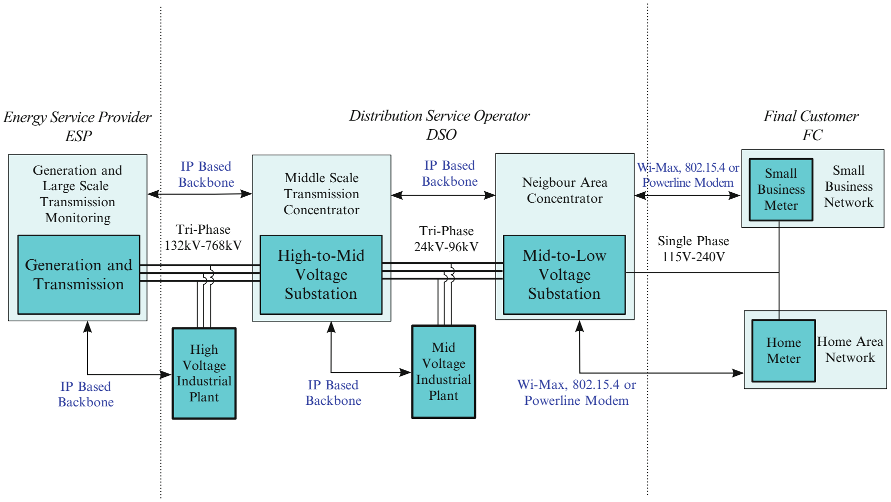
Energy Service Provider
ESP
Distribution Service Operator
DSO
Final Customer
FC
Generation and Large Scale Transmission Monitoring
Generation and Transmission
IP Based Backbone
Middle Scale Transmission Concentrator
High-to-Mid Voltage Substation
IP Based Backbone
Neigbour Area Concentrator
Mid-to-Low Voltage Substation
Wi-Max, 802.15.4 or Powerline Modem
Small Business Meter
Small Business Network
Tri-Phase 132kV-768kV
Tri-Phase 24kV-96kV
Single Phase 115V-240V
High Voltage Industrial Plant
Mid Voltage Industrial Plant
IP Based Backbone
IP Based Backbone
Wi-Max, 802.15.4 or Powerline Modem
Home Meter
Home Area Network

Fig. 3.1 Layered architecture of actors, components and communication in the power grid [1]

renewable, non-variable, such as hydroelectric, biomass, geothermal and pump storage; or non-renewable, non-variable, such as nuclear, coal and gas. The DSO, which may be the same entity as the ESP, manages (acquires and uses) metering data from the power grid. Metering data can be of two types: *consumption data*, namely the consumption of a resource (e.g., electric power) used for billing, and *technical data*, namely technical information used for power grid management, with the purpose of balancing the energy levels, of avoiding or smoothing load peaks, and of disconnecting and reconnecting customers and providers. The DSO uses consumption data for payments/billing, and for formulating custom billing plans and contracts with the "fidelized" FC (private or enterprise). It monitors and controls the status of the access points and bridges, or concentrators, through the acquisition of technical data about the meter statuses (e.g., enabled, disabled or faulty). It also manages emergencies, generates reports on consumptions based on consumption data about groups of consumers, and, in general, it performs measurements. It controls the functionalities of the meters to check if they are operative, and it is also able to send maintenance commands like "change billing contract", "connect" and "disconnect". Consumption data may also be used to generate reports and statistics, so generating consumption profiles (e.g., for certain user classes). Since a DSO is a specialization of an ESP, it can perform also energy-related operations, possibly on a smaller scale. For example, to satisfy legal constraints on the quotas of distributed energy that are derived from renewable sources, the DSO can select groups of FCs to buy renewable-energy credits and manage the "last-mile" infrastructure needed to collect the electricity into the existing power grid.

The FC is regarded in conjunction with the meter installed at his facility. He does not directly access any kind of data, as he can subscribe/unsubscribe supply contracts and require periodic reports about his consumption. Indirectly he sends measurements through the meters and receives billings. The FC consumption can also be profiled to offer him the most suitable contract. However, customer profiling should be done carefully, as it has been proven that profiling the consumptions of a household with a high time precision allows one to infer whether specific house appliances were active at a certain time. This information can also be exploited to infer the habits of the customer, thus representing a possible breach of his privacy. For these reasons, customer profiling should be limited to a time scale loose enough to prevent the leakage of private information.

The meter is the smart device used for the measurement of consumptions at local sites. It periodically sends consumption and technical data to the DSO. Consumption data are used for billing and technical data are used for load balancing. It can be connected or disconnected to/from the power line; it signals its operation and its faults to the DSO. It communicates over a secure channel with the DSO using symmetric cryptography, time-stamps and signature, in order to authenticate the DSO, and get authenticated.

A refinement of smart metering is that an FC may act as a local Provider of some resource type, usually electric power, e.g., through photovoltaic power generation. In this case he will have some of the provider/distribution services, to an extent limited by the small scale of his resource generation capability.

3.3 Security and Privacy Challenges

The design and deployment of smart meters raises several serious security and privacy issues, with different social and regulation concerns [1, 8].

A particular matter of interest for industry representatives and associations lies in the identification, assessment, and prioritization of the risks due to the potential frauds made possible by the deployment of devices with a security vulnerability [3, 17]. Indeed, if meter readings can be manipulated, either by returning false readings from credit meters or by forging authorization messages to prepayment meters, this could lead to substantial economic losses [15]. Thus, the minimization, monitoring, and control of the probability and/or impact of such unfortunate events is of great interest. In addition, at the level of the energy grid distribution, the presence of a remote off switch in all electricity meters can lead to a strategic vulnerability with respect to a capable cyber-adversary [18].

Considering the equipment suppliers, the main observation focuses on the excessive technical regulation sprung from the smart grid adoption, which threatens to drive up equipment costs in exchange for a small benefit [20, 23]. On the one side, the challenge of over-regulation leads to pessimism about the prospect of fixing security by mandating standards coming from a single authority. Moreover, the lack of universal standards for communications between meters and appliances might prevent the benefits of demand reduction being realized, as well as prevent reducing interoperability and competition [14, 25].

At the jurisdictional and organizational levels, it is possible to spot severe conflicts of interest. Indeed, the main goal of the governments is to cut energy use, which they hope to achieve by making energy use more salient to the consumers, while in most countries the meters will be controlled by energy retailers who want to maximize sales and who depend on pricing confusion. Meanwhile, the competition authorities should worry about whether giving energy retailers vast amounts of data about the customers, will adversely impact competition via increased lock-in [7, 16].

Finally, from the point of view of privacy activists, the main concern on the wide adoption of smart metering technology relates to the amount of sensitive personal information about the household usage that could be disclosed to principals able to access fine-grained consumption data [19, 22].

3.3.1 Security Engineering Requirements

From an engineering perspective, the security requirements for smart metering systems can be defined in terms of the three fundamental properties warranted to the data by secure systems: *confidentiality*, *integrity* and *authentication*. *Confidentiality* implies that a data stream, being sent from an actor to another one, should be readable only by the actors involved in the communication, and should not be eavesdropped by anyone else. This property can be warranted by means of tamper proof communication endpoints, to avoid the insertion of eavesdropper devices, and through employing symmetric cryptography to avoid possible eavesdropping on the communication mean. *Integrity* concerns the need for the transmitted data to be delivered to the recipient in whole and unmodified. Integrity may be provided via a tamper evidence mechanism, such as a message digest, coupled with an on-failure re-transmission protocol. In order to properly warrant integrity, the message digest should change radically even when parts as small as a single bit of the transmitted message are changed, and it should be computationally unfeasible to forge a message with a valid digest, different from the original one. *Authentication* concerns the possibility of identifying either the author of a data block or, analogously, of finding the identity of the other endpoint of a communication. The most common means to enforce authenticated communications and to authenticate data is to employ asymmetric key cryptography coupled with a Public Key Infrastructure (PKI) able to certify the authenticity of the public key. Through these means it is possible to provide a secure, mutually authenticated communication between two entities, or to digitally sign data and applications, so that their authorship is undeniably traceable.

The aforementioned properties provide guidelines on how the various smart grid actors securely communicate over a channel, and how they store information in a database (where it exists – typically at a provider site). Long-term data storage ought to be restricted to the provider only. The energy provider is considered to be a trusted authority, able to keep its own perimeter free from attacks. Security issues may arise when considering inter-provider adversarial relations, where a provider may cheat spoofing the others' identity to obtain economic gains. However, since the providers' reputation is effectively a company asset, such threats are unlikely to get transformed into practical attack actions. As the providers should be able to intercommunicate between themselves, a proper structure must be deployed to render the asymmetric key infrastructure interoperable among all of them. To this end, either a common PKI should be established for all of them, or each energy provider should accept certificates signed by the others. Analogously, the DSO should be regarded as a trusted entity. Since it is difficult to access the power distribution structures, the security threats concerning the tampering with their metering and information concentration infrastructure, receive implicit mitigation by the safety measures included in the step-down power stations where they are placed. On the other hand, since the communication with the power meters happens through the common low-voltage power line, such a connection has to be secured properly. Basically the threats to a DSO are related to network attacks against the flow of data from meters and towards upper levels: user impersonation, rogue server hijacking the traffic, and denials of service caused by artificial message floods. This threat class is the one commonly associated with the security issues of communication and application network protocols. Most of the threats are on the consumer side. The consumer may in fact try to lead an attack against the meters. Typically such attacks are of the following types: physical tampering, side-channel analysis, network attacks against the flow of data towards upper levels, user impersonation, and connection hijacking. Also, eavesdropping attacks may cause privacy loss in case a customer is able to gain information regarding the behavior of others. Authentication must be provided for the meters that have the ability to detach the consumer from the energy-providing grid, in order to prevent the unauthorized detachment of a single consumer or even a large scale intentional blackout targeted to cause massive disruption. Data collected from consumers should be aggregated for statistical purposes only, with no access to individual records in order to prevent fine grained privacy leakage from consumer profiling.

The aforementioned threats may be the result of a direct attack on the DSO infrastructure or, quite more likely, of a manipulation of the metering devices. In this respect, it is fundamental for the DSO to design and deploy secure meters that effectively hinder any possible malicious action by either outsiders or regular line subscribers. This goal can be achieved in two ways: either the DSO considers its own meter as a closed system where no changes to the running software (other than maintenance updates) are made, or the DSO employs the meter as an open system, allowing the customization of particular features by the line subscriber, via ad-hoc designed applications.

The first model assumes that the meter is realized as a closed embedded system, and deals with the confidentiality issues relying only on a shared secret with the DSO, which is embedded at manufacturing time. This in turn implies that the security margin provided by the infrastructure is based on the use of symmetric ciphers in order to wholly encrypt all the communications, thus providing complete confidentiality. The software maintenance updates are sent in encrypted form employing the same shared secret, without the burden of a complete PKI.

The alternative system implies that the owner of the meters is willing to run foreign, albeit certified, software on his own devices. In order to avoid the introduction of ad-hoc malware similar to recent SCADA-oriented viruses aimed at altering the measurements and/or the billing features, it is thus mandatory to employ a secure authentication infrastructure for the programs. This fully authenticated chain of trust must thus start providing authenticity warranties on the software components from the first phases of the boot, throughout the whole working cycle of the system. As this infrastructure is designed to foster collaboration and interoperability among the software produced by different meter manufacturers and smart grid stakeholders, it would be a welcome development to design common standards and criteria to provide a common platform on which to develop.

Similar efforts have already been born, and grown to a mature state for general-purpose computing: a known instance of such a consortium is the Trusted Computing Group (TCG) [26], which has built common grounds for personal computing endowed with a secure boot and chain-of-trust, realized through a specifically designed secure hardware module.

Analogously to the security issues tackled for the software, it is equally important to address hardware security issues. As a first step, the hardware components involved in a trusted system should be able to mutually authenticate, in order to avoid the insertion of rogue chips, or the bypass of critical validation components. As this is a common practice in unprotected systems, this threat should be properly addressed, as a hardware security breach results in immediate loss of trust for the whole stack of software applications running on it. These concerns can be addressed via properly designed secure hardware modules, employing cryptographically strong primitives and tamper resistant enclosures.

In addition to the choice of the primitives and the enclosure design, another fundamental aspect to be addressed is to design side-channel attack resistant hardware, since this whole class of attacks is able to breach the security of a device without the need to interfere with its own tamper proof perimeter.

3.4 System Services

In the following tables, we will list the services provided by the various identified actors of the power grid. Security-related services are in italics. The “data” label refers to both Consumption and Technical data, unless differently specified. Services are reported in verb-noun form.

Table 3.1 reports the services related to the Meter actor, Table 3.2 those of the FC, Table 3.3 those of the DSO and Table 3.4 those of the ESP.

As reported in Table 3.1, the *Basic Meter* performs secure actions to manage data confidentiality during the transmission to the DSO. The complementary part to providing the required security margin of the meter actor is warranted by the tamper

Table 3.1 Meter actor and related services

Basic meter	Advanced meter
Compute and transmit billing data	Same services as basic meter and router
Compute and transmit consumption data	Programmability (e.g., upload certified applications)
Profile consumptions	*Trusted computing base – TCB or Trusted Execution Environment*
Report consumption and billing data to FC locally or to DSO/ESP remotely	
Manage data confidentiality, integrity and authentication (for data completeness, correctness and integrity)	
Ensure tamper-evidence and tamper resistance hardware	
Initialize crypto keys and/or certificates	

Table 3.2 Final customer services

FC services
Open/close the utility provisioning contract
Configure the home network (add/remove program, start-up/shut-down appliances)
Request a report to the meter (basic billing or network status or appliance status and consumption)

Table 3.3 DSO actor and related services

Single consumer or group (e.g., those living in a city area)	Group of appliances (group of appliances of the same type)
Measure	Report consumptions by consumer or typology (e.g., private user, company, department store, appliance)
Profile load	Control appliances (hours, times, tariffs, etc.) with policy to solve conflicts with FC
Report consumers' groups	*Initialize crypto-keys and/or certificates*
Aggregate data for profiling	
Control meter (e.g., diagnosis)	
Ensure tamper-evidence and tamper resistance hardware	
Manage confidentiality, authentication, and integrity of the data received from and sent to meters	
Manage the privacy of profile (aggregated) data	
Initialize crypto-keys and/or certificates	

Table 3.4 ESP actor and related services

Normal operation on the provider side	Normal operation on the consumer side
Manage power or resource in the grid	As the meter in a basic mode
Bill the FC	
Manage or use a PKI	

proof encasing, which can be endowed with breach detection sensors. Moreover, the secret keys employed for the communication should be properly stored in a volatile memory, which is erased upon intrusion into the meter box. In addition to the tamper proof casing and secure storage of the keys, the meter should also be designed in such a way that it is not possible to obtain the secret keys via measuring environmental parameters and exploiting the measures to conduct side channel analyses.

The metering device may be conveniently designed with extended functions to stream different types of multimedia contents inside a building, as well as to run custom programs provided by third parties [2]. To this end, as shown in Table 3.1, the resulting *Advanced Meter* should also include a full-trusted computing base compliant system [24]. Indeed, the possibility of adding custom programs besides the ones needed to securely perform the basic metering functions, implies that it is not possible to perform a building-time certification of the programs run on the device. Thus, the inclusion of a computing base able to validate the execution of trusted applications is justified by the offered programmability services.

The FC is able to access services via the facilities exposed from the smart meter. In particular, since the smart meter is running trusted software from the DSO and the ESP, the client can safely update the state of a provisioning contract without the need for extra paperwork. Moreover, in an advanced smart meter, the FC is also able to poll the meter in order to understand the distribution per-appliance of the power consumption of his house. Another service performable, thanks to the ability of the meter to communicate with other appliances, is to schedule the operation of power demanding appliances in time zones when the cost of the energy is lower, such as night-time.

The DSO will provide to the meter, and thus to the FC, the backend for all the services mentioned before. Consequentially, it should be able to perform periodic diagnostic operations on the transmission and distribution lines, employing the technical data collected by the meter in order to diagnose faulty or dissipating lines. Moreover, it should be able to propagate the consumption messages to the ESP in charge of billing a specific customer, thus providing data transport support for it. In addition to this, the DSO should be in charge of initializing all the key pairs employed to encrypt the technical messages to and from the final customers, the integrity of which must be warranted, lest they cheat on the payments. The DSO will also be employing the coalesced consumption data in order to avoid service interruptions due to peak requests by the FCs.

The ESP, similarly to the FC, may offer its services only through the support infrastructure provided by the DSOs, since DSOs ultimately act as data collectors and transporters. Normally, the behavior of the ESP only takes care of the billing and contract stipulation activities. During these activities, it may be required to set up an ESP-bound PKI in order to be able to digitally sign invoices for the final customer.

3.5 Standardization Activities and Related works

In this section we will recap the ongoing standardization efforts concerning the information security in smart grids. The National Institute of Standards and Technology (NIST) has developed security guidelines and a model of the power grid infrastructure for the US [25], which defines interfaces and implementation strategies for the smart power grid.

Analogously, the Zigbee Alliance [28] has now available a full-fledged wireless network solution, which has been successfully deployed in the US and can be used for both infra-meter and meter-to-DSO communications. As one of its defining features, ZigBee provides facilities for carrying out secure communications, protecting the establishment and the transport of cryptographic keys, and enciphering communications and controlling devices. It builds on the basic security framework defined in IEEE 802.15.4. This part of the architecture relies on the correct management of cryptographic keys and the correct implementation of methods and security policies.

The HomePlug Alliance [11], Wi-Fi Alliance [27], HomeGrid Forum [10] and ZigBee Alliance [28] have agreed to create a Consortium called Smart Energy Profile version 2.0 (SEP 2) [5] to enhance the interoperability among the standards and products of many organizations, whose technologies support communications over IP.

The PoweRline Intelligent Metering Evolution (PRIME) is an initiative driven by Iberdrola, the spanish DSO, for: "the definition and testing of a new public, open and non-proprietary communication architecture that supports remote meter processing functionalities" [21]. Its security proposal addresses security at low level through providing confidentiality, authentication and data integrity at the Medium Access Control (MAC) of the communicational architecture. Several security profiles are provided to deal with the different requirements of several types of networks. Confidentiality is guaranteed by encryption and from the fact that the encryption key is kept secret. Authentication is guaranteed by the fact that each node has its own secret key known only by the node itself. Data integrity is guaranteed by the fact that the CRC of the data payload of the communication is encrypted.

Individual EU Countries have begun to standardize common guidelines for tamper proof electronic devices, able to warrant the level of physical security required by meters. For example, the German authority (Bundesamt fur Sicherheit in der Informationstechnik – BSI) has released a dedicated guideline document for tamper proof smart meters [4]. The EU has instituted a task force aimed at analyzing and building recommendations for the future of the smart grid, and has released explicit guidelines regarding data protection and security in [8]. The open challenges related to the issues of privacy management and metering data aggregation are presented in [9]. In [19] the authors highlight privacy-related threats of smart metering and propose an infrastructure for secure measurements, which relies on trusted components outside of the meter. The authors in [22] propose a protocol that uses commitments and zero-knowledge proofs to privately derive and prove the correctness of bills, but that does not address aggregation across meters. Some techniques have been extended to protocols that provide differential privacy guarantees [6]. The technologies for smart grids, smart metering and more generally power line/wireless communications, are included in a large number of standards, each of which has a different scope of intervention and is only marginally related to security issues [7, 16].

Conclusion

As the need for energy increases constantly, the smart management of power grids has become a prime topic of interest for researchers and industry alike. In this chapter we provided an overview on the smart metering scenario and its novel information security challenges. We delineated the desired security services and the actors involved in the scenario, and provided a summary of the ongoing standardization efforts in this area.

References

1. Barenghi, A., Bertoni, G.M., Breveglieri, L., Fugini, M.G., Pelosi, G.: Smart metering in power grids: application scenarios and security. In: 1st IEEE PES Innovative Smart Grid Technologies (ISGT) Asia Conference IEEE, Perth (2011)
2. Barenghi, A., Breveglieri, L., Fugini, M.G., Pelosi, G.: Smart meters and home gateway scenarios. In: Cicchetti, A., Rossignoli, C. (eds.) IX Conference of the Italian Chapter of AIS Organization Change and Information Systems: Working and Living Together in New Ways, Roma. ITHUM Srl (2012)
3. Barenghi, A., Pelosi, G.: Security and privacy in smart grid infrastructures. In: Morvan, F., Tjoa, A.M., Wagner R. (eds.) DEXA Workshops, Toulouse, pp. 102–108. IEEE Computer Society (2011)
4. Bundesamt für Sicherheit in der Informationstechnik (BSI) – Federal Office for Information Security: Protection Profile for the Gateway of a Smart Metering System. https://www.bsi.bund.de/ (2014)
5. CSEP – Consortium for SEP 2 Interoperability: The Smart Energy Profile 2. http://www.csep.org/ (2014)
6. Danezis, G., Kohlweiss, M., Rial, A.: Differentially Private Billing with Rebates. Report MSR-TR-2011-10, Microsoft Research (2011)
7. Electronic Privacy Information Center: The smart grid and privacy. EPIC report, Washington, DC. http://epic.org/privacy/smartgrid/ (2014)
8. EU Commission Task Force for Smart Grids: Roles and Responsibilities of Actors involved in the Smart Grids Deployment. Expert Group 3 Deliverable. http://ec.europa.eu/energy/gas_electricity/ (2014)
9. Garcia, F.D., Jacobs, B.: Privacy-friendly energy-metering via homomorphic encryption. In: J.C. et al. (ed.) 6th Workshop on Security and Trust Management (STM 2010), London. Lecture Notes in Computer Science, vol. 6710, pp. 226–238. Springer (2011)
10. HomeGrid Forum: Gigabit Home Networking. http://www.homegridforum.org/ (2014)
11. HomePlug Powerline Alliance: Powerline Networking. https://www.homeplug.org/home/ (2014)
12. IEEE: Smart grid conceptual framework. IEEE Smart Grid Mag. (2014). http://smartgrid.ieee.org/ieee-smart-grid/smart-grid-conceptual-model
13. IEEE Computer Society: IEEE Standard for Information technology. IEEE Standard 802.11n-2009. http://standards.ieee.org/getieee802/download/802.11n-2009.pdf (2009)
14. Inter-operable Device Interface Specifications (IDIS) Industry Association: Inter-operability specifications. http://www.idis-association.com/ (2014)
15. Jawurek, M., Johns, M., Kerschbaum, F.: Plug-in privacy for Smart Metering billing. In: 11th Privacy Enhancing Technologies Symposium (PETS), Waterloo (2011)
16. Knyrim, R., Trieb, G.: Smart metering under EU data protection law. Intern. Data Priv. Law **1**(2), 121–128 (2011)
17. Liu, Y., Ning, P., Reiter, M.K.: False data injection attacks against state estimation in electric power grids. In: Proceedings of the 16th ACM conference on Computer and communications security, CCS'09, Chicago, pp. 21–32. ACM, New York (2009)
18. McDaniel, P., McLaughlin, S.: Security and privacy challenges in the smart grid. IEEE Secur. Priv. **7**, 75–77 (2009)
19. 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, Zurich, pp. 61–66. ACM (2010)
20. Petrlic, R.: A privacy-preserving Concept for Smart Grids. In: Sicherheit in Vernetzten Systemen: 18 DFN Workshop, Hamburg, pp. B1–B14. Books on Demand GmbH (2010)
21. PRIME Project: PHY, MAC and Convergence layers. PRIME Technology Whitepaper. http://www.iberdrola.es/webibd/gc/prod/en/doc/MAC_Spec_white_paper_1_0_080721.pdf (2008)

22. Rial, A., Danezis, G.: Privacy-preserving smart metering. Technical report MSR-TR-2010-150, Microsoft Research (2010)
23. Sander, K., Roos, B.: Security analysis of Dutch smart metering systems. Technical report of Universiteit Van Amsterdam. http://www.delaat.net/rp/2007-2008/p33/report.pdf (2008)
24. Teo, J.: Features and benefits of trusted computing. In: 2009 Information Security Curriculum Development Conference, InfoSecCD'09, Kennesaw, pp. 67–71. ACM, New York (2009)
25. The Smart Grid Interoperability Panel – NIST Cyber Security Working Group: NIST IR 7628 Rev. 1 – Guidelines for Smart Grid Cyber Security. Public report. http://csrc.nist.gov/publications/PubsNISTIRs.html (2013)
26. Trusted Computing Group: Trusted Computing: A Framework for Data and Network Security. http://www.trustedcomputinggroup.org/ (2014)
27. Wi-Fi Alliance: Wireless Local Area Network Interoperability Certification. http://www.wi-fi.org/ (2014)
28. ZigBee Alliance: Zigbee Smart Energy 2.0 Standard and Documentation. http://www.zigbee.org/Standards/Downloads.aspx#821 (2014)