Norbert Pohlmann

# Hardware-Sicherheitsmodule zum Schutz von sicherheitsrelevanten Informationen

Immer mehr sicherheitsrelevante Informationen, wie z.B. geheime Schlüssel und Transaktionsdaten werden z.B. durch Bezahlsysteme und Verschlüsselungslösungen im Internet genutzt. Wie können Hardware-Sicherheitsmodule helfen, diese besonders sensiblen sicherheitsrelevanten Informationen angemessen zu schützen.

## 1 Einleitung

Das Ziel eines Hardware-Sicherheitsmodules ist ein hoher Schutz vor Auslesen und Manipulation von besonders sensiblen sicherheitsrelevanten Informationen innerhalb eines besonders geschützten Hardware-Bereiches.

Besonders sensible sicherheitsrelevante Informationen, die in einem Hardware-Sicherheitsmodul geschützt werden sollen, sind z.B.:

- Geheime Schlüssel für Verschlüsselung, Authentisierung, Signaturen, usw.
- Programme, die nicht kopiert oder modifiziert werden sollen, im Sinne eines Softwareschutzes.
- Daten, die Werte darstellen, wie z.B. Transaktionsdaten, Coins, usw.

Alle geheimen Operationen, wie z.B. „Verschlüsseln", „Signieren", „Zufallszahlen generieren", usw. finden direkt im besonders geschützten Hardware-Sicherheitsmodul statt. Geheime Schlüssel können so benutzt werden, ohne sie zu kennen. Geheime Daten und Software sind manipulationssicher im Hardware-Sicherheitsmodul gespeichert, usw.

In der Praxis haben sich unterschiedliche Umsetzungskonzepte von Hardware-Sicherheitsmodulen mit verschiedenen Sicherheitswirkungen und Einsatzumfeldern etabliert.

**Norbert Pohlmann**

Professor für Informationssicherheit und geschäftsführender Direktor des Instituts für Internet-Sicherheit an der Westfälische Hochschule Gelsenkirchen sowie Vorstandsvorsitzender des TeleTrusT – Bundesverband IT-Sicherheit.

E-Mail: pohlmann@internet-sicherheit.de

## 2 Kategorien von Sicherheitskomponenten

### Sicherheitskomponenten für Personen

Sicherheitskomponenten für Personen sind in der Umsetzung meist SmartCards, USB-Token und zunehmend NFC-Token, usw. Die Sicherheitswirkung des Schutzes der sicherheitsrelevanten Informationen eignet sich für abgeleitete Schlüssel im Personen-orientierten und lokalen Umfeld. Das Einsatzgebiet ist typischerweise die Sicherheit von sicherheitsrelevanten Informationen einer Person.

### Sicherheitskomponenten für kleinere Computer (PC, Notebooks, Smartphones, etc.)

Eine Sicherheitskomponente für kleinere Computer ist in der Umsetzung hauptsächlich ein TPM (Trusted Platform Module). Die Sicherheitswirkung des Schutzes der sicherheitsrelevanten Informationen eignet sich für abgeleitete Schlüssel im Computer-orientierten und lokalen Umfeld. Das Einsatzgebiet von TMP ist typischerweise die Sicherheit von sicherheitsrelevanten Informationen für kleinere Computer (z.B. PCs, Notebooks, Drucker, Netzwerkkomponenten, Autos und andere Dinge).

Eine neue Entwicklung ist unter dem Begriff „Trusted Execution Environment" bekannt, und wird insbesondere im Bereich von mobilen Geräten Neuerungen bringen. Hier bieten die vorhandenen Chip-Sätze der Hersteller von CPUs die Möglichkeit, sogenannte „Trusted Apps" in einer sicheren Umgebung ohne zusätzliche Hardware laufen zu lassen (siehe dazu auch den Artikel „Vertrauen und Sicherheit bei Mobiltelefonen" in dieser Ausgabe).

### Sicherheitskomponenten für das Hoch-Sicherheitsumfeld (Banken, IT-Sicherheitsdienstleister, etc.)

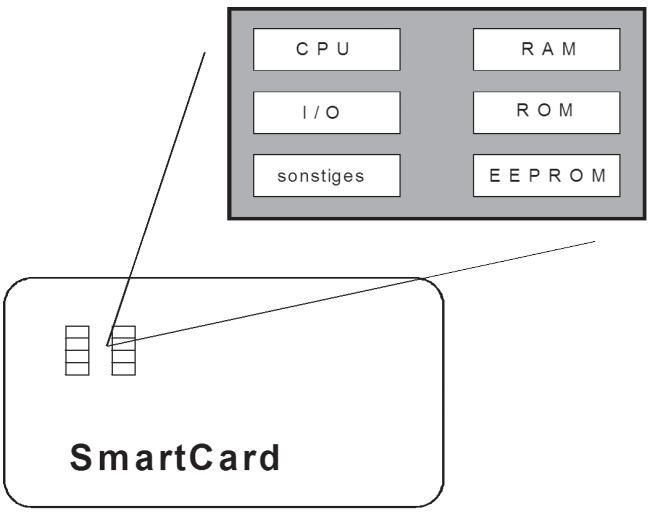
Eine Sicherheitskomponente für das Hoch-Sicherheitsumfeld ist in der Umsetzung meist ein Highsecurity Security Module (HSM). Die Sicherheitswirkung des Schutzes der sicherheitsrelevanten Informationen eignet sich für Master-Keys und Schlüssel

von globaler Bedeutung. Die Einsatzgebiete sind typischerweise Sicherheitskomponenten für größere Computer im Hoch-Sicherheitsumfeld.

### 2.1 Hardware-Sicherheitsmodul: SmartCards

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.

**Abb. 1 | SmartCard**




Eine SmartCard enthält einen Sicherheitschip mit: CPU, RAM- und ROM-Speicher, ein „schlankes" Betriebssystem im ROM, eine I/O-Schnittstelle, über die die gesamte Kommunikation stattfindet (Kontaktflächen oder kontaktloses Interface) und 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 ist beispielsweise ein Co-Prozessor, der symmetrische oder asymmetrische Verschlüsselung sehr schnell durchführt (Krypto-Prozessor) [Pohl95].

Die SmartCard Hardware bietet z.B. die folgenden Hardware-Sicherheitsmechanismen: Unter- und Überspannungsdetektion, Erkennung niedriger Frequenzen, gescrambelte 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 und Speicherschutzfunktionen.

Aber auch die SmartCard Software bietet Software-Sicherheitsmechanismen an, wie z.B.: Zugriffskontrolle auf Objekte, Zustandsautomaten, die in Abhängigkeit von Identifikations- und Authentisierungsmechanismen Befehle zulassen.

Die Sicherheit einer SmartCard beruht in der Regel auf: Wissen (PIN) und Besitz (Karte).

Geheime Schlüssel verlassen den Sicherheitschip der Smartcard nie. Alle geheimen Operationen finden direkt in der Karte statt. Geheime Schlüssel können benutzt werden, ohne sie zu kennen. Geheime Daten sind manipulationssicher in der Karte gespeichert. Typischerweise ist die Kommunikationsgeschwindigkeit mit der SmartCard langsam, mindestens 9,6 Kbit/s.

In Hardware-Sicherheitsmodulen in der Form von USB-Token, NFC-Token, usw. sind oft SmartCard-Chips enthalten. Die Nutzung der Sicherheitsdienste kann dann aber über USB und NFC vorgenommen werden. Ein aktuelles Beispiel, welches von Google zurzeit promotet wird, ist YubiKey. Dies ist eine IT-Sicherheitstechnologie einer Firma aus Schweden, die auch in den USA sehr aktiv ist. Eine FIPS 140-2 Zertifizierung wird gerade durchgeführt.

Die Aktivierung mit Hilfe einer PIN hat einige praktische Herausforderungen. In der Regel werden nur 4 Zeichen für die Aktivierung gefordert, was die Anzahl der möglichen Kombination sehr einschränkt. Oft benutzen die Anwender für alle Smartcards die PIN ihrer ec-Karte, was die Sicherheit auch nicht verbessert.

Verwendet man z.B. das Fingerabdruckverfahren anstelle der üblicherweise verwendeten PIN zur Aktivierung einer SmartCard, ist „Match on Card" ein notwendiges Sicherheitskonzept. Dabei erfolgt der Vergleich des aktuellen Fingerabdrucks mit dem gespeicherten Referenzwert direkt im Sicherheitschip der Karte. Zur Sicherheit sind mehrere Fingerabdrucktemplates in der SmartCard abgelegt. Wenn der Nutzer zum Beispiel eine Verletzung am Zeigefinger hat, kann er einen anderen Finger benutzen.

Die Vorteile des Match-on-Card-Verfahrens bezüglich Biometrie liegen vor allem in der hohen Sicherheit, da die Referenzwerte niemals den geschützten Bereich der SmartCard verlassen und nicht ausgelesen werden können (typischer Vorteil von SmartCards). Die sichere Speicherung des Referenzwerts erfüllt auch die Anforderungen des Datenschutzes. Darüber hinaus ermöglicht ein direkt auf der Karte gespeicherter Referenzwert auch die Verwendung an verschiedenen Standorten (Roaming) oder an offline betriebenen IT-Systemen.

Sehr bekannte Anwendungsfelder für SmartCards sind: ec-Karte, Kreditkarten mit Chips, der neue Personalausweis mit kontaktlosem Interface, Dienstausweise, Banken-Signaturkarten, die neue Gesundheitskarte, der Heilberufsausweis, usw.

Anwendungsfelder im Bereich Token mit Chipkarten-Chips, sind: Authentikationstoken, Bitcoin-Wallet, Verschlüsselungstoken, usw.

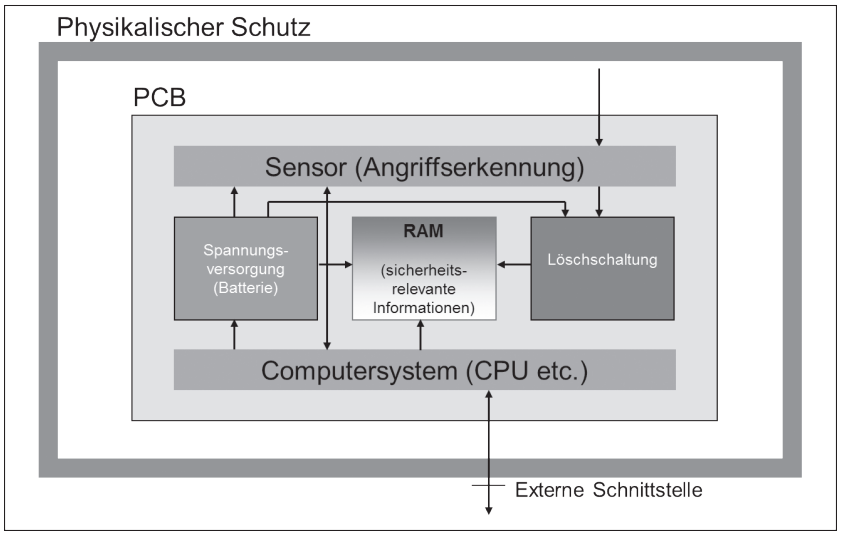
### 2.2 Hardware-Sicherheitsmodul: High-security Security Module (HSM)

Ein High-security Security Module (HSM) ist für besonders sichere, wertvolle Informationen (z.B. Master-Keys, Schlüssel von globaler Bedeutung, etc.) und für sehr hohe Performance-Anforderungen konzipiert und umgesetzt. Ein besonderer Unterschied zur SmartCards-Sicherheit ist, dass wenn ein Angriff vom High-security Security Module erkannt wird, die zu schützenden sicherheitsrelevanten Informationen innerhalb des Sicherheitsmoduls sofort aktiv und sicher gelöscht werden können. Dazu ist ein HSM typischerweise physikalisch gekapselt und mit einer aktiven Sensorik ausgerüstet, die Angriffe erkennt. Ein HSM ist in der Regel ein Vielfaches sicherer und leistungsfähiger als eine SmartCard, aber auch sehr viel teurer (mehrere tausend Euro, in Anhängigkeit der Leistung).

Die Grundidee eines HSM ist ein physikalisch geschütztes IT-System mit einem gepufferten RAM, in dem alle sicherheitsrelevanten Informationen gespeichert sind.

Alle Sicherheitsdienstleistungen werden über eine definierte externe Schnittstelle zur Verfügung gestellt [Pohl94].

**Abb. 2 | High-security Security Module (HSM)**




Mit Hilfe eines physikalischen Schutzes wird das RAM so geschützt, dass es einem Angreifer nicht möglich ist, es auszulesen oder zu manipulieren. Ein physikalischer Schutz ist z.B. eine komplex aufgebaute, flexible Leiterplatte mit vielen Layern und unterschiedlich verlaufende Leiterbahnen, die das RAM mit den sicherheitsrelevanten Daten schützen. Der physikalische Schutz ist mit Sensorik untermauert, so dass jeder denkbare Angriff sofort erkannt wird. Es gibt eine Löschschaltung, die den Inhalt des RAM aktiv und sicher löscht. Eine interne Stromversorgung sorgt dafür, dass die Löschschaltung und die Sensorik immer funktionsfähig sind. Außerdem überwacht die Sensorik die Stromversorgung. Bevor die Energie der internen Stromversorgung zu Ende geht, wird der Löschvorgang aus Sicherheitsgründen aktiv und löscht alle sicherheitsrelevanten Informationen nachhaltig sicher. Die Sensorik hat die Aufgabe, einen möglichen Angriff zu erkennen, wie z.B. Durchleuchten, Temperatur Angriffe, Mechanische Attacke, Chemische Attacke und Manipulation über Spannung und Frequenzen. Wird ein Angriff erkannt, löst die Sensorik den Löschvorgang aus und damit können die sicherheitsrelevanten Informationen nicht mehr angegriffen werden.

Bei dieser wichtigen Sicherheitsfunktion wird deutlich, dass es einen verlässlichen und sicheren Backup-Prozess geben muss, der die eigentliche und gewollte Anwendung mit den besonders sensiblen sicherheitsrelevanten Informationen verfügbar hält.

Die Leistungsfähigkeit der verwendeten CPU bei einem HSM ist sehr hoch und die Kommunikationsgeschwindigkeit mit einem HSM ist in der Regel sehr schnell. Auch Lösungen, die eine hohe Parallelität für eine höhere Performance sowie gute Verfügbarkeit zur Verfügung stellen, werden angeboten und genutzt [Pohl01].

Die Vorteile eines HSM sind seine hohe Leistungsfähigkeit und die hohe Sicherheit, im Vergleich zu Smartcards und TPMs.

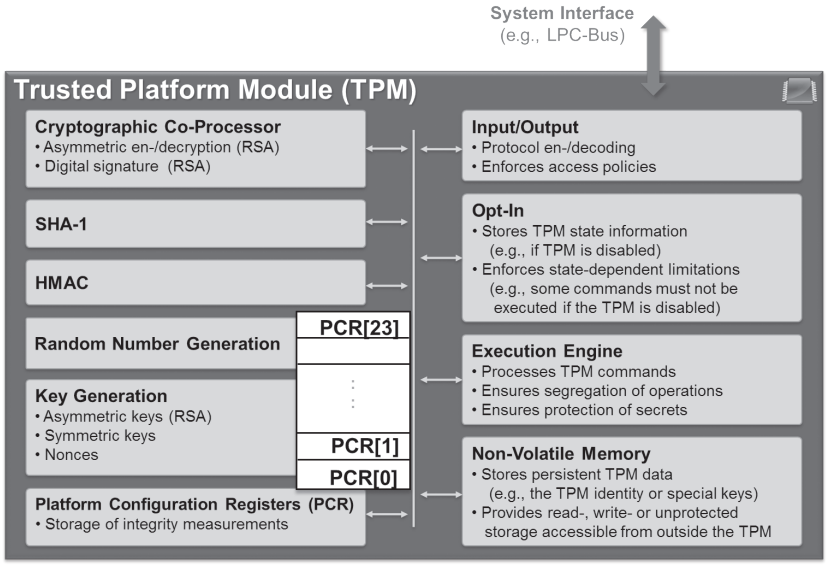
Anwendungsfälle von HSMs sind: Public Key Infrastruktur (Schlüsselgenerierung, Zeitstempeldienste), Bankenumfeld (Autorisierungsstationen für die Freigabe von Geld, wie z.B. bei ec-Cash, Speicherung von Wallets, wie z.B. für Bitcoins, usw), Sicherheit für die Netzbetreiber (z.B. im Bereich ec, Mineralölunternehmen) und Industrie (Schlüsselgenerierung für Autoschlüssel, Abrechnung in Maut-Systemen, Authentikation im Mobilfunknetz, Digitale Signatur von zentralen Prozessen, wie z.B. Rechnungen, Archivierungssystemen, usw.), im behördlichen Umfeld (IT-Sicherheitsdienste des neuen Personalausweises, Speicherung von Schlüsseln für die Verschlüsselung, …).

### 2.3 Hardware-Sicherheitsmodul: Trusted Platform Module (TPM)

TPM ist ein kleines Sicherheitsmodul für alle Computer (PC, Notebook, Smartphones, PDSs, Drucker, Router, Kühlschrank, usw.).

Trusted Computing ist der Begriff für die Idee, Computertechnologie grundsätzlich vertrauenswürdiger zu machen. Forciert werden die damit einhergehenden Sicherheitstechnologien von einem Industriekonsortium mit über 120 internationalen Mitgliedern [PoRe08]. Die Ergebnisse dieser Zusammenarbeit sind offene Spezifikationen, die grundsätzlich zum Ziel haben, die Basis für die vertrauenswürdige IT zu bilden. Insbesondere die Sicherheit verteilter Anwendungen soll mit wirtschaftlich vertretbarem Aufwand verbessert werden, d.h. es soll keine massive Veränderung existierender Hard- bzw. Software notwendig sein. Eine der Hauptideen ist die Nutzung einer manipulationssicheren Hardware-Komponente, das sogenannte Trusted Platform Module (TPM). Es soll softwarebasierten Angriffen entgegenwirken. Die TPM-Spezifikationen wurden bereits von vielen Herstellern umgesetzt. Sie sind aktuell in über 500 Millionen Computern zu finden. Fast jedes aktuelle Notebook, das Sie erwerben, beinhaltet einen solchen Sicherheitschip. Ein TPM ist im Prinzip und vom

**Abb. 3 | Trusted Platform Module (TPM)**



Sicherheitslevel ein SmartCard-Chip mit ein paar Erweiterungen, wie das Platform Configuration Register (PCR).
Das TPM wirkt als vertrauenswürdiger Anker in einem Rechnersystem (Root of Trust). Beginnend mit dem Startvorgang werden alle Hardwareelemente und Softwarekomponenten (BIOS, Betriebssystem, Anwendungsprogramme etc.) mit Hilfe von Hashfunktionen gemessen und ihre Zustände im Platform Configuration Register (PCR) des TPM gespeichert. Die Systemkonfiguration des Computersystems ist also jederzeit komplett mess- und damit auch überprüfbar.

In der Automobilindustrie entspräche das der Arbeit eines Kontrolleurs, der die gesamte Montage eines Wagens protokolliert und hinterher anhand einer zertifizierten Liste von Kontrollnummern aller Teile (z.B. des Fahrgestells) die „Integrität" des Autos beweisen kann. Wird ein Teil ersetzt, wäre das Auto nicht mehr im Originalzustand und im Vergleich mit der Liste nicht mehr vertrauenswürdig. Die Systemkonfigurationsüberprüfung durch das TPM erfolgt in identischer Weise. Damit können sich Computer gegenüber einem Nutzer oder anderen Computern hinsichtlich ihrer Systemkonfiguration „ausweisen". Dieser Vorgang wird Attestation genannt. Dies bietet ein hohes Maß an Vertrauenswürdigkeit der genutzten Software.

Außerdem bietet das TPM die Möglichkeit, Daten zu versiegeln und vertraulich zu speichern. Dabei werden die Daten während der Verschlüsselung an die Systemkonfiguration gebunden. Dieser Vorgang wird Sealing genannt. Er stellt sicher, dass auf versiegelte Daten nur wieder zugegriffen werden kann, wenn sich das Rechnersystem in einem bekannten Zustand (Systemkonfiguration) befindet. Dem entspricht im übertragenen Sinn die Möglichkeit, genau zu prüfen, ob z.B. das Bremssystem eines Autos unverändert und damit funktionsfähig ist.

Was sind die großen Vorteile von TPMs?

- Das TPM bietet eine sehr hohe Sicherheit bei geringer Investitionssumme, da ein TPM nicht mehr als ein Euro kostet.
- Die TPMs sind schon auf dem überwiegenden Teil der IT-Systeme verfügbar! D.h. die flächendeckende Einführung einer Sicherheitsplattform ist einfach! Zum aktuellen Zeitpunkt wurden bereits weit über 500 Millionen TPMs verbaut.
- Die TPMs sind in eine Sicherheitsinfrastruktur (PKI, etc.) eingebunden und daher einfach im Sicherheitsmanagement zu behandeln.

Es gibt auch Vorbehalte gegen die TPM-Nutzung: Z.B.

- Das Konsortium, die Trusted Computing Group, welches das TMP spezifiziert, handelt nicht immer transparent und der Zugang zu den Spezifikationen könnte insbesondere für kleinere Unternehmen einfacher sein.
- TMPs aus Ländern, die bekanntlich eigene Interessen haben, wären in der Lage, über Hintertüren im Chip-Design, auf die sicherheitsrelevanten Informationen zuzugreifen, wenn sie physikalischen Zugriff auf das Gerät mit dem TPM haben

### 2.4 Zusammenfassung Hardware-Sicherheitsmodule

Bei Hardware-Sicherheitsmodulen ist es wichtig, dass die Software eine hohe Qualität hat und vertrauenswürdig ist, um die Angriffe zu minimieren. Es ist zudem besonders wichtig, dass die Software nicht bösartig, sondern gutartig ist, weil die sicherheitsrelevanten Informationen die Basis der Sicherheitsmechanismen darstellt.

Die Software in Hardware-Sicherheitsmodulen hat in der Regel eine geringe Anzahl von Zeilen Code, ca. 90.000 Lines of Code plus/minus 10%. Durch die geringe Anzahl von Zeilen Code ist eine sehr vertrauenswürdige Basis vorhanden, die in der Regel auch schon semiformal verifiziert werden kann.

## 3 Wie kann die Vertrauenswürdigkeit von Hardware-Sicherheitsmodulen erlangt werden?

Vertrauenswürdigkeit hat etwas mit Vertrauen zu tun. Aber welche Kriterien zur Beurteilung der Vertrauenswürdigkeit sollten bei Hardware-Sicherheitsmodulen angewendet werden?

Im Folgenden werden ein paar Aspekte aufgezeigt, wie eine höhere Vertrauenswürdigkeit von Hardware-Sicherheitsmodulen erzielt werden kann.

### 3.1 Evaluierung/Zertifizierung

Hardware-Sicherheitsmodule werden in der Regel nach den folgenden Standards evaluiert und zertifiziert: FIPS 140-1 und 140-2, DK (Die Deutsche Kreditwirtschaft) oder Common Criteria (CC). Speziell für HSMs, die von Zertifizierungsdiensteanbietern für die Erzeugung von digitalen Signaturen verwendet werden, wurde das CC Schutzprofil CWA 14167-2 entwickelt.

In der Praxis ist es so, dass die Hard- sowie die Software-Sicherheit durch eine Evaluierung/Zertifizierung nachgewiesen werden kann.

Bei der Evaluierung und Zertifizierung müssen unabhängige und qualifizierte Organisationen die Qualität und Vertrauenswürdigkeit von IT und IT-Sicherheit in Produkten und Lösungen prüfen.

Das Problem bei IT-Sicherheit, insbesondere Kryptographie, ist, dass diese nur von Experten evaluiert werden kann, weil es nicht um die Funktionalität geht, sondern um eine sichere Umsetzung der IT-Sicherheitsmechanismen. Dass eine Funktion ver- und entschlüsseln kann, heißt noch lange nicht, dass der dahinter liegenden Algorithmus sicher ist. Weitere Beispiele sind: Erfüllt ein Zufallszahlengenerator alle notwendigen Eigenschaften, wie z.B. Gütekriterien, Streuung, Periodizität, Gleichverteilung? Sind die Sicherheitsprotokolle sicher implementiert?

## 4 Key-Management von Hardware-Sicherheitsmodulen

Das besondere an Hardware-Sicherheitsmodulen für die Umsetzung eines Key-Managements sind die folgenden Aspekte:

- Keiner hat direkten Zugriff auf die geheimen Schlüssel.
- Nur Autorisierte sind in der Lage, die unterschiedlichen Krypto-Funktionen mit den geheimen Schlüsseln im Hardware-Sicherheitsmodul zu nutzen.
- Die Software im Hardware-Sicherheitsmodul kann nur von Autorisierten in ihrer Funktionalität definiert und verändert werden.

Dadurch sind einige interessante Aspekte im Bereich von Key-Management umsetzbar.

### 4.1 Das Management von TMPs

Der Hersteller eines TMPs personalisiert die TPMs in seiner sicheren Umgebung mit einem sogenannten TPM Identität.

Die TPM Identität ist ein Zertifikat mit einem Schlüsselpaar, dem Endorsement Key (EK), welches das TPM niemals verlässt und die Eindeutigkeit und Einzigartigkeit des TPMs definiert. Der Endorsement Key ist zurzeit typischerweise ein 2048-Bit RSA-Schlüsselpaar.

Das Zertifikat mit dem öffentlichen Schlüssel wird von einer öffentlichen Public-Key-Infrastruktur verwaltet und ist damit direkt kryptographisch nutzbar.

Durch dieses Prinzip können Sicherheitssysteme, die auf der Basis von TPMs aufgebaut sind, sehr einfach aus der Ferne für bestimmte Anwendungen, wie z.B. VPN-Systeme sicher und vertrauenswürdig übernommen und individuell personalisiert werden. Das spart das übliche Personalisieren an einer gemeinsamen zentralen Stelle oder das Einbringen von Schlüsseln vor Ort durch vertrauenswürdiges Personal, was in der Regel sehr umständlich und teuer ist.

### 4.2 Vier-Augen-Prinzip

Das Vier-Augen-Prinzip besagt z.B., dass kritische Tätigkeiten nicht von einer einzelnen Person durchgeführt werden sollen oder dürfen. Ziel ist es, das Risiko von Fehlern und Missbrauch zu reduzieren.

Im Bereich von Key-Management kann dieses Prinzip mit Hilfe von Hardware-Sicherheitsmodulen unterstützt werden.

Anwendungsbeispiel: Electronic Cash System. Beim Electronic Cash System gibt es neben der Deutschen Kreditwirtschaft unterschiedliche Electronic Cash-Netzbetreiber mit eigenständiger Verantwortung.

Diese betreiben Electronic Cash-Netze mit eigenen POS-Kartenterminals und HSMs für den Übergang ins Netz der Deutschen Kreditwirtschaft. Electronic Cash-Netzbetreiber sind z.B. Ingenico, TeleCash, Deusche BP, Shell, usw.

Die Electronic Cash Netze werden mit unterschiedlichen Schlüsselsystemen betrieben, um das Risiko bei einer Kompromittierung zu minimieren.

Aus diesem Grund müssen an den Grenzen der Electronic Cash Netze die verschlüsselten Transaktionen in die verschiedenen Schlüsselsysteme umverschlüsselt werden.

Dazu treffen sich die Verantwortlichen der Electronic Cash Netze, um jeweils die dazu notwendigen Schlüssel im Sinne des Vier-Augen-Prinzips einzugeben. Dadurch, dass der Mechanismus des Vier-Augen-Prinzips im HSM implementiert ist, kann dieser nicht manipuliert werden und das Risiko eines Missbrauches kann deutlich reduziert werden.

## 5 Zusammenfassung

Die Nutzung der Kryptographie in unserer modernen Gesellschaft steigt ständig. Bezahlsysteme, zunehmend über das Internet, Verschlüsselung von Daten auf Datenträger und während der Kommunikation, Mobilfunk Verschlüsselung und Authentikation, Wegfahrsperren im Auto, usw. sind nur einige Beispiele dieses Trends.

Die dazu notwendigen Schlüssel, Software und Transaktionsdaten können in normalen IT-Systemen nicht angemessen geschützt werden. Aus diesem Grund brauchen wir Hardware-Sicherheitsmodule, die diese besonders sensitiven sicherheitsrelevanten Informationen angemessen schützen. Smartcards, TMPs und HSM sind in der Lage, auf sehr unterschiedliche Art und Weise und mit unterschiedlichen Wirkungen des Schutzes, diese Aufgabe zuverlässig umzusetzen. Da wir Nutzer nicht in der Lage sind, die komplexen Aspekte des physikalischen Schutzes der sicherheitsrelevanten Informationen, der Kryptographie in den Bereichen, Generierung von Schlüsseln, Implementierung der kryptografischen Algorithmen und ein sicheres Key-Management zu beurteilen, ist es unbedingt erforderlich, dass eine professionelle Zertifizierung der Hardware-Sicherheitsmodule auf einem angemessenen Evaluierungsniveau umgesetzt wird.

## Literatur

[Pohl94] 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

[Pohl95] N. Pohlmann: „Bausteine für die Sicherheit: Chipkarten und Sicherheits-Module", KES – Kommunikations- und EDV-Sicherheit, SecMedia Verlag, 05/1995

[Pohl01] N. Pohlmann: "Aktivierung von Smartcards durch Biometrie", KES - Kommunikations- und EDV-Sicherheit, SecMedia Verlag, 03/2001

[PoRe08] N. Pohlmann, H. Reimer: „Trusted Computing - Ein Weg zu neuen IT-Sicherheitsarchitekturen", Vieweg-Verlag, Wiesbaden 2008