Legal Regulations and Vulnerability Analysis

Markus Mackenbrock

Bundesamt für Sicherheit in der Informationstechnik (BSI)
(Federal Office for Information Security)
Germany
Introduction of the BSI

- National Authority for Information Assurance established by law in 1991
- Certification according to CC and ITSEC
- Development of test requirements like Protection Profiles (PP) and Technical Guidelines (TG)
- Accredited evaluation labs: (10 for CC)
- Types of products certified: HW, smart card controllers, OS, SW
- Protection Profiles released: >40
- ...
IT-Security Certification at BSI

- Common Criteria Certification Scheme
  - Smartcard Soft- & Hardware
  - Signature and Encryption Software
  - Operating Systems, VPN Servers, Firewalls
  - Key Management Server
- Protection Profile (PP)
  - Security Requirements for a Product Class
- Technical Guidelines (German: Technische Richtlinien TR)
  - Interoperability Requirements for IT-Security Products
- ISO 27001: System Certification for IT-Infrastructures
Product types of (main) interest for CC certification

**Software Products**

- Operating Systems
- PC Security Products
  - Security Shells
  - Integrity Protection
- Data Communication Products
- Firewalls
- Biometric Verification Products
- Signature Applications

**Hardware Products**

- Smart card Reader
- Smart card Controller
- Tachograph Components
  - Motion Sensor,
  - Vehicle Unit,
  - Smart card

Smart cards with OS and Applications, e.g. eHC, ID-card
(Political) Fields of interest

**Increasing political importance for CC Certified Products**

**EU Commission:**
- Digital Tachograph: Directive equivalent to law
- Digital Signature Directive

**NATO:**
- Infosec Technical and Implementation Guidance on the use of Common Criteria within NATO

**Multilateral Defense:**
- Airbus A 400M

**UN/G8:**
- G8 - Principles on Critical Infrastructure Protection

**Germany**
- Digital Signature Law
- Health Cards and related products
- ePassport and eID documents
- Smart Meter

**Acquisition Policies in EU/Germany:** at present in special areas (defense, health sector, ID cards)

**Trend:** increasing importance
Role of BSI

BSI law: Development of minimum security standards

Development of IT security testing requirements at the instigation of the government.

- In agreement with different ministries (or other public authorities) BSI develops evaluation requirements in cooperation with its accredited test laboratories and the IT industry

In detail:
Development of
- Protection Profiles and
- Technical Guidelines (In German: Technische Richtlinien TR) for the evaluation and certification of products and components
Role of BSI

Legislative Authority

National Laws and Provisions

Conformity testing scheme

Test Requirements
→ TG, PP

Certified Products

BSI

Common Criteria
Examples

- ePassport
- German ID card
- German eHealth system
- Digital Tachograph
- Smart Meter Gateway

The Target of Evaluation (TOE) defined in the PP is an electronic passport representing a contactless smart card.
The new German ePass includes biometrics with latest contactless smartcard (ISO 14443) and IT-security technology.

- TOE: RFID-Controller (HW), embedded-SW (OS), MRTD (ICAO) application.
- IT-Security Certification according to CC PPs and conformity-tested according to Technical Guideline.
  - Common Criteria Part 3 conformant
  - EAL 4+, augmented by ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5

Reason: open/hostile environment
The ID_Card Protection Profile (PP) defines the functional and assurance requirements for an electronic identification document.

The Target of Evaluation (TOE) defined in the PP is an Electronic Identity Card representing a contactless smart card. The major scope of an electronic identification document is to be a means which a traveller can present to the inspection system for proving his/her identity.
The TOE type is contactless smart card and comprises the circuitry of the contactless chip incl. all IC dedicated software being active in the operational phase of the TOE (the integrated circuit, IC), the IC Embedded Software (operating system), the ePassport, the eID and, optionally, the eSign applications.

- Common Criteria Part 3 conformant
- EAL 4+, augmented by ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5

**Reason:** open/hostile environment
Key Security Components to be certified:

- **eGK** - Electronic Health Card for 80 Mio citizens replacing the KVK (health insurance card).
- **HPC** - Health Professional Card for more than 500,000 health professionals.
- **B4HC** - Bit4Health Connector, provides access to the central telematics infrastructure.

**according to certified Protection Profiles**

All security relevant components of the Telematic Infrastructure will be evaluated and certified, based on testing requirements like PPs and TRs of BSI.
Data protection rule:

eHC and HPC together support that medical data can only be read or written by approval of the patient (card holder).

No one must have access to medical data without approval of the patient.

The card holder himself controls the access to his medical data.

These rules have to be implemented and realised by security functional requirements and measurements.
The eHC is a microprocessor chipcard (SmartCard) with cryptographic functions.

The personalized eHC contains essential information about the cardholder, the holder’s picture and signature.

PPs for eHC, HPC and SMC require EAL4+, augmented by AVA_VAN.5

**Reason:** open/hostile environment

The purpose of the VU is to record, store, display, print and output data related to driver activities and it also records user activity data in tachograph cards.

It is connected to a motion sensor with which it exchanges vehicle’s motion data.
Certification requirements according to EU Directive:
- specified in „Generic Security Targets“
- in conformity with the Common Criteria Protection Profile concept
- ITSEC, E3 high
- Common Criteria (CC),
  - EAL 4+, augmented by
  - ATE_DTP.2 and AVA_VAN.5

Reason: open/hostile environment
Smart Meter Gateway

**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
Smart Meter Gateway

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
Gateway Security Functionality

- **Firewall** (Separation of WAN, HAN, and LMN)
- **Secure Communication** between CLS and WAN
- **Validation of Authenticity and Integrity of Measuring Data** and processing for and distribution to valid recipients
- **Security Module**, providing cryptographic services and secure key storage
- **Audit** (System-, Consumer-, Billing-Log)
- Common Criteria PP under development:
  - EAL 4+, augmented by
  - **AVA_VAN.5** and **ALC_FLR.2**

**Reason**: attacker with high attack potential via Internet open/hostile environment
Certification Policy is part of the National Plan for Information Infrastructure Protection in Germany

Driving forces for certifications are legal regulations (and not developers); government procurement

EAL4+, augmented by AVA_VAN.5 (and other components) are often based on national requirements (and state of the art)

**Reason**: open/hostile operational environment of IT security products

Functional testing based on a catalog/check list is often not sufficient; an independent vulnerability assessment is necessary, based on design know how of the product type, where the state of the technology must be considered (lessons learned from previous evaluations).
Evaluation results must be reasonable, comparable, reproducible and cost-effective

Warranty:

- intensive monitoring of evaluation tasks by the certification body
- assessing of new vulnerabilities by the certification body
- periodical audit of the evaluation lab by the certification body
- periodical technical workshops with labs
- participation of labs in relevant technical communities
- traceable documentation of evaluation results required by certification body (high effort for evaluations)
- involvement of BSI experts in specific cases (e.g. crypto)
Contact

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Dr. Markus Mackenbrock
Godesberger Allee 185 - 189
D- 53175 Bonn

Tel:  +49 (0) 228 9582 5334

Markus.Mackenbrock@bsi.bund.de
www.bsi.bund.de