Federal Office
for Information Security

The German IT security certification scheme

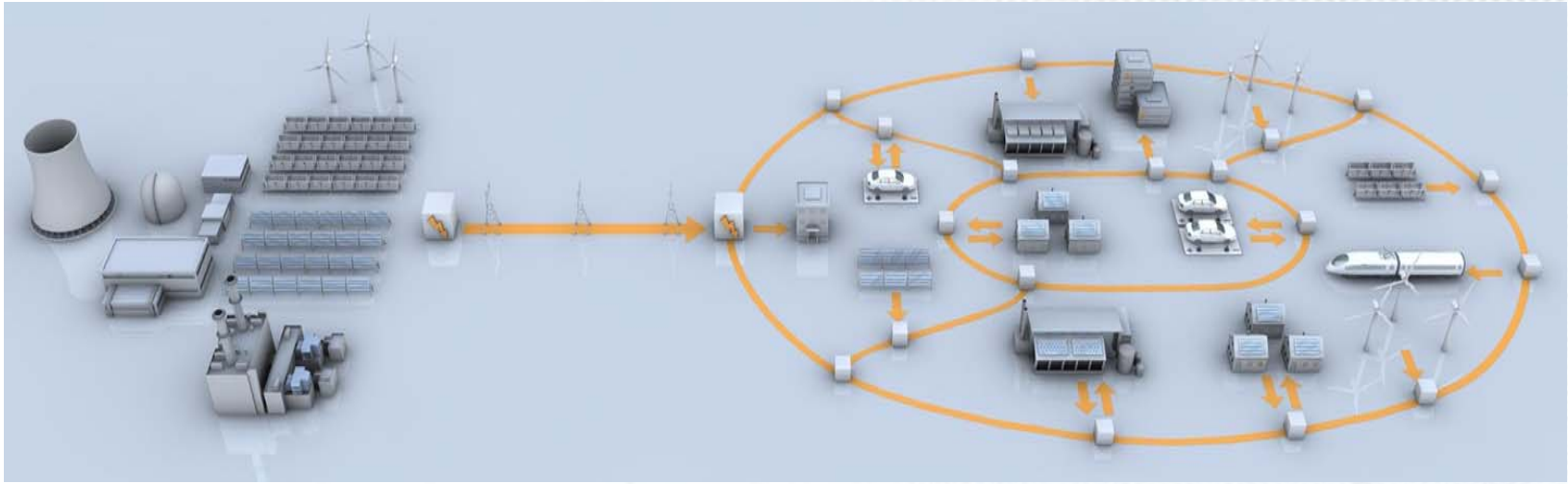
- Growing Importance of IT-Security Certification
- BSI Certification Services
- Technical Guidelines and Protection Profiles for Smart Metering in DE
- Remarks about the ENISA report
- Mutual Recognition: CCRA & SOGIS-MRA
- Certification Policy Matters
- Summary

Bernd Kowalski

Federal Office for Information Security

Heidelberg, September 30th 2014

Growing Importance of IT-Security Certification



- Economy & Society depend on availability and integrity of IT-Systems
- Lack of Privacy and Trustworthiness in mainstream products
- Public and national security affected
- Governments under pressure to set guidelines for appropriate technical standards and third party evaluation resp. certification

Federal Office
for Information Security

BSI Certification Services

Certification of products

Common Criteria
IT-Security

Technical Guidelines
Conformity

Certification of systems

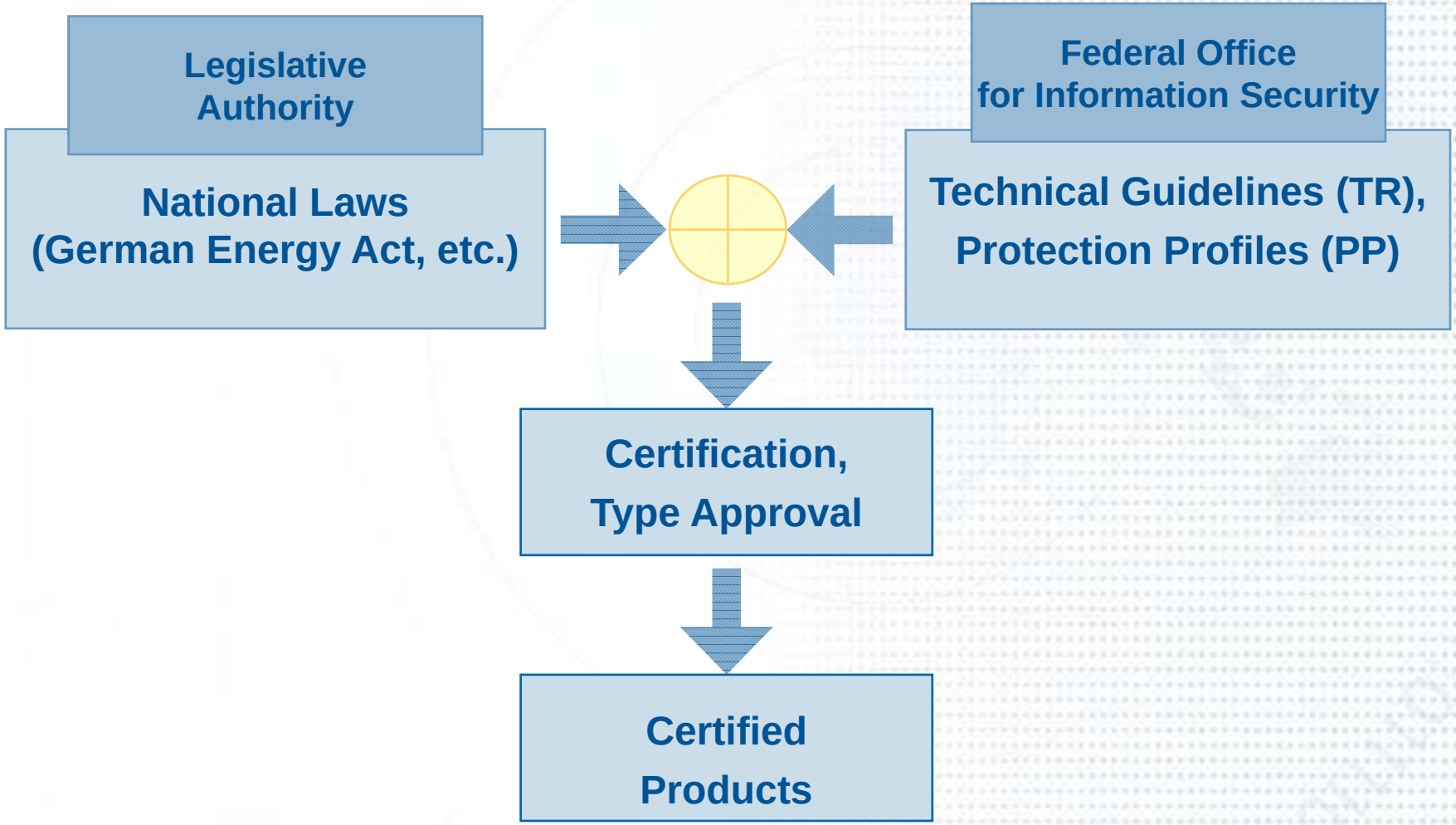
ISO 27001 / IT-GS
IT-Security

Recognition and Certification of evaluation Labs, evaluators, security service providers e.g. ISO/IEC 17025

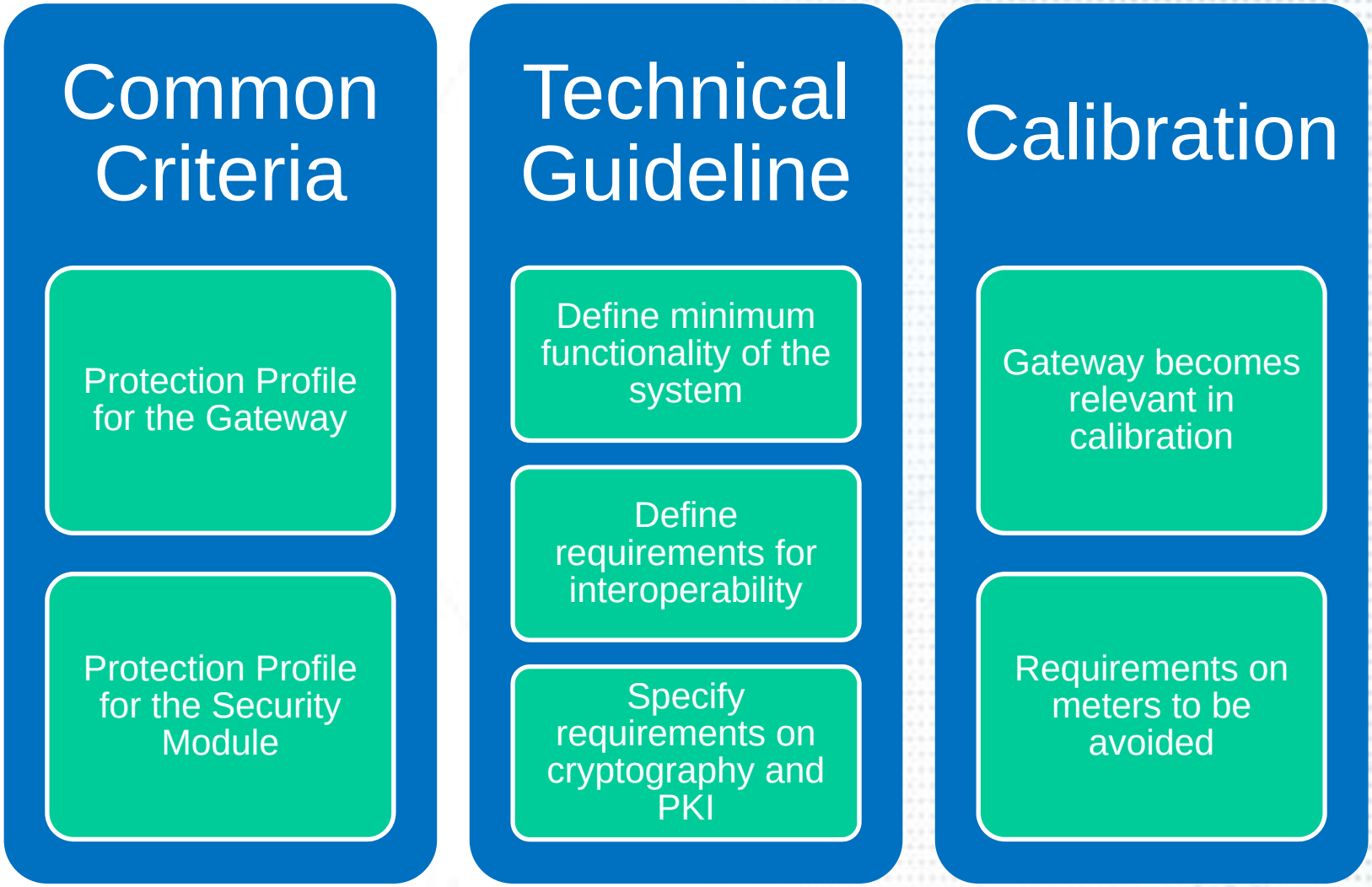
BSI Certification Services

- **Product Certificates** on the basis of **Common Criteria**/PP
  - Smartcard hardware & software
  - Digital Tachograph components
  - Operating systems, firewalls, signature applications
  - Biometric verification systems
  - eID and electronic passport
  - Smart Meter Gateway
- **Product Certificates acc. to Technical Guidelines**
  - Conformity and compatibility of IT security components
- **Certificates for IT-infrastructures acc. to ISO 27001** on the basis of IT-Grundschutz
- BSI-CC-Scheme has been **approved** under the **European Accreditation System**

Technical Guidelines and Protection Profiles
TR and PP for German Smart Metering

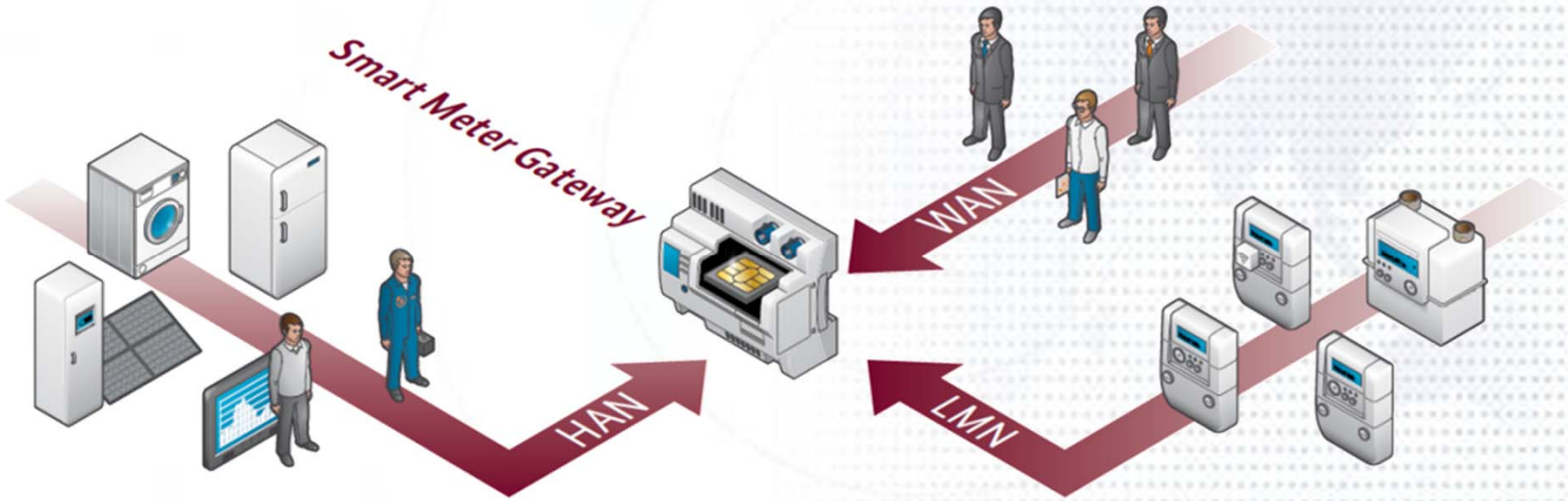


Technical Guidelines and Protection Profiles
Smart Meter Gateway - German approach



Technical Guidelines and Protection Profiles
SMGW and the Smart Grid

Wide Area Network (WAN):
Authorized clients (energy and service providers, SMGW Admin)



Home Area Network (HAN):

Authorized clients (consumers, service technicians) / Controllable Local Systems (CLS)

Local Metrological Network (LMN):
Registered meters

Remarks about the ENISA report: "Smart Grid Security Certification" (1/3)

- **"European Smart Grid Certification Scheme" as a term is misleading**
  - Existing national certification schemes
  - Organised in a Mutual Recognition Agreement limited to Europe (SOGIS)
  - Mixes up standardisation of Smart Grid Architectures, security certification of products and certification of IT-systems and infrastructures
- New EU body for accreditation of national schemes **conflicts with** existing
  - Accreditation schemes (national and European)
  - Certification schemes (national)
  - Standardisation bodies (national and European)
- Report **does not focus** on Smart Grids
  - Smart Grids rather as an example for a new European Certification Scheme
  - Existing European Measuring Instruments Directive (MID) is not even mentioned in the report, which is fundamental for a Smart Grid of measuring devices

Remarks about the ENISA report:
"Smart Grid Security Certification" (2/3)

- Smart Grid regulation in Germany has been **incompletely reported**; addition:
  - Conformity to MID-conforming regulations of PTB to be shown by notified body
  - Conformity to Technical Guidelines ensures Interoperability of components
- Introduction promises insight on Trusted Vendors or Supply Chains – **none provided**
- Report should put emphasis on **proposals on how to start European harmonisation of interoperability** and then conclude to **second step on security and risk assessment harmonisation**

Remarks about the ENISA report:
"Smart Grid Security Certification" (3/3)

- **Privacy** as one of the main drivers and success factors for acceptance is being **ignored** in the report
- Different Energy Market Stakeholder situations in Europe have **not been addressed**
- Analysis of existing schemes **should be extended**
  - Currently rather a gathering of standards, does not name a single scheme
  - Tools like Protection Profiles are not identified
  - Existing Expertise in Schemes and Agreements is not being taken into account

Mutual Recognition: CCRA & SOGIS-MRA

CCRA

Recognizing and issuing nations

- *Australia und New Zealand*
- *Canada*
- *Netherlands*
- *UK*
- *US*
- *Germany*
- *Italy*
- *Japan*
- *France*
- *Spain*
- *South Korea*
- *Norway*
- *Sweden*
- *Turkey*
- *Malaysia*
- *India*

Recognizing nations

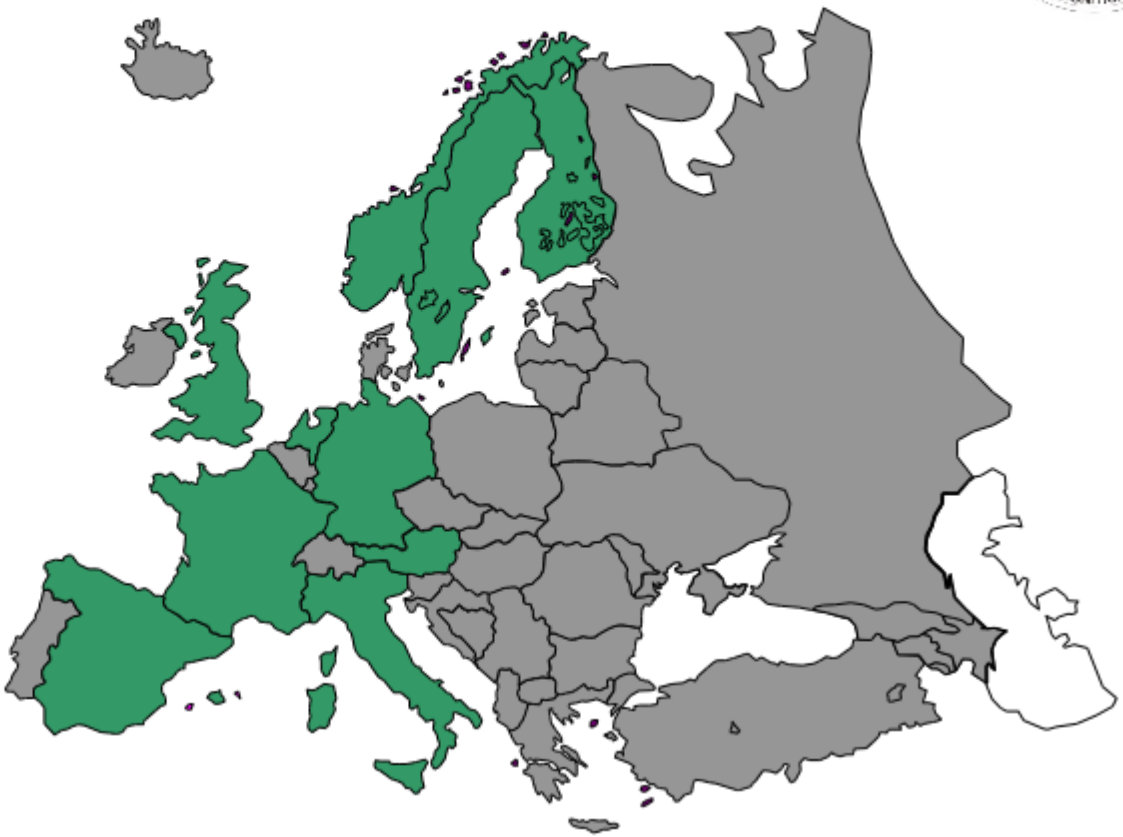
- *Finland*
- *Greece*
- *Hungary*
- *Denmark*
- *Austria*
- *Israel*
- *Czech Republic*
- *Singapore*
- *Pakistan*

www.commoncriteriaportal.org

Mutual Recognition: CCRA & SOGIS-MRA
International recognition

- Austria
- Germany
- Finland
- France
- UK
- Italy
- The Netherlands
- Norway
- Sweden
- Spain

European SOGIS-MRA



Certification Policy Matters
CCRA and SOGIS Policy

New CCRA Agreement and Policy:

- no further mutual recognition beyond EAL Level 2 or collaborative Protection Profiles (Low Assurance Policy)
- motivation: comparable evaluation results in a growing CB-community
- development of "collaborative" cPPs for COTS products starting at EAL Level 1-2 and potentially reaching EAL4 at most.

SOGIS-MRA Policy:

- keep European **High** Assurance Policy up to EAL Level 7
- keep backward compatibility with new CCRA on common standard ISO 15408
- motivation: longterm experience with high assurance PPs and evaluations
- EAL must be fixed to threats, black box evaluation not appropriate

Certification Policy Matters
SOGIS and BSI Policy

Government involvement

- National & European regulations for critical infrastructures require increasing number of PPs to preserve

Certification policy beyond SOGIS-MRA (CCRA and others)

- associated partnerships with selected partners (e.g. Japan)
- combined procedures for low and high level certificates per product
- secure elements are key technology for cloud and mobile services
- defend high assurance standards in TTIP-negotiations

Summary

- Trustworthiness, Security & Privacy rely on Third party evaluation
- Need for Protection Profiles for evaluation
- Application of international Common Criteria standard (CCRA)
- Continue SOGIS-MRA High Assurance Certification Policy
- Public Security and critical infrastructures challenges require government involvement in certification policies and standards
- European High Assurance standards shall not become invalid through TTIP
- Secure Elements are the core technology for trustworthy IT-Systems

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