

## **Hardware-Sicherheitsmodule**

Prof. Dr. (TU NN)

Norbert Pohlmann

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



## 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.

## 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

## Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfällsche Hochschule, Gelsenkirchen

## **Idee eines HSM**



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





## 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

## **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.

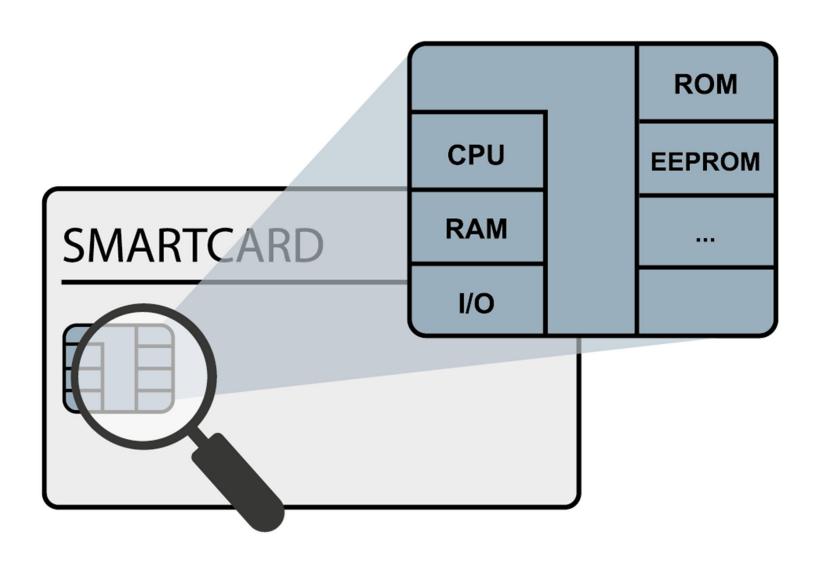
## Eine SmartCard enthält:

- 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.

# © Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

## **HSM:** Smartcards → Überblick (2/2)





## Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule,

## **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

## Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule,

## **HSM: Smartcards**

## internet-sicherheit.

## → Sicherheitsmechanismen einer Smartcard (1/2)

## 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**





## Smartcard Software:

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

## Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

## **HSM:** Smartcards → Vorteile



 Smartcards bieten erhöhte Sicherheit im Vergleich zu reinen Software Lösungen.

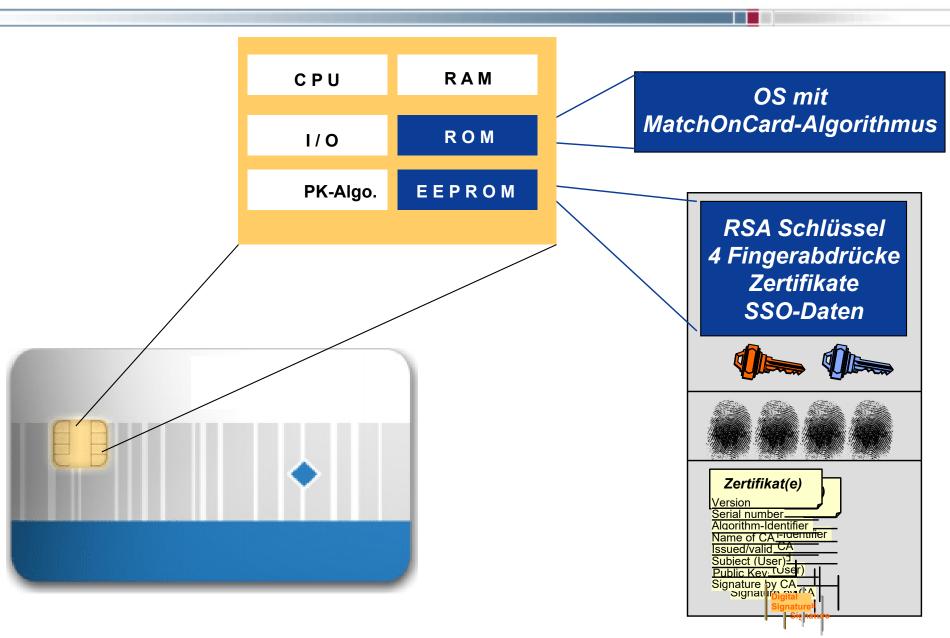
## Die Sicherheit beruht auf:

- 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.

# © Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

## **HSM: Smartcards**→ Die biometrische Smartcard





## **HSM: Smartcards**→ Alternative zur Smartcard



## Yubico:

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











## Gelsenkirchen Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule,

## Smartcard → Anwendungsfelder



- Sehr bekannte Anwendungsfelder für Smartcards mit Sicherheitschips sind:
  - EC-Karte
  - Kreditkarten
  - Personalausweis
  - Dienstausweise
  - Banken-Signaturkarten
  - (die neue) Gesundheitskarte
  - der Heilberufsausweis
  - Authentifikationstoken
  - Verschlüsselungstoken
  - Bitcoin-Wallet
  - USW.

## **Smartcard → Level an IT-Sicherheit**



- Diskussion über den Level an IT-Sicherheit, der mit einem smartcardbasierten Hardware-Sicherheitsmodul erzielt werden kann:
- Die IT-Sicherheit soll in der Wirkung so stark sein, dass erst mit einem Aufwand von mehr als 1. Mio. EUR ein erfolgreicher Angriff auf die Sicherheitsinformationen umgesetzt werden kann.
- Daher werden in der Regel nur abgeleitete Schlüssel auf der Smartcard gespeichert.
- Das bedeutet, wenn im Falle einer Bankkarte die Smartcard geknackt wurde, kann nur der geheime Schlüssel des Bankkunden ausgelesen und damit auch nur das Konto des betroffenen Bankkunden mit einem begrenzten Schaden ausgeraubt werden.
- Die gesamte Sicherheit des Bankensystems und aller anderen Bankkunden bleibt bestehen.
- Typischerweise können Smartcards auch gesperrt werden.

## 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

## **HSM:** Trusted Platform Module → Idee (1/2)



- TPM ist ein kleines Sicherheitsmodul für alle Rechnersysteme (PC, Notebook, PDA, Drucker, Router, Kühlschrank, usw.)
- Beispiel: Die meisten Notebooks haben TPM-Bausteine integiert.
- Kosten sollen kleiner als ein € sein!



## **HSM:** Trusted Platform Module → Idee (2/2)

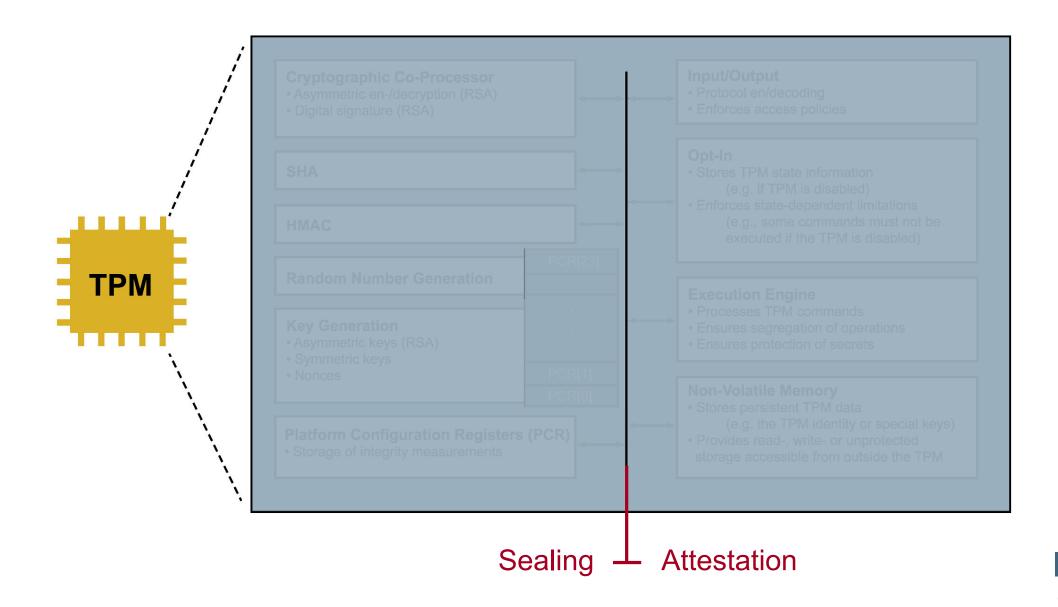


- Gesteuert durch die Trusted Computing Group (TCG).
   Hauptmitglieder: Microsoft, Intel, HP, IBM, AMD, Sony, SUN, aber auch Infineon, Utimaco, ...
- Einheitliche Standard-Software im TPM.
- Die einzelnen Unternehmen machen dann ihre eigene Lösung.
- Z.B. Microsoft: Next Generation Secure Computing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

## Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

## **HSM:** Trusted Platform Module → Sicherheitsmechanismen



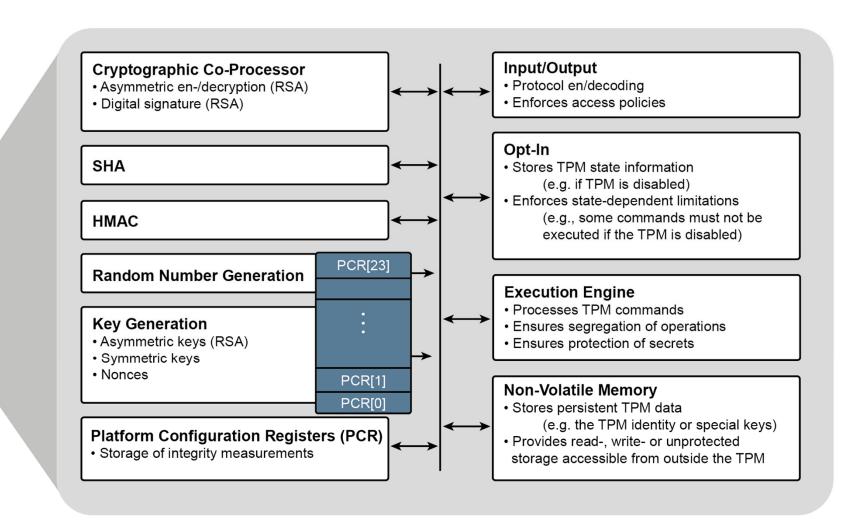


# © Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

**TPM** 

## **HSM: Trusted Platform Module** → Sicherheitsmechanismen





## Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule,

## **HSM:** Trusted Platform Module → Vor- und Nachteile



## 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.

## Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

## **HSM:** Trusted Platform Module → Anwendungsfelder



- Die Sicherheitswirkung des Schutzes der Sicherheitsinformationen von TPMs eignet sich, wie bei Smartcards, für abgeleitete Schlüssel im IT-System-orientierten und lokalen Umfeld.
- Das Einsatzgebiet von TPMs ist typischerweise die Sicherheit von Sicherheitsinformationen für kleinere IT-Systeme, wie zum Beispiel
  - PCs
  - Notebooks
  - Drucker
  - Netzwerkkomponenten
  - Autos
  - und andere Dinge

## Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

## **HSM:** Trusted Platform Module → Level an IT-Sicherheit



- Diskussion über den Level an IT-Sicherheit:
  - Da ein TPM auf der Basis eines Smartcard-Sicherheitschips arbeitet, ist auch der Level an IT-Sicherheit gleich mit dem Sicherheitschip einer Smartcard.

## 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

## **HSM:** High-Level Security Module → Ziele

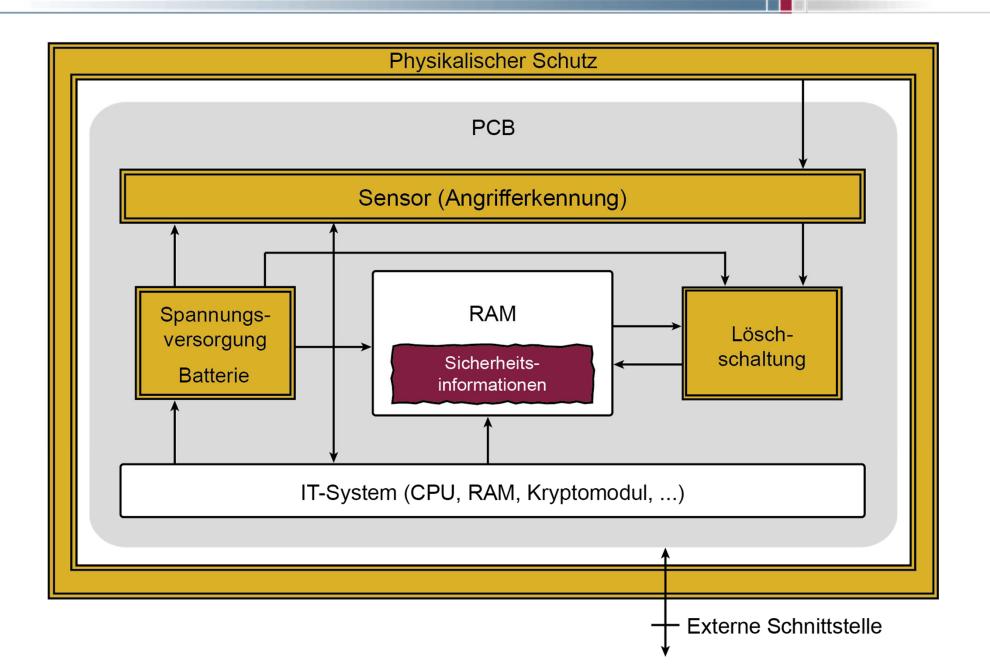


- High-security und high-performence Security Module für
  - besonders sichere, wertvolle Informationen (z.B. Master-Keys)
  - sehr hohe Performence-Anforderungen
- Wenn ein Angriff vom Sicherheitsmodul erkannt wird, sind die zu schützenden sicherheitsrelevanten Informationen innerhalb des Sicherheitsmoduls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

# © Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

## **HSM:** High-Level Security Module → Sicherheitsmechanismen



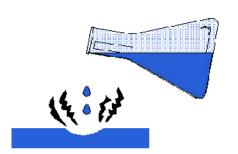


## © Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule,

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



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









## Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

## **HSM:** High-Level Security Module → Anforderungen (1/2)



- 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

## **HSM:** High-Level Security Module → Anforderungen (2/2)

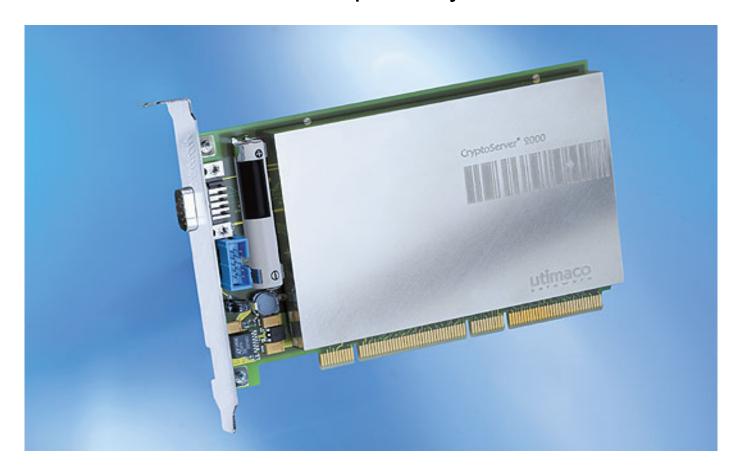


- Übergang der kryptographischen Hoheit an die Verantwortung eines Betreibers
- Umstellungsmöglichkeit auf neue kryptographische Verfahren
- Vertrauenswürdige Basis (z.B. geringe Anzahl an "Lines of Code")

## **HSM:** High-Level Security Module → Beispiel CryptoServer



Generisches standalone Computer-System

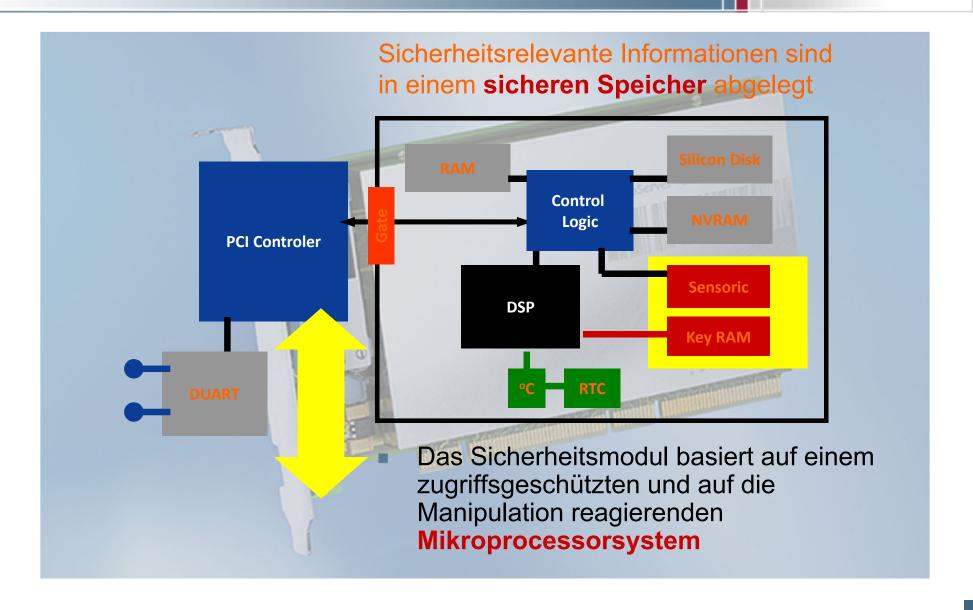


 Die zusätzliche Trägerkarte mit Interfaces bildet das Co-Processor Board

## Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

## **HSM:** High-Level Security Module → Hardware (1/2)





## **HSM:** High-Level Security Module → Hardware (2/2)



- Sicherheitsmodul plus Kommunikationseinheit
  - Kommunikationsrechner
  - Gbit Ethernet
  - Hardware Watchdog onboard



## **HSM:** High-Level Security Module → Anwendungen



- Public Key Infrastruktur: (eIDAS)
  - Schlüsselgenerierung, Zeitstempeldienste ...
  - Fernsignatur ... Aktivierung ... digitale Signatur
- Bankenumfeld:
  - Autorisierungsstationen für die Freigabe von Geld (Girocard ...)
  - Speicherung von Wallets, wie für Bitcoins usw
  - Sicherheit für die Netzbetreiber (z.B. im Bereich EC-Cash, Mineralölunternehmen)
- Industrie:
  - Schlüsselgenerierung für Auto-Schlüssel
  - Maut-Systeme (Abrechnung)
  - Authentifikation im Mobilfunknetz
  - Digitale Signatur von zentralen Prozessen (Rechnungen, usw.)

# © Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkircher

## **HSM:** High-Level Security Module → Level an IT-Sicherheit



- Diskussion über den Level an IT-Sicherheit, der mit einem High-Level Security Module erzielt werden kann:
- Die Wirkung gegen Angriffe auf die Sicherheitsinformationen im High-Level Security Module kann nur mit einem Aufwand von weit über 10. Mio. EUR umgesetzt werden.
- Daher werden in dem High-Level Security Module auch Master-Schlüssel und Schlüssel von globaler Bedeutung gespeichert.
- Das bedeutet, wenn das High-Level Security Module einer Bankanwendung geknackt wurde, ist die ganze Bankenanwendung kompromittiert und das ganze Bankensystem kann nicht mehr sicher genutzt werden.

## 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

## 



- Nachweis der Hard- und Software-Sicherheit.
- Durch unabhängige und qualifizierte Organisationen (TÜVs, BSI ...).
- 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?

## Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule,

## Rahmenbedingungen → Key-Management (1/2)



- 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 eine öffentliche PKI verwaltet/signiert.
  - Einfache Einbindung für verschiedene Anwendung (z.B. VPN-Systeme).

## Rahmenbedingungen → Key-Management (2/2)



- Management nach dem Vier-Augen-Prinzip:
  - Kritische T\u00e4tigkeiten sollten nicht von einer einzelnen Person durchgef\u00fchrt 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-performence Security Modules
  - High-security und high-performence Security Module werden typischerweise als Sicherheitskomponenten für größere Rechnersysteme im Sicherheitsumfeld eingesetzt.
- Einsatzumfeld von TPM
  - TPMs werden wahrscheinlich als Sicherheitskomponenten für kleinere Rechnersysteme eingesetzt.



## **Hardware-Sicherheitsmodule**

Prof. Dr. (TU NN)

Norbert Pohlmann

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



## **Anhang / Credits**



## Wir empfehlen

Cyber-Sicherheit

Das **Lehrbuch** für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung", Springer Vieweg Verlag, Wiesbaden 2022 <a href="https://norbert-pohlmann.com/cyber-sicherheit/">https://norbert-pohlmann.com/cyber-sicherheit/</a>



7. Sinn im Internet (Cyberschutzraum)
 https://www.youtube.com/cyberschutzraum



Master Internet-Sicherheit
 https://it-sicherheit.de/master-studieren/



## Besuchen und abonnieren Sie uns :-)

WWW

https://www.internet-sicherheit.de

**Facebook** 

https://www.facebook.com/Internet.Sicherheit.ifis

**Twitter** 

https://twitter.com/ ifis

https://twitter.com/ProfPohlmann

YouTube

https://www.youtube.com/user/InternetSicherheitDE/

Prof. Norbert Pohlmann https://norbert-pohlmann.com/

## **Quellen Bildmaterial**

Eingebettete Piktogramme:

Institut f
ür Internet-Sicherheit – if(is)

## **Der Marktplatz IT-Sicherheit**

(IT-Sicherheits-) Anbieter, Lösungen, Jobs, Veranstaltungen und Hilfestellungen (Ratgeber, IT-Sicherheitstipps, Glossar, u.v.m.) leicht & einfach finden. <a href="https://www.it-sicherheit.de/">https://www.it-sicherheit.de/</a>



## **Literatur**→ **Artikel / Bücher**



- N. Pohlmann: "Security-API eines Sicherheits-Moduls für den Einsatz in heterogen Rechnerumgebungen". In Proceedings der GI-Fachgruppe Verlässliche IT-Systeme Konferenz Konzepte, Anwendungen und Einsatzbeispiele, Hrsg.: W. Fumy, G. Meister, M. Reitenspieß, W. Schäfer, Deutscher Universitäts Verlag, 1994
- N. Pohlmann: "Bausteine für die Sicherheit: Chipkarten und Sicherheits-Module", KES Kommunikations- und EDV-Sicherheit, SecMedia Verlag, 05/1995
- N. Pohlmann: "Aktivierung von Smartcards durch Biometrie", KES Kommunikations- und EDV-Sicherheit, SecMedia Verlag, 03/2001
- N. Pohlmann: "Höchste Sicherheit für Zugang zur IT: Biometrie anstelle von PINs", Organisator Management / Business / People / IT / Finance, Verlag Organisator, Berneck/Schweiz 09/2001
- N. Pohlmann: "Hardware-Sicherheitsmodule zum Schutz von sicherheitsrelevanten Informationen", DuD Datenschutz und Datensicherheit Recht und Sicherheit in Informationsverarbeitung und Kommunikation, Vieweg Verlag, 10/2014

https://norbert-pohlmann.com/wp-content/uploads/2015/08/320-Hardware-Sicherheitsmodule-zum-Schutz-von-sicherheitsrelevanten-Informationen-Prof-Norbert-Pohlmann.pdf

N. Pohlmann: "Cyber-Sicherheit – Das Lehrbuch für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung", ISBN 978-3-658-25397-4; 594 Seiten, Springer-Vieweg Verlag, Wiesbaden 2019

https://norbert-pohlmann.com/cyber-sicherheit/