Applying a Security Kernel Framework to Smart Meter Gateways

Michael Gröne[1] · Marcel Winandy[1,2]

[1] Sirrix AG security technologies
Im Stadtwald, Geb. D3.2, 66123 Saarbrücken, Germany
{m.groene | m.winandy}@sirrix.com

[2] Horst Görtz Institute for IT-Security
Ruhr-University Bochum, Germany
marcel.winandy@trust.rub.de

Abstract

New challenges for the electrical grid need complex IT systems and networking of most of all entities in today's power grid. Smart grids are a heavily discussed topic in the European Union and many other countries. Smart Meter Systems are going to be deployed worldwide. However, due to their complexity and interconnectivity, they have to deal with strict security and privacy requirements. As a result, German regulatory bodies decided a proactive approach and developed a protection profile for Common Criteria evaluation, i.e., specifying explicitly security requirements for gateway components.

We describe the challenges and requirements that have to be fulfilled to build a smart meter gateway according to the BSI protection profile in Germany. Moreover, we present and discuss a modular security framework approach that can be used to realize such gateways in order to fulfill the requirements of the protection profile. This security framework is based on a security kernel approach that has been developed within various other projects. The proposed security kernel framework offers a solution to meet these security requirements while keeping the architecture modular and flexible to be used for other implementations as well. As it can be used to realize various security architectures – ranging from desktops to mobile devices – our framework may also be suitable to be adapted to other smart meter gateway designs, not only for Germany.

1 Introduction

Smart grids are a heavily discussed topic in many countries. The expected increasing deployment of new electricity-powered devices (e.g., automobiles) in combination with distributed electricity generation based on regenerative energy (e.g., solar and wind energy) will result in new challenges for the electrical grid. The most important challenge will probably be high dynamics due to unknown consumption and production capacities. In addition, consumers demand more flexible power supply and flexible billing schemes adjusted to their needs. The smart grid is supposed to build a flexible, adjustable, and secure supply of energy. As part of this grid, metering systems deliver the required meter data to measure and adjust the energy supply, provide the basis for billing procedures, and eventually will be used when controlling other electronic devices that are connected to a home network (e.g., smart household appliances). To fulfill these requirements, more and more meter systems will be enhanced with additional electronic and information technology (IT) components, such as wired or wireless network connections, to become “smart meter” systems, allowing them to communicate with other electronic systems, especially with Internet based systems. Besides electricity, other consumables like water and heat are also considered as part of such a smart metering systems.

In Germany, for example, the introduction and deployment of such smart metering systems is becoming mandatory by law (“Energiewirtschaftsgesetz“, EnWG). This includes both legal and technical requirements. As part of the technical regulations and to address end-user privacy, beside smart meters, a new component is required: the “smart meter gateway”. This component operates as a gateway between the local smart meter systems, optional controllable household appliances, and remote systems that are connected via Internet access. As such, on the one hand these smart meter gateways offer the realization of new business cases for value-added services, both for the suppliers as well as the consumers. On the other hand, these gateways should include features to protect the privacy of end users. However, compared to classical meter infrastructures, smart meter gateways are very complex and offer a higher attack surface due to their connectivity to open networks. Thus, smart meter gateways need to protect themselves and the communication to devices they are connected with. To address these risks, the German Federal Office for Information Security (BSI) has developed a Common Criteria (CC) [CC09] protection profile for smart meter gateways [BSI12], defining strict security requirements and requiring assurance according to the evaluation level EAL4+. In this case, EAL4 is augmented with additional requirements for the gateway to be resistant against attacks by an adversary with high attack potential, and to provide defined security flaw remediation procedures. This poses new challenges and additional requirements for vendors that previously built classical meters, smart meters, “normal” meter gateways, or meter infrastructure components as the new devices have to be evaluated and certified according to the protection profile. Besides these new challenges, the BSI protection profile is the first application of the Common Criteria (CC) in the metering industry. There was no CC evaluation with level EAL3 of an ICT gateway for smart metering before, so nearly no experience could be made by vendors ahead to the developments and documentation that are necessary now to get a certification from BSI. Since CC evaluation and certification of complex IT products often are time consuming and certified products should be in market by begin of 2013, an adequate proceeding for the metering industry should be to learn from IT security industry and use existing approaches to counter high attack potential for example.

This paper describes the challenges and requirements that have to be fulfilled to build a smart meter gateway according to the BSI protection profile. Moreover, we present and discuss a modular security framework approach that can be used to realize such gateways in order to fulfill the requirements of the protection profile. This security framework is based on a security kernel approach that has been developed within various other projects, e.g. [EMSCB], [OpenTC], [ASSS+06]. It can be used to not only fulfill the smart meter gateway protection profile, but it is also the basis for an instantiation of the High Assurance Security Kernel (HASK) protection profile [KKSW+08]. As such, it can be used to realize various security architectures, ranging from desktop computers [CLMS+10] to mobile devices, such as smartphones [SSFG10], and embedded systems.

This publication was made during the drafting of the "Common Criteria Protection Profile for the gateway of a smart metering system" of the BSI and the BSI Technical Guideline TR 03109. These documents contain technical specifications for smart metering systems, which will be regulative implemented by laws and regulations in cooperation between governments, regulatory bodies and industry.

2 Background: Smart Meter Gateway

The smart meter gateway connects devices of three networks: meter systems from a Local Metrological Network (LMN), controllable local systems (CLS, e.g., smart household appliances) and external user display devices from a Home Area Network (HAN), and authorized external systems from an Internet connection as a Wide Area Network (WAN). Figure 1 illustrates the role of the gateway between these networks and its information flows.

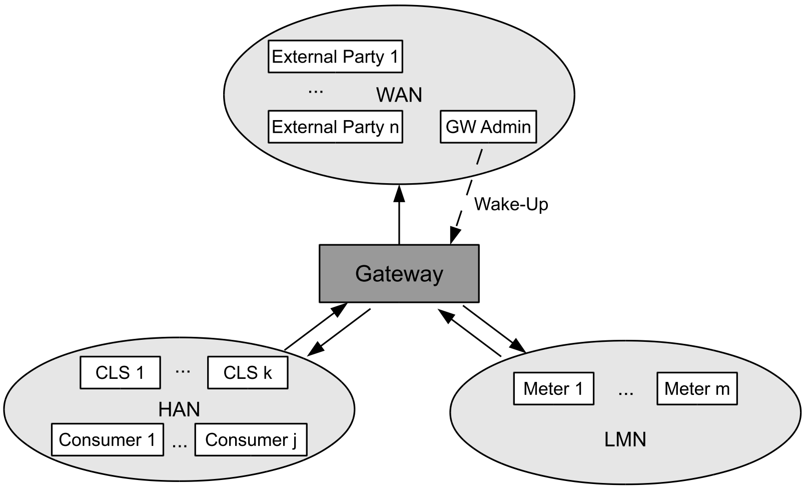

Figure 1: Smart Meter Gateway information flows

Mainly, the smart meter gateway has to provide the following four logical functions:

- collecting and processing meter data from the LMN;
- receiving and executing commands from an authorized gateway administrator from the WAN;
- providing an interface for controllable local systems to authorized WAN endpoints;
- providing a proxy for communication between controllable local systems and authorized external entities via WAN; and
- providing an interface to external user display devices in the HAN.

All these functions have to fulfill superior security requirements, i.e., the protection of the confidentiality of personal identifiable data of the consumers, the protection of the integrity of the data for logging, audit, and billing processes, and the protection of the smart meter gateway and infrastructure against unauthorized usage and manipulation.

In particular, the gateway has to ensure controlled information flows between the different networks and communication endpoints. Information flow is allowed according to the following rules (see also Figure 1):

- External parties from the WAN are not allowed to initiate a communication with the gateway. Only the gateway administrator (GW Admin) can send a simple wake-up call to the gateway, and the gateway contacts a pre-defined destination in the WAN for further requests. Through this communication channel, established by the gatway, other parties in the WAN can then communicate with the gateway, e.g., to receive meter data.
- Meter systems in the LMN cannot directly communicate with other parties in other networks. They can only directly communicate with the gateway. It is up to the gateway to process (and pseudonymize) the meter data before it is sent (by the gateway) to

authorized parties in the WAN. A communication between LMN and HAN is not allowed.

- Controllable local systems (CLS) in the HAN are also not allowed to communicate directly with external parties in the WAN. Similar to meters, they can only contact the gateway. In contrast to meter data, the gateway does not extra processing on the data sent by CLS; instead it provides a proxy service for CLS to communicate securely via TLS-encrypted channels to authorized end-points in the WAN.
- Finally, consumers can look up information about the data that was processed on the gateway and that "belongs" to them, i.e., they can only see meter data that came from their associated meters, and not from other consumers. To enable consumers to look up these information, the gateway provides a display service, e.g., a web browser interface that is accessible from the HAN and only by authenticated consumers.

2.1 Challenges

One of the most challenging parts of the smart meter gateway protection profile is the requirement to provide an information flow control of all communication going through the gateway and according to information flow rules of different networks and categories of communication endpoints as stated above. This disqualifies an approach using a regular operating system, such as Linux, to implement a firewall or gateway appliance without additional security measures. In particular, additional requirements on the collection and processing of meter data include the pseudonymization and separation of the data according to the consumers that are associated to the originating metering devices. Moreover, as the gateway has to provide several different functions, the resulting processes running on such a device need to be adequately separated from each other to prohibit unwanted information flow.

3 Security Kernel Framework Approach

Our proposed framework, the TURAYA.SecurityKernel [Sirrix12] addresses these topics by providing security and protection mechanisms that not only fulfill the requirements of the protection profile, but also anticipate the execution of future applications as additional services on top of the gateway. The main ideas behind the security kernel framework are to provide:

- a common and simple security model that allows to define high-level security policies that are transparently enforced by low-level components;
- a modular set of security services that can be integrated as needed;
- a flexible and auditable development and build environment that fulfills the needs for Common Criteria evaluations of at least EAL5; and
- the possibility to realize different implementations of the framework on top of various hardware and software architectures (e.g., x86 or ARM).

A key feature of the security kernel framework is that it allows executing isolated application domains on top of it [GJPS+05,CLMS+10]. Applications belonging to one domain can communicate freely with each other. A communication to other domains is prevented by default. If communication between domains (or to external systems) should be allowed, then this must be stated in the security policy of the system. In addition, restricted communication (e.g., allowing only certain data types to be exchanged) can also be defined, and will be enforced by the security services of the framework.

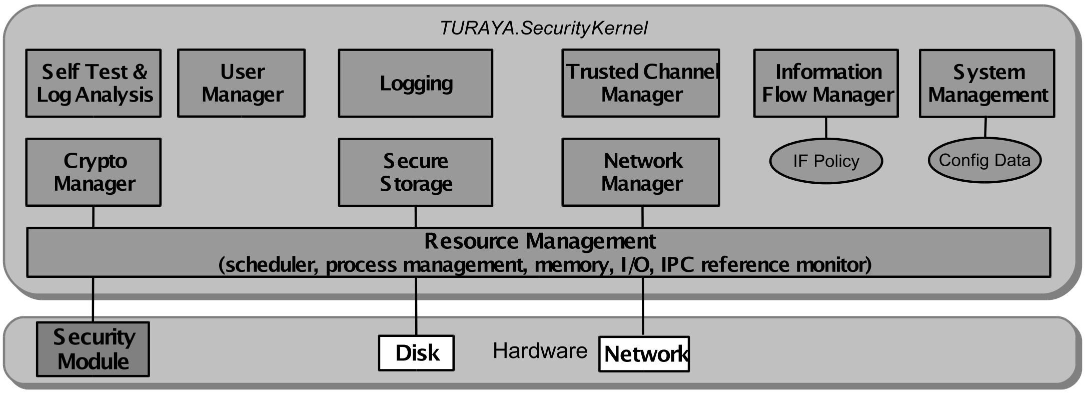

Figure 2: Overview of the security kernel framework

The main components of the security kernel framework are the following (see Figure 2):

- **Resource Management:** This is the basic functionality to execute and isolate processes, and to control inter-process communication (IPC) according to a mandatory security policy. There are different options to realize this component, e.g., a hypervisor or a microkernel in case of very high assurance or robustness requirements, or a hardened operating system kernel with mandatory type enforcement support in case of moderate to high assurance requirements (as in the case of the smart meter gateway).
- **Crypto Manager**: Provides cryptographic operations, and in particular support of hardware security modules.
- Secure Storage: Provides encrypted and integrity-protected storage that protects confidentiality and integrity of persistently stored data. This can include the entire disk volume (full-disk encryption).
- **Network Manager**: Controls access and operation of all physical network interfaces.
- **Trusted Channel Manager**: Provides (mutually) authenticated and encrypted communication channels over network connections as provided by Network Manager.
- **Information Flow Manager**: Enforces the system-wide information flow policy, acting as policy decision point. While there are different ways for communication between applications (IPC, via network, etc.), the Information Flow Manager provides centrally information flow decisions for all communication channels while they are enforced with the help of other services, e.g., Trusted Channel Manager.
- **System Management**: Provides interfaces for authorized administration of the system, e.g., inspecting or updating configuration options, or enabling a system update.

3.1 Applying the Framework to Smart Meter Gateways

In the instantiation of our framework for the smart meter gateway, we isolate the execution of all services that are used to realize the logical functions of the gateway. In particular, we define four security domains, one for each of the logical main functions, and in addition one security domain for the basic services of our security kernel. As other applications might be introduces later, we can define further security domains to separate them from the main logical functions and the basic security services. The separation of these security domains has the advantage that we can provide controlled information flow between the logical components. The isolation of security domains is enforced by the underlying security kernel framework. Data belonging to one domain are only accessible in this domain: persistently stored data are encrypted with a key associated to that domain, and sensitive data transmitted over networks are always protected by mutually authenticated secure channels (trusted channels).

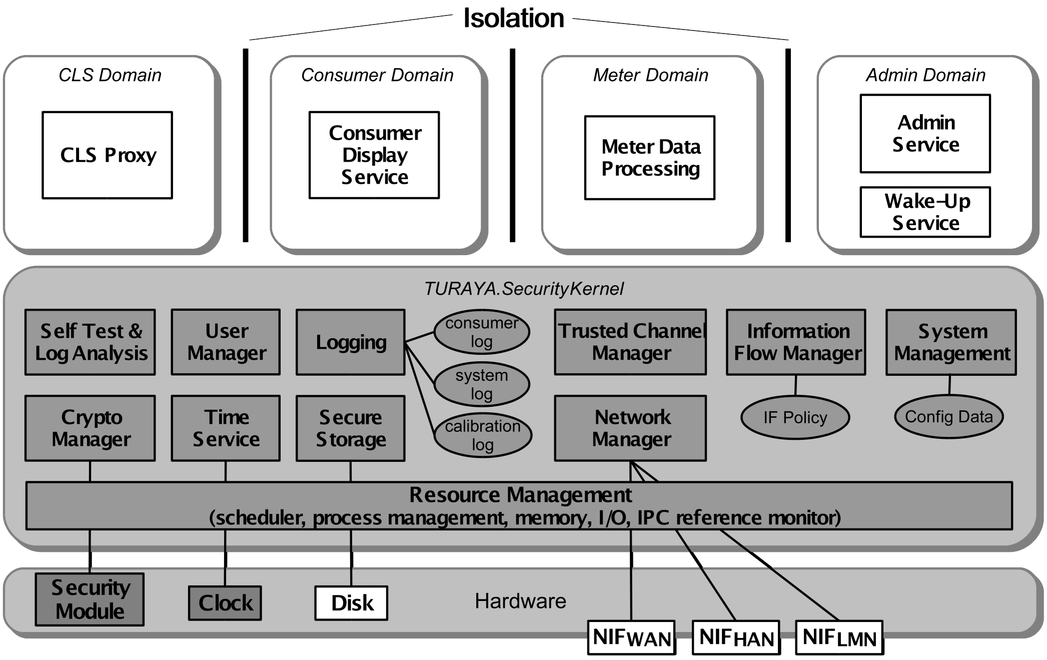

Figure 3: Realizing the Smart Meter Gateway with the Security Kernel Framework

As one possible instantiation of the framework, we use type enforcement mechanism to provide mandatory access control and labeling of all data and network connections. This is enhanced by additional components (security services) that control all incoming and outgoing network connections and those that enforce the information flow control of the software components within the gateway. In particular, our security kernel offers the following security services (among others):

- mandatory establishment of TLS-protected channels to outside communication endpoints (trusted channels);
- policy-driven information flow control of network, storage, and inter-process communication;
- secure storage providing protection of confidentiality and integrity of data based on their association to security domains;
- secure system configuration and system update; and
- support of cryptographic hardware security modules.

Our framework allows adapting particular security services to individual needs of concrete systems. For example, the smart meter gateway protection profile [BSI12] requires a mandatory security module (smart card) to be used in case of establishment of trusted channels and secure storage of encryption keys. However, our framework also allows to use other security modules if needed, e.g., a Trusted Platform Module (TPM) [TPM11] in case of PC/laptop computer systems.

The central idea of enforcing the information flow rules of the smart meter gateway with our framework, is to establish a separate application domain that corresponds to each of the four main information flow rules (see Section 2). There is one domain that handles the proxy functionality for CLS, one domain for providing a display service (e.g., web server interface) for consumers, one domain for collecting and processing the meter data, and one domain for the gateway administrator to configure and update the system. An essential part is their connection to the three physical network interfaces: All communication channels are going through the Trusted Channel Manager, which works together with the Information Flow Manager. As such, all communication requests must pass the central information flow decision. More importantly, the applications in the corresponding application domain do not need to take care of establishing the correct and encrypted network connections, i.e., taking care of TLS establishment. Instead, this is always handled by the Trusted Channel Manager. This component knows (by the system policy of the Information Flow Manager) which are authorized communication endpoints, for which requests, and which cryptographic credentials (i.e., TLS certificates) should be used in which case.

4 Conclusion

Critical infrastructures of the future, such as smart grids, smart metering intelligent power distribution and management, are use cases our security kernel framework is aiming at. Consisting of a multitude of distributed nodes, networked based on the IP protocol, smart grids will benefit from existing, mature technology and proven mechanisms. Security technology such as our security kernel framework can be seen as an enabler for smart grids, or at least it dramatically improves its security compared to standard operating systems for metering and gateway components. Using secure infrastructures is a requirement to be met to reach new business models, flexibility and cost-savings in smart grids.

In the future, even more and more mobile and autonomous entities will be accessing the smart grid. For example, energy management gateways controlled via smart phones will become reality soon. Hence, advanced security concepts should be also used on mobile user devices, such as smartphones and tablets as well as on desktop and server systems. Then a coherent level of security can be guaranteed.

The overall solution resulting of conceptual work and development of the proposed security kernel framework is one example that establishes security guarantees on the data processed in a smart meter gateway. The security and assurance requirements for such smart meter gateways are comparable to current smart cards, i.e., considering an adversary with high attack potential. The goal is to deploy gateways executing only certified software that do not affect external workflows and build trust in smart metering infrastructures. The proposed security kernel framework offers a solution to meet these security requirements while keeping the architecture modular and flexible to be used for other implementations as well.

References

[Alpe11] Alperovitch, Dmitri: Revealed: Operation Shady RAT, McAfee Labs, 2011. Available online at: http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf

[ASSS+06] A. Alkassar, M. Scheibel, C. Stüble, A.-R. Sadeghi, M. Winandy: "Security Architecture for Device Encryption and VPN", Proceedings of Information Security Solutions Europe (ISSE 2006).

[BSI12] Bundesamt für Sicherheit in der Informationstechnik (BSI): Protection Profile for the Gateway of a Smart Metering System, v 1.1.1 (final draft), 2012, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartMeter/PPSmartMeter.pdf?__blob=publicationFile

[CC09] Common Criteria for Information Technology Security Evaluation (CC), Version 3.1, Release 3, 2009. http://www.commoncriteriaportal.org/cc/

[CLMS+10] L. Catuogno, H. Löhr, M. Manulis, A.-R. Sadeghi, C. Stüble, M. Winandy: „Trusted Virtual Domains: Color Your Network“, Datenschutz und Datensicherheit (DuD), 2010, pp. 289-298.

[EMSCB] European Multilaterally Secure Computing Base, http://www.emscb.de

[GJPS+05] J. L. Griffin, T. Jaeger, R. Perez, R. Sailer, L. van Doorn, R. Cáceres: "Trusted Virtual Domains: Toward Secure Distributed Services", Proceedings of the 1st IEEE Workshop on Hot Topics in System Dependability (HotDep'05), 2005.

[KKSW+08] H. Kurth, G. Krummeck, C. Stüble, M. Weber, M. Winandy: HASK-PP: Protection Profile for a High Assurance Security Kernel, 2008, http://www.sirrix.com

[OpenTC] Open Trusted Computing, http://www.opentc.net/

[Sirrix12] Sirrix AG security technologies. TURAYA.SecurityKernel. 2012 http://www.sirrix.com/content/pages/securitykernel_en.htm

[SSFG10] M. Selhorst, C. Stüble, F. Feldmann, U. Gnaida: „Towards a trusted mobile desktop“, Trust and Trustworthy Computing (TRUST 2010), Volume 6101 of LNCS, Springer, 2010, pp. 78–94.

[TPM11] Trusted Computing Group (TCG), TPM Main Specification, Version 1.2, Revision 116, March 2011.

Index

Smart Grid, Smart Metering, Smart Meter Gateway, Security Kernel, Information Flow Control, Isolation, Trusted Computing, Trusted Virtual Domains