



BSI - Federal Office for Information Security

Evaluation and Certification of IT Security Technology in Germany



- The BSI - History, Tasks and Services
- Product Certification
- Common Criteria
- Role of Certification in Public Acquisition
- Future Market Requirements

Bernd Kowalski
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Federal Office for Information Security

Office History and Structure



History and Figures

- Office founded by law in 1991.
- Associated with the Federal Ministry of Interior.
- Annual budget: € 45 Mio.
- Employees: 380.
- Location: Bonn.

„The BSI is the German Federal IT Security Authority associated with national and international partners in the field of Cryptography, Internet-Security and Certification. „

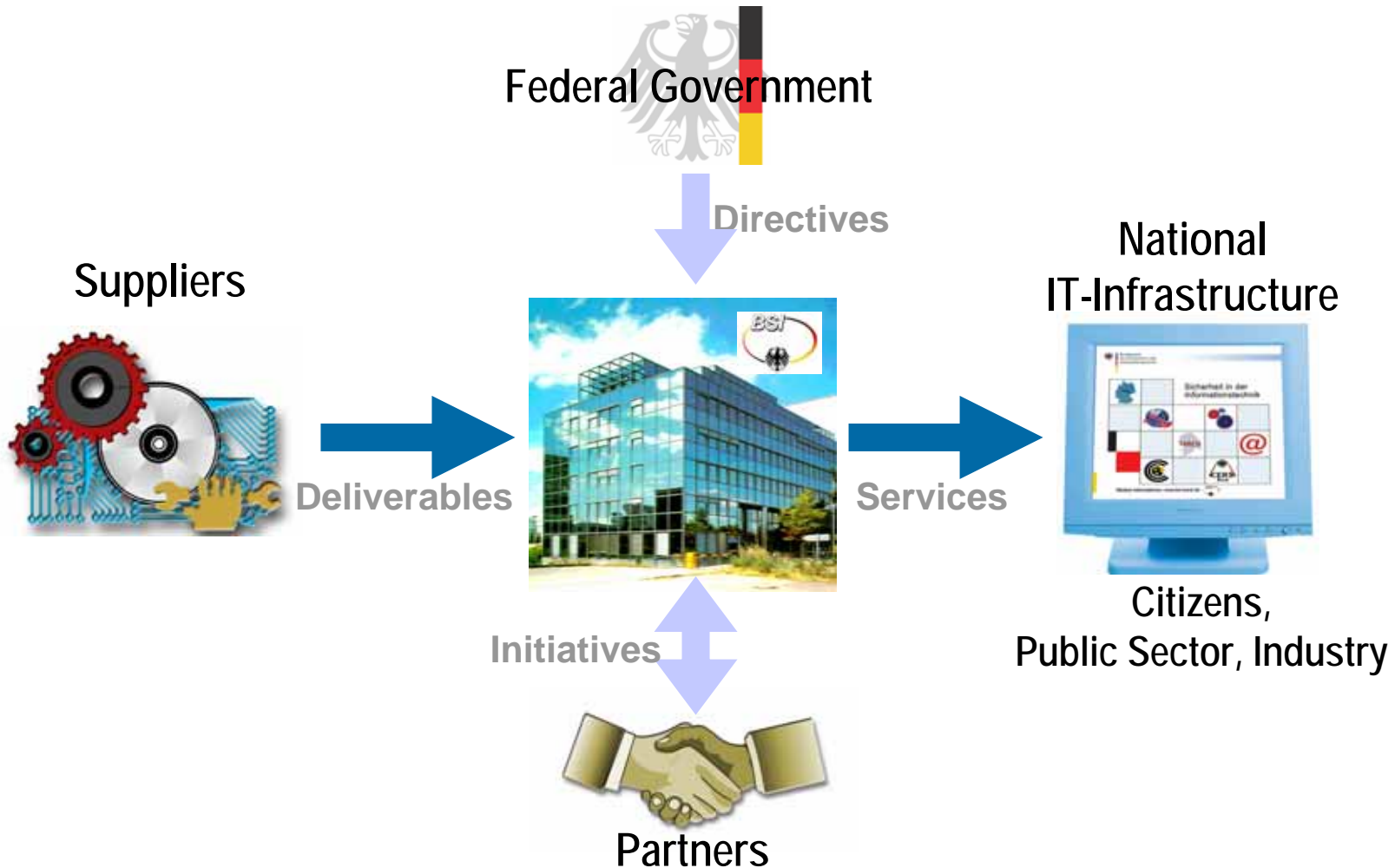
Tasks and Services

Tasks by Law

- ✘ Analysis of IT-threats and -risks.
- ✘ Improve national IT-Security in cooperation with industry.
- ✘ Security Evaluation and Certification of IT systems.
- ✘ Provide the protection of classified information.
- ✘ Operation of central security services like Keymanagement.

Tasks and Services

BSI as a part of the national IT-Security Environment



Tasks and Services

Services:

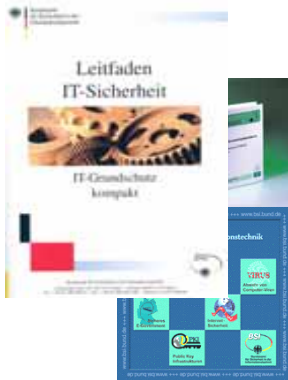


✎ Citizens *(consuming IT-Security)*

- ✎ **Webportal service www.bsi-für-bürger.de,**
information about Internet security issues

✎ Gov` t & Industry: *(consuming IT-Security)*

- ✎ **baseline security standard „Grundschutz“**,
for corporate IT-infrastructures with medium-level requ.
- ✎ **Critical Information Infrastructure Protection:**
provide means for extraordinary security events.
- ✎ Warning & Alerting services in case of security events:
Federal-CERT serving the German Federal Gov` t.
- ✎ Devices & services to **protect classified communication**
in gov` t & industry.
- ✎ **Counter-eavesdropping** services&standards
for Fed.Gov` t, incl. physical -, emission -, mobile security



✎ Manufacturers & Service Prov` s: *(offering IT-Security)*

- ✎ Security **Certification&Approval** of IT-Products&Systems



Product Certification

Objectives

- ❏ Evaluation of security features of IT-Products.
- ❏ Improve both security and quality of IT-infrastructures.
- ❏ Independant and trustworthy product evaluation and certification.
- ❏ Consideration of national security requirements.
- ❏ Strategic support for national IT-Security industry.

Legal Framework

- ❏ BSI is the national authority for the German certification scheme.
- ❏ No general legal obligation to purchase certified products.
- ❏ Except: approval of products for the processing of classified information, and special regulated areas.



Product Certification

Why should manufactures apply for a certificate ?

- ❏ Improve product quality and security.
- ❏ Use public product certificate for product marketing.
- ❏ Government requirements in certain areas:
German Signature Law, EU- and NATO-Directives etc.

Why should Buyers request for a certified product ?

- ❏ Product has been evaluated by an independant, accredited body.
- ❏ Manufacturer is responsible for evaluation expenses not the buyer.
- ❏ Certificate may help to provide evidence for resistance against certain threats.

Certification Criteria

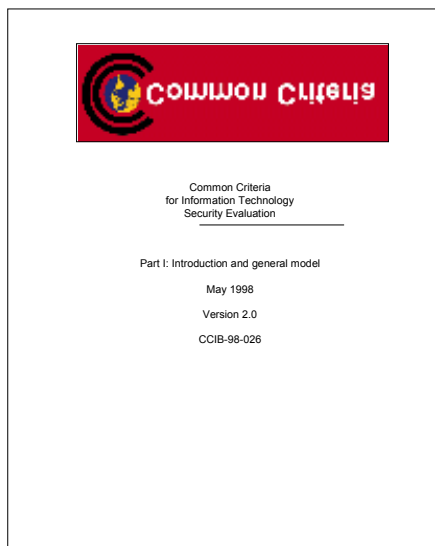
History



1985: US-Orange Book
IT-Security acquisition requirements
from the US DoD for special systems.

1989: The BSI Greenbook for Germany.

1991: European Information Technology
Security Evaluation Criteria (ITSEC).

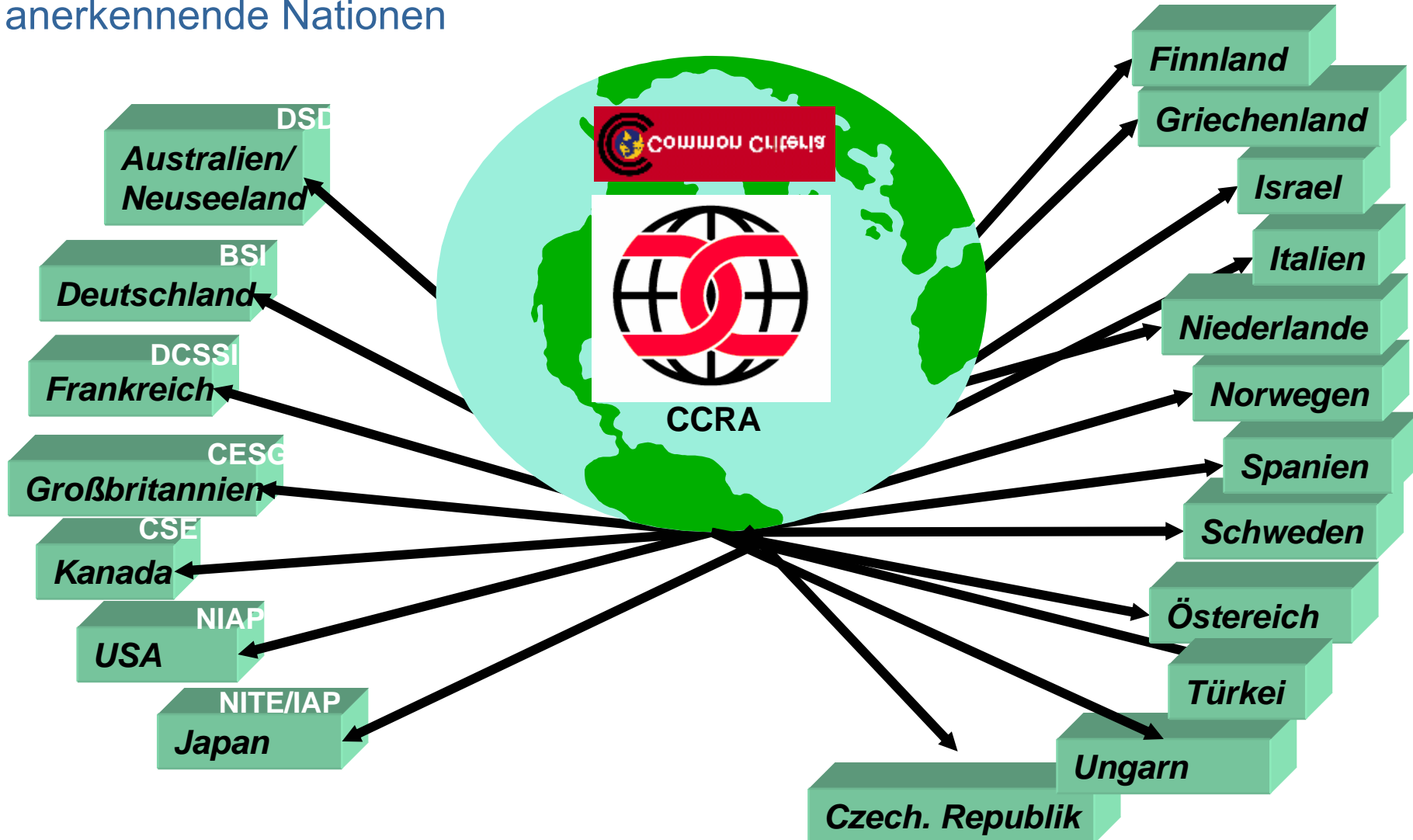


1999: Common Criteria (CC) V2.1 -
the first agreed international
certification standard
published under ISO/IEC 15408

Common Criteria

Zertifizierende und
aner kennende Nationen

Aner kennende Nationen



Product Certification

Contributors in the Certification procedure

Manufacturer:

- ✘ requests for a certificate
- ✘ provides complete product documentation

Evaluation Facility:

- ✘ design evaluation, penetration tests
- ✘ audits in development and production
- ✘ evaluation report to certification body

Certification body:

- ✘ develop certif. criteria together with CCRA-partners
- ✘ accept evaluation report, issue product certificate

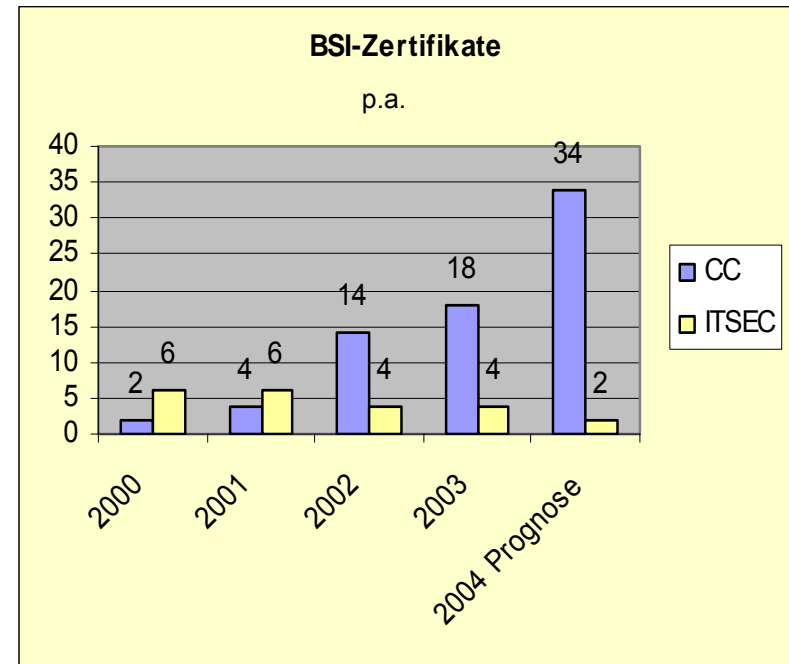
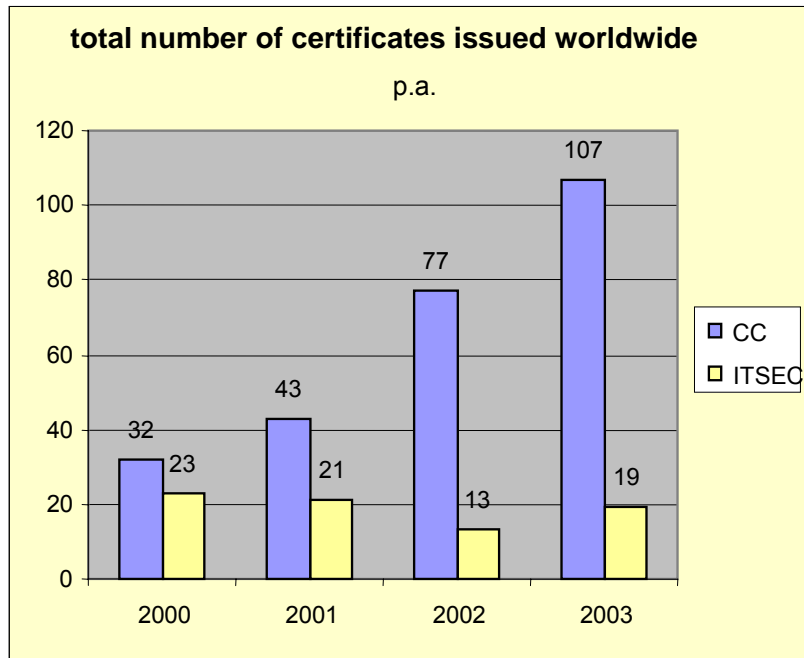
Product Certification

Product Certificates recently issued by the BSI:

❏ Infineon	Smartcard-Controller (Smart Card IC SLE66CX322P)
❏ Gemplus	Smart Card Betriebssystem(GemXpressoPro E64PK)
❏ SuSE	Betriebssystem (Linux)
❏ IBM	Betriebssysteme, Directory-Server, Tivoli
❏ Microsoft	Firewall
❏ GeNUA	Firewall
❏ Utimaco	PC-Sicherheitsprodukte
❏ Renesas (Hitachi)	Smartcard-Controller (AE43C Version 01)
❏ Philips	Smartcard-Controller (P16WX064V0C)
❏ G + D	Tachosmart Card (STARCOS 2.4 Tach.Card Applic.)

Common Criteria

Number of CC-Certificates issued

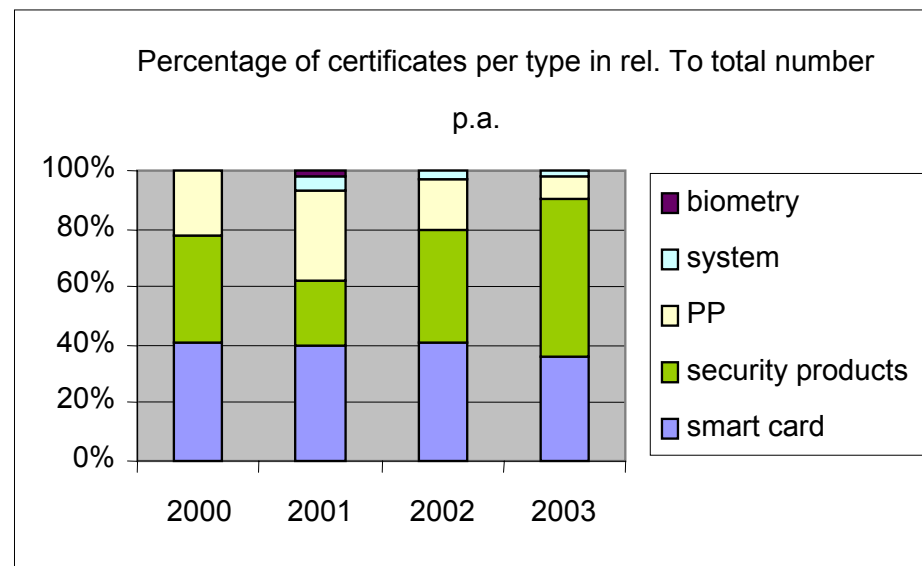
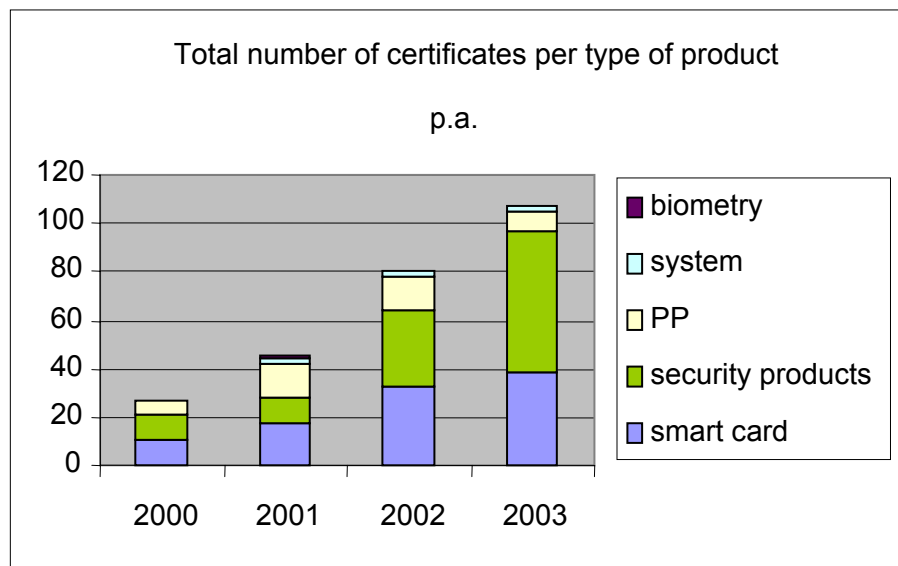


evaluation facilities worldwide: 36, Germany: 12

Quelle: CCRA, MC 2003

Common Criteria

Certificates per Type of Product



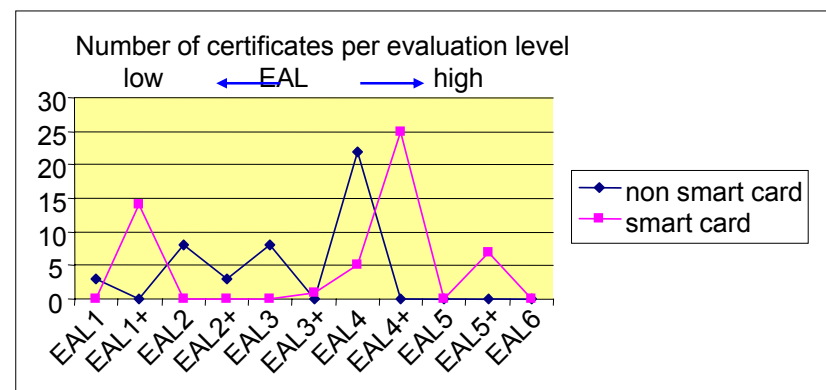
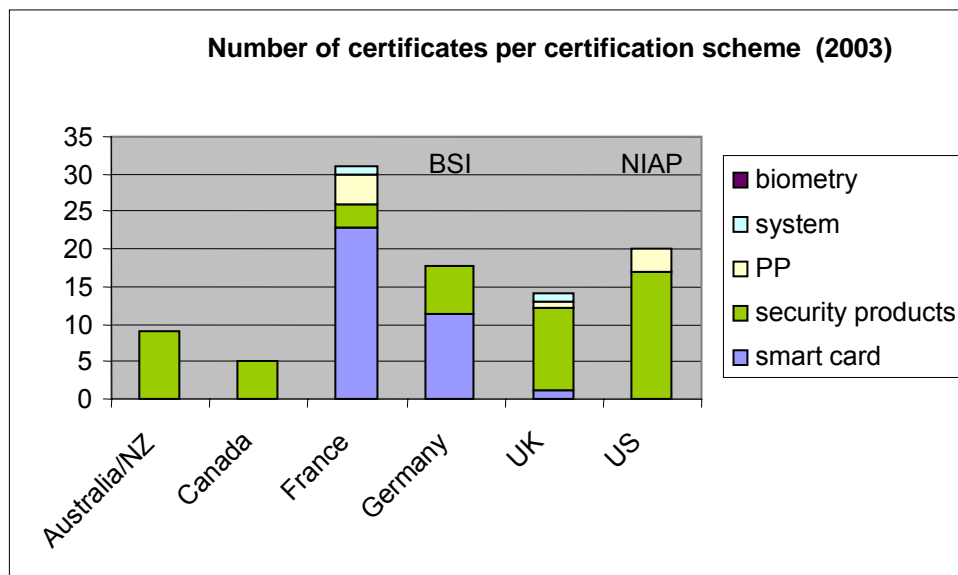
Quelle: CCRA, MC 2003

Characteristics:

- ✗ many products are smartcard related
- ✗ certification focussing on components
- ✗ little relevance to customer / end-user solutions
- ✗ therefore: CC not yet usable for End-User marketing

Common Criteria

Certificate Numbers per Scheme and Evaluation Level



Characteristics

- ▶ European schemes are leading in smartcards
- ▶ BSI scheme also used by US IT-manufacturers
- ▶ preference for high evaluation levels

Role of Certification in Public Acquisition

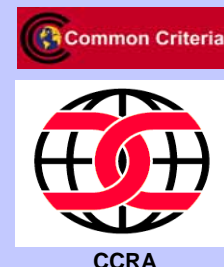
US-Government Obligations to use CC-Certification:



FACT SHEET

NSTISSP No. 11

National Information Assurance Acquisition Policy



„By July 2002 - the acquisition of all COTS IA and IA-enabled IT products to be used on systems specified, shall be limited only to those which have been evaluated and validated [acc to CC, NIST/NSA/NIAP or FIPS program].“

Legend:

COTS: Commercial of the shelf

IA: Information Assurance

NST/ISSP: National Security Telco and Info Systems Security Policy

The US-Directive #11 might have a significant future impact on the global IT market.

Role of Certification in Public Acquisition

European/German Situation

- EU Kommission:** → **Digital Tachograph: EU-Directive (law-level)**

- NATO:** → **Infosec Technical and Implementation Directive on the use of Common Criteria in NATO**

- Multilateral Defense:**
 - **Airbus A 400M**
 - **Eurofighter 2000**

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

- D:**
 - **German Signature Law**
 - **Smartcards for German healthcare system**

European/German acquisition in the Public Sector requires CC-approval on a per project basis.

Future Market Requirements

Problems with present Product Certification Procedures

- Product Certification is costly and time-consuming.
- Certification works mainly for components not for end-user products.
- Present Certification does not include the complete product value chain.
- Only few Certificates address mass market / COTS products.
- Number of moderate evaluation levels (EAL 1 or 2) is very low.

Product Certification must also meet the requirements of mass market products: low-cost, short time-to-market, based on Common Criteria for international acceptance.

Future Market Requirements

Results of a BSI investigation on mass market product certification

- Classic CC-approach does not meet requirements concerning cost and time.
- There is a big interest among those manufactureres in CC-certification.
- Action: Development of a draft enhanced certification procedure based on CC.

Characteristics of the draft enhanced procedure

- Evaluation level: EAL1+ combined with additional requirements.
- Consider additional checks at the manufacturer.
- Limitation of the certificate validation time.
- Consider continous Life-Cycle checks at the event of new releases or threats occur.

**Additional procedures at the manufacturers
compensate possible draw-backs from lower evaluation levels.**

Thank You for Your Attention !

Contact



Bernd Kowalski

**Bundesamt für Sicherheit
in der Informationstechnik
Godesberger Allee 185-189
53175 Bonn**

Phone: +49 0 228 9582-700

Fax: +49 0 228 9582-455

**Bernd.Kowalski@bsi.bund.de
www.bsi.de**