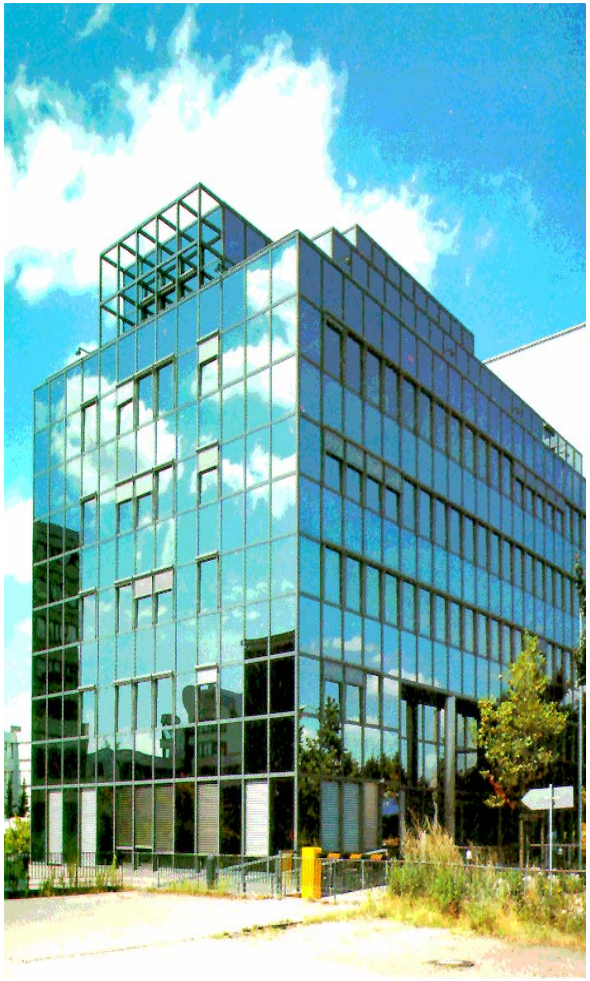
THE BSI CERTIFICATION SCHEME AND RECENT DEVELOPMENTS IN THE GERMAN IT SECURITY MARKET

Dipl.-Math. Irmela Ruhrmann

Head of Section Certification, Approval
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)

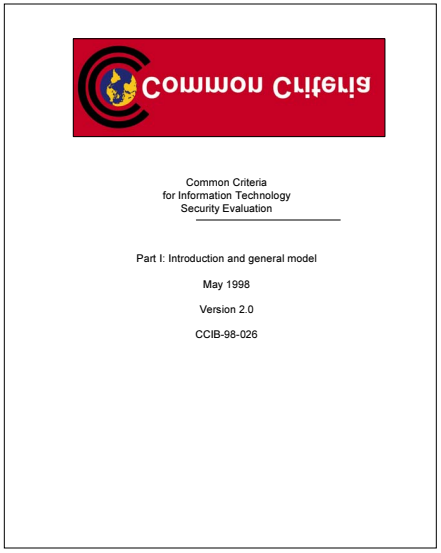
IT-SECURITY CRITERIA

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

EVALUATION FACILITIES

Basic Accreditation (ISO/IEC 17025) → **Technical-Organizational Prerequisites**

BSI - Training
Licensing → **Technical Competence CC**

Accreditation Agreement or Supplement

Re-assessment → **Technical and Quality Audit**

EVALUATION FACILITIES

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

INTERNATIONAL RECOGNITION

International Recognition of Certificates

- International Agreement (2000) / Common Criteria / up to EAL4 / 21 Nations world-wide

- European Agreement (1998) / Common Criteria + ITSEC / all Evaluation levels / 12 European Nations

CERTIFICATION PROCEDURE

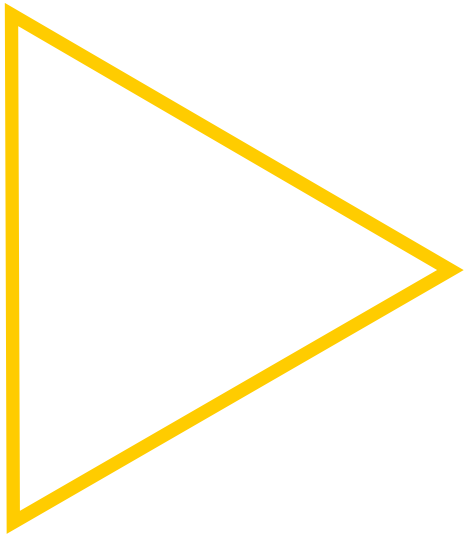
Types of certification procedures

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

CERTIFICATION PROCEDURE

Involved Partners

DEVELOPER



EVALUATION FACILITY

- provides Know-How of criteria and evaluation methods

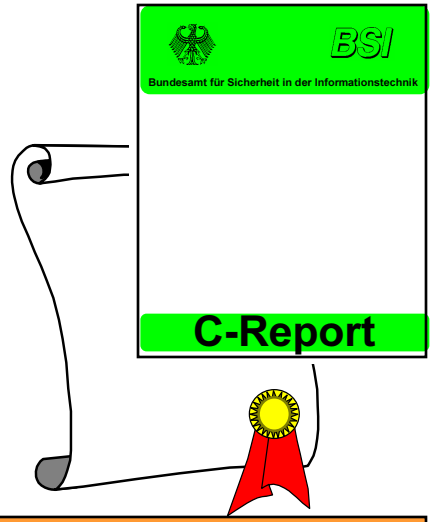
CERTIFICATION BODY

- 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 Teams

- 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

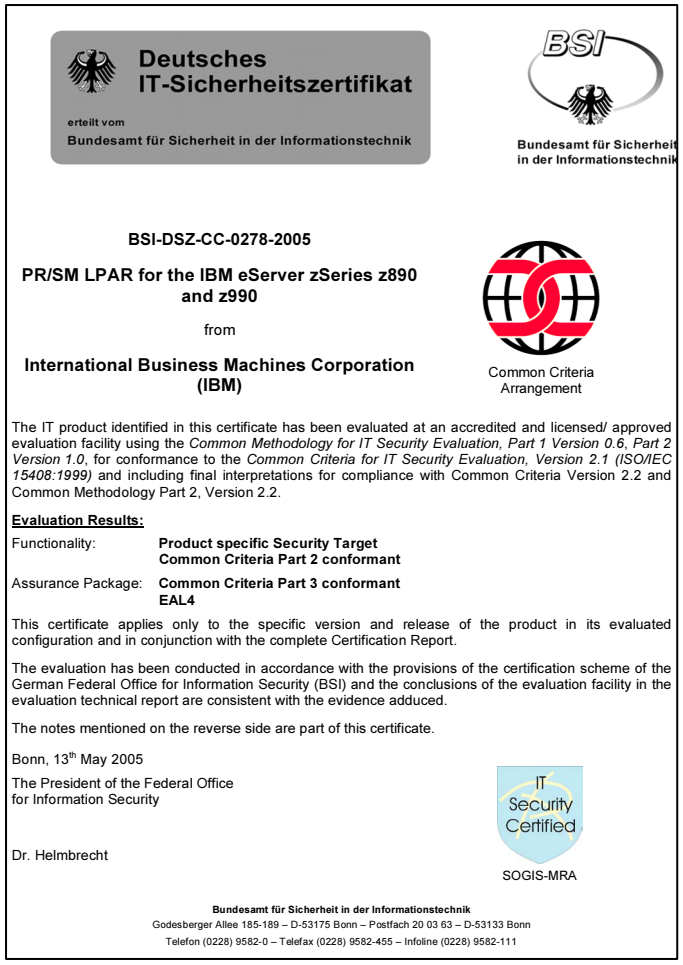
Evaluation (IV)

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-0278-2005

PR/SM LPAR for the IBM eServer zSeries z890 and z990

from

International Business Machines Corporation (IBM)

Common Criteria Arrangement

The IT product identified in this certificate has 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*, 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:

Functionality: **Product specific Security Target**
Common Criteria Part 2 conformant

Assurance Package: **Common Criteria Part 3 conformant**
EAL4

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, 13th May 2005

The President of the Federal Office
for Information Security

Dr. Helmbrecht

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
Telefon (0228) 9582-0 – Telefax (0228) 9582-455 – Infoline (0228) 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

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

CERTIFIED PRODUCTS

Product-types Certified / under Certification

Software Products

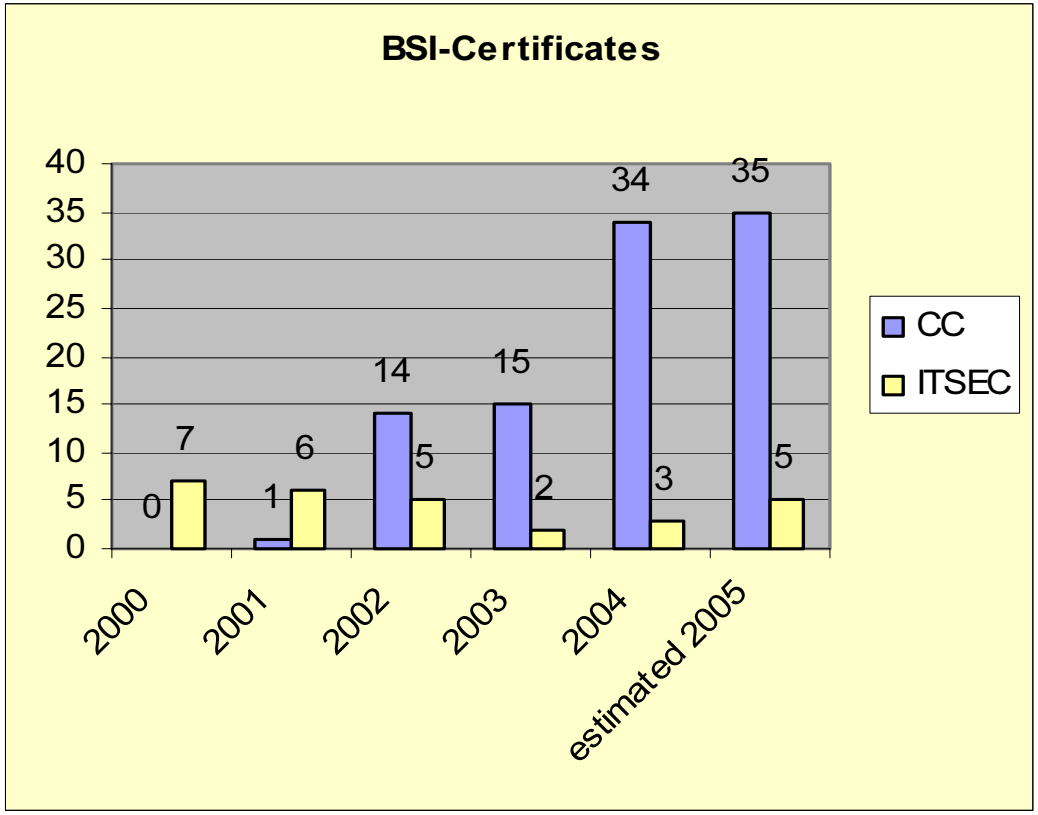
- Operating Systems
  - Mainframe
  - Midsize (F-C2, F-B1)
  - Smartcards
- PC Security Products
- Data Communication Products
- Firewalls
- Biometric Security Products
- Smartcard Applications

Hardware Products

- Chipcard Reader
- Smartcard Reader
- Smartcard Controller

SIGNIFICANCE OF CERTIFICATION

Market development of CC certified Products



SIGNIFICANCE OF CERTIFICATION

Recent Protection Profile Developments

- Low Assurance Protection Profile for a Software Based Personal Firewall for home Internet use
- Low Assurance Protection Profile for an Office Based Photocopier Device
- Low Assurance Protection Profile for a VPN Gateway
- Low Assurance Protection Profile for a Voice over IP Infrastructure

SIGNIFICANCE OF CERTIFICATION

Recent Protection Profile Developments

- Protection Profile - Biometric Verification Mechanism
- Protection Profiles for Health Sector, e.g. Health Professional Card
- Protection Profile - Machine Readable Travel Document with “ICAO Application” (e-Passport)

SIGNIFICANCE OF CERTIFICATION

Recent Certificates (Examples)

- **Infineon** Smartcard-Controller (SLE66C82P/m1474a15 and SLE66C42P/m1495a15)
- **Renesas** Smartcard-Controller (Renesas AE46C1 - HD65246C1
- **SuSE** Operating Systems (SUSE Linux Enterprise Server)
- **IBM** Operating Systems, e.g. z/OS, AIX, PR/SM Directory-Server, Tivoli Access Manager
- **Microsoft** Firewall (ISA Server 2000)

SIGNIFICANCE OF CERTIFICATION

Recent Certificates (Examples)

- 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

Acquisition Policies for CC certified Products in Europe

EU Commission:	➔ Digital Tachograph: Directive equivalent to law
NATO:	➔ Infosec Technical and Implementation Directive on the use of Common Criteria in NATO (Draft)
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

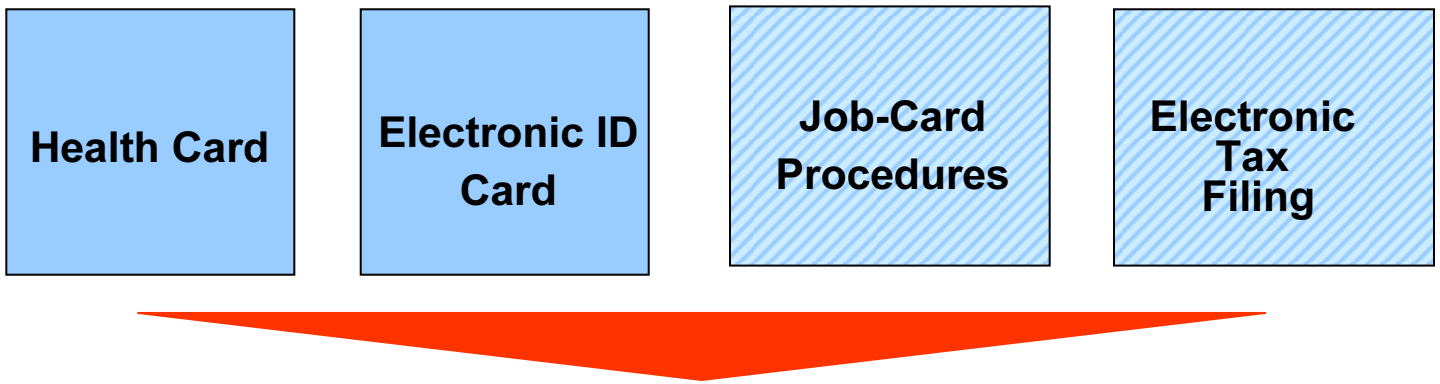
SIGNIFICANCE OF CERTIFICATION

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.
- **Protection Profiles:** standardised technical evaluation rules according to CC-standard within product classes (CC) are increasing rapidly.
- Market forecast: Product certification is becoming a competition criteria.

E-CARD STRATEGY

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 in 1999.
- CC are increasingly part of governmental acquisition policies: US-Gov't Directive, G8-CIP-Principles, EU, NATO

Federal Office for
Information Security
Referat III 2.2
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