Federal Office
for Information Security

The BSI Certification Scheme Smart Metering Gateway PP/TR

Bernd Kowalski

Head of Department S – Secure Electronic IDs, Certification and Standardisation

Brussels, June 27th 2012

BSI at a glance

- We are **Germany's national IT-security agency**
- Founded in 1991
- Certification according to CC and ITSEC
- Accredited Evaluation Labs: 15
- Types of Products certified:
  HW, smartcard-controllers, OS, SW
- Protection Profiles released: >20
- Conformity Testing since 2005

German Certification Scheme

Certification of products

Common Criteria
IT-Security

Technical Guidelines
Conformity

Certification of systems

ISO 27001 / IT-GS
IT-Security

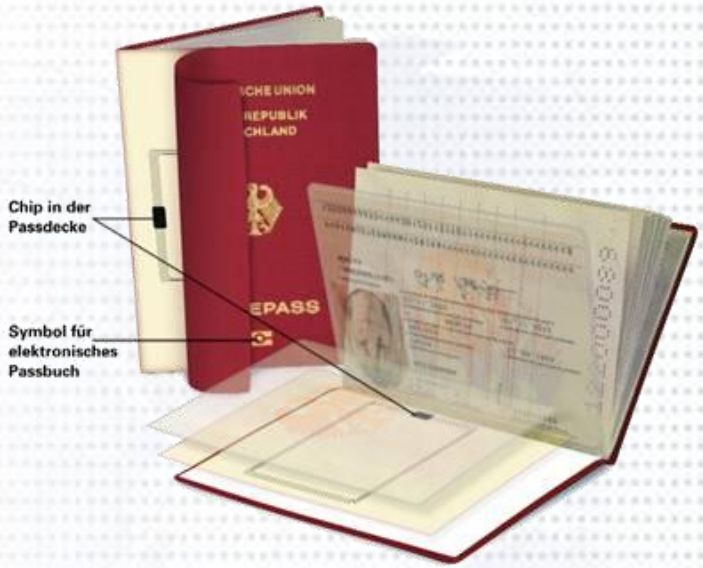
Accreditation and Certification of facilities and persons

Increasing need for IT-Security Certification

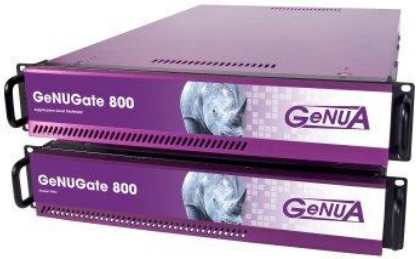
Fingerprint sensor

Digital Tachograph

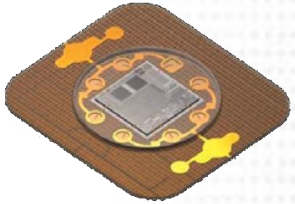
Mainframe OS



Electronic passport (ePass)



Firewall



Smartcard Controller

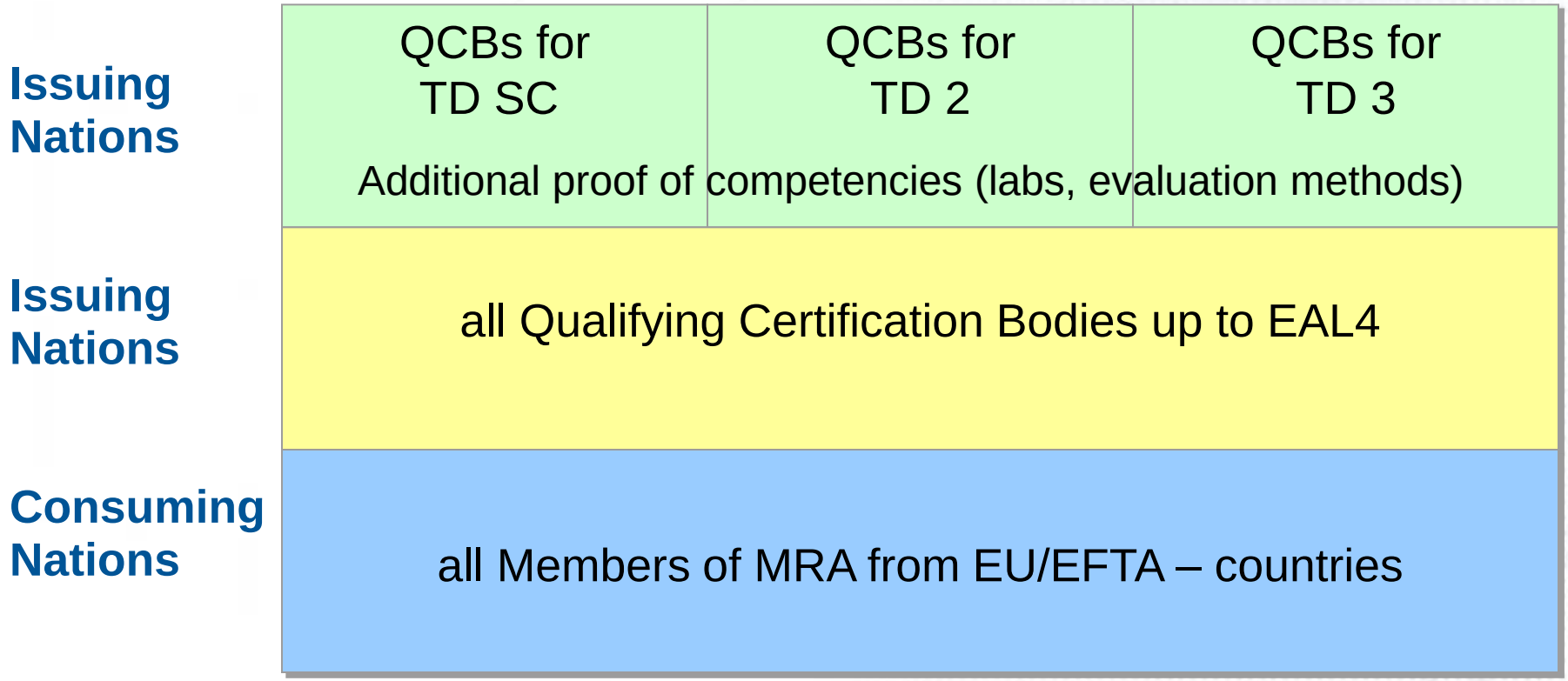
Trusted Platform Module

History SOGIS – MRA
- In a nutshell -

- EU Council Decision of 31 March 1992 (92/242/EEC) in the field of security of information systems
- Council Recommendation of 7 April 1995 (95/144/EC) on common information technology security evaluation criteria
- SOGIS - Mutual Recognition Agreement
  - first issue 21 November 1997
  - SOGIS MRA V2.0 (April 1999)
  - SOGIS MRA V3.0 (April 2010)
- « Saragossa Agreement »

Saragossa Agreement – Key Points

Recognition Status MRA V3.0



TD: IT – Technical Domain / SC: Smart card and similar devices

European Perspectives for SOGIS – MRA

European projects rely on CC evaluation

- making recognition an essential issue (electronic signature, tachograph, SEPA/banking sector, epass, GALILEO, A400M, …)
- create opportunity for EU Directives to initiate or reference SOGIS-MRA standards

EU member states

- should keep control and take the lead in establishing IT-Security certification policies in Europe.

The SOGIS-MRA group

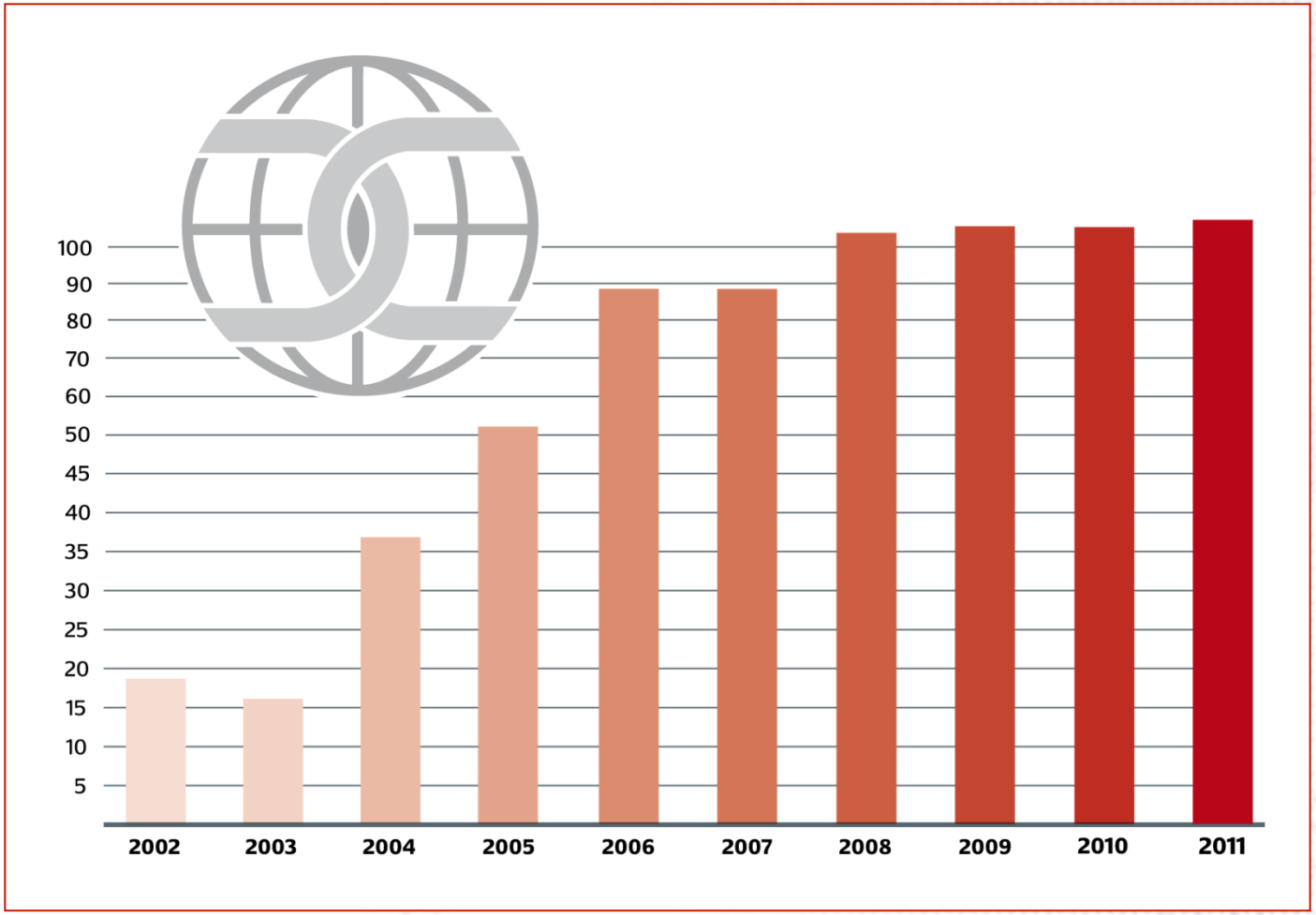
- seems to be the ideal group to define and implement
  - European IT-Security certification policies,
  - standards for product evaluation and
  - European policies for mutual recognition of such certificates.

Mutual Recognition - CCRA

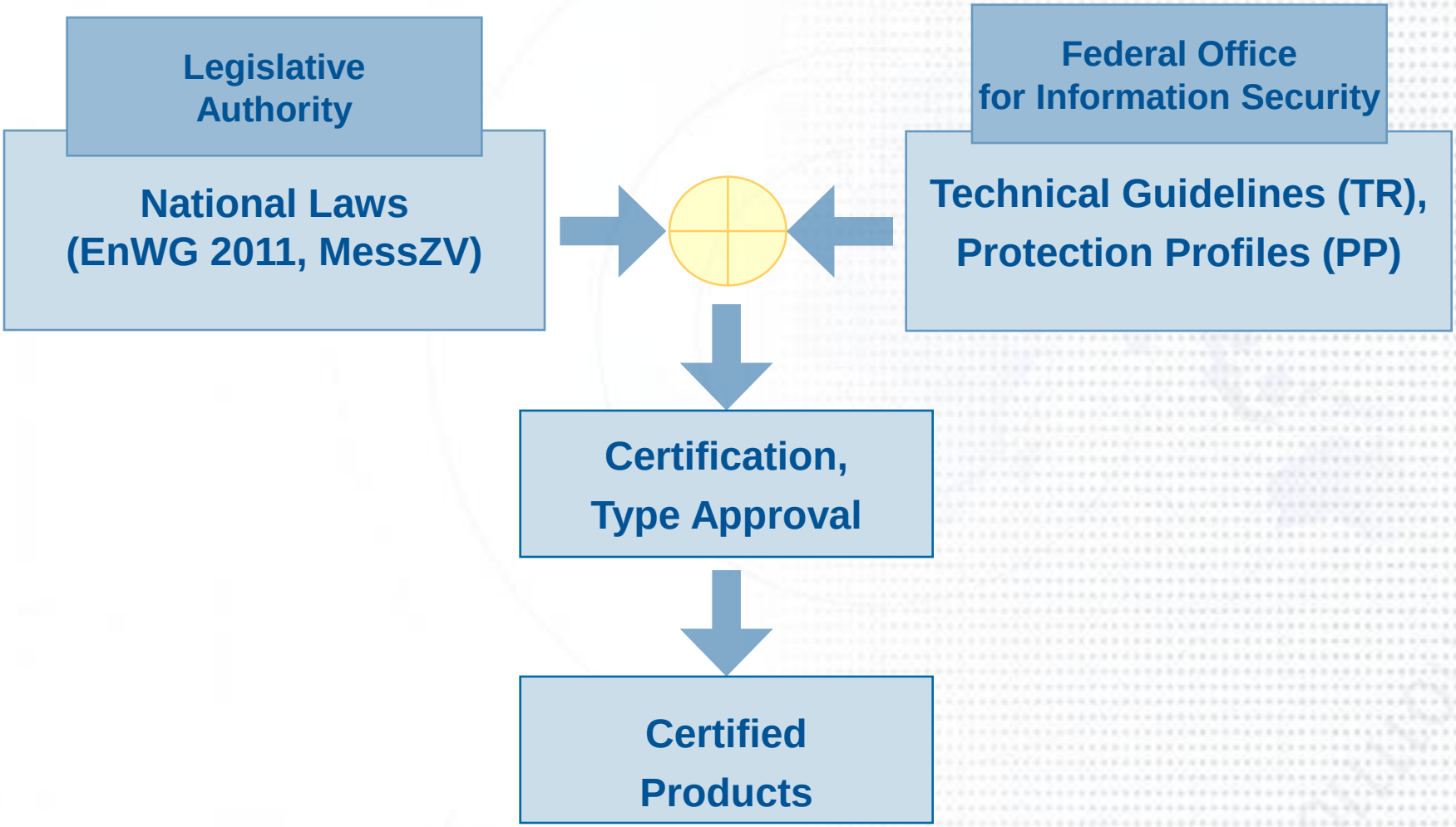
Certificate issuing and consuming Nations		Certificate consuming Nations	
Australia/ New Zealand	USA	Finland	Greece
Canada	Germany	Israel	Malaysia
United Kingdom	France	Denmark	Hungary
Norway	Netherlands	Czech Republic	Rep. of Singapore
Japan	Spain	Austria	Pakistan
Sweden	South Korea	India	
Italy	Turkey		

Market development of CC certified Products

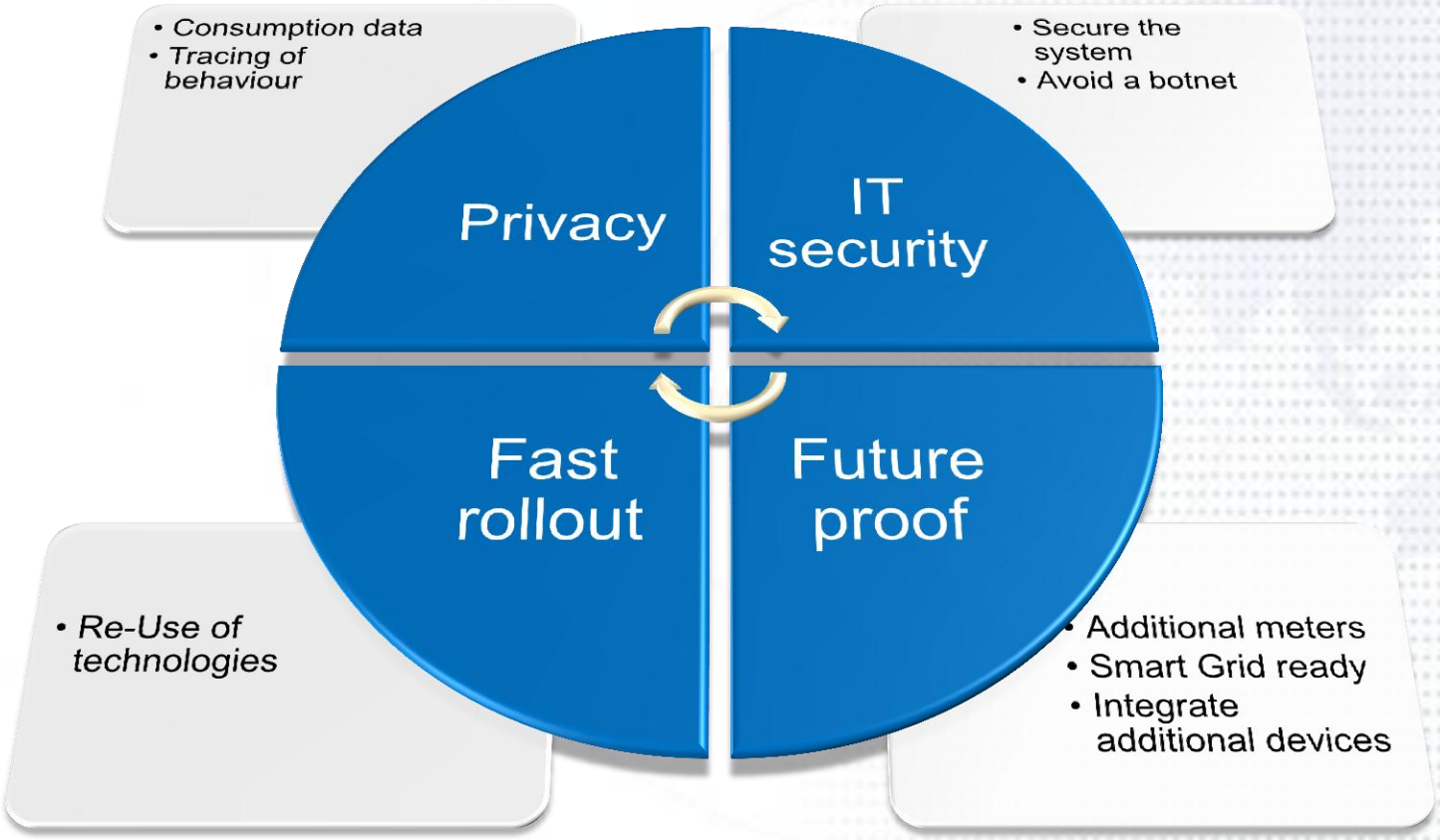
BSI Certificates



Normative IT-Security Standards
e.g. Smart Meter Gateway



Smart Meter Gateway
The technical challenge



Smart Meter Gateway
The German approach

Common Criteria

- Protection Profile for the Gateway
- Protection Profile for the Security Module

Technical Guideline

- Define minimum functionality of the system
- Define requirements for interoperability
- Specify requirements on cryptography and PKI

Calibration

- Gateway becomes relevant in calibration
- Requirements on meters to be avoided

Smart Meter Gateway
The project

- The project started in October 2010
- Gateway PP and Technical Guideline (TR) have been developed by the BSI
- Along with the development of the Protection Profile / Technical Guideline six symposiums were held to keep relevant stakeholder involved
- More than 2.000 comments have been received and discussed during the development of the PP / TR
- The PP is currently available as a final draft, the TR as a draft V0.50

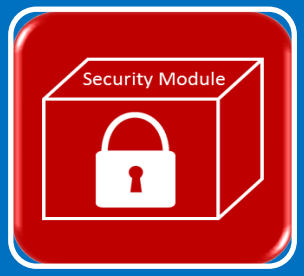
The international context

- Common Criteria has been chosen to use an internationally recognized set of criteria
- The concept of Protection Profiles allows the definition of minimum requirements but still allows a developer to extend the functionality
- Other standards (e.g. Conformity to European M/441 Smart Meter Coordination Group) have been considered
- Requirements on meters have been avoided in order to allow the further use of MID conformant meters

The system approach

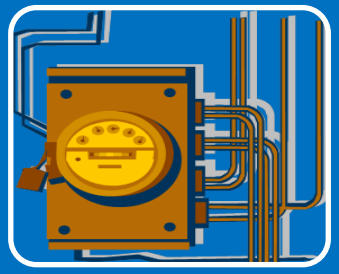
Gateway

- Central component of the smart metering system
- Rich in functionality
- Evaluated in depth



Security Module

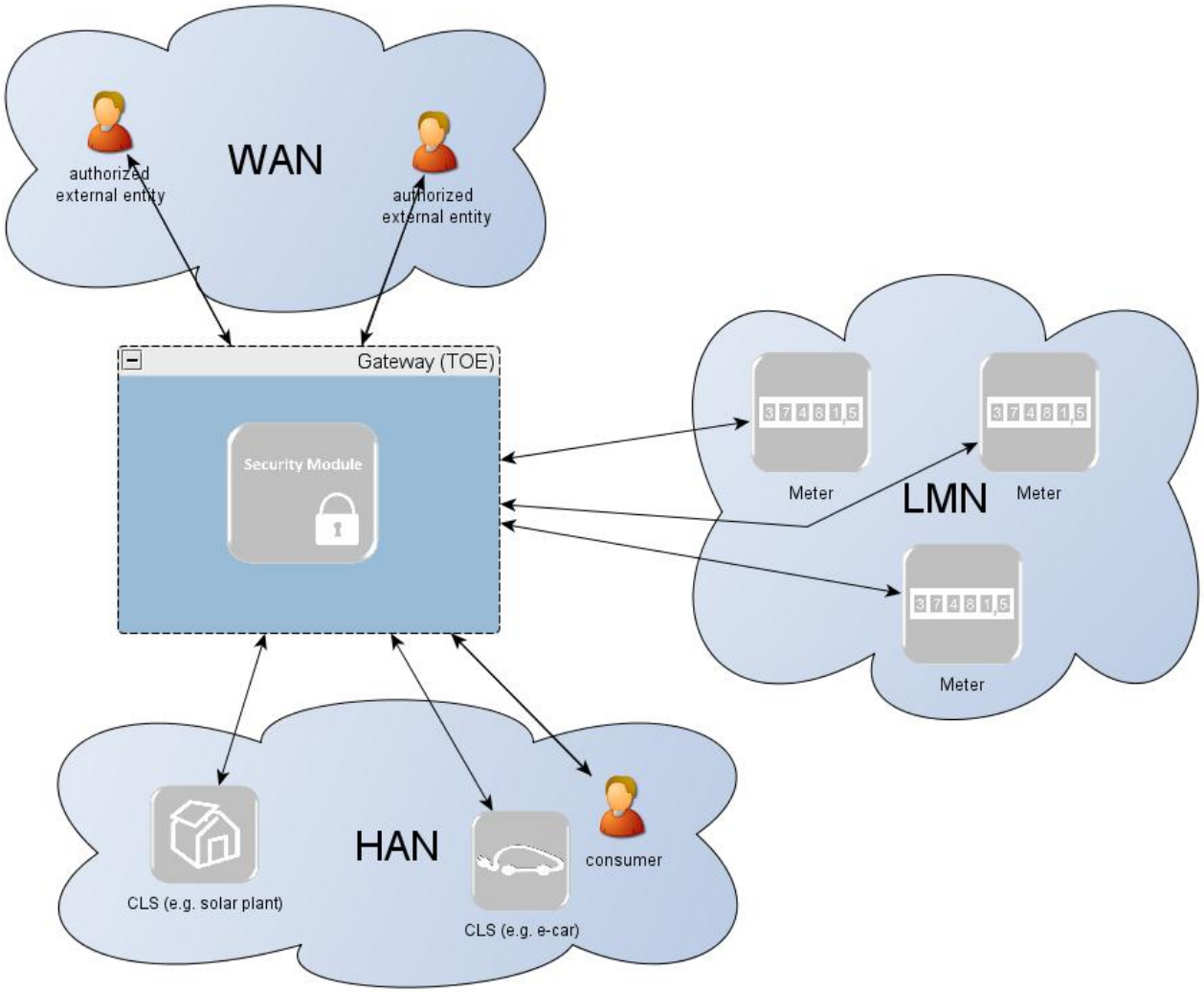
- Implementation of cryptographic primitives
- Secure Handling of key material
- Facilitate a fast rollout by re-use of existing technologies



Smart Metering System

- Comprising a Gateway and multiple meters

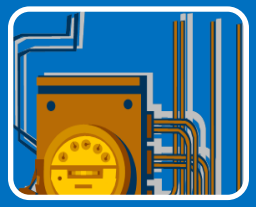
The system from the perspective of the Gateway



Main functionality of the Gateway

Firewalling

- The Gateway has control over all information flows
- Connections may only have their origin locally
- The Gateway is not directly contactable



Metering Policies

- The Gateway receives data from meters
- The Gateway processes the data according to installed profiles
- The Gateway submits the processed data to external parties in the WAN

Privacy Protection

- All information flows are transparent for the user
- The Gateway only allows encrypted and authenticated information flows
- The Gateway is able to conceal information flows if necessary

Communication for CLS

- The Gateway allow Controllable Local Systems to contact parties in the WAN
- The CLS have to follow the policies for information flow of the Gateway

Functionality of the Security Module

Cryptography

- Key Negotiation for TLS
- Key Transport for content data
- Signature Generation and Verification

Storage of Key Material

- Asymmetric key material as the identity of the Gateway
- Symmetric keys to be used by the Gateway

Random Number Generation

- For internal use
- For various purposes to be used by the Gateway

Main points of discussion

- Smart Meter Gateway in context of other requirements
- Centralized vs. De-centralized approaches
- Physical Security
- Local visualization
- Local management and the local attacker
- Connection policy

Centralized approaches vs. de-centralized

- The centralized approach
  - Many business cases and processes around smart metering base on a centralized concept
  - The Smart Metering system will send consumption data in high resolution to a centralized system
  - The system will apply tariffs, control the data and share the data with authorized parties
- The de-centralized approach
  - The Smart Metering System itself (the Gateway to be precise) handles the data
  - Only results of tariffs are submitted to external parties
  - The consumer keeps control over their data (at least physically)
- The German requirements support both approaches

Aspects of the smart grid
Controllable Local Systems (CLS)

- Smart Meter Gateway supports communication with various external parties
- Gateway supports flexible tarifs
- Gateway provides communication channels to local systems (CLS)
- Those CLS may comprise
  - Local energy production facilities (e.g. control solar plants, § 6 EEG)
  - Energy management facilities (control local consumption facilities [§ 14a EnWG], control local production facilities [§ 6 EEG])

Conclusions and Perspectives

- CC-Certification improves IT-Security & IT-Product quality
- World-wide increasing number of certificates and PPs
- Success factors:
  - Mutual recognition according to CCRA/SOGIS-MRA
  - Common Criteria as an International Standard
  - European coordination by SOGIS-MRA members
  - Referenced by European/national regulation and public procurement
- Certification required in both, the public and private Sector
- Certification Policy is part of the National Plan for Information Infrastructure Protection in Germany
- Development of Protection Profiles as a collaborative action between European standards bodies and SOGIS-MRA

Contact

Federal Office
for Information Security (BSI)

Bernd Kowalski
Godesberger Allee 185-189
53175 Bonn
Germany

Bernd.Kowalski@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de
www.bsi.bund.de/SmartMeter