

# Zertifizierung von IT-Systemen

**TÜV Informationstechnik GmbH**

**The Trust Provider**

**- TÜViT -**

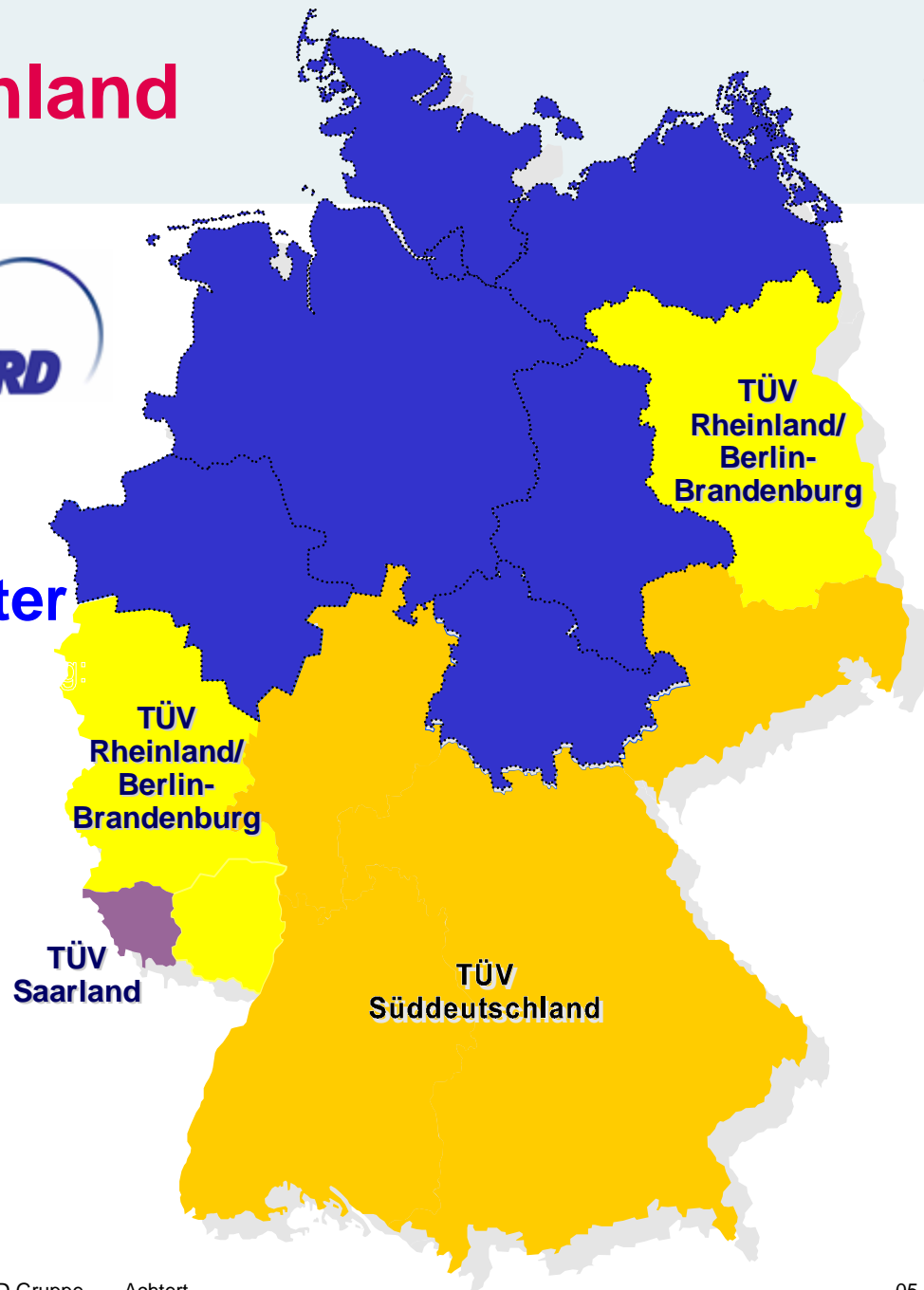


- Abgrenzung von Begriffen rund um die Zertifizierung
- Gegenstand der Prüfung und Zertifizierung
- Inhaltliche Aspekte der Zertifizierung
- Nutzen von Zertifizierungen
- Offene Fragen und Diskussion

# TÜV's in Deutschland

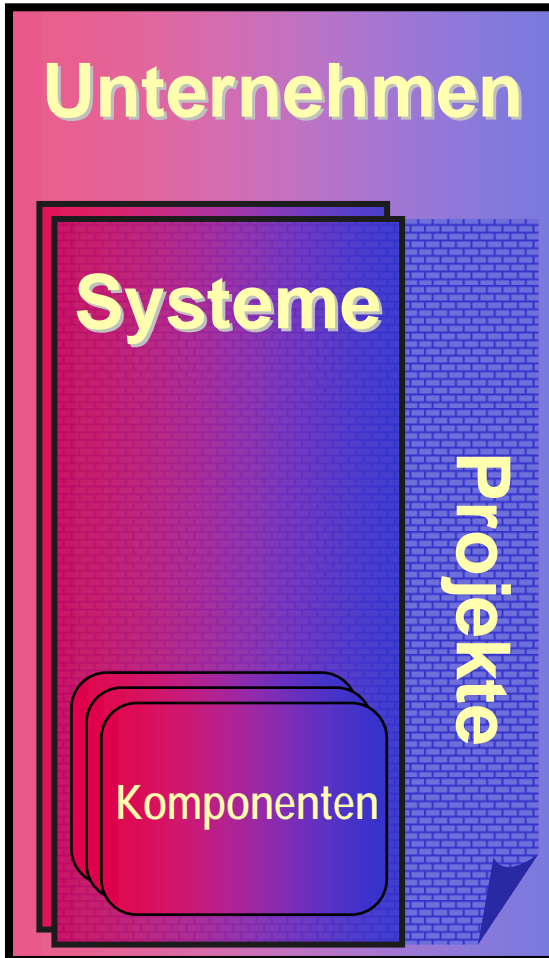


**TÜV NORD:**  
**Mehr als 7000 Mitarbeiter**  
**600 Mio. EUR Umsatz**  
**(2003)**









## Prüfung der IT-Sicherheit

**Datenschutz  
Sicherheitsmanagement**

**physikalische Sicherheit  
Netzwerksicherheit  
sicherer eBusiness**

**Evaluation von  
Sicherheitssoftware  
Sicherheitshardware**

## Optimierung der IT-Qualität

**Qualitätsmanagement  
Servicemanagement**

**Usability  
Mobile Service Quality  
Zuverlässigkeit**

**Prozessverbesserung  
Vorgehensmodelle  
Projektmanagement**

**Qualitätssicherung  
Funktionaler Test**



## IT-Sicherheit

quid! / ULD  
ISO 17799 / BS7799-2  
GSM SAS / TU.4  
IT-Grundschutz

## IT-Qualität

ISO 9000  
ITIL

---

### Trusted Site

- Infrastructure
- Usability
- Security
- Quality
- Privacy

Abnahme CA bzgl. SigG

PK-DML

---

CMMI

SPICE

V-Modell XT

RUP

---

Common Criteria / ITSEC

IEEE 1233

FIPS 140

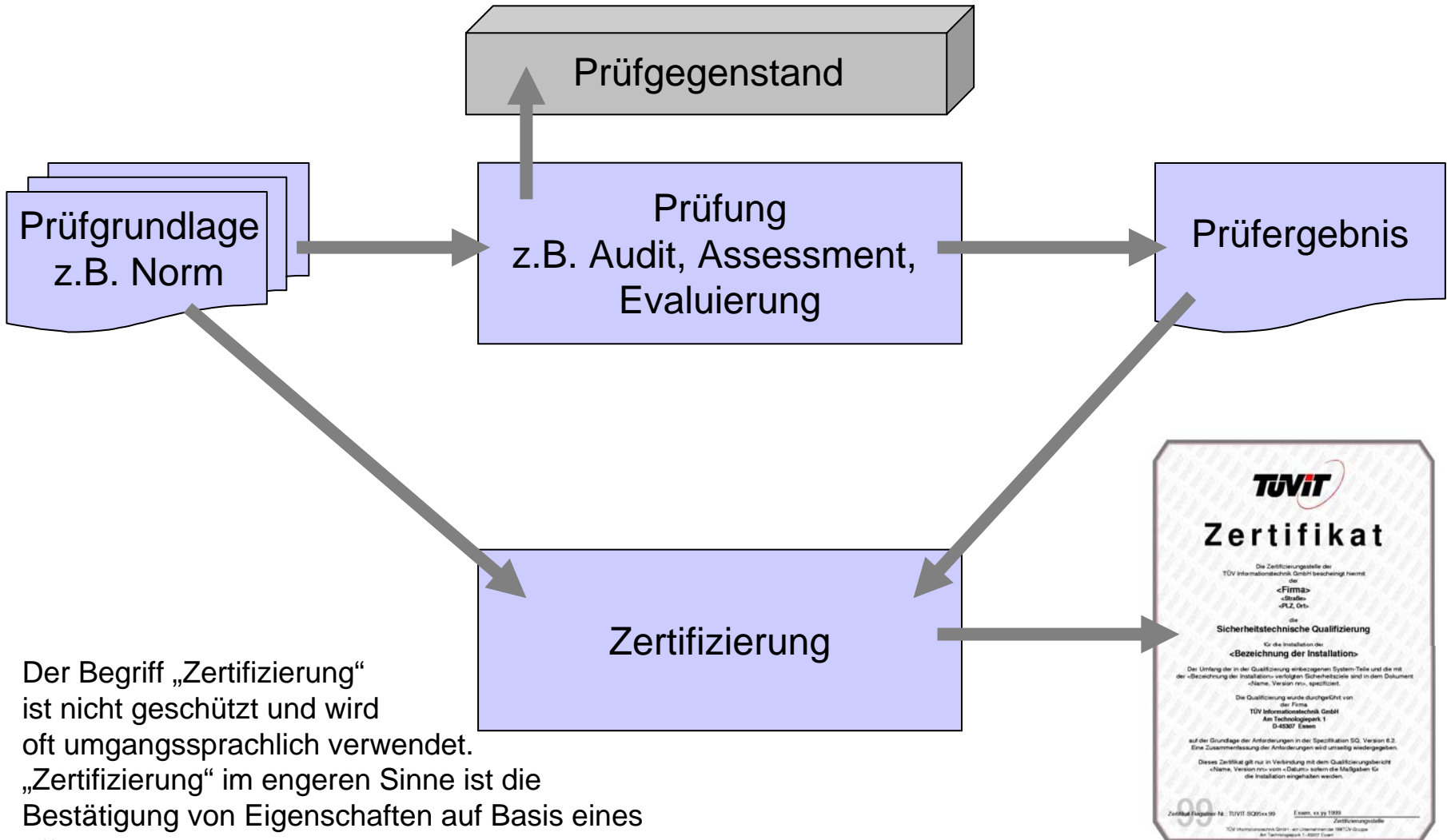
ISO 12119

ZKA-Kriterien

ISO 9241

Hardware Labor

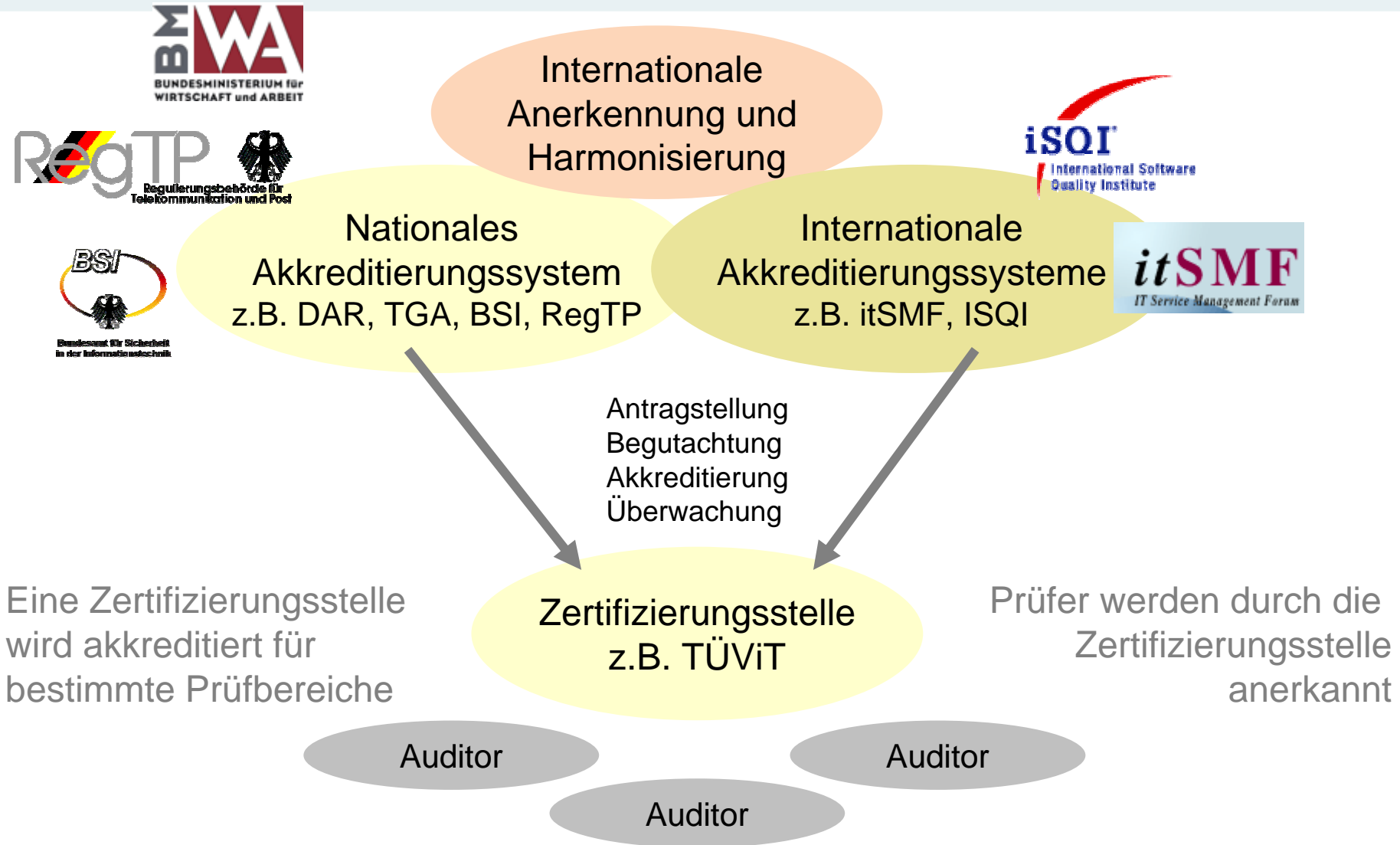
# Begriffe rund um die Zertifizierung



Der Begriff „Zertifizierung“ ist nicht geschützt und wird oft umgangssprachlich verwendet. „Zertifizierung“ im engeren Sinne ist die Bestätigung von Eigenschaften auf Basis eines offiziellen Regelwerkes.

- ... Audit
  - Externe Prüfung, ob geplante Qualitätsregelungen (z.B. ein QM-System) wirksam umgesetzt werden
- ... Assessment
  - Interne/externe Bewertung eines Managementsystems gegen ein Referenzmodell als Grundlage eines Verbesserungsprozess
- ... Evaluierung
  - Prüfung der Eigenschaften eines Objektes anhand definierter Prüfkriterien

# Aufbau einer Zertifizierungsstelle



## ➤ Regional

Abhängig von der Akkreditierung der Zertifizierungsstelle und wechselseitigen Anerkennungen

(Ziel ist weitgehende Freizügigkeit, dem stehen in manchen Fällen wirtschafts/sicherheitspolitische Interessen entgegen!)

## ➤ Zeitlich

➤ Produkt-Zertifikate i.d.R. unbeschränkt, solange das Produkt nicht verändert wird

➤ Systemzertifikate i.d.R. beschränkt mit regelmäßigen Wiederholung der Prüfung

## ➤ Inhaltlich

Eingeschränkt auf ein Prüfobjekt (Produkt/System/Person) und die geprüften Eigenschaften

- Einzelne Komponenten
  - SW-Module, z.B. Web-Services, Treiber
  - HW-Komponenten, z.B. Chipkarte, Kartenleser
- Produkt
  - SW-Produkte, z.B. Mailserver, Grundbuchverwaltung
  - HW-Produkte, z.B. Geldkartenautomat
- Personen
  - Bestätigung von Kenntnis/Leistungsstand  
z.B. Auditor für ISO 9000, ITIL Service Manager, CMMI  
Appraiser, SPICE Assessor

## ➤ Prozesse

- Entwicklungsprozesse, z.B. CMMI, SPICE
- Service Management, z.B. BS 15000, ITIL

## ➤ Systeme

- Managementsysteme, z.B. ISO 9000
- Sicherheitsmanagement, z.B. ISO 17799, Grundschatz
- Konkrete Installation von HW/SW-Produkten, z.B. eBusiness-System, System für Elektronische Steuererklärung

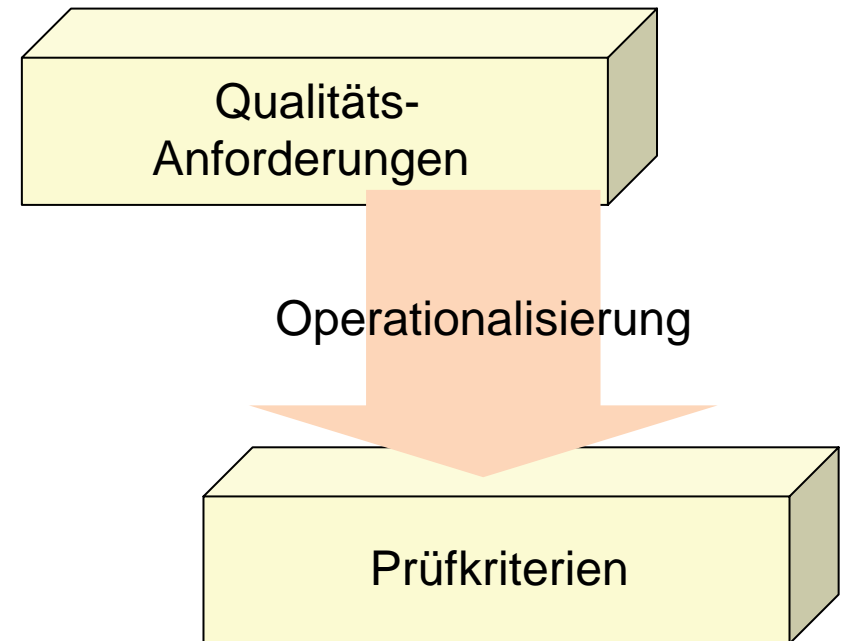
- Im Rahmen einer Prüfung wird ein Prüfgegenstand anhand von Kriterien bewertet, Quellen für Kriterien sind ...

- Normen
- Industriestandards
- Best practice

- Bedingungen für Prüfkriterien ...

- Validität
- Nachvollziehbarkeit
- Messbarkeit

- Für eine Zertifizierung müssen die Anforderungen und das Verfahren zur Ableitung der Prüfkriterien öffentlich verfügbar ein.



# Zertifizierung von Komponenten/Produkten



Kriterium	Prüfgrundlage	Beispiele
Qualität in der SW-Entwicklung	ISO 9126	
Übereinstimmung der Produkteigenschaften mit der Produktbeschreibung und Benutzerdokumentation	ISO 12119	Prüfung von Finanzbuchhaltungssystemen
Gebrauchstauglichkeit	ISO 9241-10,11	Grundbuchführung
Erfüllung von Sicherheitskriterien	ITSEC, CC (ISO 15408)	SW für Chipkarten
Stärke von Kryptographieverfahren	FIPS-140	Frankiersysteme
Funktionale Sicherheit	IEC 61508-3	Safety Integrity Level
Sicherheit von Produkten für elektronische Signatur	Signaturgesetz	Prüfung von Signaturkarten
Sicherheit im Zahlungsverkehr	Regelwerke ZKA	Geldausgabeautomaten
Konformität mit technischen Anforderungen	TÜViT Trusted Product	Materna WAP Gateway
Haushaltsrechtliche Korrektheit	OKKSA Kriterienkatalog	Kommunal-SW

# Zertifizierung von Prozessen/Personen



Kriterium	Prüfgrundlage	Beispiel
Reifegrad von Entwicklungsprozessen	ISO 15504 (SPICE)	SW-Entwicklung in der Automobile-Industrie
Reifegrad von Entwicklungsprozessen und Organisationen	CMMI	SW-Entwicklung für Projekte im US-government
Qualität von Prozessen zum Service Management	BS15000, ITIL	Service-Management bei Banken
Servicemanager nach ITIL Practitioner nach ITIL	itSMF	
SPICE-Assessor	INTACS	
CMMI- Lead Appraiser	CMMI	

# Zertifizierung von Systemen (I)



Kriterium	Prüfgrundlage	Beispiel
Anwendung eines prozessorientierten QM-Systems	ISO 9000:2000	
Sicherheit eines installierten Systems	Sicherheitstechnische Qualifizierung TÜViT	Skalierbare Unternehmens-Firewall Systemarchitektur (Microsoft) Remote Service (Heidelberger Druckmaschinen) Netzwerkinfrastruktur des akkreditierten Trust Centers (TC Trustcenter) Firewall für das Internet-Banking (Bank für Vorarlberg und Tirol)
Physikalische Sicherheit der IT-Infrastruktur	Trusted Site Infrastructure TÜViT	Accenture Data Center Flughafen München DATEV
Dokumentenmanagement gem. GoBS	Prüfkriterien (PK-DML) gem. TÜViT und VOI	Airbus Deutschland

# Zertifizierung von Systemen (II)



Kriterium	Prüfgrundlage	Beispiel
Maßnahmen für mittleren Schutzbedarf	Grundschrift-HB des BSI	Sicherheitskonzept für EU-Zahlstellen
Sicherheitsmanagement	BS 7799-2	Eurotel, Prag
Sicherheitsmanagement bei der Herstellung sicherheitsrelevanter Produkte	DeTeCardService/ TÜViT TU4®	Waferfertigung (Infineon Technologies Austria) Scratch-Off-Kartenproduktion (Datacolor Dialog-Medien GmbH ) Scratch-Off- und Chipkartenproduktion (Allami Nyomda, Budapest)
Sicherheitskonzept für Trust Center	Signaturgesetz	Hanseatische Steuerberaterkammer DATEV eG Deutsche Telekom AG TC TrustCenter AG
Einhaltung Vorgaben zum Datenschutz	Gesetze und Verordnungen zum Datenschutz	quid!, ULD

- Ein Zertifikat ist die Feststellung eines unparteiischen Dritten, dass ein Objekt bestimmte von einer unabhängigen Stelle festgelegte Forderungen erfüllt.
  - In einzelnen Bereichen ist die Zertifizierung gesetzlich vorgeschrieben. Hier liegt der Nutzen in der Erlaubnis zur Nutzung eines Produkts/Systems.
  - Im unregulierten Bereich wird der Nachweis der Sorgfaltspflicht im Sinne der Produkthaftung durch Zertifikate erleichtert.
  - Die Hersteller von Produkten dokumentieren durch Zertifikate die Qualität ihrer Produkte und versprechen sich davon bessere Marktchancen.
  - Zulieferer weisen durch Zertifikate gegenüber ihren Kunden die Qualität ihrer Prozesse und Produkte nach.

Werner Achtert

Bereichsleiter Projekt- und Qualitätsmanagement

Langemarckstraße 20

45141 Essen

Telefon: +49 201 8999 – 504

Telefax: +49 201 8999 – 544

E-Mail: [w.achtert@tuvit.de](mailto:w.achtert@tuvit.de)

URL: [www.tuvit.de](http://www.tuvit.de)