

# **Overview of Common Criteria Smart Card Evaluation Activities**

**Bertolt Krüger**  
**6th ICC 2005**

- **Fields of smart card usage**
  - **Some specific (technical) evaluation aspects**
  - **Some rough numbers on certificates**
  - **Some name of active parties and initiatives**
- ▶ **Note: The following slides are rather sketchy due to the wide span of the topic**

- **Health Applications**

- ▶ For example in Germany health insurance companies will issue an electronic health card – the PP was written by me
- ▶ cards for the health professionals

- **electronic passport (ePass, ICAO-specifications)**

- ▶ No need to say that BSI is active in this field...

- **eGovernment / eCard**

- ▶ **Goal:** to fit as many applications as possible onto one card in order to avoid multiple cards for every citizen
- ▶ BSI is very active to promote this concept in Germany
- ▶ **Social insurance** also related to this

- **Digital Signatures**
  - ▶ As you know CC evaluation is required here by law in germany and other countries
- **Digital Tachographs**
  - ▶ Smart cards will be used in trucks in Europe instead of paper disks in order to store driving times and similar data
- **Access Control in companies and organisations**
- **Public Transport**

- **Example: SRC presently conducts eval's for**
  - ▶ **electronic health card, banking applications, digital signature applications, tachograph cards...**
- **All in all a high number of smart card related evaluations is presently ongoing**
- **Increasing number of combined applications**
  - ▶ **Example: banking cards together with digital signature (often based on the SECCOS OS in Germany)**

- **Composite Evaluation of hardware and software (and may be between operating system and applications)**
  - ▶ Guides for this are published as JIL/supporting documents
- **Many PPs: one either has to choose or to try to be consistent with several PPs (will be much easier in CC 3.0)**
  - ▶ Hardware PPs, platform/OS-PPs, application specific PPs
- **Smart card specific attacks have to be considered due to the high security level of smart cards**
  - ▶ Some buzz words: DPA, Light Attacks and so on
  - ▶ ISCI group works on unified lists of relevant scenarios – European certification schemes are involved

- **smart card related certificate numbers (counted on official web sites):**
  - ▶ German BSI scheme about 50 (30 hardware, 20 composition)
  - ▶ French DCSSI scheme about 80,
  - ▶ UK CESG scheme about 5
  - ▶ None in the other schemes (at least one ongoing in Japan)
- **Two main ranges of Evaluation levels:**
  - ▶ EAL1 /EAL1+ (older evaluations - more for learning purposes)
  - ▶ EAL 4+ / EAL 5+ - Most evaluations have Sof “high” and AVA\_VLA.4 because of High-Security Properties of Smart Cards

- **Names taken from officially published certificates for products (not for PPs) – sorry if I forgot somebody**
  - ▶ **Hardware-Vendors: ATMEL, Philips, Renesas (former Hitachi), Infineon (former Siemens), Samsung, ST microelectronics**
  - ▶ **Smart-Card-Vendors: Oberthur, Gemplus, AXALTO (former Schlumberger), IBM, Sony, ORGA Card Systems, T-Systems (Telesec), ASK, Gieseke & Devrient, Austria Card, Siemens**
  - ▶ **Other software/application issuers are mainly related to the banking/payment field: Soc. T. Europienne de Monnaie Electronique (a French electronic purse society), Mondex, other banks and credit card companies**



- **Names taken from officially published certificates for products (not for PPs)**
  - **sorry if I forgot somebody**
  - ▶ **Germany: T-systems (former debis), SRC, TUEV-IT**
  - ▶ **France: CEA LETI, SERMA, CEACI (TES - CNES)**
  - ▶ **UK: Logica**

- **eEurope has developed PPs and some evaluation and testing guidelines**
- **Eurosmart, a group of smart card vendors was active in eEurope and many other activities and in founding the next:**
- **ISCI, International Security Certification Initiative - initiative composed of certification bodies, evaluation labs and smartcard industry**
  - ▶ **One of the most important groups for smart card evaluation related activities today**
  - ▶ **An example of the ISCI work will be presented in another presentation here**

- **The German CC scheme, which is maintained by the German Federal Office for Information Security (BSI), takes a leading role in many of the activities mentioned in the presentation. BSI's experience in the area of smart card evaluation provided valuable input for this overview.**

SRC Security Research & Consulting GmbH  
Bertolt Krüger  
Graurheindorfer Str. 149a  
53117 Bonn  
Germany  
Tel. +49-(0)228-2806-122  
Fax: +49-(0)228-2806-199  
E-mail: [bertolt.krueger@src-gmbh.de](mailto:bertolt.krueger@src-gmbh.de)  
www: [www.src-gmbh.de](http://www.src-gmbh.de)