



IT-Sicherheit

05-Hardware-Sicherheitsmodule

Gerrit Kalkbrenner

Gerrit.Kalkbrenner@hwr-berlin.de

Teile: Norbert Pohlmann



Hardware-Sicherheitsmodule

Inhalt

- Ziele und Ergebnisse der Vorlesung
- Idee eines Hardware-Sicherheitsmoduls
- HSM: Smartcards
- HSM: Trusted Platform Module (TPM)
- HSM: High-Level Security Module (HLSM)
- Rahmenbedingungen
- Zusammenfassung



Hardware-Sicherheitsmodule

Inhalt

- **Ziele und Ergebnisse der Vorlesung**
- Idee eines HSM
- HSM: Smartcards
- HSM: Trusted Platform Module (TPM)
- HSM: High-Level Security Module (HLSM)
- Rahmenbedingungen
- Zusammenfassung



Ziele und Ergebnisse der Vorlesung

- Hardware-Sicherheitsmodule
 - Gutes **Verständnis** zu der Bedeutung von **Hardware-Sicherheitsmodule** im Bereich der Cyber-Sicherheit.
 - **Profundes Wissen** über die verschiedenen und aktuellen **Hardware-Sicherheitsmodule**.
 - Erlangen der **Kenntnisse** über prinzipielle Hardware-Sicherheitsmodule und zur **Umsetzung von konkreten Lösungen**.



- Inhalt

Hardware-Sicherheitsmodule

- Ziele und Ergebnisse der Vorlesung
- **Idee eines HSM**
- HSM: Smartcards
- HSM: Trusted Platform Module (TPM)
- HSM: High-Level Security Module (HLSM)
- Rahmenbedingungen
- Zusammenfassung

Idee eines HSM

- 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)





- Inhalt

Hardware-Sicherheitsmodule

- Ziele und Ergebnisse der Vorlesung
- Idee eines HSM
- **HSM: Smartcards**
- HSM: Trusted Platform Module (TPM)
- HSM: High-Level Security Module (HLSM)
- Rahmenbedingungen
- Zusammenfassung

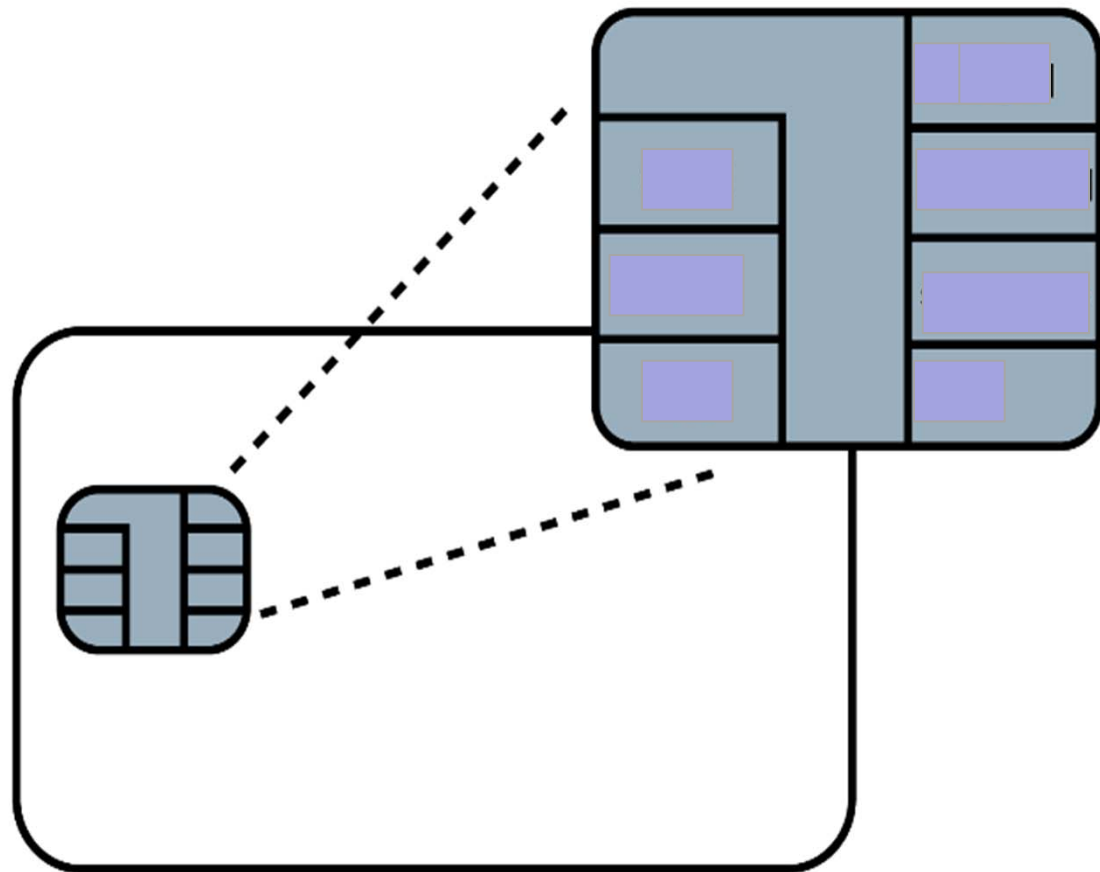


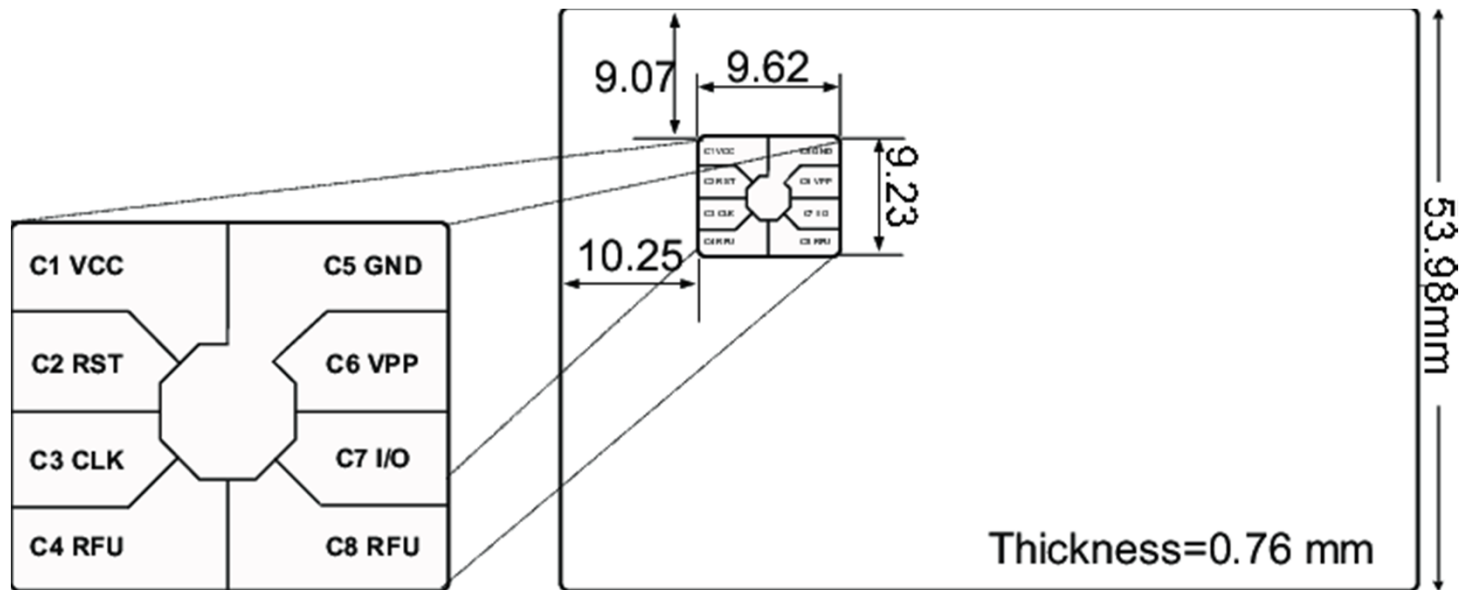
HSM: Smartcards • Überblick (1/2)

- Eine SmartCard ist ein IT-System in der genormten Größe der EC-Karte (86 x 54 x 0,76 mm) mit Sicherheitsdienstleistungen.
- **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 Krypto-Prozessor.

HSM: Smartcards

- Überblick (2/2)
- CPU
- RAM/ROM
- I/O-Schnittstelle
- EEPROM / Flash
- Krypto-Prozessor





HSM: Smartcards

- 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



HSM: Smartcards

- Sicherheitsmechanismen einer Smartcard (1)
 - **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



HSM: Smartcards

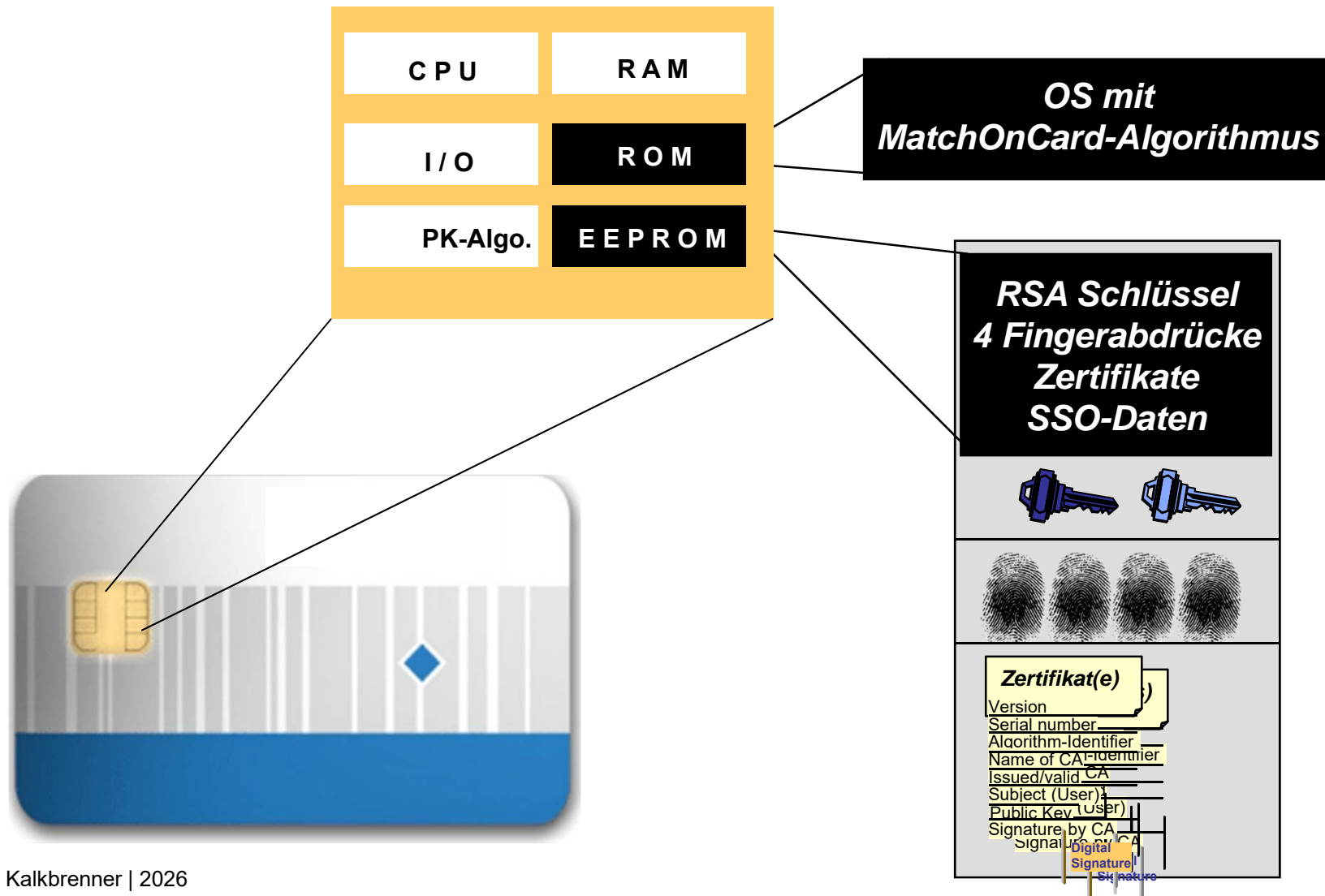
- Sicherheitsmechanismen einer Smartcard (2)
 - **Smartcard Software:**
 - Zugriffskontrolle auf Objekte
 - Zustandsautomaten, die in Abhängigkeit von Identifikations- und Authentisierungsmechanismen Befehle zulassen

- Vorteile

HSM: Smartcards

- 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.
- Geschätzter Aufwand eines erfolgreichen Angriffs: 1 Mio. €

HSM: Smartcards • Die biometrische Smartcard



- Alternative zur Smartcard
HSM: Smartcards
 - **Yubico:**
 - FIPS certification
 - Secure manufacturing process
 - Easy to program own secrets
 - Tamper proof casing
 - Hardware two-factor authentication
 - AES encryption





- Inhalt

Hardware-Sicherheitsmodule

- Ziele und Ergebnisse der Vorlesung
- Idee eines HSM
- HSM: Smartcards
- **HSM: Trusted Platform Module (TPM)**
- HSM: High-Level Security Module (HLSM)
- Rahmenbedingungen
- Zusammenfassung

- Idee (1/2)

HSM: Trusted Platform Module

- TPM ist ein kleines Sicherheitsmodul für alle Rechnersysteme (PC, Notebook, Smartphone, Drucker, Kühlschrank, usw.)



TPM

- Beispiel: IBM (Lenovo) hat seit längerem eine Notebook-Business-Lösung, auf der schon TPM vorhanden sind.
- Kosten kleiner als 1€ !



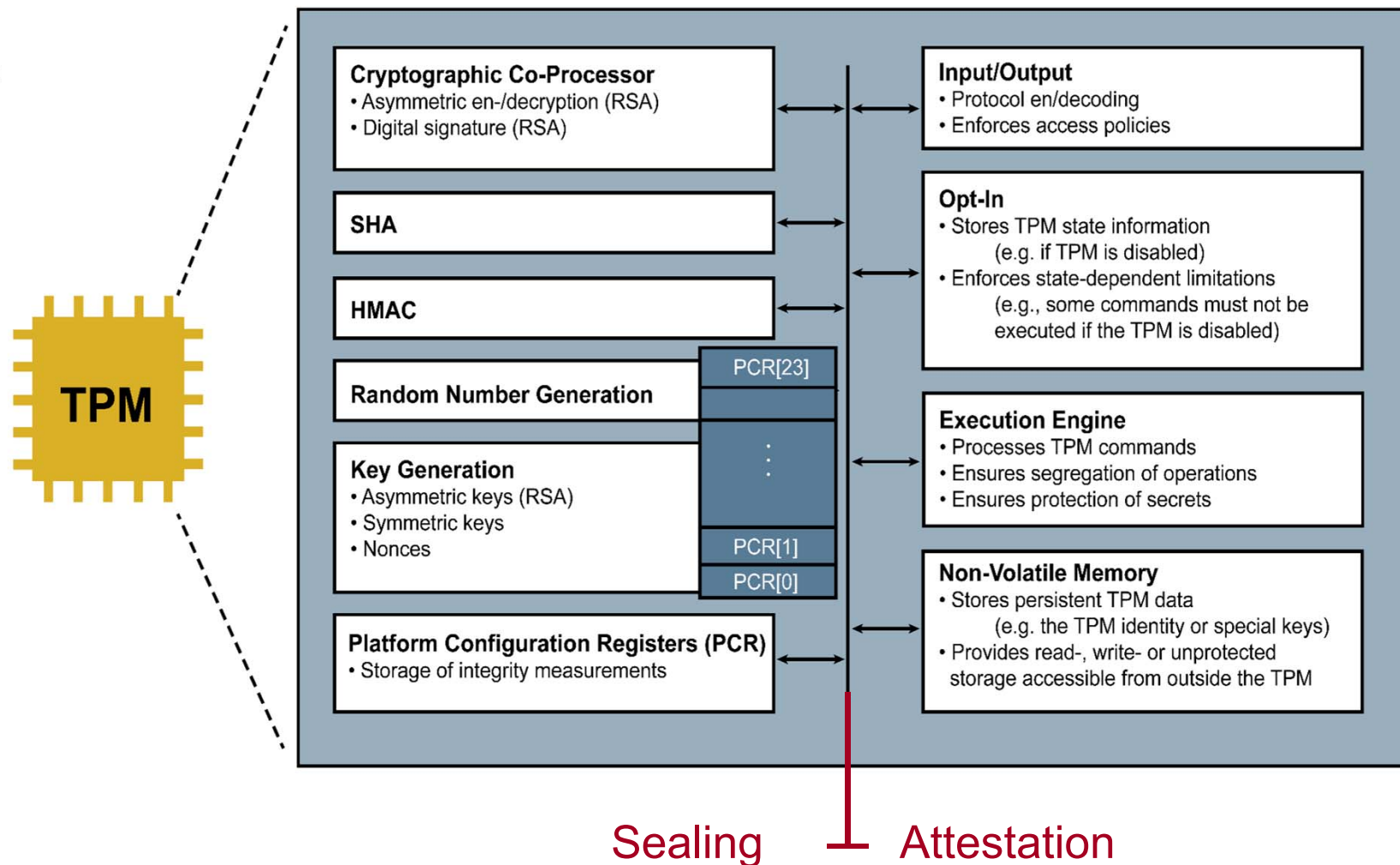
- Idee (2/2)

HSM: Trusted Platform Module

- Gesteuert durch die Trusted Computing Group (TCG). Hauptmitglieder: Microsoft, Intel, HP, IBM, AMD, Sony, Oracle, aber auch Infineon, Utimaco, Lenovo...
- Einheitliche Standard-Software im TPM.
- Die einzelnen Unternehmen machen dann ihre eigene Lösung.
- Z.B. Microsoft: Next Generation Secure Computing Base (NGSCB)

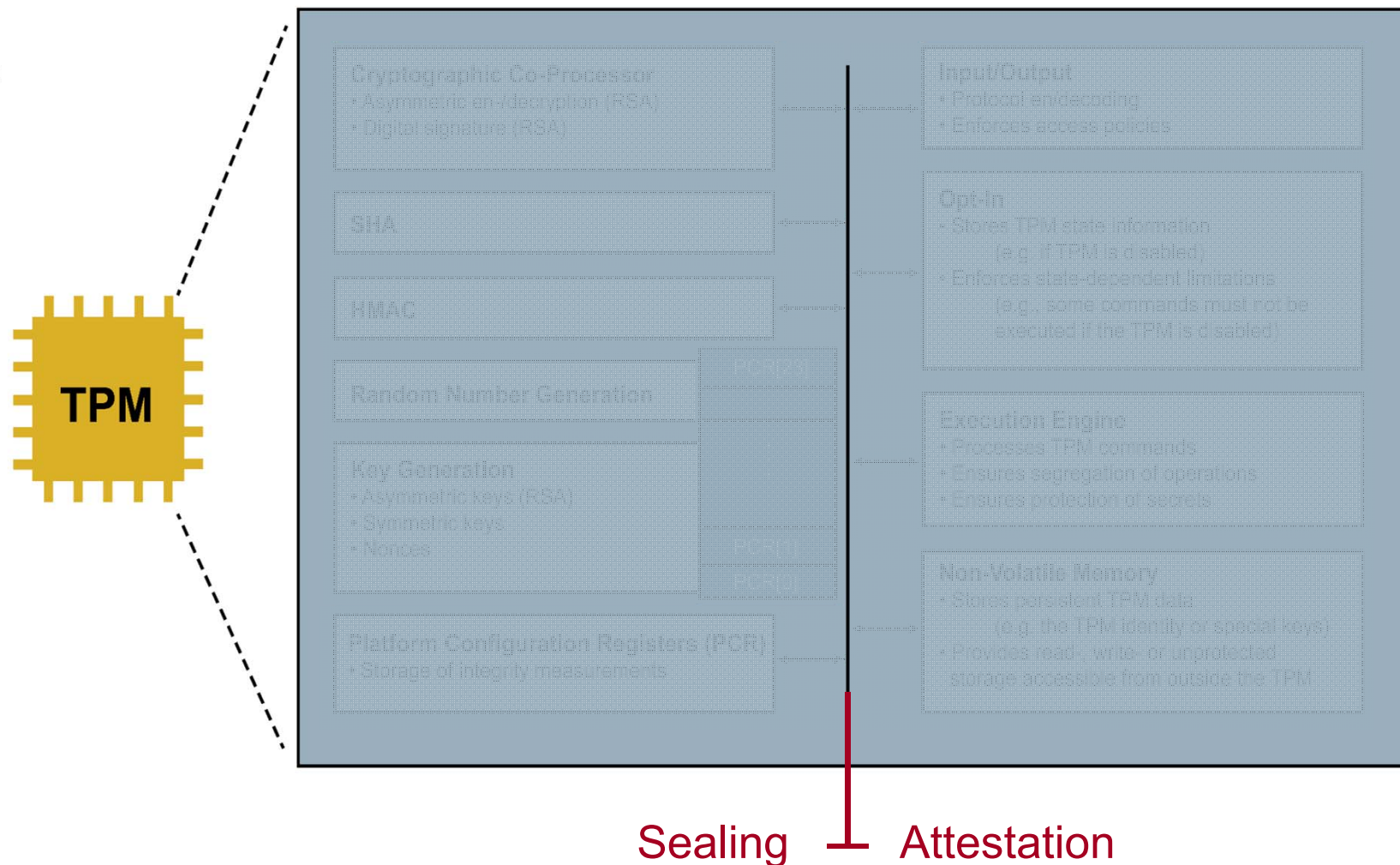


HSM: Trusted Platform Module





HSM: Trusted Platform Module



HSM: Trusted Platform Module

- **Vorteile:**

- Sehr hohe Sicherheit bei geringer Investitionssumme (ein €).
- Sicherheit gleicht einer Smartcard.
- Microsoft Readiness in den meisten Fällen gegeben.
- Einfaches Sicherheitsmanagement durch Einbindung in eine Sicherheitsinfrastruktur (PKI, etc.).

- **Nachteile:**

- Intransparenz der TCG.
- Physikalische Backdoors möglich.



- Inhalt

Hardware-Sicherheitsmodule

- Ziele und Ergebnisse der Vorlesung
- Idee eines HSM
- HSM: Smartcards
- HSM: Trusted Platform Module (TPM)
- **HSM: High-Level Security Module (HLSM)**
- Rahmenbedingungen
- Zusammenfassung

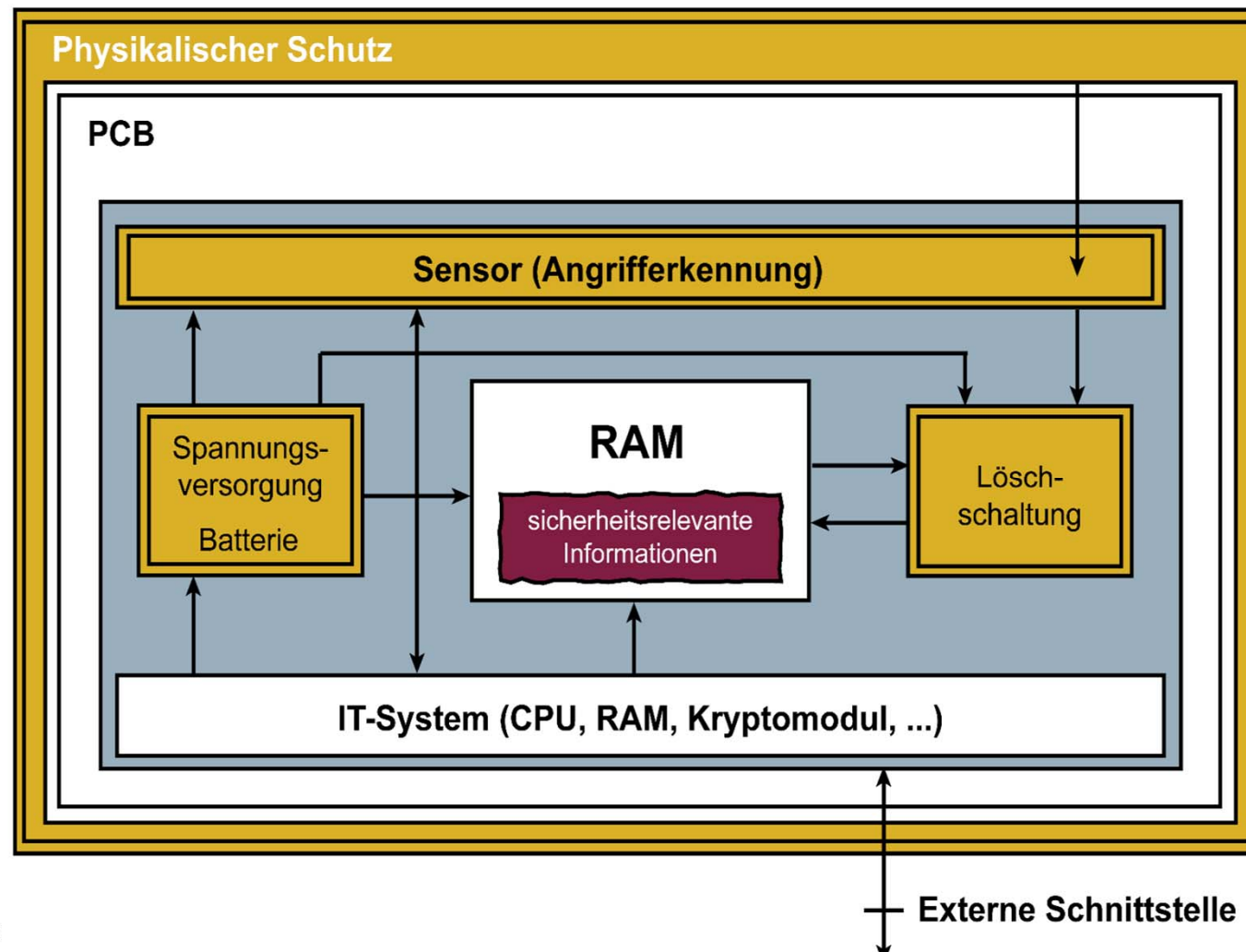
- Ziele

HSM: High-Level Security Module

- 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.

HSM: High-Level Security Module

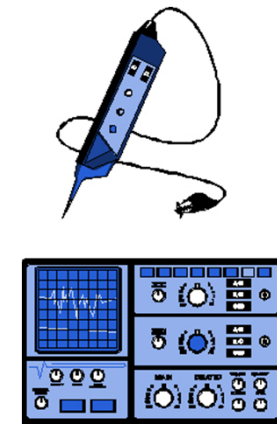
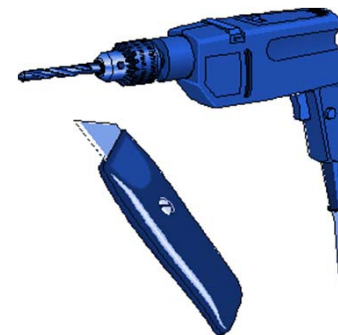
- Sicherheitsmechanismen





- **Potentielle Angriffe**
HSM: High-Level Security Module

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





- Anforderungen (1/2)

HSM: High-Level Security Module

- 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



- Anforderungen (2/2)

HSM: High-Level Security Module

- Übergang der kryptographischen Hoheit an die Verantwortung eines Betreibers
- Umstellungsmöglichkeit auf neue kryptographische Verfahren
- Vertrauenswürdige Basis (z.B. geringe Anzahl an „Lines of Code“)



- Anwendungen (1/2)

HSM: High-Level Security Module

- Geschätzter Aufwand eines erfolgreichen Angriffs: 5 Mio. €
 - z.B. Sicherung von Master-Schlüsseln
- Public Key Infrastruktur:
 - Schlüsselgenerierung (Signaturgesetz - Unterschrift!)
- Bankenumfeld:
 - Autorisierungsstationen (Freigabe von Geld)
 - Sicherheit für die Netzbetreiber
(z.B. im Bereich ec, Mineralölunternehmen)



- Anwendungen (2/2)

HSM: High-Level Security Module

- Industrie:

- Schlüsselgenerierung für Auto-Schlüssel
- Maut-Systeme (Abrechnung)
- Authentifikation im Mobilfunknetz
- Digitale Signatur von zentralen Prozessen (Rechnungen, usw.)



Hardware-Sicherheitsmodule

Inhalt

- Ziele und Ergebnisse der Vorlesung
- Idee eines HSM
- HSM: Smartcards
- HSM: Trusted Platform Module (TPM)
- HSM: High-Level Security Module (HLSM)
- **Rahmenbedingungen**
- Zusammenfassung

- Evaluierung und Zertifizierung
Rahmenbedingungen
 - Nachweis der Hard- und Software-Sicherheit
 - unabhängige qualifizierte Organisationen
 - Beispiele für Standards:
 - FIPS 140-1
 - FIPS 140-2
 - CC Schutzprofil CWA 14167-2
 - Beispiele für Fragestellungen:
 - Erfüllt ein Zufallszahlengenerator alle notwendigen Eigenschaften, wie z.B. Gütekriterien, Streuung, Periodizität, Gleichverteilung?
 - Sind die Sicherheitsprotokolle sicher implementiert?



- **Key-Management (1/2)**
Rahmenbedingungen
 - **Generelle Anforderungen:**
 - Keiner hat direkten Zugriff auf die geheimen Schlüssel.
 - Nutzung der Krypto-Funktionen (z.B. geheime Schlüssel) nur nach Autorisierung.
 - Definition und Veränderung von Funktionalitäten nur nach Autorisierung.
 - **Management von TPMs:**
 - Personalisierung des TPMs durch einen einzigartigen Endorsement Key (EK).
 - EK wird von einer öffentlichen PKI verwaltet/signiert.
 - Einfache Einbindung für verschiedene Anwendungen (z.B. VPN-Systeme).



- **Key-Management (2/2)**
Rahmenbedingungen
 - **Management nach dem Vier-Augen-Prinzip:**
 - Kritische Tätigkeiten sollten nicht von einer einzelnen Person durchgeführt werden.
 - Electronic Cash-Netze werden z.B. durch HLSMs miteinander verbunden.
 - Verwendung von unterschiedlichen Schlüsselsystemen.
 - Um-Verschlüsselung der Transaktionen nötig.
 - Schlüssel werden nach dem Vier-Augen-Prinzip eingegeben.



Hardware-Sicherheitsmodule

- **Inhalt**
- Ziele und Ergebnisse der Vorlesung
- Idee eines HSM
- HSM: Smartcards
- HSM: Trusted Platform Module (TPM)
- HSM: High-Level Security Module (HLSM)
- Rahmenbedingungen
- **Zusammenfassung**



Hardware-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 überwiegend als **Sicherheitskomponenten für kleinere Rechnersysteme** eingesetzt.