Security concept for gateway integrity protection within German smart grids

Prof. Dr. Kai-Oliver Detken[1],
Carl-Heinz Genzel[2], Olav Hoffmann[3], Prof. Dr. Richard Sethmann[4]

[1] DECOIT GmbH
[2,3 und 4] University of Applied Sciences of Bremen

Table of Contents

ECSaR 2014: Workshop on Engineering Cyber Security and Resilience, Stanford CA, USA

Motivation

<u>Changes of the energy market</u>

- Fluctuating decentralized energy generation versus stability
- Consideration of different interests
- Intelligent regulated energy grids
- German law EnWG §21 postulates intelligent systems

<u>Intelligent ≠ Secure</u>

- Critical infrastructure has to be secure
- Personal allowance data has to be protected
- Creation of trust by security mechanisms is important
- The German Federal Office for Information Security (BSI) defines security requirements and specification for critical infrastructure

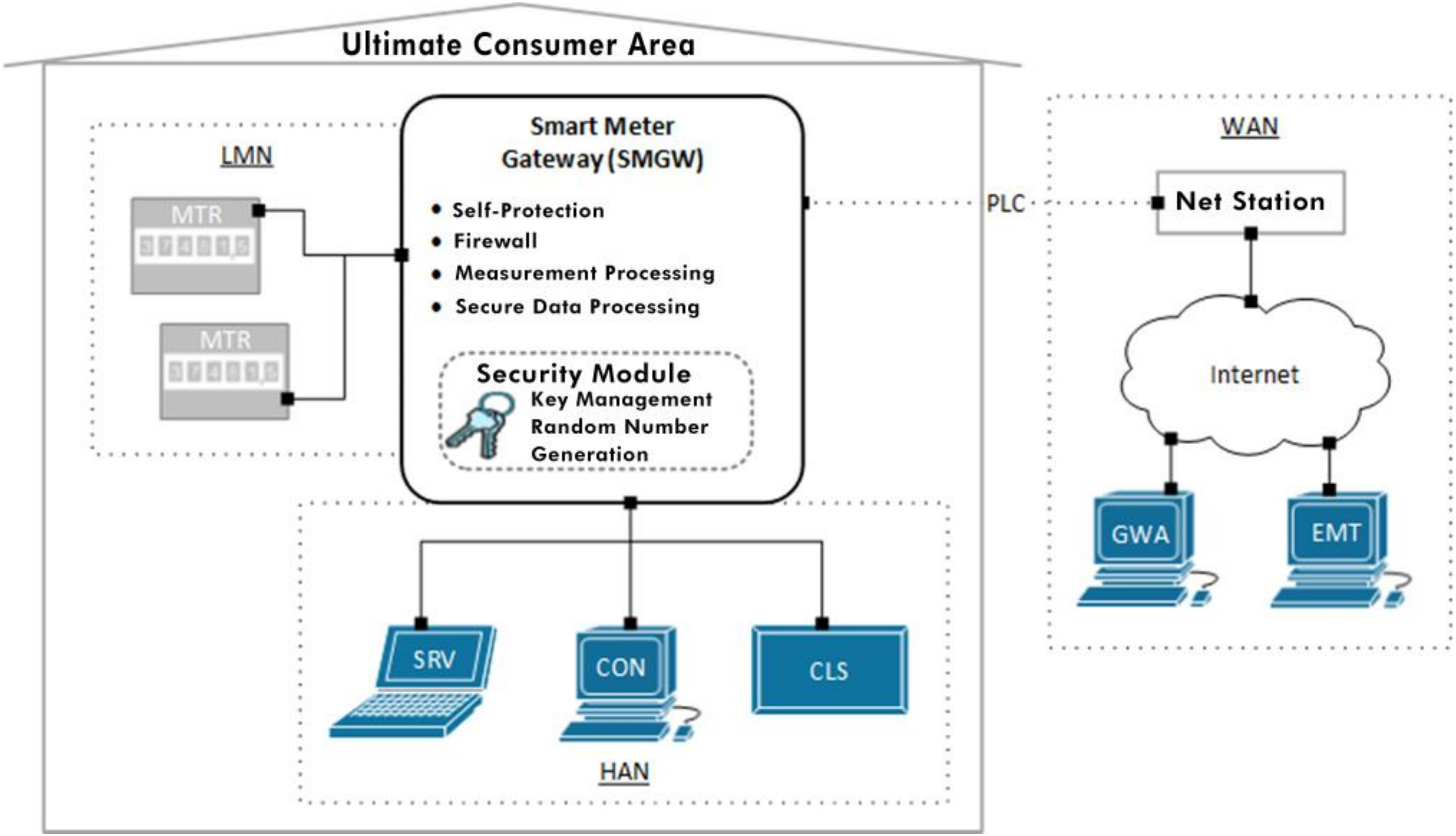
National project SPIDER

- Secure Power-line Data communication within intelligent energy grids (SPIDER)
  - 2 years project of ZIM (BMWi)
  - Lifetime: 1st March 2013 till 28th February 2015
  - Budget: 1.2 million Euro
  - Project goal: Development and BSI certification of a Smart Meter Gateway (SMGW)
  - Partners:
    - Industrial partners: DECOIT GmbH, devolo AG (project leader)
    - Academical partners: University of Applied Sciences of Bremen, Fraunhofer FOKUS, University of Siegen
    - Associated partners: Maxim Integrated, datenschutz cert
    - Energy providers: Vattenfall, RWE

Bundesministerium für Wirtschaft und Technologie

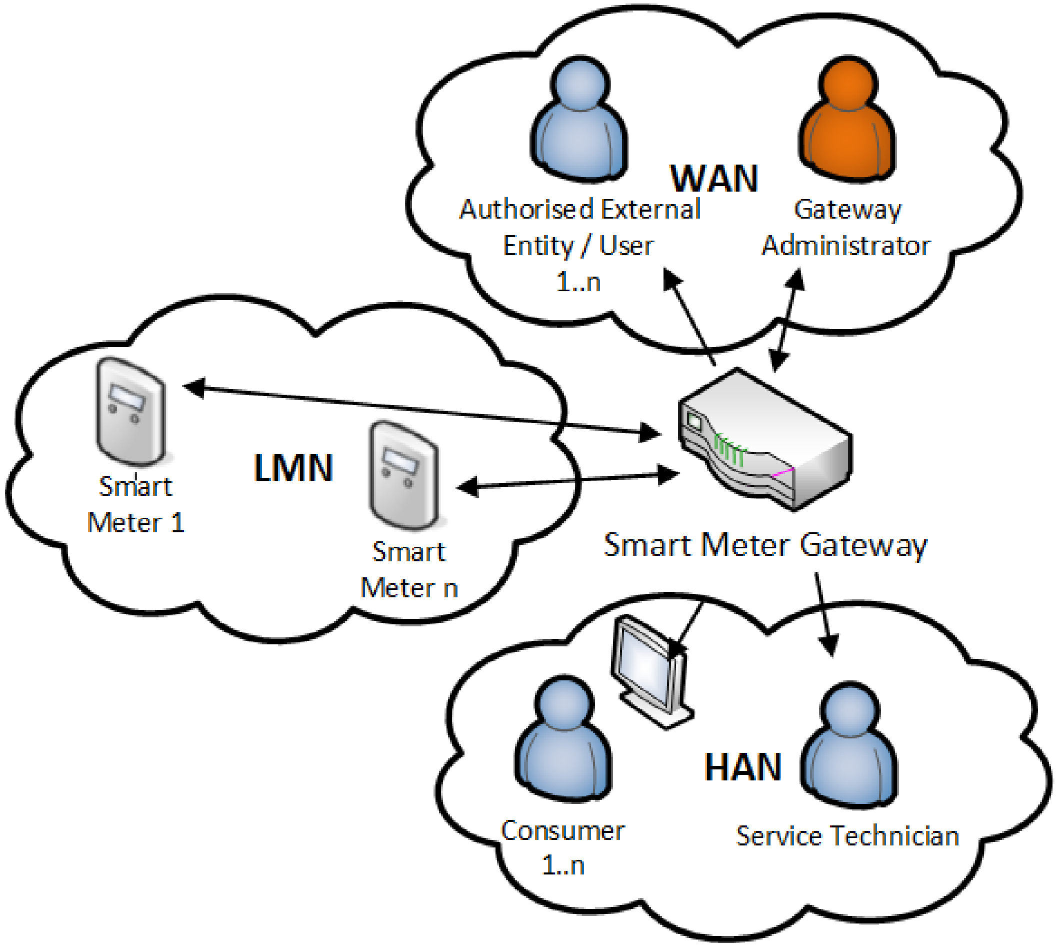
ZIM Zentrales Innovationsprogramm Mittelstand

Smart meter scenario (1)



Smart meter scenario (2)

- *Local Metrological Network (LMN):* SMs for various commodities (e.g. electricity, gas and water) are connected with the SMGW through the LMN.
- *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 by its SMs. A service technician is able to readout SMGW system events for troubleshooting purpose through the HAN connection.
- *Wide Area Network (WAN):* The GWA is able to interact with a SMGW through the WAN for management purpose. The SMGW may also communicate measurement data to authorized external entities via the WAN.



Threat analysis

Threat categories

- The BSI defined three categories of security threats based on the described scenario
  - Disclosing data of the infrastructure by data collection
  - Manipulation of data of the SMGW by fraud or disruption
  - Alteration and control of involved systems (e.g. CLS, SMGW)
- Motivation for attackers
  - Attacker from the WAN interface → high motivation (external person)
  - Attacker from the HAN → small motivation (energy customer)

STRIDE approach

STRIDE approach - further analysis after security requirements

- STRIDE = Spoofing, Tampering, Repudiation, Information disclosure, Denial of service und Elevation of privilege
- Using STRIDE additional threats were discovered (e.g. in the class of tampering and denial of service)
- From BSI's point of view, integrity can be established by a hardware seal only
- However, solutions exist in Trusted Computing to recognize and control the threads more effectively

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

State of the art (1)

Trusted Computing (TC) of the Trusted Computing Group (TCG)

- Trusted Platform Module (TPM)
  - Hardware-based identity (hardware trust anchor, Root of Trust)
  - Integrity measurement of hard- and software
  - Trusted boot process (Trusted Boot)
- Trusted Network Connect (TNC)
  - System integrity validation (remote attestation)
  - Can be used for authentication and monitoring

Comparison of TC technologies with requirements of BSI

Requirements	**Trusted Computing**	**BSI**
Identity	TPM (solid integrated, physical protection for manipulation, private key)	Security module (solid integrated, physical protection for manipulation, private key)
Status measurement	TPM (measurement of system attributes and secure storage)	Self-test (analysis of secure-relevant functionality and data)
Integrity test	TNC (remote attestation)	Self-test (analysis of secure-relevant functionality and data)
Trusted basis	Trusted Boot (measurement of system integrity during booting, status measurement)	No comments

State of the art (3)

Security module for secure data storage and communication

- Security module requirements in common
  - Secure storage of certificates and keys
  - Key generation and key agreement using elliptic curves
  - Digital signature generation and verification
  - Reliable random number generation
- TPM version 1.2 is not suitable, because it does not fulfil the cryptographic requirements by the BSI standards (e.g. use of elliptic curve based algorithms)
- Future TPM versions like 2.0 may be used (has to be evaluated)
- First solution in SPIDER: use a compliant security module and implement the TNC approach as software

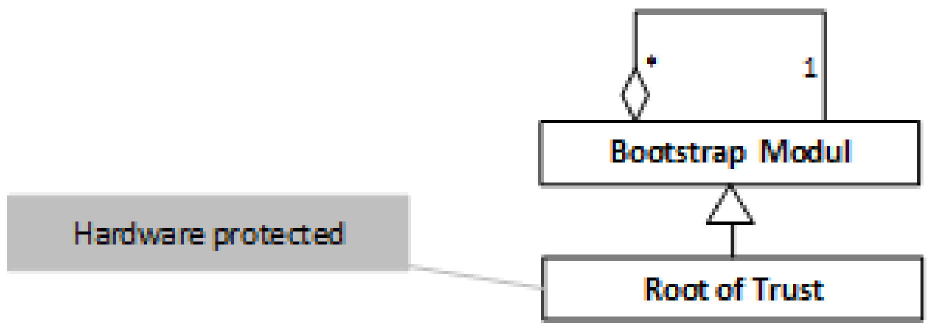
SMGW integrity (1)

Securing of the hardware

- Passive sealing of the SMGW box (defined by BSI)
- Electronical sensor for box opener
- Tamper resistant grid for some components

Securing of the basis integrity

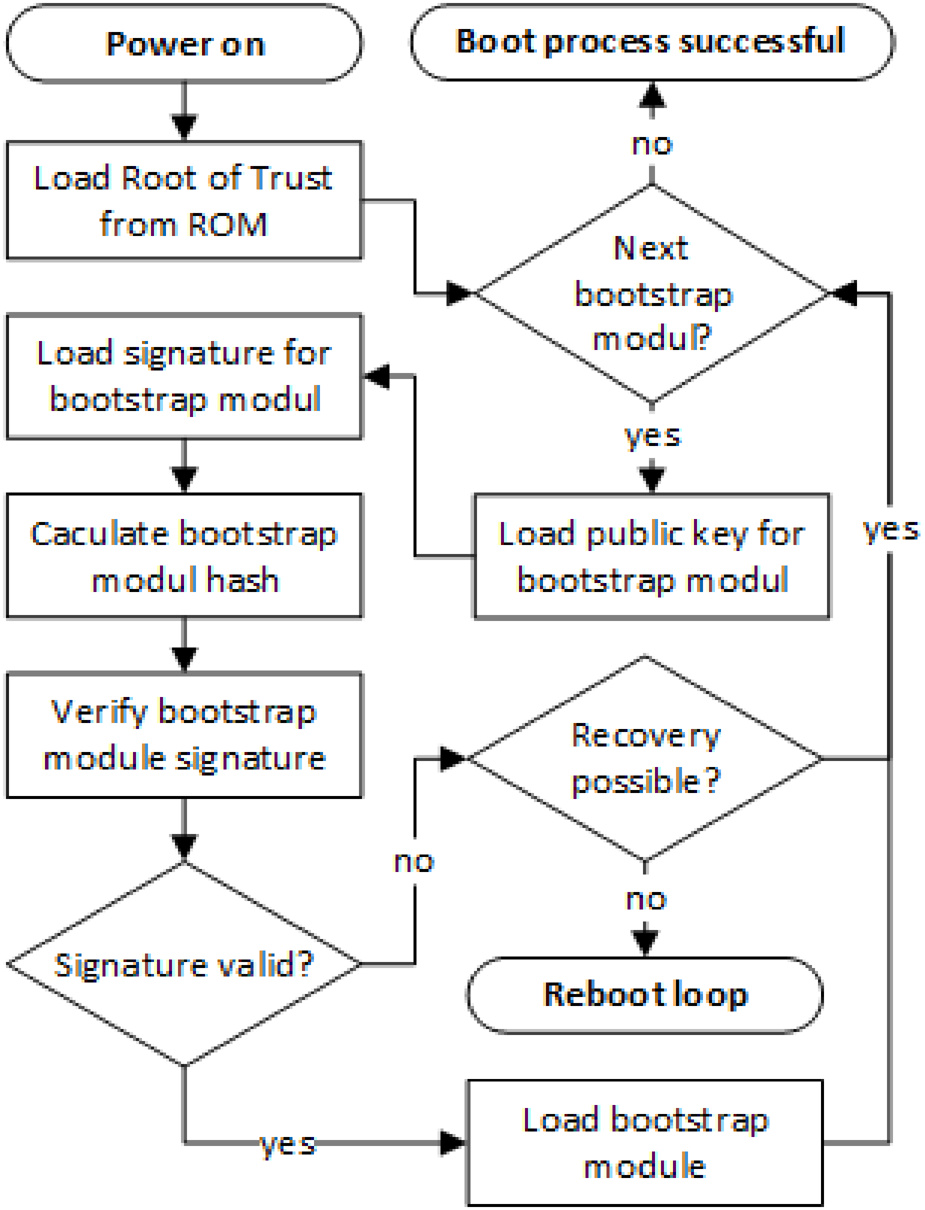
- Use of Secure Boot and Root of Trust combined
- The boot process is organized as a list of bootstrap modules
- The first module in this list is the Root of Trust, which is protected by hardware



SMGW integrity (2)

Boot process with Secure Boot

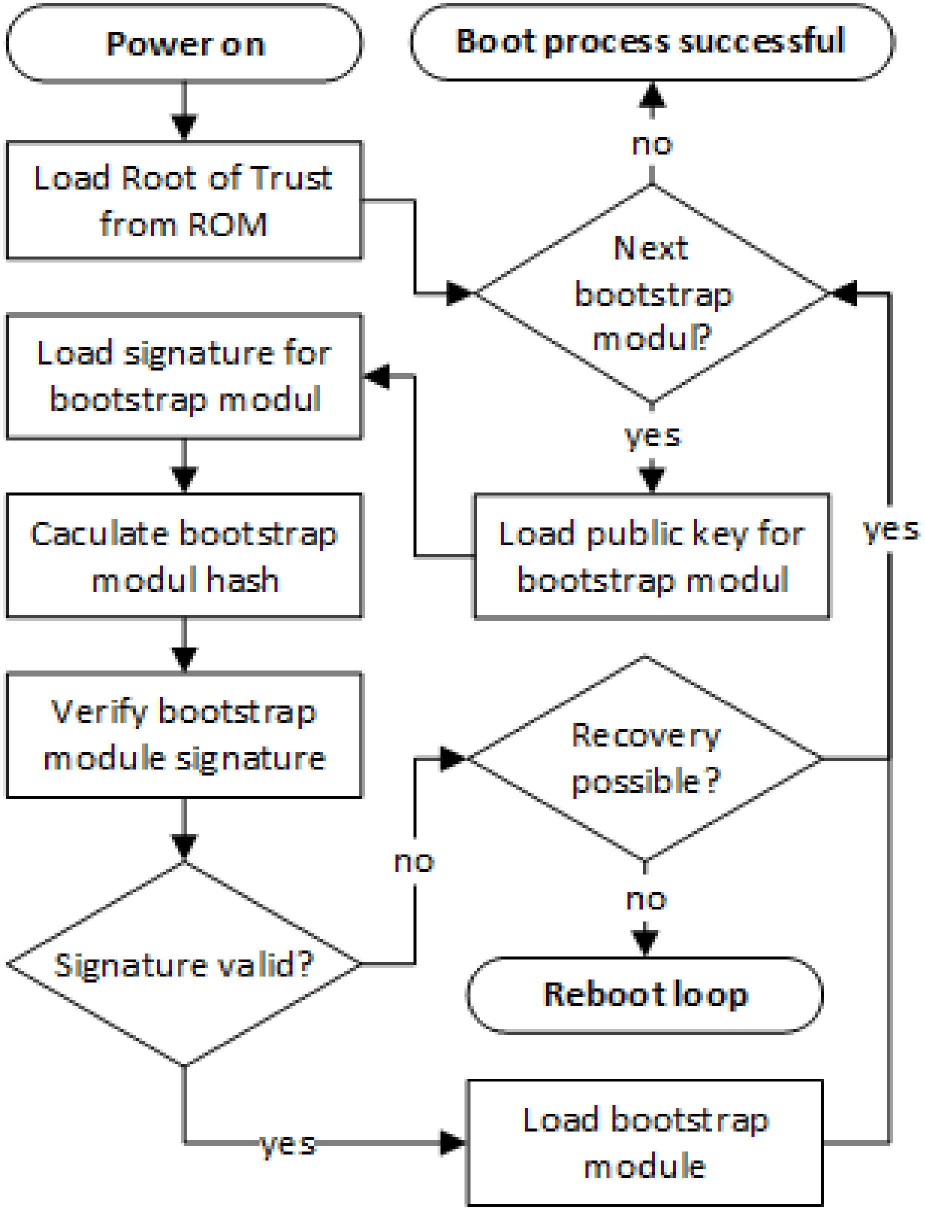
- The Root of Trust holds a reference to the next boot stage, the basic boot loader (bootstrap module *n*)
- Before this module is loaded, the boot loader is verified against a known signature by the Root of Trust, using a configured fixed public key
- Only if the signature of the boot loader is valid, 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 using a known signature and the corresponding public key



SMGW integrity (3)

Boot process with Secure Boot

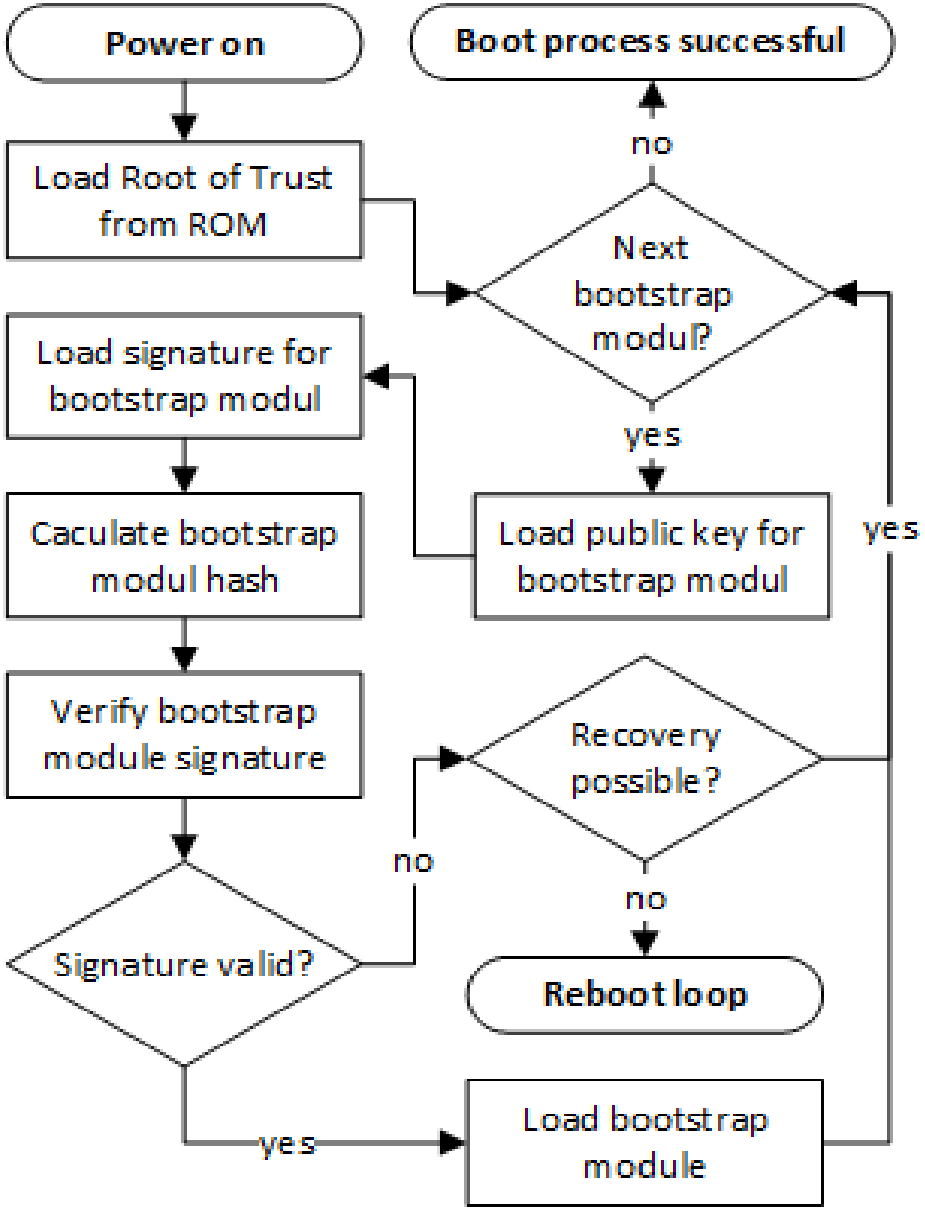
- If the signature is correct, the operating system is loaded and in turn may verify additional software (bootstrap module *n+m*) by using known signatures and public keys
- As soon as the verification fails, the boot process is interrupted and the system returns to a secure state, if system recovery 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



SMGW integrity (4)

Boot process with Secure Boot

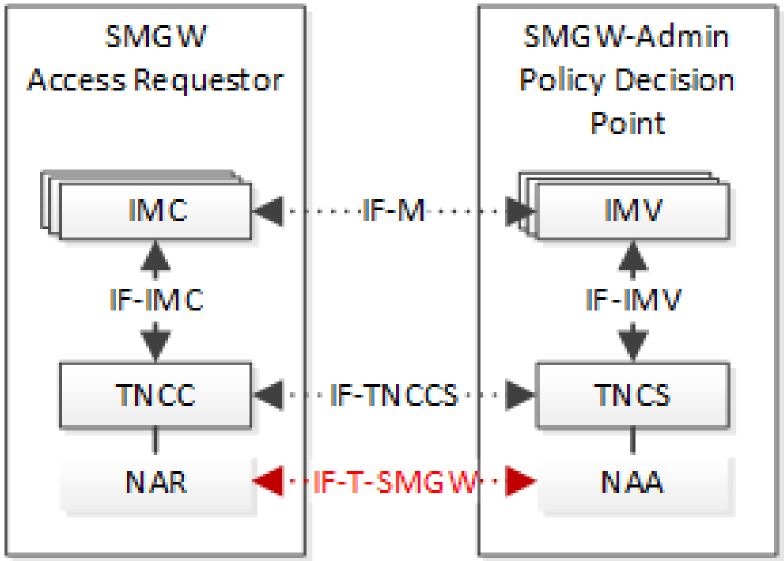
- As long as the boot loader is verified correctly, it is possible to load the firmware from the second partition, if the firmware from the first partition is compromised
- Only if both firmware versions are compromised, the reboot loop is entered
- This ensures that a SMGW is only in use, if the initial boot process was trustworthy



SMGW integrity (3)

Continuous integrity measurements with TNC

- TNC represents a significant security enhancement for smart grids
- SMGW works as access requestor and GWA as policy decision point
- To measure the system’s integrity, the IMC calculates hash values from various system components (e.g. firmware, configuration files or hardware configuration) periodically
- The IMC communicates the measured values to the Integrity Measurement Verifier (IMV) inside the GWA
- IF-T-SMGW is a missing specification in TNC for alert and event messaging (web service specification from BSI is used alternatively)



Conclusion

- Integrity measurement and remote attestation is important
  - Enhancement of the security of the SMGW
  - Improvement of the authenticity of data
  - BSI specifications do not mention similar solutions
- Secure Boot enables basis integrity
  - It is possible to set up a trust chain with TNC
  - Integrity verification is also applied at runtime
  - The measured values of hard- and software components are stored tamper-proof in the file system, because of missing a BSI suitable TPM chip

Outlook

- Standardization of the IF-T-SMGW interface by the TCG(?)
- TPM 2.0 can be used as security module if it will support similar functionality
- Smart grids can be monitored with the optional TNC extension of the interface metadata access point (IF-MAP)
- Central information collection in smart grids for future SIEM (Security Information and Event Management) integration should be prepared

References (1)

(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

References (2)

(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*

Thank you for your attention!

…and I'm open for discussions.