Update on the German Scheme

Dipl.-Math. Irmela Ruhrmann

Head of Certification
Federal Office for Information Security
(Bundesamt für Sicherheit in der Informationstechnik - BSI)

BSI CERTIFICATION

The Federal Office for Information Security (BSI) was established by the German Parliament in 1991.
§ 3 of the Act on the Establishment of the BSI, dated 17.12.1990 (Federal Law Bulletin I p. 2834) defines the tasks of BSI.

BSI CERTIFICATION

Tasks defined by § 3 of the Act

1. Study Security Risks ...
2. Development of Criteria ...
3. Test and Evaluate the Security of IT Systems or Components and Issue Security Certificates
4. ...
5. ...

BSI CERTIFICATION

Act on Establishment of BSI
(BSIG: December 1990)

BSI Certification Ordinance (BSI ZertV)

Decrees of the Federal Minister of the Interior
(e.g. handling of cryptographic problems)

Schedule of Costs (BSI-KostV)

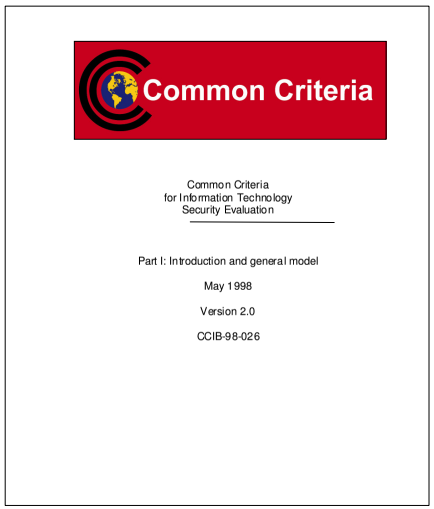
IT-SECURITY CRITERIA

History

1985: US-Orange Book

1989: Green Book of BSI

1991: Information Technology Security Evaluation Criteria (ITSEC)



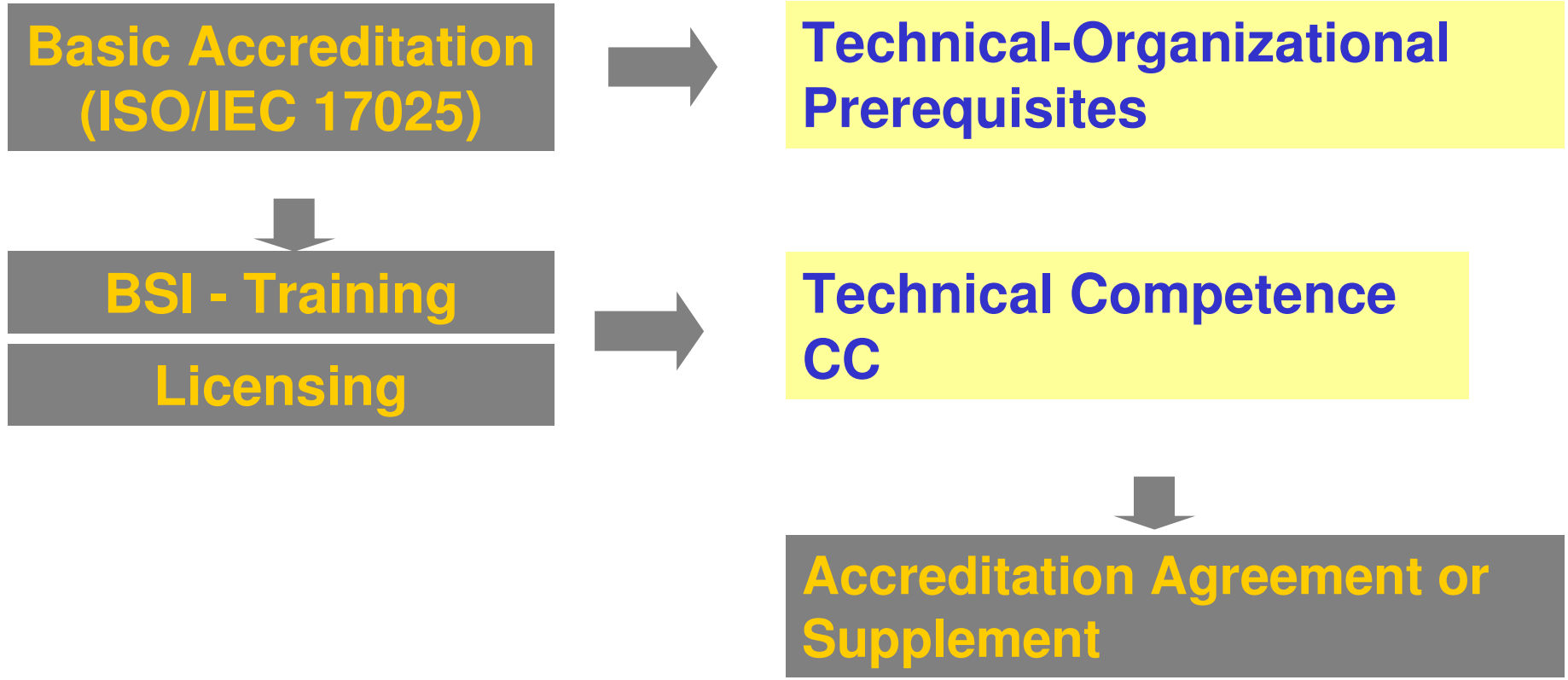
1999: Common Criteria (CC) V2.1 - Standard ISO/IEC 15408

2004: Common Criteria (CC) V2.4 - ASE/APE Trial Use Version

2005: CC V 3.0 Trial Use Version

2006: CC V 3.1

EVALUATION FACILITIES



EVALUATION FACILITIES

- atsec information security
- Atos Origin GmbH
- CSC Ploentzke AG
- datenschutz nord GmbH
- DFKI (German Research Institution for Artificial Intelligence)
- Industrieanlagen-Betriebsgesellschaft (IABG) mbH
- media transfer AG
- secunet SwissIT AG
- SRC Security Research & Consulting GmbH
- Tele Consulting (TC) GmbH
- TNO-ITSEF BV
- T-Systems GEI GmbH
- TÜV Informationstechnik (TÜVIT) GmbH

International Recognition of Certificates

- International Arrangement (2000) / Common Criteria / up to EAL4 / 24 Nations world-wide

- European Agreement (1998) / Common Criteria + ITSEC / all Evaluation levels / 14 European Nations

IT Security Certified

CERTIFICATION PROCEDURE

Types of certification procedures

- Certification parallel to the product development
- Certification of a finished TOE
- Assurance Continuity
  - Re-Evaluation
  - Maintenance

CERTIFICATION PROCEDURE

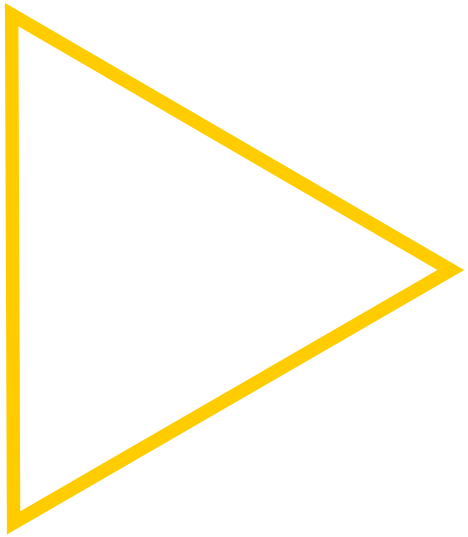
Recent Maintenance Examples

Infineon Technologies AG (BSI-DSZ-CC-0266-2005-MA-03)	Infineon Smart Card IC (Security Controller) SLE66CX322P/m1484b 14 and m1484f18	Smartcard Controller	Inclusion of already evaluated site Singapore
Gemplus SA (BSI-DSZ-CC-0281-2005-MA-01)	JavaCard Platform GXP3.2-E64PK-CC	Smartcard with Signature Application	Relevant documents were updated and the Security Target was updated due to editorial changes.
Philips Semiconductors GmbH Business Line Identification (BSI-DSZ-CC-0348-2006-MA-01)	Philips Secure Smart Card Controller P5CD072V0P, P5CD036V0P, P5CN072V0P and P5CN036V0P	Smartcard Controller	Data sheets changed for editorial reasons. New TOE configuration generated but using only fully evaluated HW. ST and HW unchanged
Renesas Technology Corporation (BSI-DSZ-CC-0379-2006-MA-01)	Renesas AE55C1 (HD65255C1) smartcard integrated circuit version 03	Smartcard Controller	Changes at the level of mask size and production parameters
T-Systems Enterprise Services GmbH SSC Testfactory & Security (BSI-DSZ-CC-0316-2005-MA-01)	TCOS Passport Version 1.01 / P5CT072 and TCOS Passport Version 1.01 / SLE66CLX641P	Passport Application	Integration of two additional already evaluated initialisation sites

CERTIFICATION PROCEDURE

Involved Partners

DEVELOPER



EVALUATION FACILITY

- provides Know-How of criteria and evaluation methods

CERTIFICATION BODY

- ensures equivalence of evaluation methods
- ensures neutrality as impartial third party

CERTIFICATION PROCEDURE

Phases

Preparation:
Application for certification
Security Target
Milestone plan
Evaluation Contract

Certification

CERTIFICATION PROCEDURE

Preparation

- Consulting with the Applicant
- Defining Security Target
- Utilizing Protection Profile if Available
- Determining Evaluation Schedule

- CB Agrees to the Security Target and Schedule
- Certification ID is Assigned by CB

CERTIFICATION PROCEDURE

Evaluation (I)

Evaluation Team

- Examines TOE and documentation provided
- Interacts with the Developer and Certification Body
- Prepares Evaluation Reports
  - delivered to CB and applicant

CERTIFICATION PROCEDURE

Evaluation (II)

- Oversight by the Certification Body (CB)

Ensures

- Consistency
- High Standards of Competence
- Impartiality

CERTIFICATION PROCEDURE

Evaluation (III)

CB

- Ensures Compliance with Scheme Rules
- Advises on the Use of Criteria and Evaluation Methodology
  - Actively Participates in Problem Solution
  - Issues Scheme Notices (AIS)
  - Guidance Documents
- Co- Audit of the Development Environment
- Attend Testing and Penetration Testing

CERTIFICATION PROCEDURE

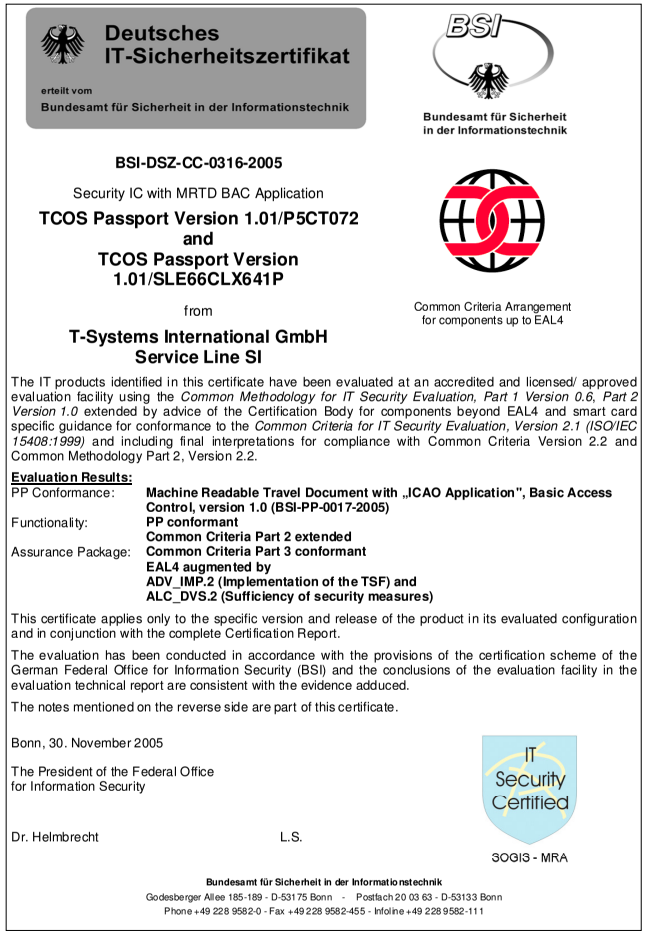
Evaluation (IV)

Conclusion of Evaluation

CB Approves
Evaluation Technical Report (ETR)

CERTIFICATION PROCEDURE

Certification Report



Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0316-2005

Security IC with MRTD BAC Application

TCOS Passport Version 1.01/P5CT072 and TCOS Passport Version 1.01/SLE66CLX641P

from

T-Systems International GmbH Service Line SI

Common Criteria Arrangement for components up to EAL4

The IT products identified in this certificate have been evaluated at an accredited and licensed/ approved evaluation facility using the *Common Methodology for IT Security Evaluation, Part 1 Version 0.6, Part 2 Version 1.0* extended by advice of the Certification Body for components beyond EAL4 and smart card specific guidance for conformance to the *Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC 15408:1999)* and including final interpretations for compliance with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2.

Evaluation Results:

PP Conformance:	**Machine Readable Travel Document with „ICAO Application", Basic Access Control, version 1.0 (BSI-PP-0017-2005)**
Functionality:	**PP conformant Common Criteria Part 2 extended**
Assurance Package:	**Common Criteria Part 3 conformant EAL4 augmented by ADV_IMP.2 (Implementation of the TSF) and ALC_DVS.2 (Sufficiency of security measures)**

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

The notes mentioned on the reverse side are part of this certificate.

Bonn, 30. November 2005

The President of the Federal Office for Information Security

Dr. Helmbrecht L.S.

IT Security Certified

SOGIS - MRA

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 228 9582-0 - Fax +49 228 9582-455 - Infoline +49 228 9582-111

- **Details of the Certification Procedure**
- **Advice on the Product:**
  - > Description of the
    - – Area of Application
    - – Security Functions
    - – Evaluation Assurance Level (EAL) or Assurance Package
  - > Detailed User Notes
- **Mutual Recognition Requirements**

CERTIFICATION PROCEDURE

Important Projects

Site Certification:
- Lead Nation Project (Lead BSI)

PP/ST Guide:
- Lead Nation Project (Lead BSI, UK)

Guidance for Developer's Documents

Guidance for Evaluation Reports

CERTIFICATION PROCEDURE

Publication of Certificates

Available on BSI-Web-Site:

- Current list of certificates to download
- Certification reports of all German IT-Security certificates of the BSI to download
- Certified Protection Profiles
- Links to the Web-Sites of the Partner Organisations

http://www.bsi.bund.de/zertifiz

Further information on Web-Site:

http:// www.commoncriteriaportal.org

CERTIFIED PRODUCTS

Product-types Certified / under Certification

Software Products

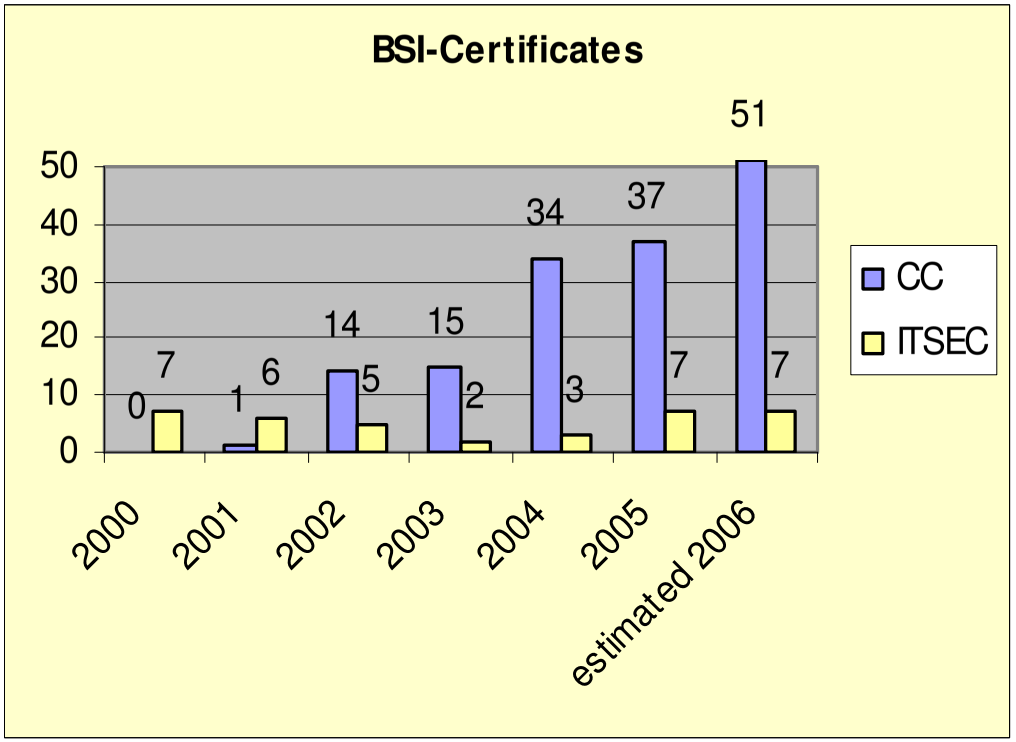
- Operating Systems
  - Mainframe
  - Midsize
  - Smartcards
- PC Security Products
  - Security Shells
  - Integrity Protection
- Data Communication Products
- Firewalls
- Biometric Security Products
- Smartcard with Applications
- Signature Apllications

Hardware Products

- Chipcard Reader
- Smartcard Reader
- Smartcard Controller
- Tachograph Components (Motion Sensor, Vehicle Unit, Smartcard)

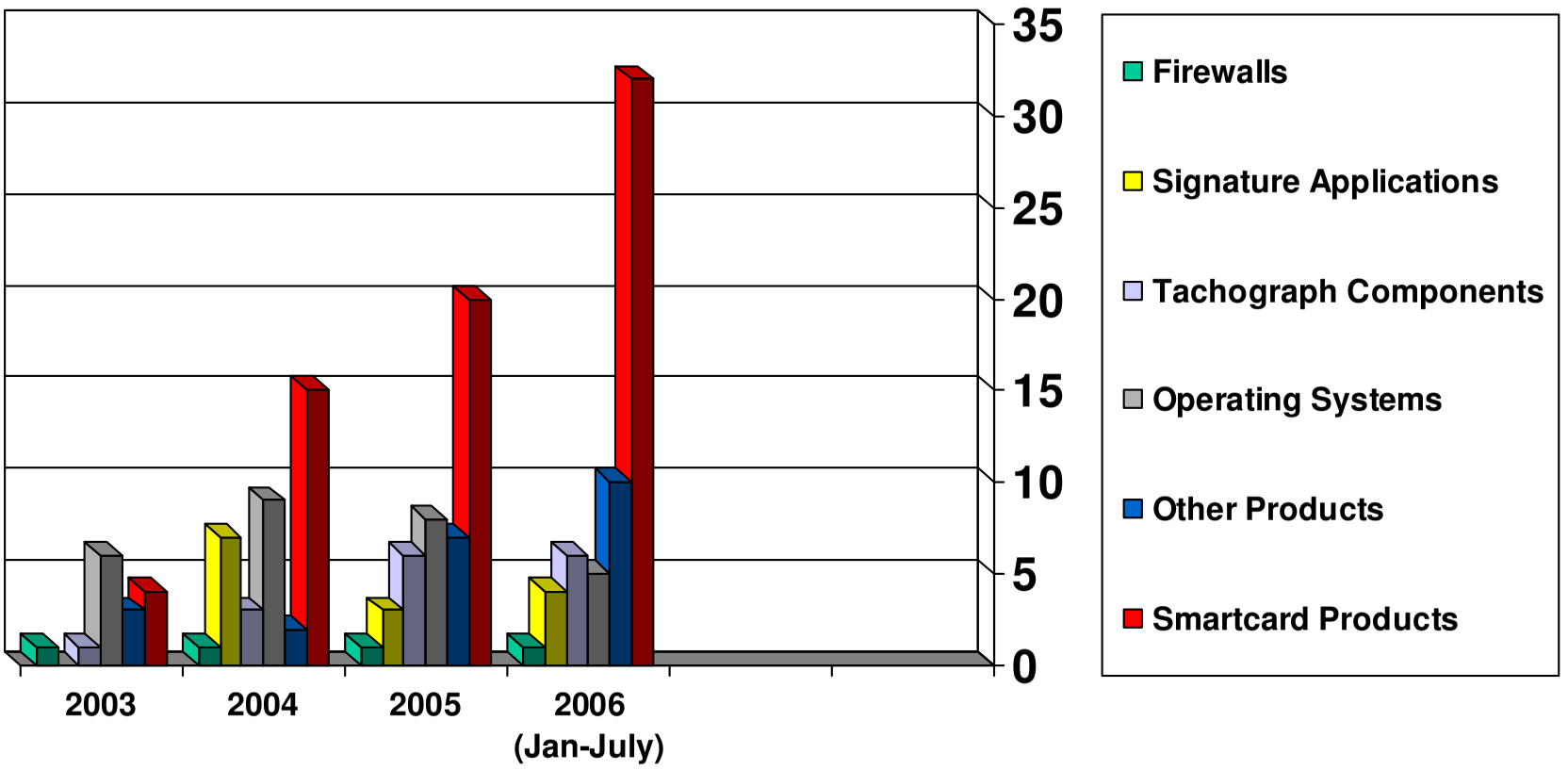
SIGNIFICANCE OF CERTIFICATION

Market development of CC certified Products



SIGNIFICANCE OF CERTIFICATION

Market development of CC certified Products



SIGNIFICANCE OF CERTIFICATION

Motivation for manufactures

- Independent product evaluation by external organisation
- Quality improvement of the product concerning the security functionality
- Documented Design, documented evaluation
- Competent commercial Evaluation Facilities (accredited and licensed for CC)
- Monitoring of the examination by superordinate certification body
- National certification body guarantees neutrality and international recognition of the certificate
- Market advantage by recognised certificate

SIGNIFICANCE OF CERTIFICATION

Recent Protection Profile Developments (I)

- Electronic Health Card (eHC)
  – elektronische Gesundheitskarte (eGK)
- Secure Module Card (SMC)
  – Sicherheitsmodul-Karte
- Health Professional Card (HPC)
  – Heilberufsausweis (HBA)
- Protection Profile for Biometric Verification Mechanisms

SIGNIFICANCE OF CERTIFICATION

Recent Protection Profile Developments (II)

- Video protection Profile
  - Closed Circuit Television (CCT)

- Electronic Voting

- Protection Profile for cryptographic components

SIGNIFICANCE OF CERTIFICATION

Recent Protection Profile Developments

Protection Profile for Machine Readable Travel Document with "ICAO Application", Basic Access Control (BAC)

Definition of security objectives and requirements for the contactless chip of machine readable travel documents (MRTD) based on ICAO standard for the security method BAC.

TOE: contactless chip, the IC Dedicated Software, the IC Embedded Software (operating system), the MRTD application and the associated guidance documentation.

Product life cycle described in terms of four life cycle phases:

- → Development,
- → Manufacturing,
- → Personalization of the MRTD,
- → Operational Use.

SIGNIFICANCE OF CERTIFICATION

Recent Protection Profile Developments

Machine Readable Travel Document with „ICAO Application "Extended Access Control (EAC)

Definition of security objectives and requirements for the contactless chip of machine readable travel documents (MRTD) based on ICAO standard for the security method EAC
and chip authentication similar to the Active Authentication
in the Technical reports of the ICAO New Technology Working Group

TOE: contactless chip, the IC Dedicated Software, the IC Embedded Software (operating system), the MRTD application and the associated guidance documentation.

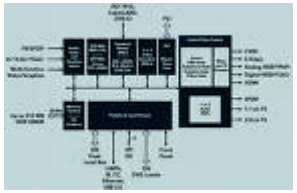
Product life cycle described in terms of four life cycle phases:

- → Development,
- → Manufacturing,
- → Personalization of the MRTD,
- → Operational Use".

SIGNIFICANCE OF CERTIFICATION

Recent Certificates (Examples I)

- **Infineon** Smartcard-Controller (SLE66CX322P/m1484b14 and m1484f18)



- **Renesas** Smartcard-Controller (Renesas AE55C1 - HD65255C1)
- **SuSE** Operating Systems (SUSE Linux Enterprise Server)

- **Microsoft** Microsoft Exchange Server, Firewall (ISA Server 2004), Directory-Server
- **IBM** Operating Systems, e.g. z/OS, AIX, PR/SM, Directory-Server, Tivoli Access Manager

SIGNIFICANCE OF CERTIFICATION

Recent Certificates (Examples II)

- **GeNUA** Firewall (GeNUGate)

- **Utimaco** PC-Security Products (SafeGuard Easy)

- **Philips** Smartcard Controller (P5CC036V1C and P5CC009V1C5)

- **Sony** IC Card Reader / Writer (RC-S940 - CXD9768GG)

- **Sharp** Smartcard Controller (SM4128)

SIGNIFICANCE OF CERTIFICATION

Recent Certificates (Examples III)

- OPENLiMiT Sign Cubes AG — Signature application software (S-TRUST Sign-it base)

- Siemens VDO Automotive AG — Tachograph (Digital Tachograph DTCO 1381)

- Oce Technologies B.V. — Printer Controller (Océ Smart Imager 8.3.3.39 as used in the Océ VP 2090 R3.3)

SIGNIFICANCE OF CERTIFICATION

Acquisition Policies for CC certified Products

EU Commission:	→ Digital Tachograph: Directive equivalent to law
NATO:	→ Infosec Technical and Implementation Guidance on the use of Common Criteria within NATO
Multilateral Defense:	→ Airbus A 400M → Eurofighter 2000
UN/G8:	→ G8 - Principles on Critical Infrastructure Protection
Germany	→ Digital Signature Law → Health Cards → Passports and ID documents

Acquisition Policies in EU/Germany at this point in time concern special areas (public, defense)
Trend: increasing importance

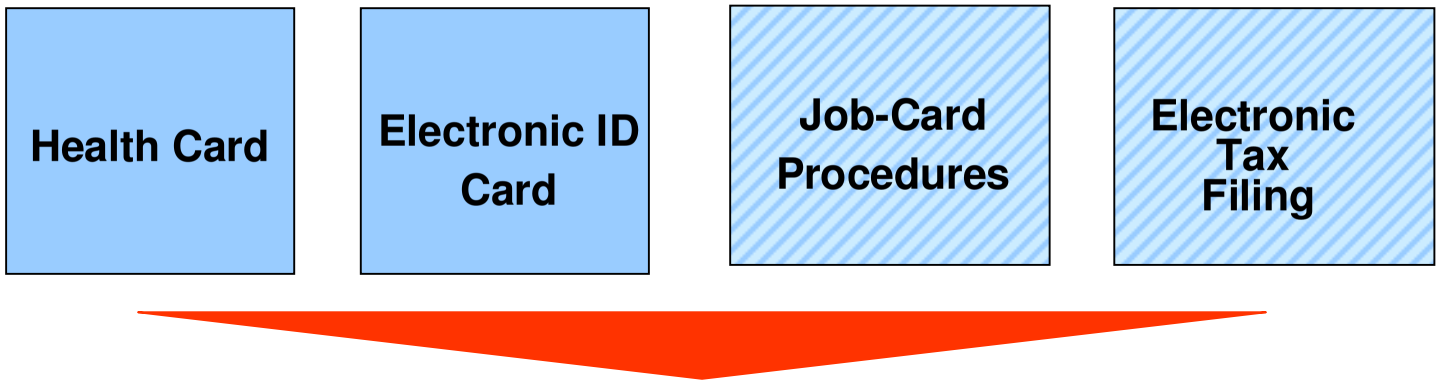
SIGNIFICANCE OF CERTIFICATION

Medium term effects of the present market trend

- Complete product ranges of IT market leaders are being certified in accordance with CC.
- In the long run the whole IT-market will be affected because IT-security is of increasing importance in system solutions.
- Development of Protection Profiles as an implementation-independent set of IT security requirements for categories of IT products with increasing trend.
- Market forecast: Product certification is becoming a competition criteria.

E-CARD STRATEGY

Ongoing Projects of the German Government



9th March 2005: Resolution of the Federal Cabinet for the eCard Strategy of the Federal Government

E-CARD STRATEGY

Objectives

- Interoperability of the Smartcards through common Reference of Standards
- Broad Introduction of electronic Authentication
- Preparation of all Smartcards for qualified digital signatures
- Production and supply of smartcards, certificates for signatures and the Public Key Infrastructure (PKI) are tasks of the private industry
- Distribution of signature cards in different application fields
- Efficiency increase of public administration and health services

CONCLUSION

- IT-Security Certification leads to improved Quality of IT-Products
- Increasing Importance of Product Certification with the introduction of the Common Criteria
- CC are increasingly part of governmental acquisition policies: US-Gov't Directive, G8-CIP-Principles, EU, NATO

Bundesamt für Sicherheit
in der Informationstechnik
Referat 322
Postfach 20 03 63
D-53133 Bonn
Germany
Infoline: +49 228 9582-111
Fax: +49 228 9582-455
eMail: zerti@bsi.de
Internet:
http://www.bsi.bund.de/zertifiz