



Technical Security in Smart Metering Devices: A German Perspective

S4 SCADA Security Scientific Symposium
2012-01-18, Miami Beach FL / USA

Dr. Stephan Beirer
s.beirer@gai-netconsult.de

Holm Diening
h.diening@gai-netconsult.de

Sichere eBusiness Lösungen ...

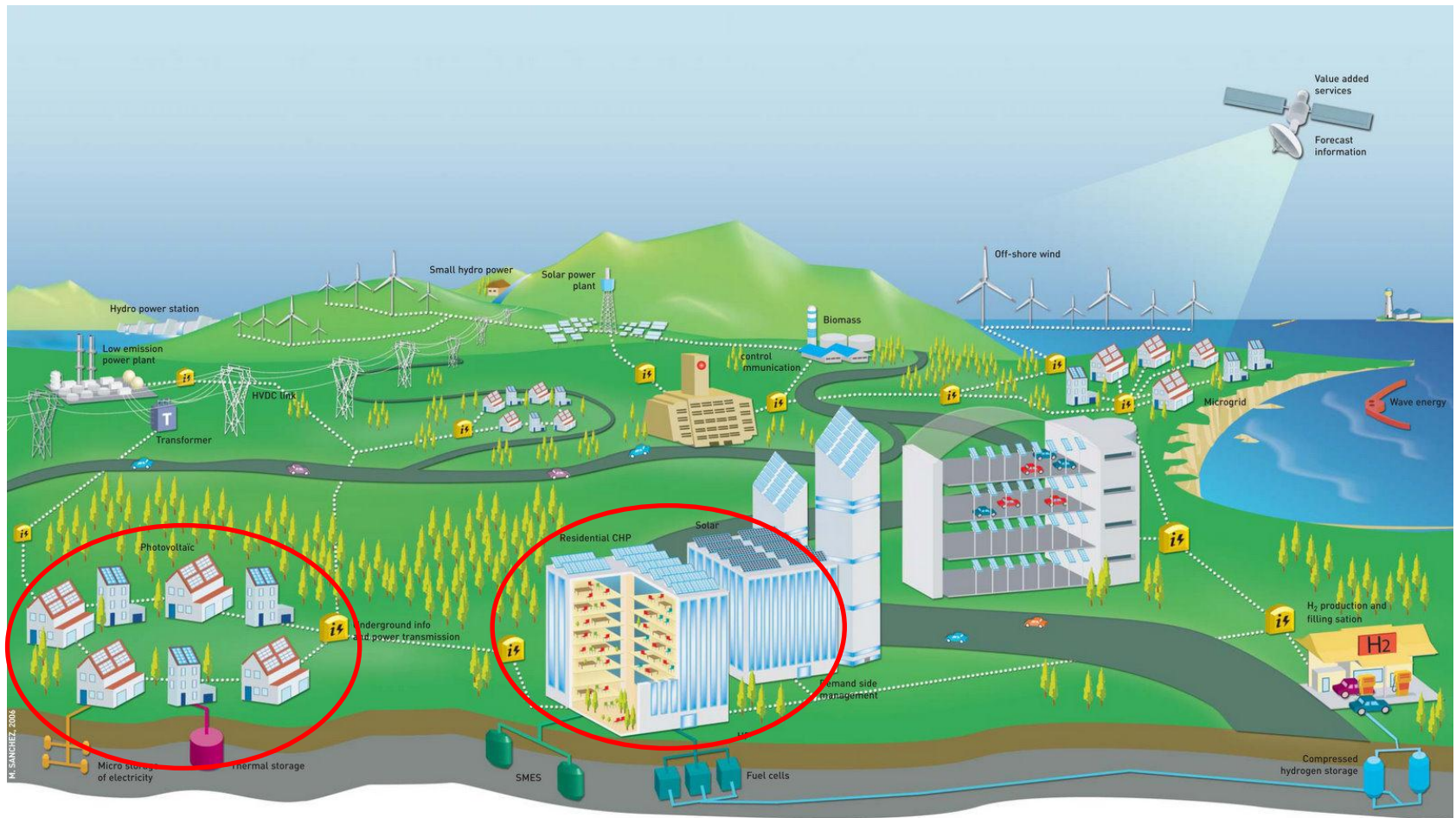
... komplett aus einer Hand.

Am Borsigturm 58, 13507 Berlin/Germany

Tel / Fax: +49 30 417898-0/-300
E-Mail: info@gai-netconsult.de
Web: www.gai-netconsult.de

- Background of the Protection Profile development
- A (very) short introduction to Protection Profiles / Common Criteria
- The German Smart Meter Protection Profile: an overview
- Future development and roadmap

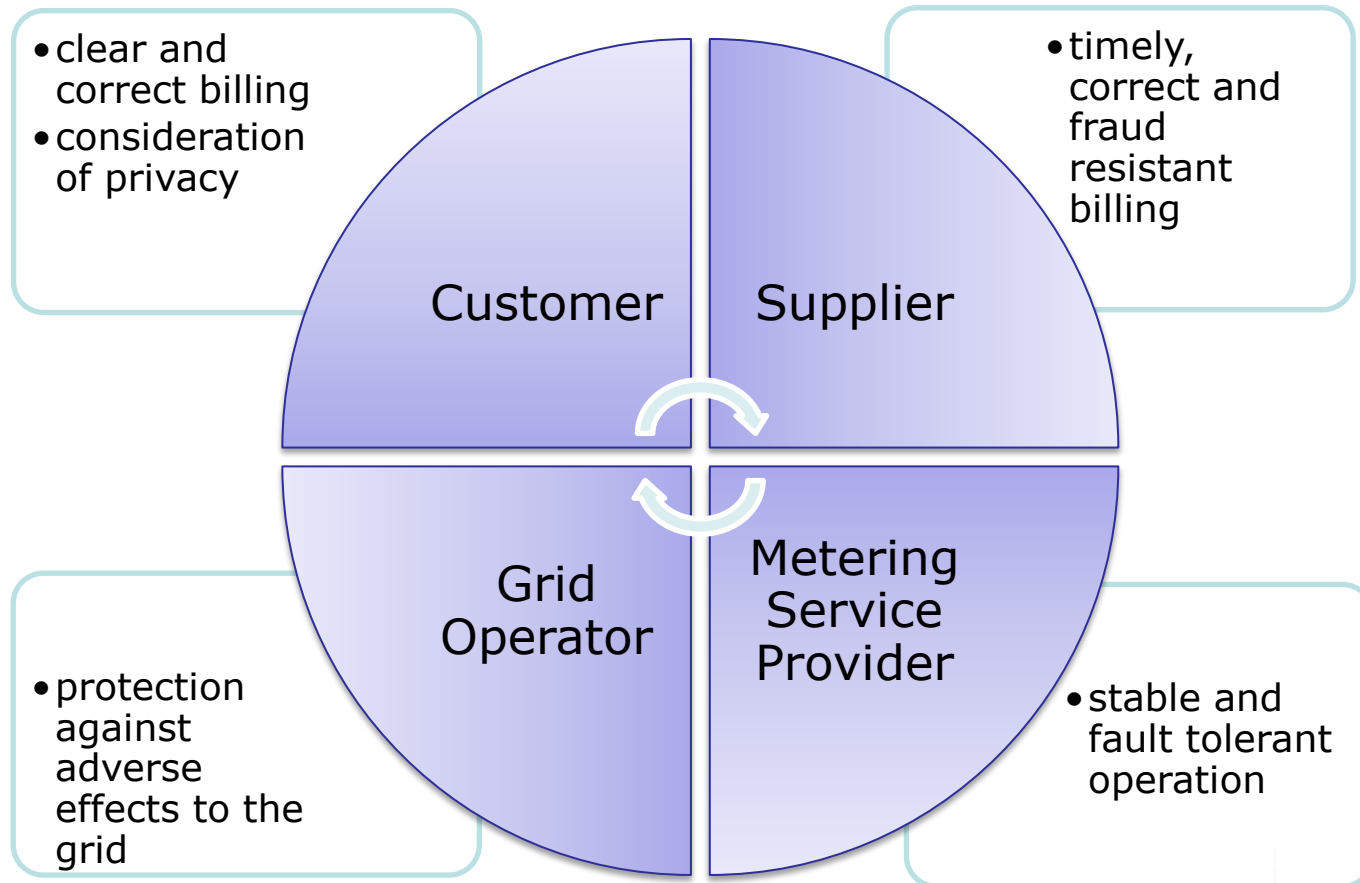




SRC: smartgrids.eu

- Smart Metering devices are the link between the future Smart Grid and the consumer and local small-scale generation

- Which expectations do stakeholders associate with the term „Secure Smart Metering“?



- First version of the Smart Meter Protection Profile is one deliverable of the „e-energy / EDeMa“ research project (2009)



- ❖ Funded by the German Federal Government
- ❖ Participants: Utilities, vendors and academia



- Main goals of the EDeMa project (very simplified)

- ❖ deal with dynamics of distributed generation by stimulating flexible demand on the client side
- ❖ develop a marketplace for automatic energy trade that includes the “prosumer” (producer & consumer) as an active trader
- ❖ develop a Smart Metering gateway for home installations that is capable of the required functions **and secure**

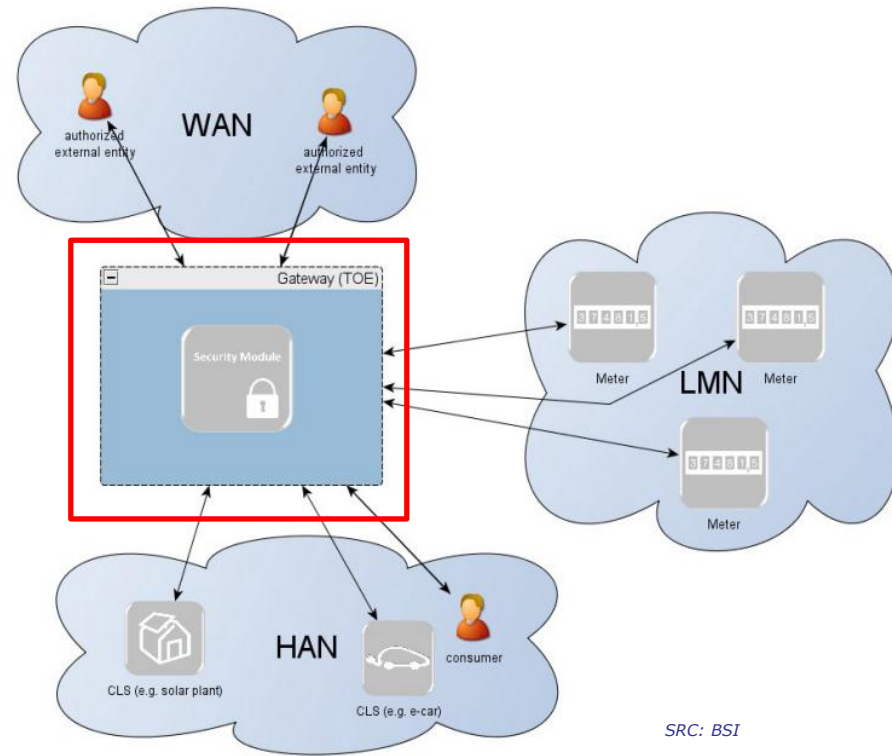


■ TOE is the **gateway** between:

- ❖ WAN, i.e. external parties
- ❖ the local meters for electricity, gas, heat..
- ❖ Automation devices, e.g. home automation and local generation (solar power system, CHP etc.)

■ Gateway Function:

- ❖ Securely relay metering data
- ❖ Provide secure access to automation gear, e.g. for load shedding



SRC: BSI



- Current legislation requires to deploy remote accessible Smart Meter devices in every new installation
 - ❖ Discussion about mandatory replacement of existing meters
- As German consumers may be forced by law to accept Smart Meter devices ...
 - ❖ it is necessary that a federal agency defines the security standards
 - ❖ high level security and privacy standards are required to gain commitment from
 - Federal Commissioner for Data Protection and Freedom of Information
 - Federal Ministry of Consumer Protection
 - several consumer protection NGOs and ...
 - **the general public**
 - ❖ German "BSI" issued a revised version of the EDeMa PP:
"Protection Profile for the Gateway of a Smart Metering System"



- Background of the Protection Profile development
- **A (very) short introduction to Protection Profiles / Common Criteria**
- The German Smart Meter Protection Profile: an overview
- Future development and roadmap



■ Common Criteria (CC): „Common Criteria for Information Technology Security Evaluation“

- ❖ Current Version: 3.1 (ISO/IEC 15408 is still V2.3!)
- ❖ Joint project of AU, NZ, DE, FR, UK, JP, CA, ES, US

■ Goal:

- ❖ development of a formal language for the definition of security requirements for technical products
- ❖ definition common methodology for the evaluation
- ❖ mutual recognition of evaluation results among contributing countries

■ non-Goal:

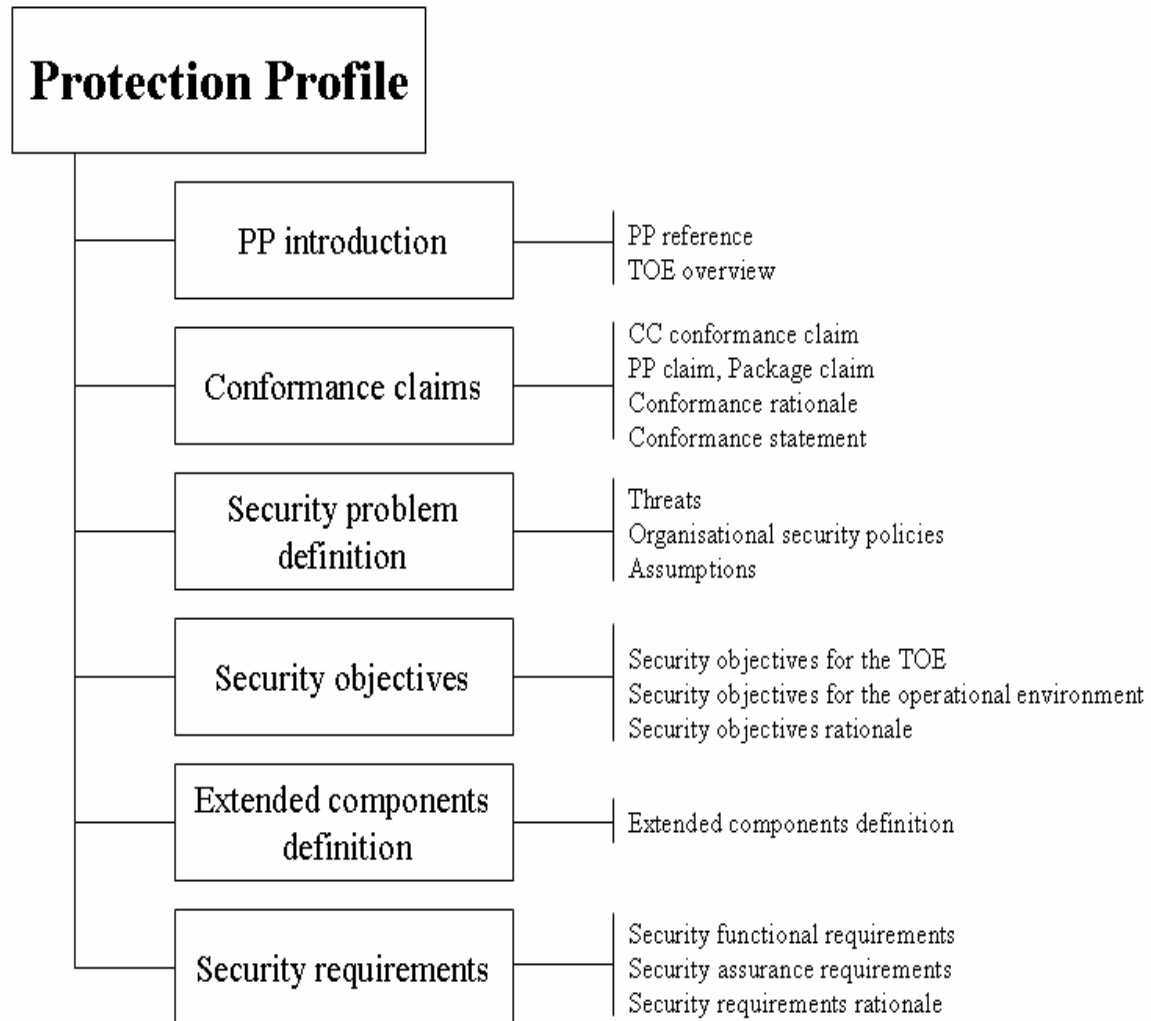
- ❖ aspects of information security in large IT environments or secure IT operations in general (contrary to ISO 27001, IEC 62443, ISA 99 etc.)



- Protection Profile = specification of security requirements for a group of products
 - ❖ Definition of the “security problem” (threats, assumptions, ..) and the requirements to address that problem
 - ❖ Requirements for the assurance measures that the TOE meets the security specifications
 - ❖ A PP does not dictate detailed specifications
 - but it may give hints on preferred implementations for the author of the final „security target“



- Which **threats** do we consider?
- Which **assumptions** must be considered as being provided?
- Which **security objectives** shall we focus on?
- Required security features of the TOE



- Background of the Protection Profile development
- A (very) short introduction to Protection Profiles / Common Criteria
- **The German Smart Meter Protection Profile: an overview**
- Future development and roadmap



■ Essential threats considered:

- ❖ an attacker (local or remote) tries to **gain access** to the metering data or the Smart Meter configuration / firmware
- ❖ an attacker may try to **intercept** meter readings or configuration / firmware **data during transmission**
- ❖ an external attacker may try **to gain control** over the gateway, the meter(s) or controllable local systems (e.g. controllable loads, generation units or lockdown devices)
- ❖ an external party may try to **obtain more detailed information** from the gateway than actually required to fulfill the tasks defined by its role or the contract with the consumer.



■ Essential security objectives and requirements:

- ❖ Encrypted and authenticated communication with all parties (also with meters if not physically the same device!)
- ❖ Protection of integrity / authenticity of meter data and SW updates
- ❖ Control transmission of meter readings and access to configuration data according to a predefined (updatable) Access Control Profile
- ❖ Pseudonymization of transmissions if applicable (e.g. current load information for the grid operator)



■ Essential security objectives and requirements (cont'd.):

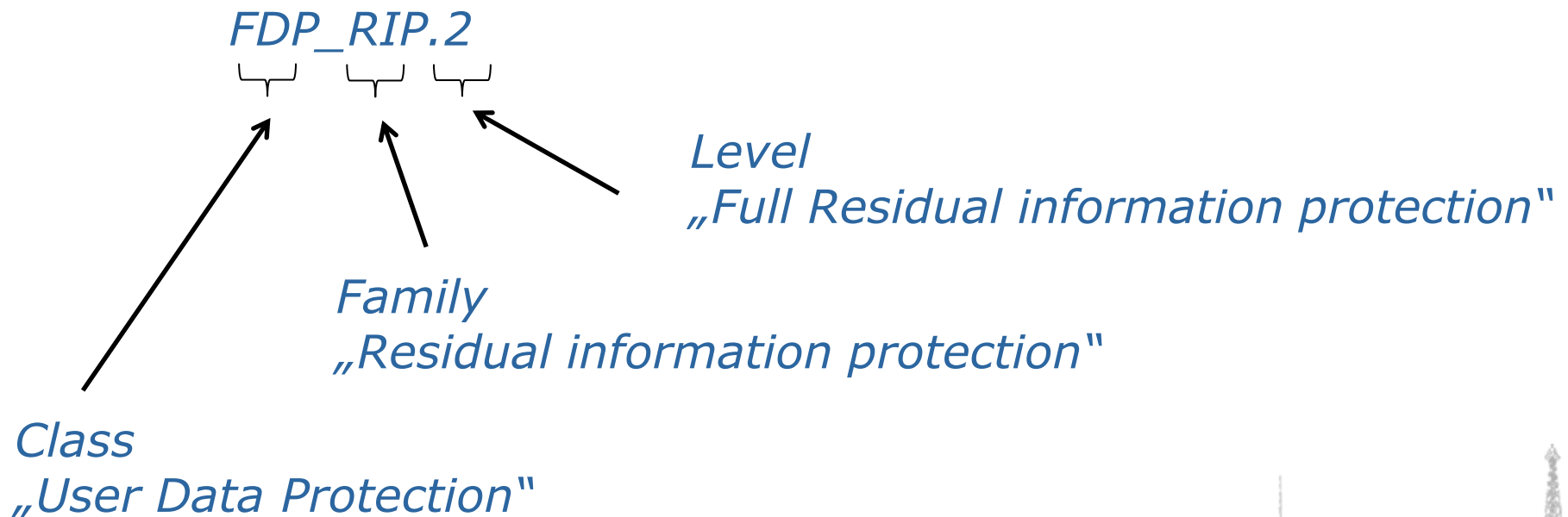
- ❖ Enforce establishment of communication from GW to external parties only (wake-up service for triggering connection establishment)
- ❖ Usage of a security module (e.g. „Smart card“) for crypto functions
- ❖ Detection of physical tampering
- ❖ Comprehensive logging features
- ❖ Concealment of communication [!]



Quelle: willhackforsushi.com /
Joshua Wright



- The Common Criteria use a certain nomenclature to describe "Security Functional Requirements" (CC V3.1 Part 2)
- Example:



- Some important “Security Functional Requirements” of the PP:
 - ❖ Several items from class Security Audit (FAU_*)
 - responsible to enable the user to monitor communication and the admin to maintain the device
 - ❖ Enforced proof of origin (FCO_NRO.2)
 - functions to ensure non-repudiation of transmitted meter readings
 - ❖ Several items from class Cryptographic Support (FCS_*)
 - responsible for communication encryption, signing, signature verification and key management (the utilization of an additional security module is mandatory for the majority of these functions)
 - ❖ Communication concealing (FPR_CON.1)
 - extended (custom) component to describe concealment functions



- Some important “Security Functional Requirements” of the PP (cont’d.)
 - ❖ Several items from class User Data Protection (FDP_*)
 - rules for access to meter and configuration data
 - ❖ Several items from class Identification and Authentication (FIA_*)
 - e.g. for access to controllable loads and generation
 - ❖ Passive detection of physical attack (FPT_PHP.1)
 - physical tampering must be detectable (e.g. broken seals)
 - the highest level “Resistance to physical attack” (FPT_PHP.3) has not been chosen in order to reduce manufacturing costs
 - ❖ ... and many more



- The Smart Meter PP expects the implementation of „Assurance Components“ according to package EAL4 („Evaluation Assurance Level“)
- Augmented by two additional components (EAL 4+):
 - ❖ ALC_FLR.2 Flaw reporting procedures
 - ❖ AVA_VAN.5 Vulnerability Assessment (higher level than in EAL4)
- Aspects of Evaluation in EAL4:
 - ❖ Development
 - ❖ Guidance Documents
 - ❖ Life-cycle support
 - ❖ Tests
 - ❖ Vulnerability assessment



■ Example „Life-cycle Support“

	Assurance components
in EAL4 included	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
augmented by (EAL4 +)	ALC_TAT.1 Well-defined development tools
	ALC_FLR.2 Flaw reporting procedures



■ Example ALC_TAT.1 (Well-defined development tools)

Developer action

The developer shall identify each development tool being used for the TOE.

The developer shall document the selected implementation-dependent options of each development tool.

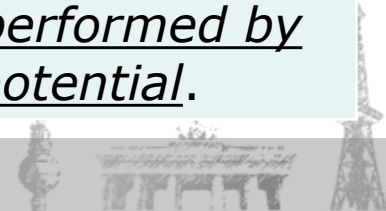
Evaluator action

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.



- Example AVA_VAN.5 “Advanced methodical vulnerability analysis” (highest order Assurance Component from „Vulnerability Assessment“)

Developer action	Evaluator action (The evaluator shall ...)
The developer shall provide the TOE for testing.	- perform a search of public domain sources to identify potential vulnerabilities in the TOE.
	- perform an independent, methodical vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE.
	- conduct penetration testing based on the identified potential vulnerabilities to determine that the TOE is <u>resistant to attacks performed by an attacker possessing high attack potential.</u>



- Background of the Protection Profile development
- A (very) short introduction to Protection Profiles / Common Criteria
- The German Smart Meter Protection Profile: an overview
- **Future development and roadmap**



■ Current status

- ❖ Version 1.1.1 „Final Draft“ is published
- ❖ Evaluation started 2011/08/26
- ❖ A technical guideline for the assurance of interoperability of Smart Metering gateways and the PKI is currently in development

■ Summer 2012: Decision about mandatory replacement of existing meters

- ❖ based on a cost/benefit analysis which is currently being carried out by the Ministry of Economics and Technology



■ Further information

- ❖ www.bsi.bund.de/DE/Themen/SmartMeter/smartmeter_node.html
(German only)
- ❖ www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartMeter/PP-SmartMeter.html
(Protection Profile, English)



- Smart metering gateways are an important part of the future Smart Grid infrastructure
 - ❖ Secure processing of metering data
 - ❖ Secure control of loads and distributed generation

- *A Protection Profile for the Gateway of a Smart Metering System* has been developed by the German BSI

- The German Energiewirtschaftsgesetz (energy industry act) will require the use of CC certified gateways for future installations



Q & A

