



**Westfälische  
Hochschule**

Gelsenkirchen Bocholt Recklinghausen  
University of Applied Sciences

# Sicherheitsmodule

Prof. Dr. (TU NN)

**Norbert Pohlmann**

Institut für Internet-Sicherheit – if(is)  
Westfälische Hochschule, Gelsenkirchen  
<http://www.internet-sicherheit.de>

**if(is)**  
internet-sicherheit.

- **Ziele**
- **SmartCard (Chipkarten)**
- **High-security und high-performance Sicherheitsmodule**
- **Trusted Platform Module (TPM)**
- **Zusammenfassung**

## ■ Ziele

- SmartCard (Chipkarten)
- High-security und high-performance Sicherheitsmodule
- Trusted Platform Module (TPM)
- Zusammenfassung

# Ziel eines Sicherheitsmoduls

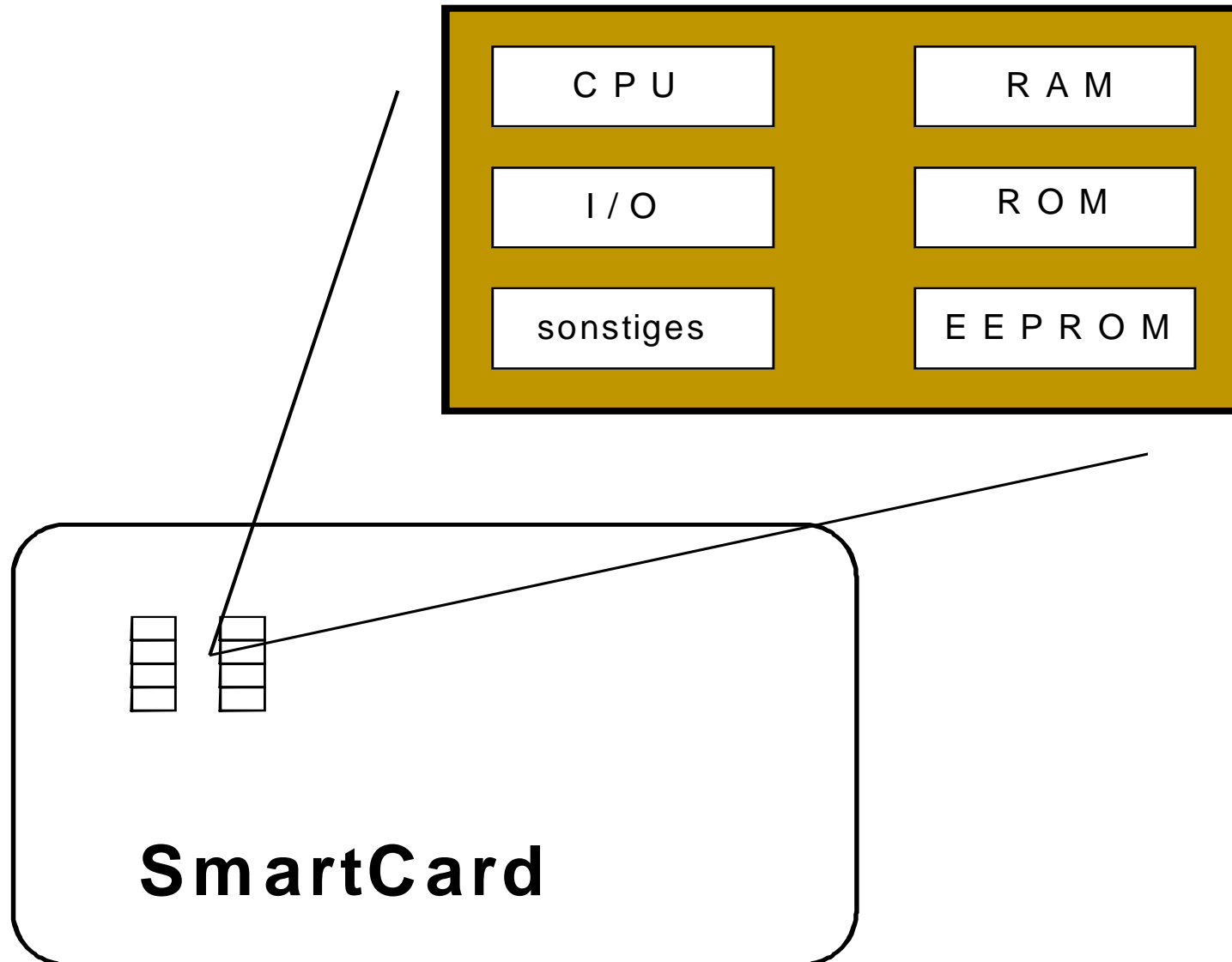
- Schutz vor Auslesen und Manipulation von sicherheitsrelevanten Informationen innerhalb eines geschützten Bereiches, meist Hardware
- **Sicherheitsrelevante Informationen** sind:
  - **Geheime Schlüssel**  
(für Verschlüsselung, Authentisierung, Signaturen, ..)
  - **Programme**  
(die nicht kopiert oder modifiziert werden dürfen)
  - **Daten**  
(z.B. Transaktionsdaten, die Werte darstellen)

- Ziele
- **SmartCard (Chipkarten)**
- High-security und high-performance Sicherheitsmodule
- Trusted Platform Module (TPM)
- Zusammenfassung

# SmartCard (Chipkarten)

- Eine SmartCard oder intelligente Chipkarte ist ein IT-System in der genormten Größe der EC-Karte (86 x 54 x 0,76 mm), das dem Nutzer Sicherheitsdienstleistungen zur Verfügung stellt.
- Eine SmartCard enthält:
  - eine CPU
  - RAM- und ROM-Speicher
  - ein »schlankes« Betriebssystem im ROM
  - eine I/O-Schnittstelle, über die die gesamte Kommunikation stattfindet (Kontaktflächen oder kontaktloses Interface)
  - ein EEPROM, auf das die geheimen Schlüssel, z. B. ein privater RSA-Schlüssel oder andere symmetrische Schlüssel, sowie persönliche Daten (Passworte etc.) sicher gespeichert sind
  - Sonstiges, beispielsweise einen Co-Prozessor, der symmetrische oder asymmetrische Verschlüsselung sehr schnell durchführt (Krypto-Prozessor)

# SmartCard



# SmartCard

## → Sicherheitsdienste

- Eine SmartCard stellt dem Nutzer in der Regel folgende Sicherheitsdienstleistungen zur Verfügung:
- Laden und Entladen von Werteinheiten für elektronisches Bezahlen (auch ohne Krypto-Prozessor)
- Kryptographische Anwendungen wie Digitale Signaturen usw.
- Identifikation/Authentisierung des Nutzers (Aktivieren der SmartCard)
- Single Sign On-Anwendungen (z. B. Passwort und PIN für unterschiedliche Anwendungen)
- Sicheres Speichern von Daten auf der SmartCard
- Lesen gespeicherter Servicedaten
- Ausführen sonstiger Rechenoperationen



### ■ SmartCard Hardware:

- Unter- und Überspannungsdetektion
- Erkennung niedriger Frequenzen
- gescramblete Busse
- Sensoren für Licht, Temperatur usw.
- Passivierungs- bzw. Metallisierungsschichten über Bus- und Speicherstrukturen oder über der gesamten CPU
- Zufallszahlengenerator in der Hardware
- spezielle CPU-Befehle für kryptographische Funktionen
- Speicherschutzfunktionen

### ■ SmartCard Software:

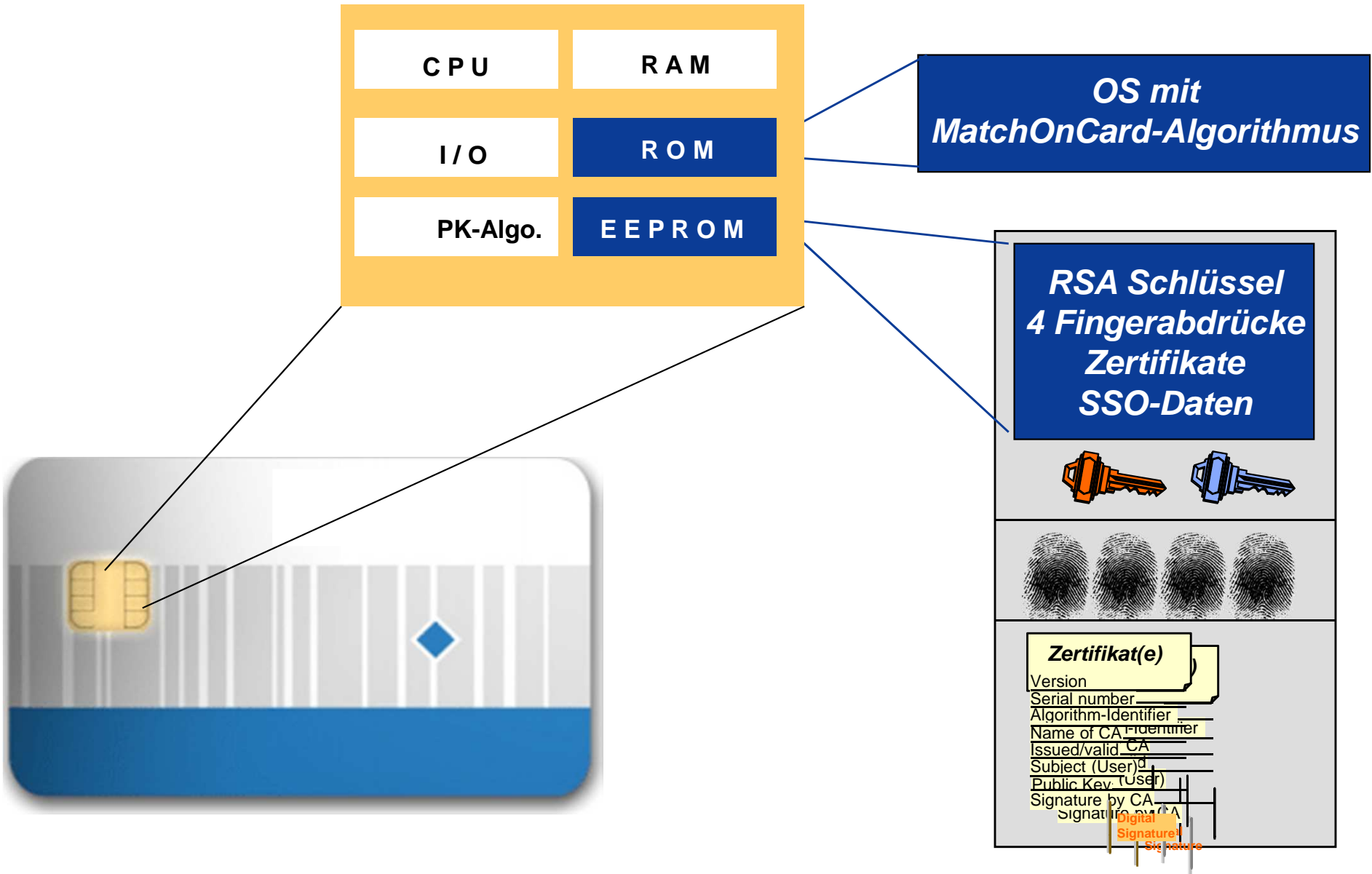
- Zugriffskontrolle auf Objekte
- Zustandsautomaten, die in Abhängigkeit von Identifikations- und Authentisierungsmechanismen Befehle zulassen

# SmartCard

## → Vorteile

- SmartCards bieten erhöhte Sicherheit im Vergleich zu reinen Software Lösungen.
- **Die Sicherheit beruht auf:**
  - Wissen (die PIN) und
  - Besitz (die Karte).
  - Geheime Schlüssel verlassen die Karte nie
  - Alle geheimen Operationen finden direkt in der Karte statt.
  - Schlüssel können benutzt werden, ohne sie zu kennen
  - Geheime Daten sind manipulationssicher in der Karte gespeichert.

# Die biometrische SmartCard



# Alternative zur SmartCard

## Yubico

- FIPS certification
  - Secure manufacturing process
  - Easy to program own secrets
- Tamper proof casing
- Hardware two-factor authentication
- AES encryption



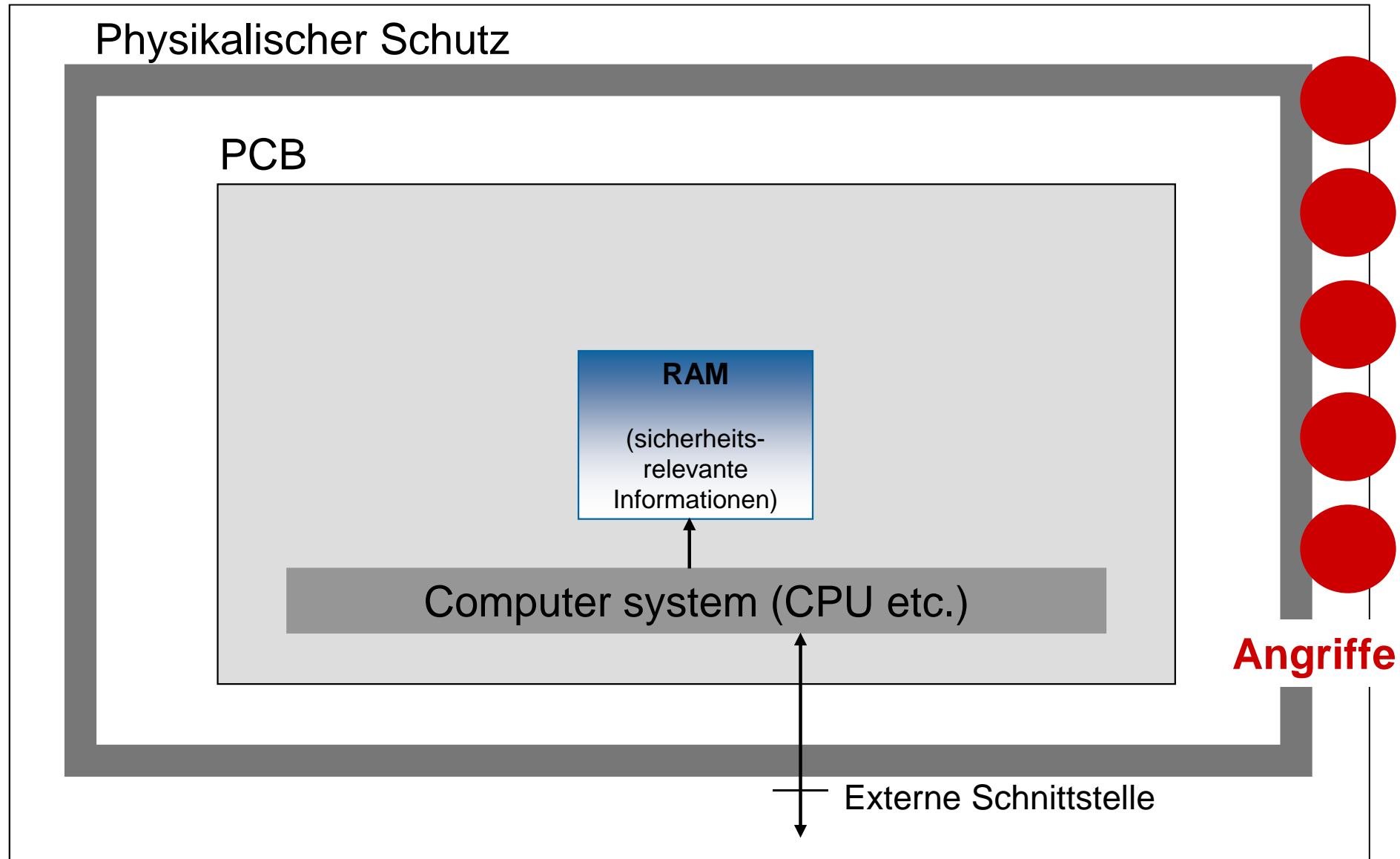
- Ziele
- SmartCard (Chipkarten)
- **High-security und high-performance Sicherheitsmodule**
- Trusted Platform Module (TPM)
- Zusammenfassung

# High-security und high-performance SM

## → Ziele

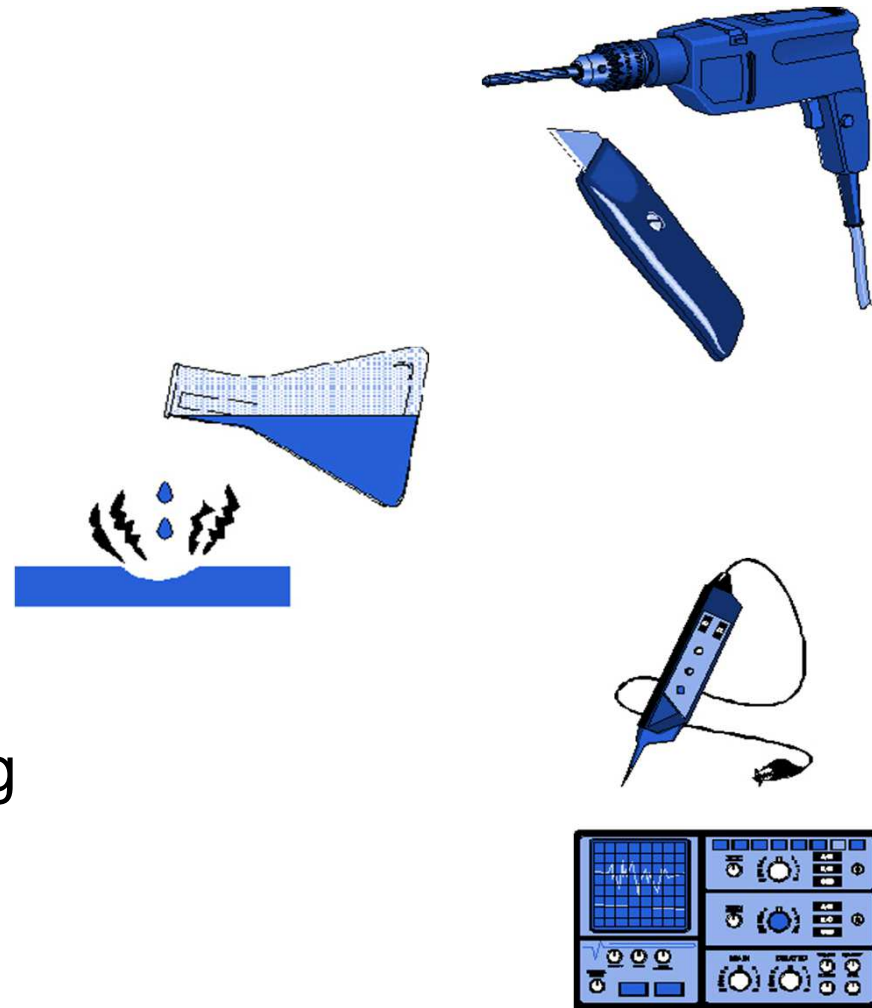
- High-security und high-performance Security Module für
  - besonders sichere, wertvolle Informationen (z.B. Master-Keys)
  - sehr hohe Performance-Anforderungen
- **Wenn ein Angriff** vom Sicherheitsmodul erkannt wird, sind die zu schützenden sicherheitsrelevanten Informationen innerhalb des Sicherheitsmoduls sofort **aktiv** zu **löschen**.

# High-security und high-performance SM → Idee



# High-security und high-performance SM → potentielle Angriffe

- Durchleuchten
- Temperatur Angriffe
- Mechanischen Attacke
- Chemischen Attacke
- Manipulation über Spannung



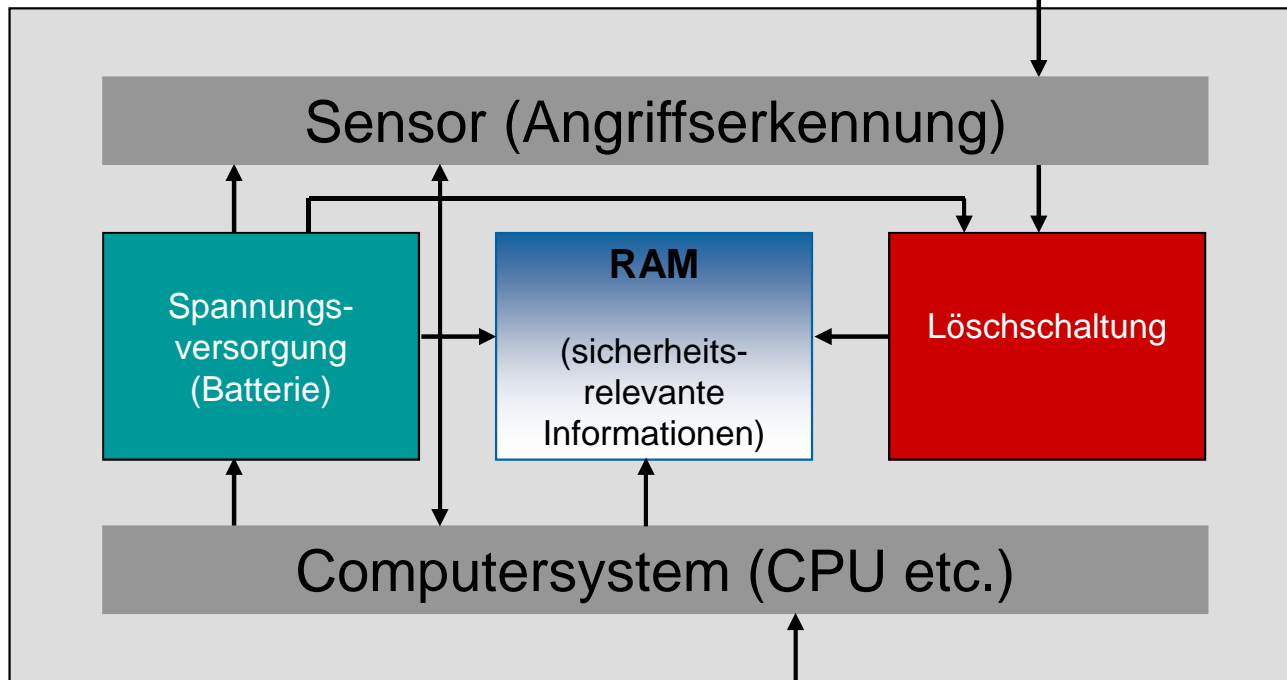
**Angriffe**



# High-security und high-performance SM → Idee

## Physikalischer Schutz

PCB



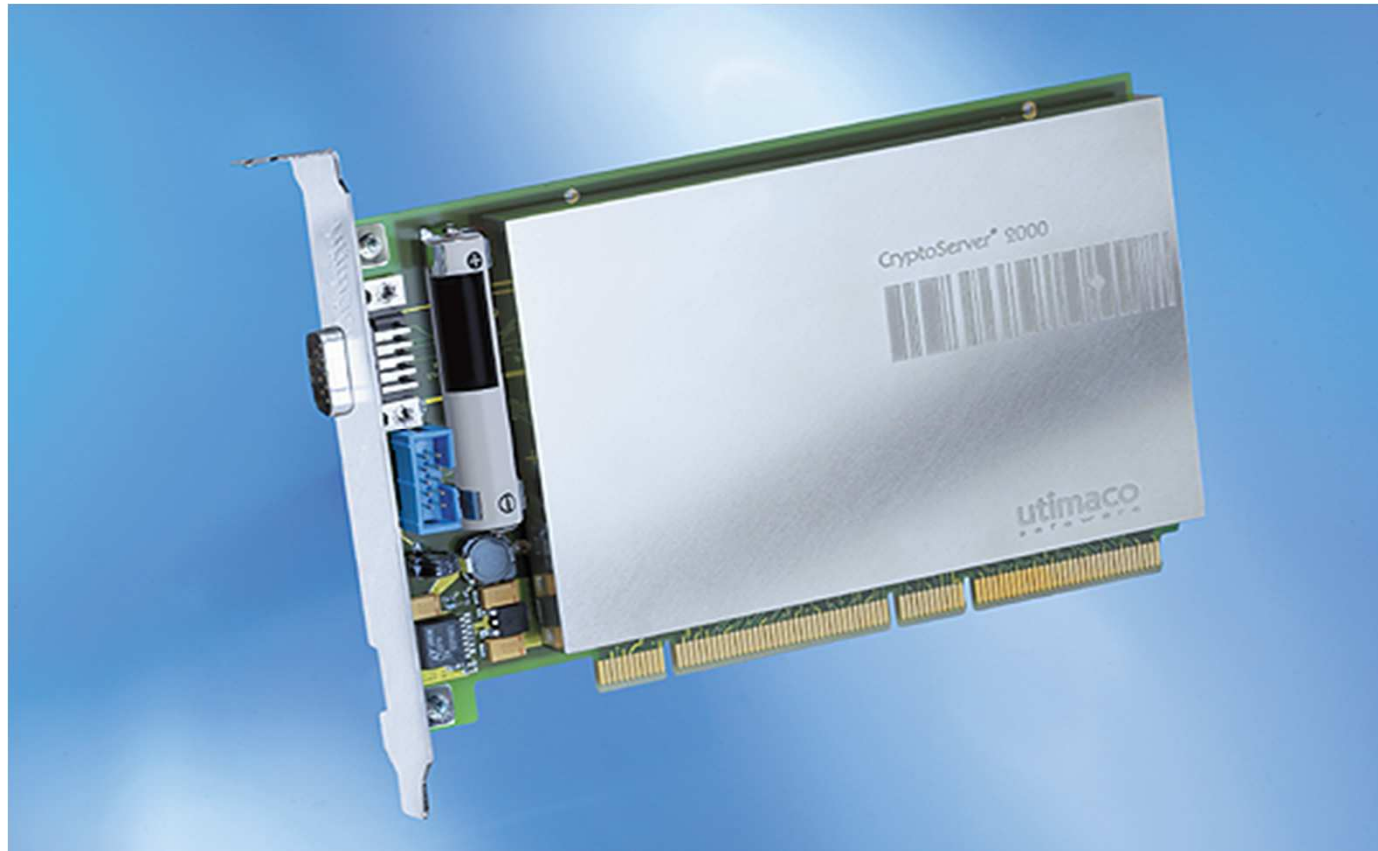
Externe Schnittstelle

# High-security und high-performance SM → Anforderungen

- Grundanforderungen an Sicherheitsmodule in transaktionsbasierten Systemen:
  - Performance
  - Skalierbarkeit
  - Verfügbarkeit
  - flexible Schnittstellen zu den Host - Systemen
    - physikalisch: TCP/IP (100MBit, 1GBit, FDDI, ... )
    - logisch: Support von bestehenden Schnittstellen
- Übergang der kryptographischen Hoheit an die Verantwortung eines Betreibers
- Umstellungsmöglichkeit auf neue kryptographische Verfahren

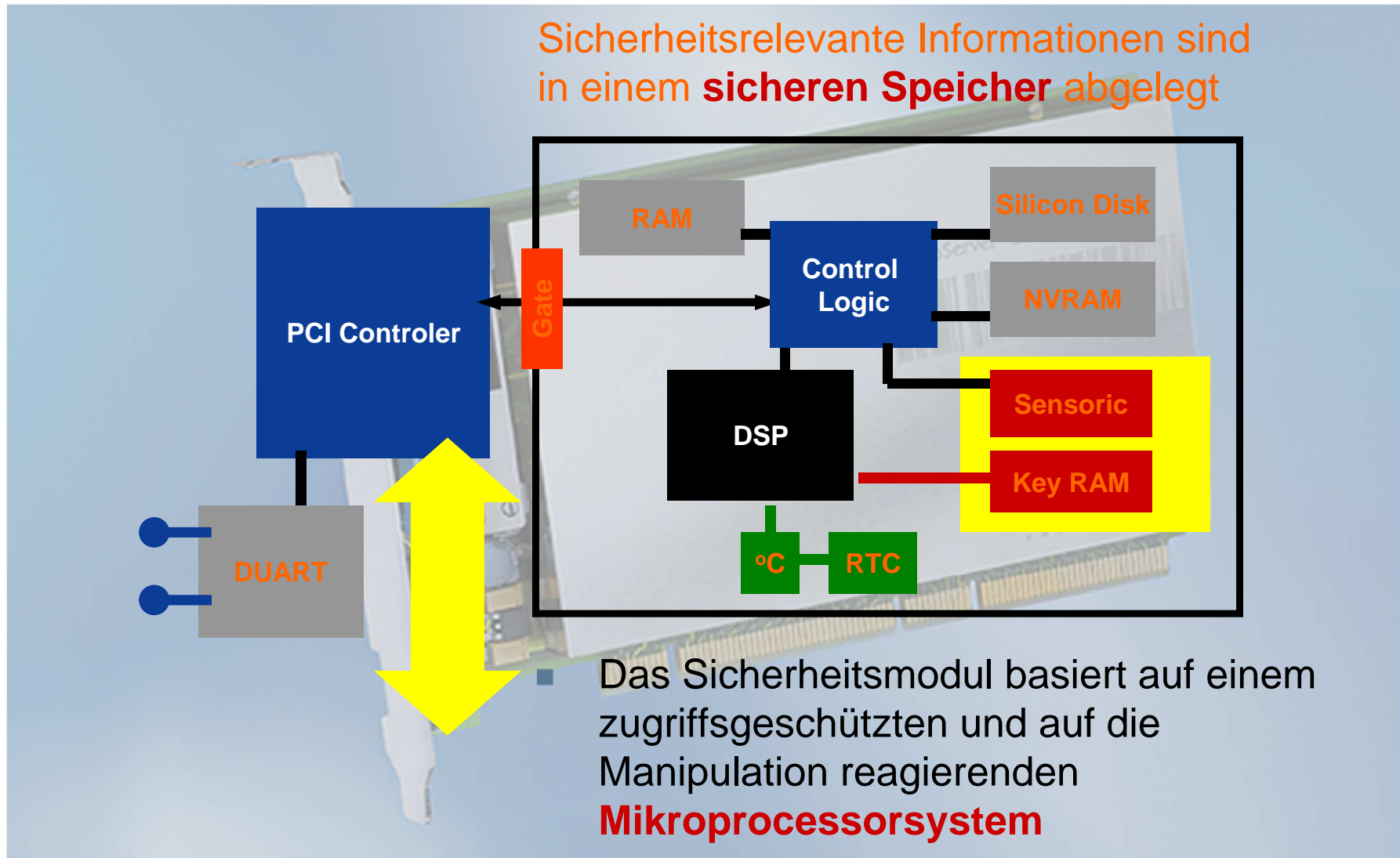
# High-security und high-performance SM → Beispiel CryptoServer

- Generisches standalone Computer-System



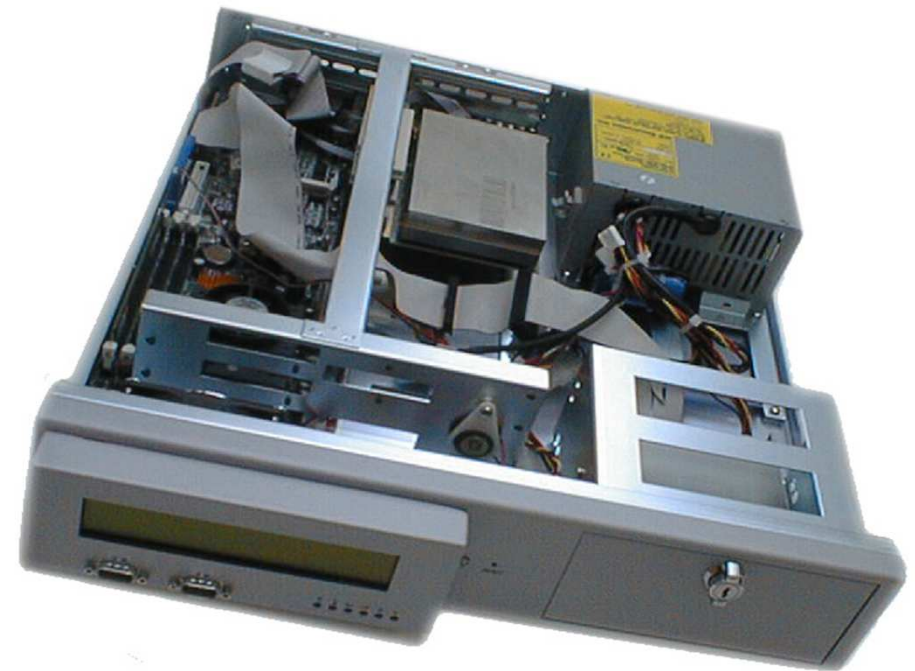
- Die zusätzliche Trägerkarte mit Interfaces bildet das Co-Processor Board

# High-security und high-performance SM → Hardware (1/2)



# High-security und high-performance SM → Hardware (2/2)

- Sicherheitsmodul plus Kommunikationseinheit
  - Kommunikationsrechner
  - 10/100 Mbit Ethernet
  - Flash Disk
  - Hardware Watchdog onboard
  - 4 x 40 Display + Navigation Panel
  - wahlweise mit CD writer



# High-security und high-performance SM → Anwendungen

- Public Key Infrastruktur
  - Schlüsselgenerierung (Signaturgesetz - Unterschrift!)
- Bankenumfeld
  - Autorisierungsstationen (Freigabe von Geld)
  - Sicherheit für die Netzbetreiber (z.B. im Bereich ec, Mineralölunternehmen)
- Industrie
  - Schlüsselgenerierung für Auto-Schlüssel
  - Maut-Systeme (Abrechnung)
  - Authentikation im Mobilfunknetz
  - Digitale Signatur von zentralen Prozessen (Rechnungen, usw.)

- Ziele
- SmartCard (Chipkarten)
- High-security und high-performance Sicherheitsmodule
- **Trusted Platform Module (TPM)**
- Zusammenfassung

# Trusted Platform Module (TPM)

## → Idee

- TPM ist ein kleines Sicherheitsmodul für alle Rechnersysteme (PC, Notebook, PDA, Drucker, Router, Kühlschrank, usw.)
- Beispiel: IBM hat eine Notebook-Business-Lösung auf der schon TPM-Bausteine vorhanden sind.
- Kosten sollen kleiner als ein € sein!
- Gesteuert durch die Trusted Computing Group (TCG). Hauptmitglieder: Microsoft, Intel, HP, IBM, AMD, Sony, SUN, aber auch Infineon, Utimaco, ...
- Einheitliche Standard-Software im TPM.
- Die einzelnen Unternehmen machen dann ihre eigene Lösung.
- Z.B. Microsoft: Next Generation Secure Computing Base (NGSCB)

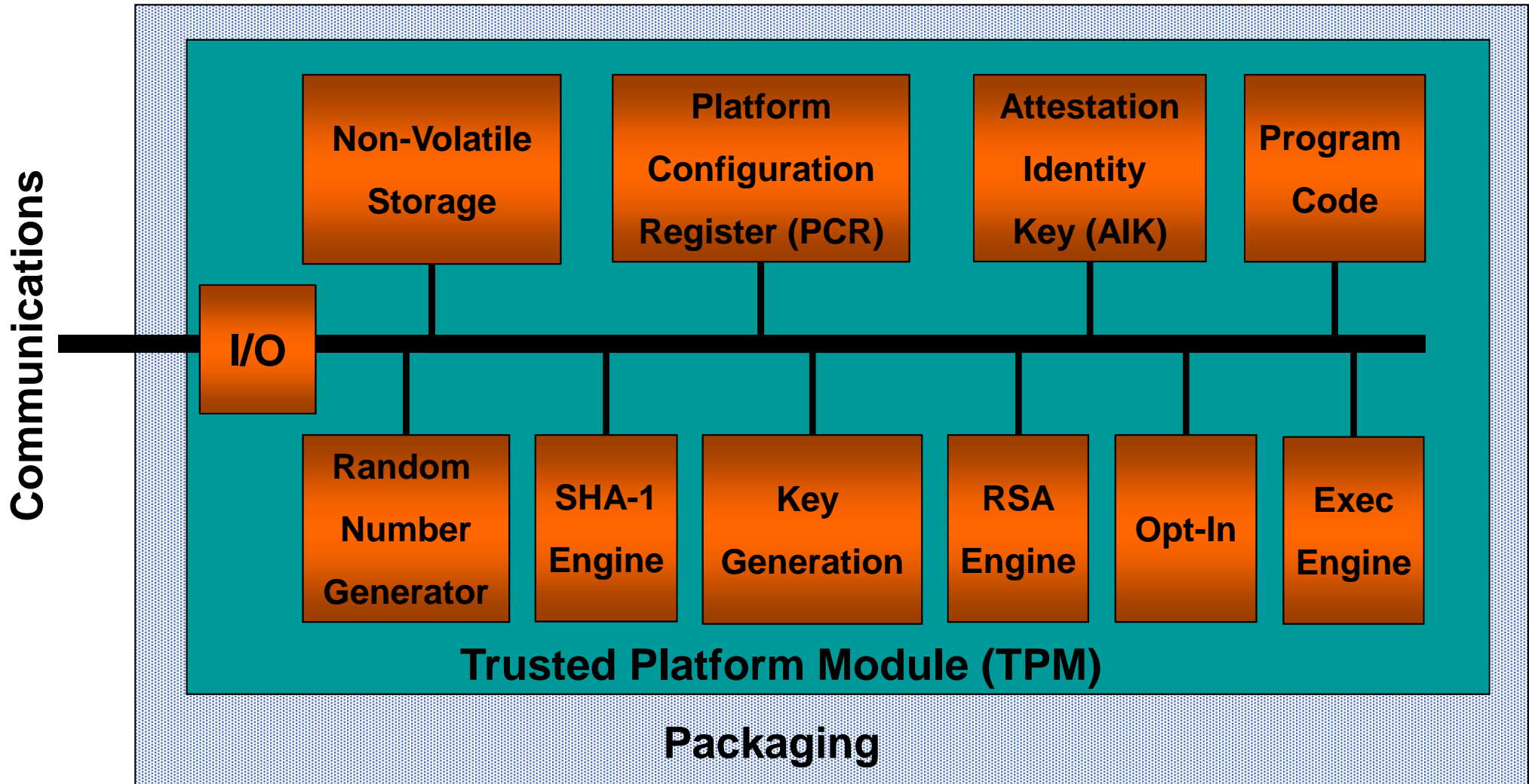


TPM

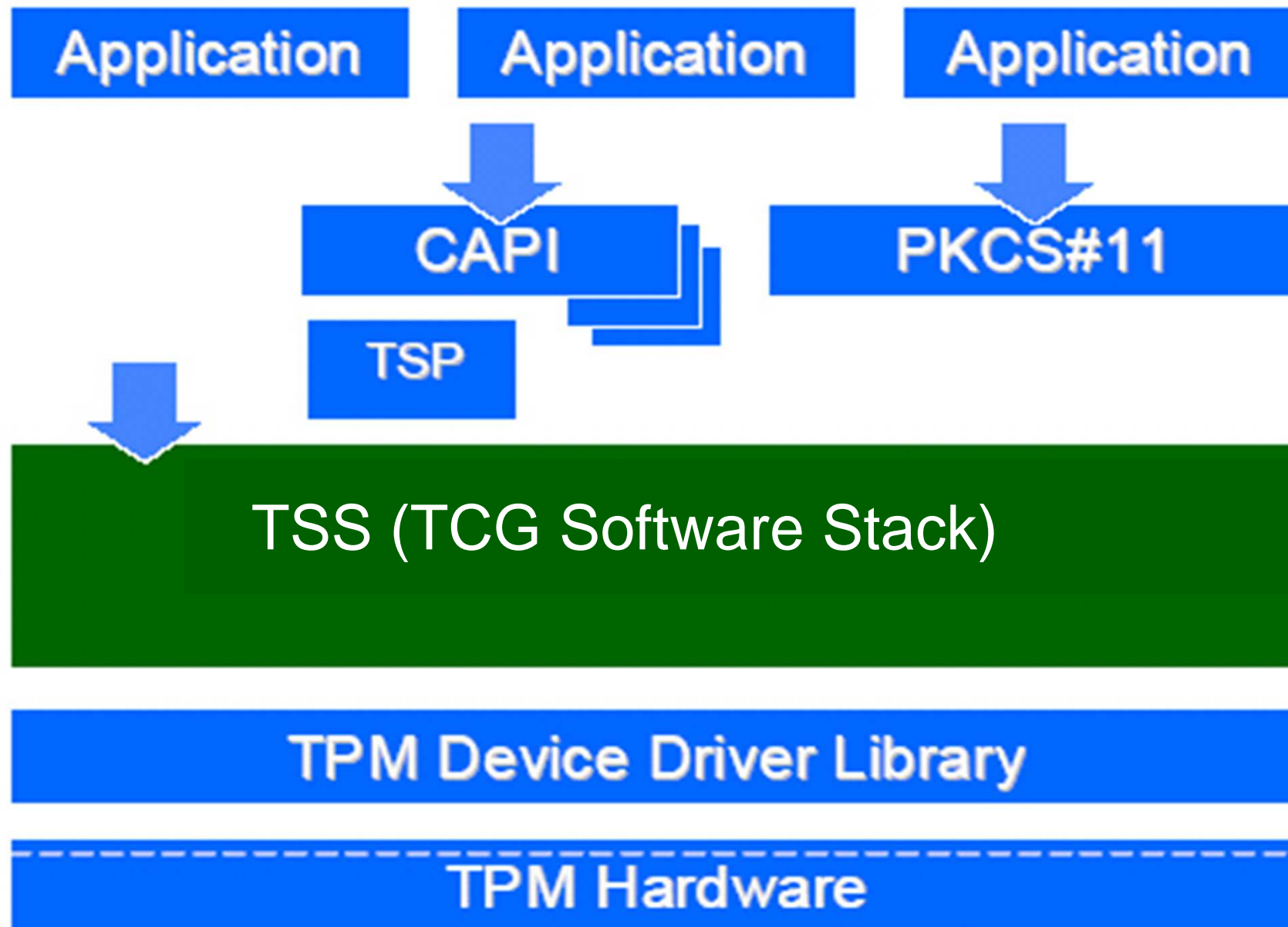


# Trusted Platform Module (TPM)

## → Basisfunktionen im TPM



# Trusted Platform Module (TPM) → Software Stack (TSS)



- Ziele
- SmartCard (Chipkarten)
- High-security und high-performance Sicherheitsmodule
- Trusted Platform Module (TPM)
- **Zusammenfassung**

# Sicherheitsmodule

## → Zusammenfassung

### ■ Einsatzumfeld einer SmartCard

- SmartCards werden typischerweise als **Sicherheitskomponenten für Personen** eingesetzt.

### ■ Einsatzumfeld eines high-security und high-performance Security Modules

- High-security und high-performance Security Module werden typischerweise als **Sicherheitskomponenten für größere Rechnersysteme im Sicherheitsumfeld** eingesetzt.

### ■ Einsatzumfeld von TPM

- TPMs werden wahrscheinlich als **Sicherheitskomponenten für kleinere Rechnersysteme** eingesetzt.



**Westfälische  
Hochschule**

Gelsenkirchen Bocholt Recklinghausen  
University of Applied Sciences

# Sicherheitsmodule

**Vielen Dank für Ihre Aufmerksamkeit  
Fragen ?**

Prof. Dr. (TU NN)

**Norbert Pohlmann**

Institut für Internet-Sicherheit – if(is)  
Westfälische Hochschule, Gelsenkirchen  
<http://www.internet-sicherheit.de>

**if(is)**  
internet-sicherheit.