Security concept for gateway integrity protection within German smart grids

Prof. Dr. Kai-Oliver Detken
DECOIT GmbH,
Fahrenheitstr. 9, D-28359 Bremen
Email: detken@decoit.de

Carl-Heinz Genzel, Olav Hoffmann,
Prof. Dr. Richard Sethmann
University of Applied Sciences of Bremen,
Flughafenallee 10, D-28199 Bremen
Email: carl-heinz.genzel/ohoffmann/sethmann@hs-bremen.de

ABSTRACT

In order to meet future challenges of energy grids, secure communication between involved control systems is necessary. Therefore, the German Federal Office for Information Security (BSI) has been published security standards concerning a secure communication unit for smart metering systems, which is named Smart Meter Gateway (SMGW). This present security concept of this paper takes these standards into consideration, but extends their level of information security by integrating elements from the Trusted Computing approach. A tamper-resistant grid has been integrated with chosen hardware modules and a trustworthy boot process has been applied. To measure and evaluate the SMGW's integrity continuously the specification Trusted Network Connect (TNC) from the Trusted Computing Group (TCG) has been used furthermore. This work is an outcome of the German research project SPIDER from BMWi, which started in March 2013 and will end in February 2015.

I INTRODUCTION

1 Future energy grids

Future energy grids need to enable volatile and peripheral energy production without impacting the grid's stability. Additionally, different external entities and their varying interests have to be considered [4, p. 14]: Metering point operators responsible for metering systems, measurement service providers, which readout and provide data measured by metering systems, distribution grid operators, which maintain and support local energy grids, energy suppliers, which act as energy merchants using the infrastructure provided by distribution grid operators, gateway administrators (GWA), which configure, control and monitor SMGWs within their lifecycle and consumers (CON), which may operate their own local power plant.

To fulfill the new requirements an overall intelligent energy grid, also called smart grid, needs to be developed. This is "a commodity network that intelligently integrates the behavior and actions of all entities connected to it […] in order to efficiently ensure a more sustainable, economic and secure supply of a certain commodity"[17].

However, because the energy grid is considered a critical infrastructure, high security requirements are demanded. In Germany, the BSI is responsible to define those requirements in form of national standards. The present security concept keeps in mind these standards while improving the security level additionally. It has been developed within the German research project SPIDER (www.spider-smartmetergateway.de).

2 Scenario description

Because of the critical nature of energy grids, their future challenges may only be satisfied, if energy production and energy consumption is coordinated using secure communication between the different connected entities. Therefor two components have been introduced by the BSI to German energy grids. They represent the basic building blocks for so called Smart Metering Systems. The Smart Meter (SM) describes an intelligent meter for energy commodities. It is connected to the SMGW. The SMGW is a central communication and storage unit for measurements collected via the SMs.

Figure 1 shows the important components and areas of a Smart Metering System as described by the BSI specifications (see [4], [5], [7], [8]).

The SMGW is responsible for the reliable processing and secure storage of measurement data provided by several connected SMs. Furthermore, it provides a secure communication between the individual external entities. The BSI has categorized these individual entities into different networks (see [4, pp. 13-15]) as listed on the next page:

a. *Local Metrological Network (LMN):* SMs for various commodities (e.g. electricity, gas and water) are connected with the SMGW through the LMN.

b. *Home Area Network (HAN):* Controllable local systems (CLS) (e.g. local solar power plants) are connected through the SMGW via the HAN. Utilizing the SMGW as proxy, CLSs can be controlled by external entities (e.g. solar power plant vendors for maintenance). The consumer can interact with the SMGW across the HAN to access the measurement data gathered from its SMs. A service technician is able to readout SMGW system events for troubleshooting purpose through the HAN connection.

c. *Wide Area Network (WAN):* The GWA is able to interact with an SMGW through the WAN for management purpose. The SMGW may also communicate measurement data to authorized external entities via the WAN too.

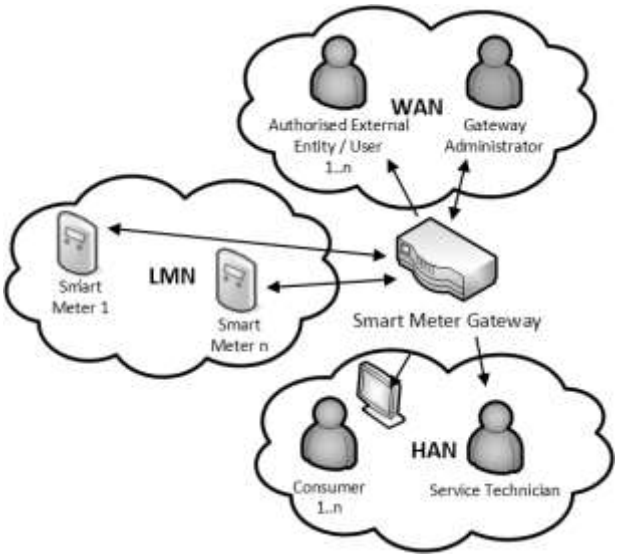

Figure 1: Smart Metering scenario

Besides that, the SMGW acts as a firewall, separating the described networks and their participants from each other both logically and physically [4, pp. 13-15].

For secure data storage and communication, an SMGW makes use of a so called security module that provides cryptographic functionality such as: [5, p. 9]

a. Secure storage of certificates and keys

b. Key generation an key agreement using elliptic curves

c. Digital signature generation and verification

d. Reliable random number generation

The SMGW is able to receive, process and store measurement data from SMs. An SM differs from a usual metering system by being able to communicate with the SMGW in a cryptographically secured manner. Furthermore, an SM is controllable by the SMGW [4, pp. 15-16].

To facilitate the integration of the described components at the customer's premises, further components are needed. Especially the WAN connection is established using the local energy grid. G3 Power Line Communication (PLC) enables the connection to a local substation across the "last mile". At the substation the communication is routed to the WAN using a common WAN technology (e.g. fiber channel) [3, p. 333].

For privacy reasons the data, which may be communicated into the WAN and other areas is specified by BSI standards as well. All measurement data provided by an SM and all derived data calculated by an SMGW are owned by the consumer, who is assigned to the SM. Authorized external entities are interested in using these data (e.g. for billing or tariffing purpose). The data may also be used to manage an energy grid. The GWA has no access to these data. Instead, the GWA is able to access and store data relevant to maintain an SMGW (e.g. configuration files, system log and calibration log). The service technician is only permitted to perform system diagnosis. Therefore the technician is allowed to read data relevant to maintain the SMGW, but is not able to store such data like the GWA does. In general every individual participant is only allowed to access the SMGW via the network, it is associated with (see figure 1) [4, pp. 118-119].

3 Threat analysis

The BSI defined three categories of security threats, based on the described scenario (see [7, p. 33]). These categories are organized by their impact on a Smart Metering system, in the following list:

a. *Disclosing data*, which are stored on or processed by the SMGW (measurement data, configuration data), with the intention to

gather information about the smart metering infrastructure.

b. *Manipulating data*, which are stored on or processed by the SMGW (measurement data, tariff data), with the intention to change the data in order to gain advantage or to interrupt the proper operation of components.

c. *Alteration and control of involved systems* (CLS, SMGW, etc.) with the intention to compromise the smart metering infrastructure.

Every category may be further distinguished by its origin. An attacker from the WAN side is generally characterized to be more motivated than an attacker from the HAN side. If an attack from the WAN is successful, it can be easily extended to further systems. HAN attacks may be more limited to local peculiarities instead [7, p. 33].

Based on the BSI insights, a complementary threat analysis was conducted within the research project SPIDER using the STRIDE approach by Microsoft [15]. STRIDE as shown in table 1 is an acronym, which enables the classification of threats focusing on security aspects impaired by them, while not quantifying them.

Threat	Security aspect
Spoofing	Authentication
Tampering	Integrity
Repudiation	Data acceptance
Information disclosure	Confidentiality
Denial of Service	Availability
Elevation of privilege	Authorization

Table 1: STRIDE approach (threats and security aspects)

Using STRIDE additional threats were discovered, most of them fall into the classes tampering and denial of service [3]. The latter class may only be mitigated e.g. by supervising system resources and using prioritization. However, solutions exist in Trusted Computing to effectively recognize and control the threads of the first class. The provided security concept takes these results into consideration and emphasizes on security aspects that are less cared about within the BSI standards.

II STATE OF THE ART

In the following, important technologies from the field of Trusted Computing are explained, which help to recognize and control tampering attempts by monitoring system integrity.

1 Trustworthy boot process

The manipulation and replacement of a system's hardware parts is considerably difficult, because in most cases they are protected by mechanical means. Instead the manipulation of software is considerably simple. Hence, a measurable protection of the software's integrity is key to protect a system, which provides security functionality. This requirement involves a circular dependency, because the measurement of software integrity is only possible by using software as well [12, p. 569, p. 570].

In order to overcome this dependency amongst others, a concept called Root of Trust is used in Trusted Computing. Literature describes the term Root of Trust as a non-deniable characteristic or aspect of a single person or thing, which justifies its trustworthiness (see [11 p. 31]).

Therefore, it has to resist tampering to a high degree or make it even impossible. Thus, the Root of Trust may form the basis for the integrity measurement of a system or platform. According to that, the Trusted Computing Group (TCG) describes the term Chain of Trust. It expresses a system's integrity as a calculated trust chain, which is built at boot time, starting at the Root of Trust across various hierarchically organized components of the system. A component (n) inside this chain knows the proper integrity state of its successive component and evaluates it against this state. Finally it creates an evaluation record. If the evaluation is successful, the successive component (n+1) starts evaluating its next component (n+m). If the entire chain evaluation is successful, all successive components should be in an expected state, assuming that the Root of Trust is most widely not changeable. Hereby manipulations (e.g. by an attacker) on hard- and software are recognizable [10, pp. 4-7], [13, pp. 7 - 8].

This process is widely called trustworthy boot process and is distinguished in three categories (see [16, p. 50]) as follows:

a. *Trusted Boot:* Evaluation of components using analysis and measurement methods. Only one valid system state exists.

b. *Secure Boot:* Evaluation of components using analysis and measurement methods including actions, if the evaluation results in a compromised system. Only one valid system state exists.

c. *Authenticated Boot:* Evaluation of components using analysis and measurement methods including actions, if the evaluation results in a compromised system. This process knows several valid system states.

Unfortunately these categories are often used interchangeably [16, p. 50].

2 Trusted Computing – TNC mechanisms

"The [TCG] is a not-for-profit organization formed to develop, define and promote open, vendor-neutral, global industry standards, supportive of a hardware-based root of trust, for interoperable trusted computing platforms." The published standards shall aid in the detection of alterations on IT platforms/systems including, but not limited to, software attacks, configuration changes, security flaws and faulty applications. [14]

A major challenge within the field of IT security is in ensuring trustworthiness of an IT system, because in most cases it is not obvious if a system's hard- or software is tampered with. Software on its own is not able to solve this problem, as software is more prone to tampering, than hardware is. The TCG has developed a Trusted Platform Module (TPM) standard, which describes an additional hardware component. It contains a fixed, non-public key pair, which is considered to be the modules identity. The TPM is tightly integrated inside a system and can acts as a Root of Trust, because it is most widely not changeable. It also provides functionality to measure a system in form of a trusted boot process [13].

The TNC standard by TCG describes an architecture, which provides instruments to validate the system integrity of endpoints in a network to facilitate trustworthy communication. TNC defines two scenarios: [13], [14]

a. The first scenario describes an *authentication process* which evaluates a system's integrity in addition to any provided credentials.

b. The second scenario describes the *monitor of the system's integrity* continuously.

In both scenarios measured system attributes (e.g. attributes from the trust chain) are used to determine a system's state and its integrity. TNC is often used in combination with a TPM, because a TPM can provide these values in a secure manner.

3 Comparison of TC and BSI requirements

To determine, which measures of Trusted Computing could be helpful to further the SMGW's integrity, security measures from the BSI's standards are compared to measures of Trusted Computing.

TPM is a central element in Trusted Computing providing the system's identity. The security module in turn holds the identity of an SMGW. Both modules use private keys, (see [14, p. 1], [5, p. 56]) and both are tightly integrated inside their surrounding systems. Further, they need to sustain physical tampering to certain extent [13, p. 47], [2, p. 12, 30].

Besides a fixed identity, Trusted Computing uses TNC to measure and certify a system's integrity. Remote attestation is a TNC concept, which allows certifying the integrity by sending measured system attribute values to a remote entity for evaluation [13, pp. 8-10]. According to this, the BSI only requires some form of self-tests to verify security relevant functions and data [7, p. 38, p. 79]. By securely measuring and certifying a system's integrity, hard- and software tampering is recognizable. This aids in the reduction of possibilities to conquer an SMGW permanently. The introduction of integrity control would further strengthen the authenticity of data being communicated also. In fact, a successful authentication must not certainly indicate a proper functioning SMGW, instead only if its authentication and its integrity are valid, the SMGW most certainly works as expected. However, this security aspect is treated only shallowly by the BSI standards.

Finally, the TNC standard in combination with some sort of trustworthy boot processes including a Root of Trust represents the most valuable security enhancement in contrast to BSI standards. However, the current TPM version 1.2 is not suitable, because it does not fulfil the cryptographic requirements by the BSI standards. The BSI requires elliptic curve based algorithms, which are

not part of a TPM version 1.2. Future TPM versions like 2.0 may eventually be evaluated.

III Security Concept

The following concept to secure the integrity of an SMGW is based on the insights of section I using the identified technologies described in section II to enhance the system's security beyond the BSI standards as stated in section II subsection 3.

1 Hardware integrity protection

Basically, all hardware parts are tightly integrated into a SMGW chassis. The chassis is protected by a visible, physical, permanent seal, which is destroyed, if the chassis is opened and the opening is signaled to the SMGW software by an electronic switch. Additionally certain hardware parts (e.g. CPU and security module) are protected by an electronic tamper resistant grid, which shall detect hardware tampering attempts and signal them to the SMGW software.

2 Basic integrity protection

Basic integrity protection is realized by a trustworthy boot process. Secure Boot does not rely on a TPM and defines actions to be taken if the system's integrity is compromised. Technologies like co-processors or the Trustzone [1] used in ARM-CPUs may aid in the implementation of a secure boot process [12, p. 572]. Figure 2 shows the pattern of Secure Boot (see [12, p. 570]), which has been applied to this concept.

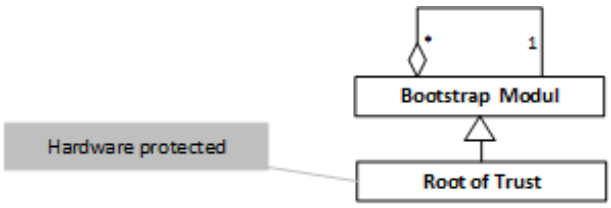

Figure 2: Secure Boot pattern [12, p. 570]

The boot process is organized as list of bootstrap modules. The first module in this list is the Root of Trust, which is protected by hardware. According to this pattern, the boot sequence in figure 3 results.

After powering up the system, the Root of Trust is loaded from the hardware ROM. The Root of Trust holds a reference to the next boot stage, the basic boot loader (bootstrap module n). Before this module is loaded, the boot loader is verified against a known signature by the Root of Trust, using a configured fixed public key. Only if the signature of the boot loader is valid, it is loaded. The boot loader continues the boot process and verifies the system's hardware integrity (e.g. state of the tamper resistant grid and the chassis). Additionally it verifies the operating system software (bootstrap module n+1) using a known signature and the corresponding public key. If the signature is correct, the operating system is loaded and in turn may verify additional software (bootstrap module n+m) the same way, using known signatures and public keys.

As soon as the verification fails, the boot process is interrupted and the system returns to a secure state, if system recovery is not possible. In this case a secure state is a reboot loop. System recovery is possible due to a second partition, which contains a duplicate firmware. As long as the boot loader is verified correctly, it is possible to load the firmware from the second partition, if the firmware from the first partition is compromised. Only if both firmware versions are compromised, the reboot loop is entered. This ensures that an SMGW is only in use, if the initial boot process was trustworthy.

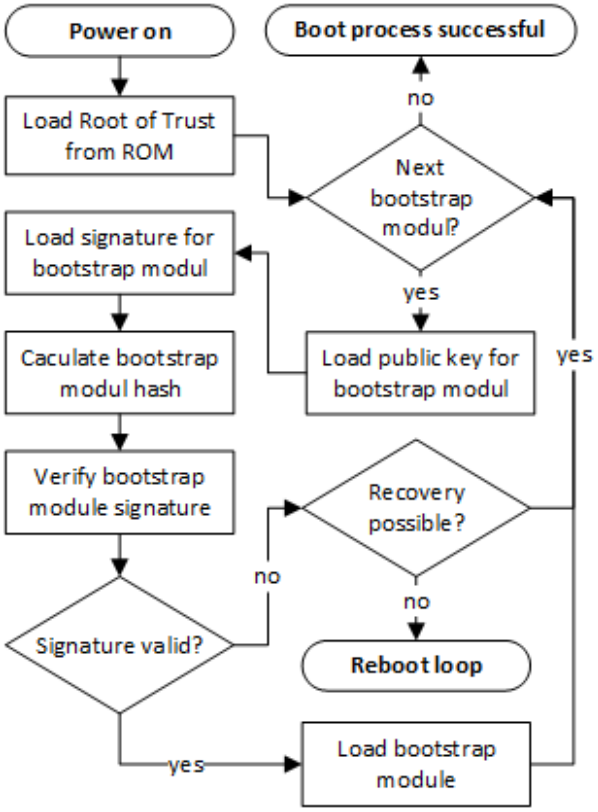

Figure 3: Secure boot process

3 Ongoing SMGW integrity verification

TNC represents a significant security enhancement, as explained in section II. Because the underlying architecture of TNC is intended to be customizable, the use of TNC for ongoing integrity verification for SMGWs is possible. Although, TNC does support authentication too, the use of TNC is especially focused towards monitoring tasks. Authentication is implemented according to the BSI standards. Figure 4 shows the SMGW and the GWA in terms of TNC. The SMGW acts as Network Access Requestor (NAR) while the GWA acts as Network Access Authority (NAA).

The Integrity Measurement Collector (IMC) is located inside the NAA and custom software. It is used for integrity measurement and value collection and replaces the corresponding TPM functionality, which is not used for obvious reasons (see section II, subsection 3). To measure the system's integrity, the IMC calculates hash values from various system components (e.g. firmware, configuration files or hardware configuration) periodically. Measured values are stored in the file system and are protected using the multiuser abilities and file system permissions supported by the Linux operating system. Because file system permissions are evaluated at kernel level, they are difficult to compromise.

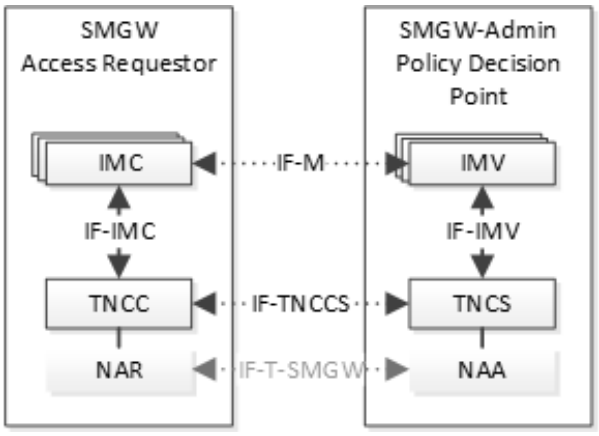

Figure 4: TNC architecture model with relevant components

The IMC communicates the measured values to the Integrity Measurement Verifier (IMV) inside the GWA. As well as the IMC, the IMV is custom software, which knows how to interpret these values. TNC-Client (TNCC) and TNC-Server (TNCS) handle the communication between IMC and IMV and react on the results from the IMV after the verification of the measured values. Existing libraries already implement these two components and custom implementations may not be necessary. However, for security reasons, the GWA is obliged to act upon the TNCS, if the verification of the measured values results in a compromised integrity. Because of the software based measurement approach it is necessary to emphasize, that a system must be used, which verifies the integrity of the TNC software at boot time.

In figure 4, a communication channel named IF-T-SMGW is shown. Because no existing specification in the TNC standard is applicable at this point without neglecting the superior BSI standard, a new specification has to be obtained here. In fact an existing web service, specified by the BSI standard for alarm and event notifications, could be used. All other specifications for the SMGW WAN interface are left unchanged (see [4, p. 22]). For backwards compatibility with GWAs, only compliant to the BSI standards, TNC data is marked for identification but can be handled as simple event notifications too. Instead, TNC compatible GWAs search for these marked event notifications to send them to an IMV. Because most of the TNC components are plain software, no other parts of the BSI standards are influenced by the use of TNC.

IV Conclusion and Prospects

The relevant aspect of Trusted Computing to enhance the SMGW security is the measurement and verification of an SMGW's integrity using TNC. The BSI standards do not mention similar solutions. When using TNC, it is especially important to protect the measurement logic, to ensure the trustworthiness of the measured values. This security concept complies with this requirement by generating a trust chain. Integrity verification is first applied at boot time, utilizing secure boot and establishing the trust chain including the TNC software. Integrity verification is also applied at runtime, utilizing the (at boot time) verified TNC software. The measured values of hard- and software components are stored tamper safe in the file system. This leads to an advanced gateway security, which affects all adjacent components.

In the future the integration of the TNC concept may be extended, to enable an integrated monitoring approach for the whole smart metering infrastructure. The Meta Data Access Point (MAP), defined by TCG to extend the TNC architecture,

specifies monitoring interfaces, which may be used to realize a central monitoring system with security information and event management capabilities (SIEM system) for smart grids. That will be a further step into a really secure smart grid infrastructure.

ACKNOWLEDGEMENT

The authors give thanks the BMWi-ZIM [9] for the financial support as well as all other partners involved into the research project SPIDER for their great collaboration. The project consists of the industrial partners develo AG and DECOIT GmbH, and the research partners University of Siegen, Fraunhofer FOKUS, and University of Applied Sciences of Bremen. Further associated partners are the energy provider Vattenfall and RWE, the hardware vendor Maxime, and the certification expert datenschutz cert. [19]

REFERENCES

[1] ARM Ltd: *TrustZone*. http://www.arm.com/products/processors/technologies/trustzone/index.php, May 2014, last access at 22.11.2013

[2] Bare, J. C.: *Attestation and Trusted Computing*. University of Washington, Washington 2006

[3] Becker, C: *Bedrohungsanalyse für Smart Grids und Anpassung des Sicherheitskonzeptes*. Hochschule Bremen, Bremen 2013

[4] Federal Office for Information Security (BSI): *Technical Guideline BSI TR-03109-1: Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems*. BSI, Bonn 2013

[5] Federal Office for Information Security (BSI): *Technical Guideline BSI TR-03109-2 Smart Meter Gateway Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls*. BSI, Bonn 2013

[6] Federal Office for Information Security (BSI): *Technical Guideline BSI TR-03109-4 Smart Metering PKI - Public Key Infrastruktur für Smart Meter Gateways*. BSI, Bonn 2013

[7] Federal Office for Information Security (BSI): *Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP)*. BSI, Bonn 2013

[8] Federal Office for Information Security (BSI): *Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP)*. BSI, Bonn 2013

[9] Federal Ministry for Economic Affairs and Energy: Central Innovation Program SME: http://www.zim-bmwi.de, May 2014, last access at 14.05.2014

[10] ISO/IEC: *ISO/IEC 11889-1 Information technology — Trusted Platform Module — Part 1: Overview*. ISO copyright office, Geneva 2009

[11] Kinney, S.: *Trusted platform module basics: using TPM in embedded systems*. Elsevier, Amsterdam (et al.) 2006

[12] Löhr, H., Sadeghi, A.-R., Winandy, M: *Patterns for Secure Boot and Secure Storage in Computer Systems*. Available in IEEE: ARES '10 International Conference on Reliability, and Security, pp.569-573, Krakow 2010

[13] Trusted Computing Group: *TCG Specification Architecture Overview*. TCG PUBLISHED, Beaverton 2007

[14] Trusted Computing Group: *TCG Trusted Network Connect TNC Architecture for Interoperability*. TCG PUBLISHED, Beaverton 2012

[15] Microsoft: *Threat Modeling Uncover Security Design Flaws Using The STRIDE Approach*. [Online] Available from: http://msdn.microsoft.com/en-us/magazine/cc163519.aspx, May 2014, last access at 14.05.2014

[16] Smith, S. W: *Trusted Computing Platforms: Design and Applications*. Publishing house Springer, New York 2005

[17] SMART METERS CO-ORDINATION GROUP (SM-CG) Item 5: *M/441 first phase deliverable – Communication – Annex: Glossary* (SMCG/Sec0022/DC)

[18] Trusted Computing Group: *TPM Main - Part1 Design Principles*. Specification Version 1.2, Revision 116, 1st March, 2011

[19] SPIDER project website: http://www.spider-smartmetergateway.de, May 2014, last access at 14.05.2014