# Trusted Computing und IT-Sicherheit

**Wilhelm Dolle**
**Director Information Technology**
**interActive Systems GmbH**

**DFN - CERT**
**11. Workshop „Sicherheit in vernetzten Systemen“**
**03. / 04. Februar 2004, Hamburg**

# Agenda

- Ziele / Hintergründe / Historie
- Status Quo
- Technik hinter TCG und dem TPM
- IBM-Linux-Experimentalpaket / MS Palladium
- Fluch oder Segen?

# Ziele von Trusted Computing / IT-Sicherheit

- Schutz vor Malware
- Integritätsüberprüfung des Betriebssystems vor dem Booten
- Authentisierung von Hard- und Software gegenüber dem Betriebssystem und externen Kommunikationspartnern
- Verbesserter Datenschutz und verbesserte Sicherheit beim Aufbewahren und Übertragen von Daten
- Vertraulichkeit, Integrität, Verfügbarkeit

# Nebenwirkungen von Trusted Computing

- Zensur
- Verletzung der Privatsphäre
- Einschränkung der Nutzung des Computers und von Daten (DRM)

# Trusted Computing / Sicherheitsmodelle

- **Bell-LaPadula Modell**
  - Verschiedene Sicherheitsstufen
  - No read-up / no write-down
  - Fokus: Vertraulichkeit (militärische Nutzung)
- **Biba Modell**
  - No read down / no write up
  - Fokus: Integrität von Daten (kommerzielle Nutzung)
- **Clark-Wilson Modell**
  - Zugriff auf Daten nur durch berechtigte Programme
  - Separation of duties
  - Audit wird zwingend vorgeschrieben

# Trusted Computing / Sichere Systeme

- Referenzmonitor: abstrakte Maschine die alle Zugriffe auf Objekte (Dateien, Ressourcen, Programme) überwacht und vermittelt
- Trusted Computing Base (TCB, Orange Book): Einheit von integrer Hard- und Software zur Durchsetzung von Sicherheitsrichtlinien
- TCB sollte einfach und kompakt sein

# TCPA (Trusted Computing Platform Alliance)


- 1999 von Microsoft, Intel, IBM, Compaq und HP gegründetes Hersteller-Konsortium
- 180 Mitglieder (u.a. Infineon, Siemens, RSA, Nokia)
- Erste Veröffentlichung der Spezifikationen in Version 0.9 im August 2000
- Ziel: Durch den Einsatz von spezieller Krypto-Hardware und darauf aufbauenden Betriebssystemen die Sicherheit verbessern

# TCG (Trusted Computing Group)

TCG

- **Anfänglich von AMD, HP, Intel und Microsoft gegründet**
- **Seit April 2003 Rechtsnachfolger der TCPA**
- **Nicht ganz so basisdemokratisch wie TCPA**
  - Kein Veto für Mitglieder mehr (2/3 Mehrheit)
  - Promotor (50.000$/Jahr), Contributor (15.000$/Jahr), Adopter (7.500 $/Jahr, kein Stimmrecht)
- **Ziel: Entwicklung und Support von offenen Industriestandards für „Trusted Computing“ auf verschiedenen Plattformen (PC‘s, Server, Handys und PDA‘s)**

# TCG Spezifikationen


- Hardware: TPM (Trusted Platform Module)
- Software: TSS (Trusted Software Stack)

- TCG TPM Main Specification (alte Version 1.1b)
- TCG Software Stack Specification (Version 1.1, September 2003)

- TCG TPM Specification Version 1.2 (November 2003)
  - Design Principles
  - Structures of the TPM
  - TPM Commands

# Status Quo

- **TPM nach 1.1b Spezifikation erhältlich von**
  - Atmel, Infineon, National Semiconductor
- **Konforme Systeme werden ausgeliefert von**
  - IBM (ThinkPad Notebooks, NetVista Desktops) und HP
- **Applikationen mit wachsendem Support**
  - RSA Secure ID, Checkpoint VPN, Verisign PTA
- **Software von IBM**
  - Windows: verändertes Login, rudimentäre Verschlüsselungswerkzeuge
  - Linux: Testpaket (samt Quellen) mit Kernel-Modul, Bibliothek, API und Beispielprogrammen

# TPM (Trusted Platform Module)

- **Nach US-Senator Fritz Hollings benannter Prozessor „Fritz Chip“**
- **In Zukunft direkt in der CPU eingebaut (LaGrande von IBM, AMD-Prozessoren, als Firmware-Version in Transmetas Crusoe TM5800)**


- **Kryptographische Funktionseinheiten**
  - Random Number Generator (RNG)
  - Hash-Einheit (SHA-1)
  - HMAC (Keyed Hashing for Message Authentication)
  - Generator für RSA-Schlüssel mit bis zu 2.048 Bit
  - RSA Engine zum Erzeugen von Signaturen (nicht prüfen) sowie Ver- und Entschlüsseln

# TPM – Blick in den TCPA-Chip

| Funktionale Einheit | Nicht flüchtiger Speicher | Flüchtiger Speicher |
|---|---|---|
| Random Number Generator | Endorsement Key (2048 Bit) | RSA Key Slot-0<br>...<br>RSA Key Slot-9 |
| Hash (SHA-1) | Storage Root Key (2048 Bit) | PCR-0<br>...<br>PCR-15 |
| HMAC | Owner Auth Secret (160 Bit) | Key Handle |
| RSA Key Generation | | Auth Session Handle |
| RSA Encrypt/Decrypt | | |

# TPM – Nicht flüchtiger Speicher

- **Endorsement Key**
  - 2.048 Bit RSA Schlüsselpaar (öffentlich/privat)
  - Wird beim Herstellungsprozess zufällig generiert
  - Kann nicht gelöscht oder geändert werden (ab TCG TPM 1.2 ist dies möglich)
  - Privater Schlüssel verlässt den Chip nie
  - Öffentlicher Schlüssel dient zur „attestation“
  - Öffentlicher Schlüssel dient zur Verschlüsselung von sensitiven Daten die an den Chip gesendet werden (zum Beispiel beim „Besitz übernehmen“)
  - Da der öffentliche Schlüssel aus Sicht der Privatsphäre kritisch ist, kann er durch den Benutzer abgeschaltet werden

# TPM – Nicht flüchtiger Speicher

- **Storage Root Key (SRK)**
  - 2.048 Bit RSA Schlüsselpaar (öffentlich/privat)
  - Initial ist dieser Speicherplatz leer
  - Wird beim „Besitz übernehmen“ generiert
  - Schlüssel verlässt den Chip nie
  - Kann vom Systembesitzer gelöscht werden
  - Dient zum Verschlüsseln (wrap) von privaten Schlüsseln die außerhalb des Chips gespeichert werden sollen, sowie beim Entschlüsseln dieser privaten Schlüssel wenn sie wieder in den Chip geladen werden
- **Owner Authorization**
  - 160 Bit Schlüssel den der Besitzer mit dem Chip teilt
  - Wird beim „Besitz übernehmen“ in den Chip geladen
  - Autorisierung von sensitiven Benutzerbefehlen

# TPM – Flüchtiger Speicher

- **Zehn Plätze für temporäre RSA Schlüssel**
  - Extern gespeicherte Schlüssel können hier in den Chip geladen und von dort genutzt werden
  - Können hinausgeworfen (evicted) werden um Platz zu schaffen
  - Eigentlich flüchtig – in IBM Chips aber normalerweise auch nach einem Ausschalten noch vorhanden
- **16 Plätze für PCR‘s (Platform Configuration Register)**
  - 160 Bit ermittelte Hash-Werte der Integritätsmessungen
  - Beim Booten können z.B. Messungen vom BIOS, erweitertem BIOS, MBR, GRUB bootstrap stages, anderen Dateien wie dem Kernel, aber auch von Hardware die dies unterstützt erzeugt und hier gespeichert werden

# TPM – Flüchtiger Speicher (cont.)

- **Key Handles**
  - Um temporär geladenen Schlüsseln Namen zur weiteren Bearbeitung zuzuweisen
  - Werden gelöscht wenn der Schlüssel aus dem Chip geworfen wird
- **Authorization Session Handle**
  - Wird genutzt um den Status der Autorisation für mehrere hintereinander abfolgende Befehle beizubehalten
- **Ab TPM 1.2 zusätzlich einige mindestens 20 Byte große Speicherplätze (Data Integrity Register)**

# Neu in TCG TPM 1.2

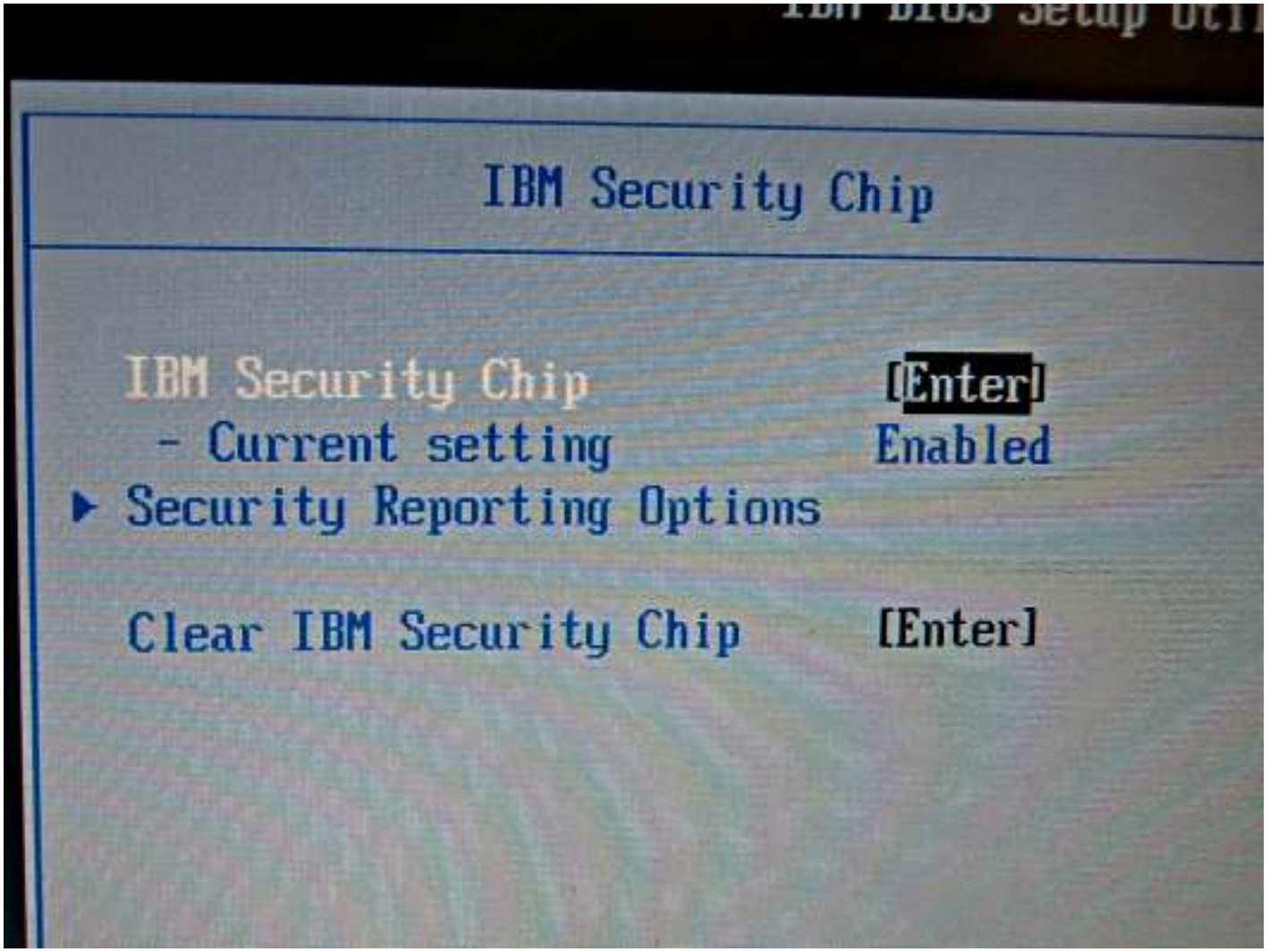
- **Direct Anonymous Attestation (DAA)**
  - Anonyme Attestierung der Identität ohne Zugriff auf eine Drittinstanz ("Direct Proof" oder "Zero Knowledge Attestation")
- **FIPS 140-2 (Wer evaluiert?)**
- **Removable Endorsement Key (aufwändig)**
- **AES192, AES256, Triple-DES**
- **Warum noch 160 Bit SHA1?**
- **Warum Unterstützung von Schlüsseln mit weniger als 2048 Bit (512, 768, 1024)?**

# Aktivieren und Löschen des TPM

- **BIOS gibt TPM beim Einschalten des Rechners ein Startkommando (drei Möglichkeiten)**
  - TPM deaktivieren (kann bis zum erneuten Einschalten nicht mehr aktiviert werden)
  - TPM starten und Reset der PCR-Register, Inhalte der PCR werden neu berechnet beim Booten
  - TPM starten und PCR-Register wieder herstellen (falls vorher gespeichert – resume-Modus)
- **BIOS kann TPM „komplett“ resetten (ForceClear)**
  - Benötigt Beweis der physikalischen Präsenz (Fn beim Systemstart gedrückt halten und mit F1 ins BIOS wechseln)
  - Wirft alle geladenen Schlüssel und Handles raus und löscht SRK sowie das Owner Authorization Secret

# IBM R32 ThinkPad (BIOS)

# IBM R32 ThinkPad (BIOS)

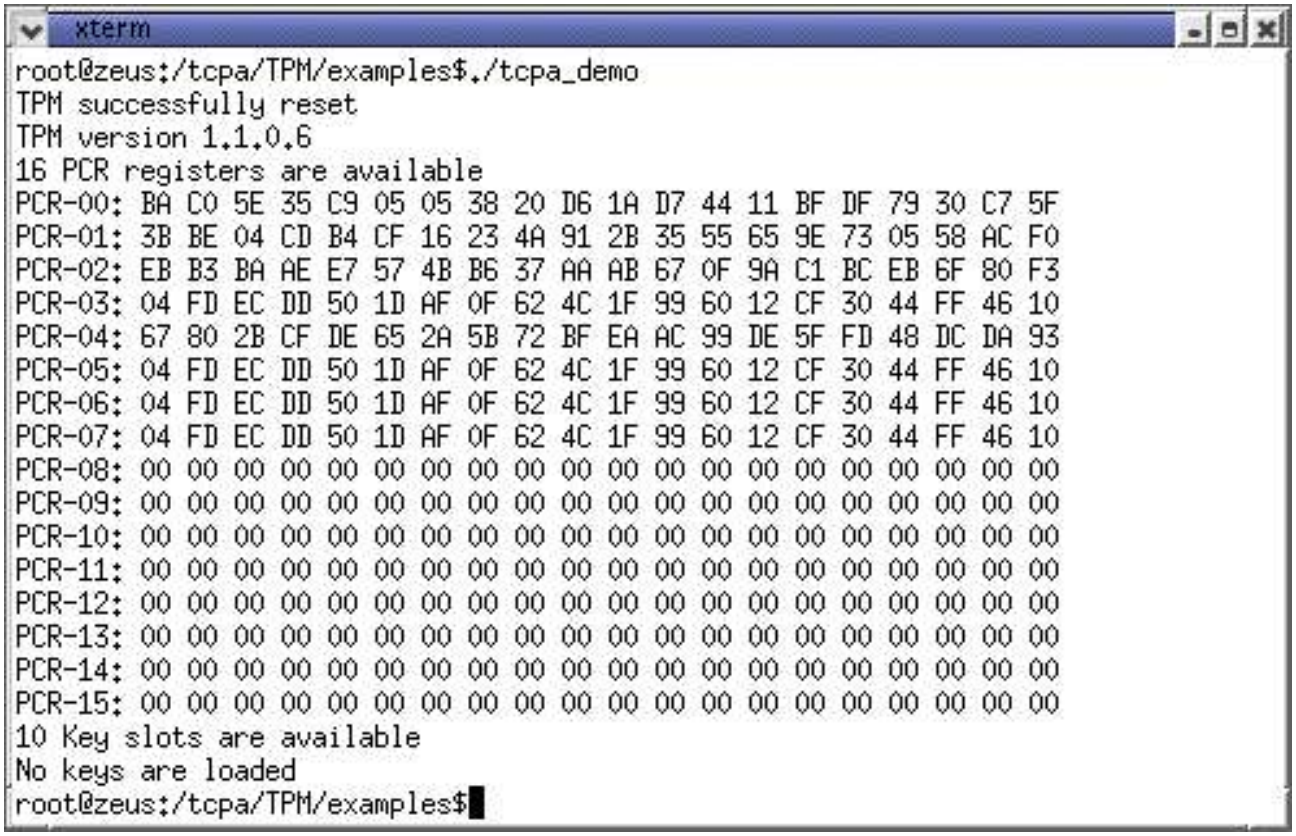


# IBM R32 ThinkPad (BIOS)

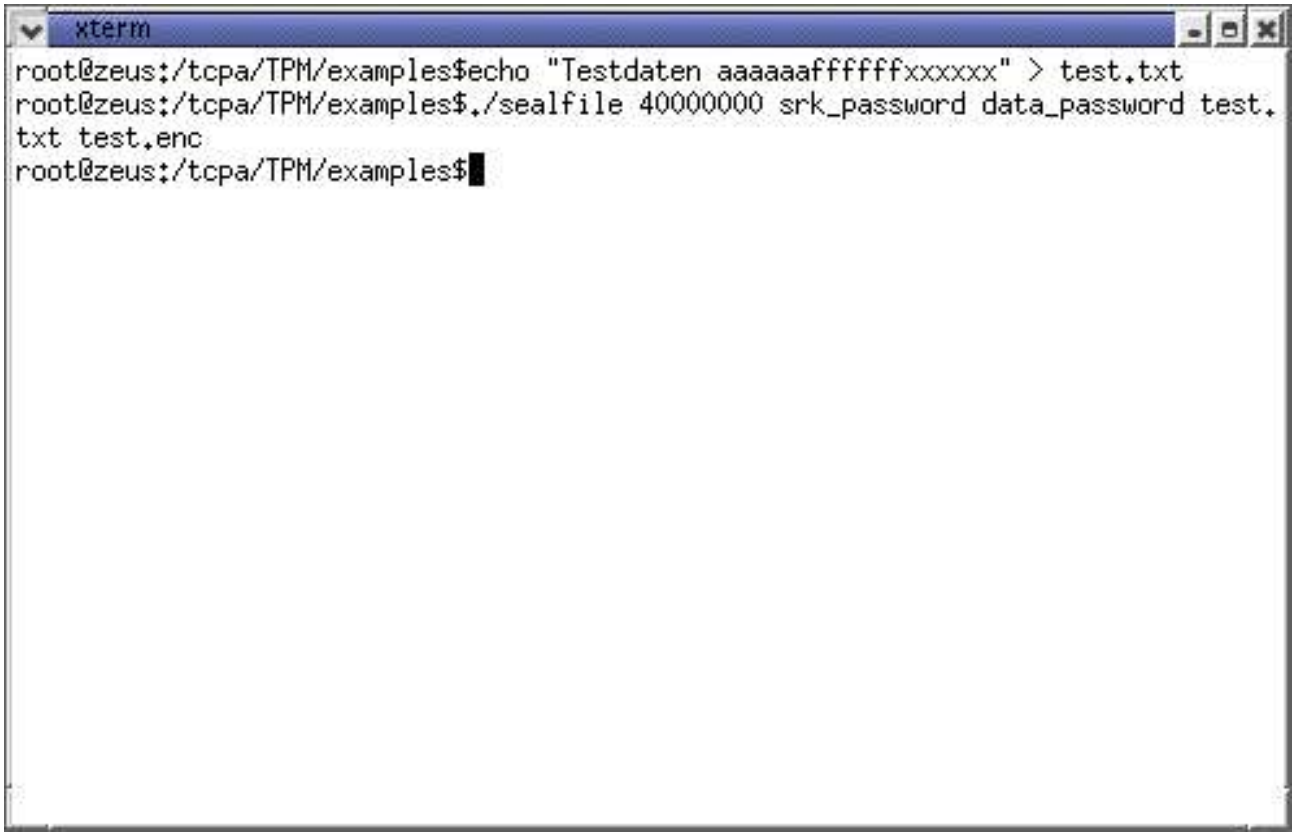
# Funktionen von TCG-Implementierungen

- **Sealing**
  - Systemkonfiguration wird beim Booten bestimmt
  - Ver- und Entschlüsselung funktioniert nur anhand dieser Konfiguration
  - über einen Hash-Wert aus der Systemkonfiguration werden Daten und Applikationen an diese Konfiguration „gebunden“
- **Authentifizierung der Systemkonfiguration**
- **Schutz kryptographischer Schlüssel**
- **Sicherer Timer**
- **Sicherer Zufallsgenerator**

# IBM R32 ThinkPad und IBM Linux-Experimentalpaket (Inhalt des TPM)

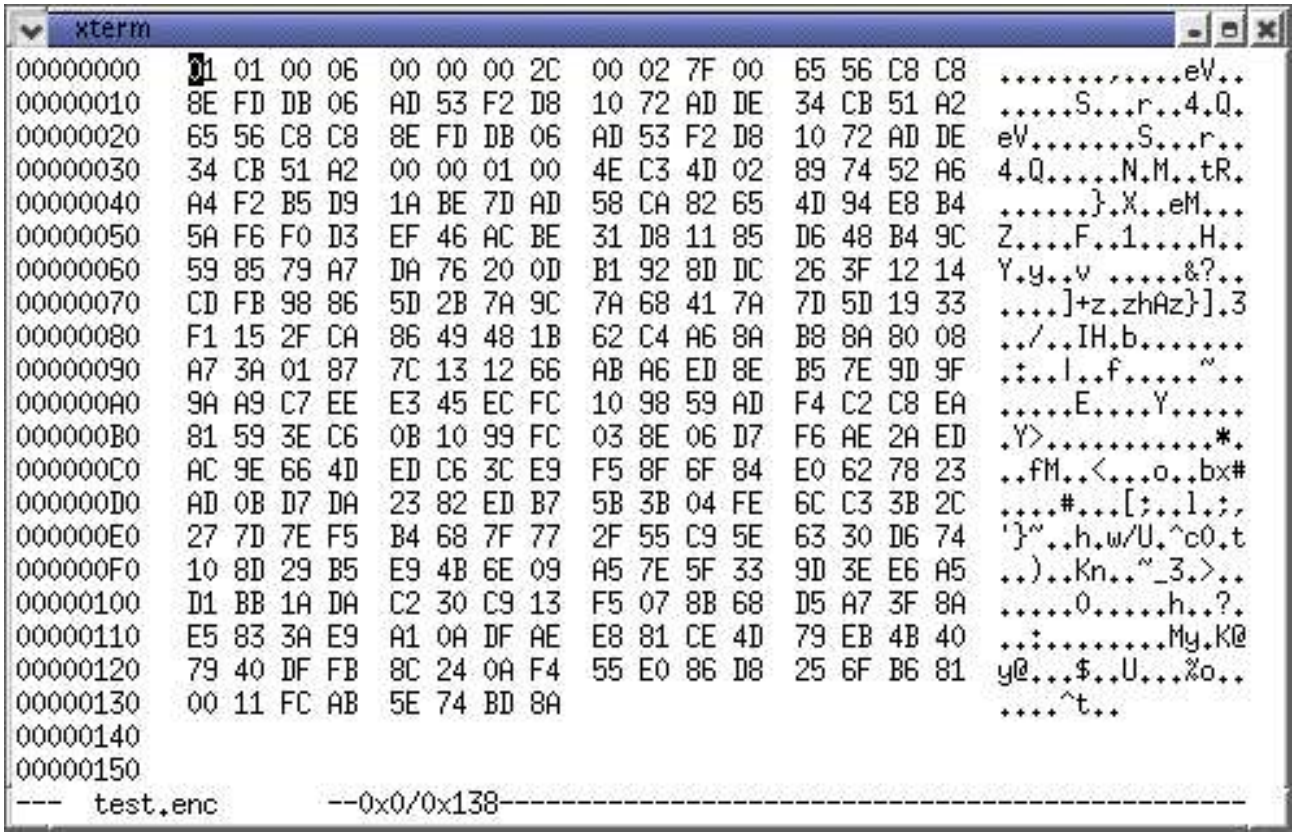


# IBM R32 ThinkPad und IBM Linux-Experimentalpaket (Sealfile)

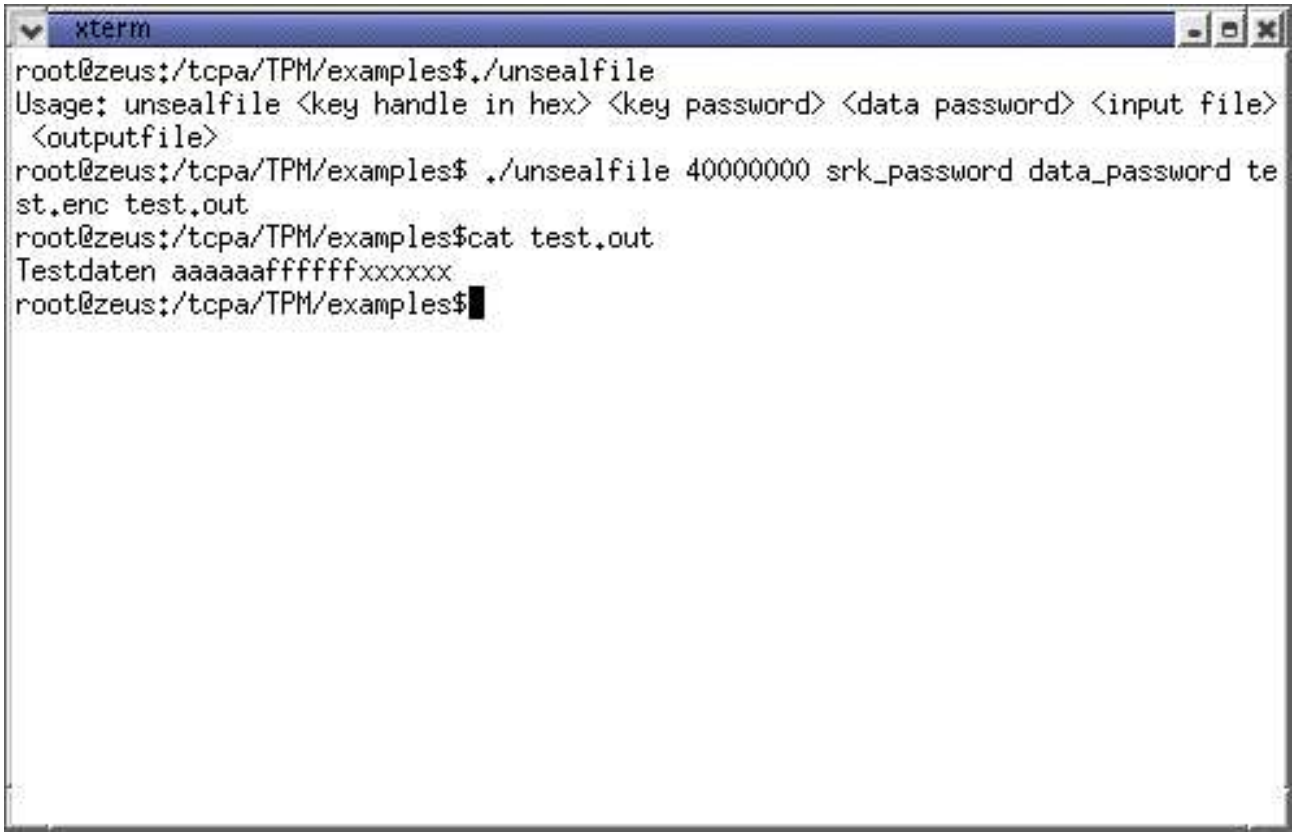


# IBM R32 ThinkPad und IBM Linux-Experimentalpaket (Sealfile)

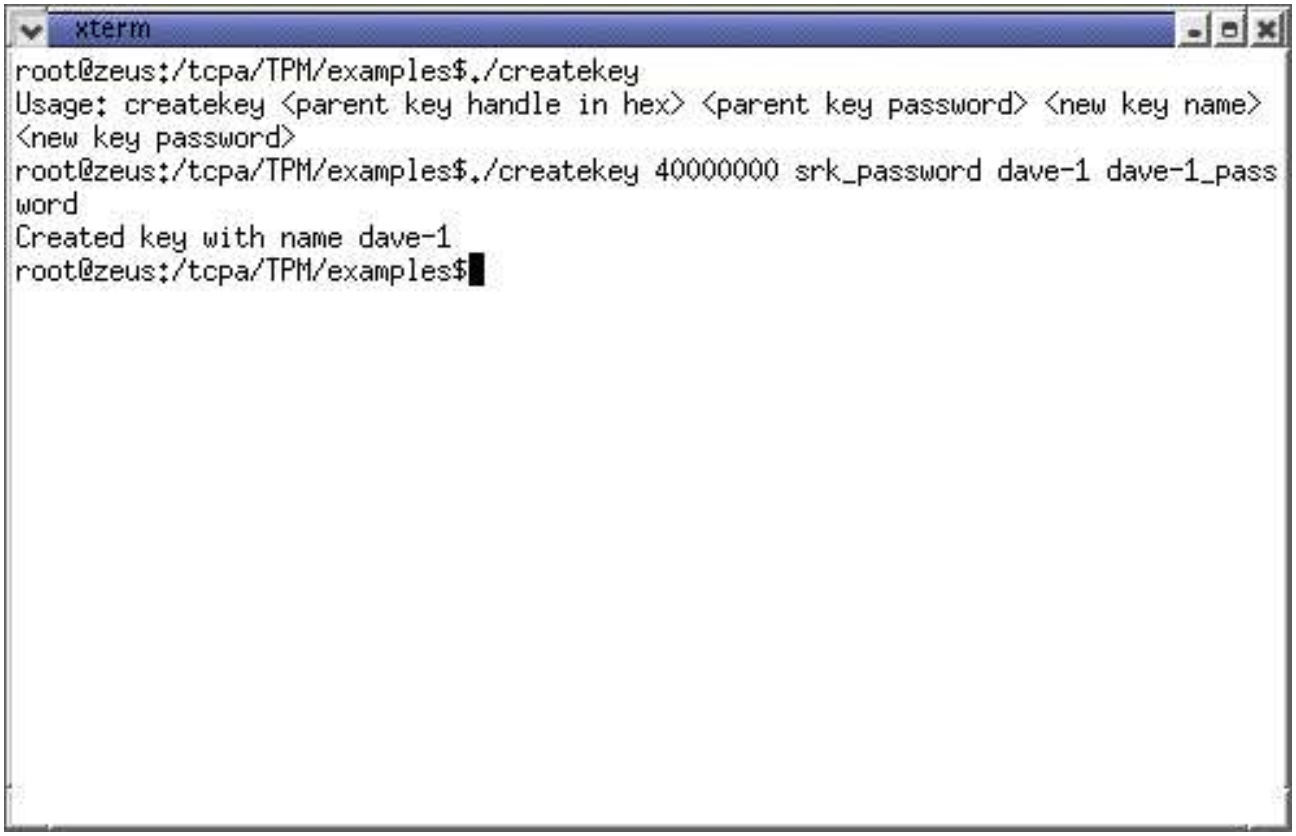
# IBM R32 ThinkPad und IBM Linux-Experimentalpaket (Sealfile)



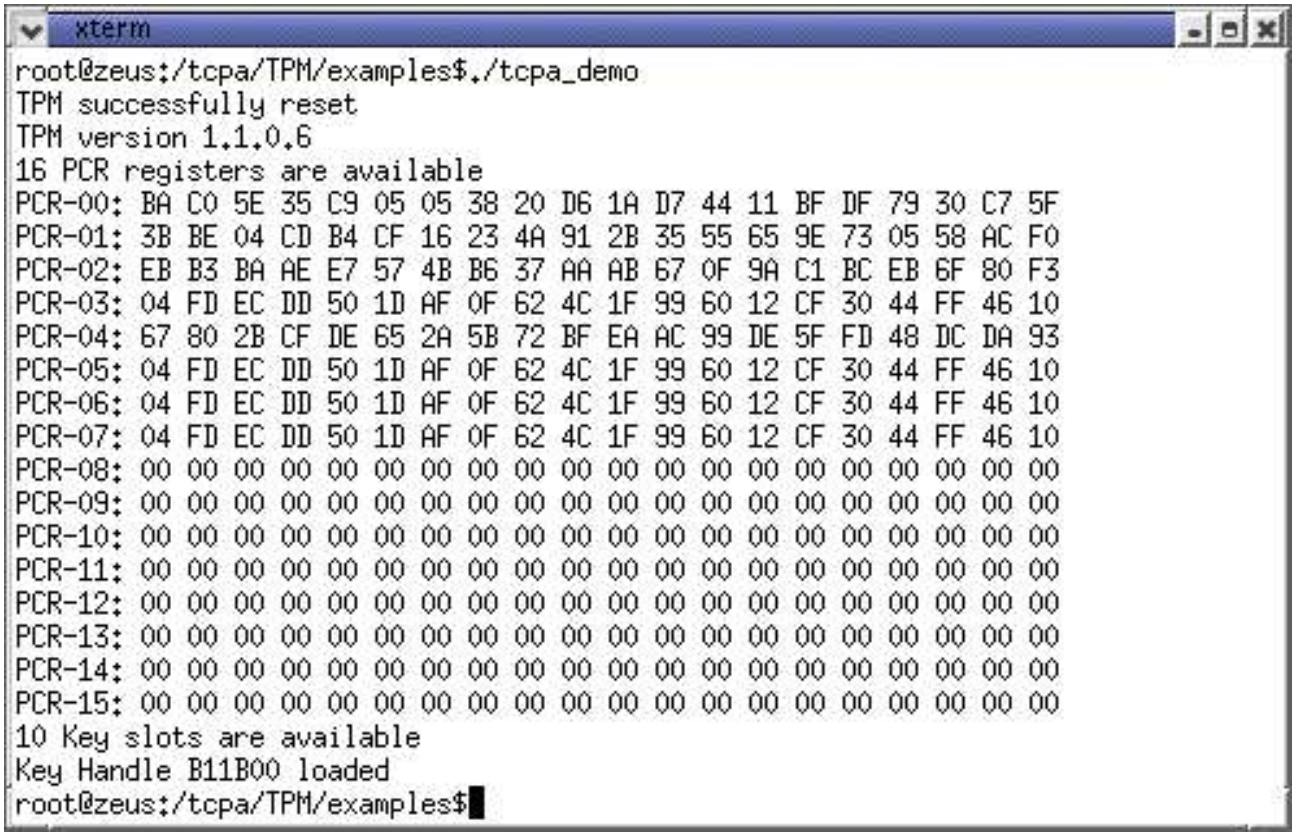
# IBM R32 ThinkPad und IBM Linux-Experimentalpaket (Unsealfile)



# IBM R32 ThinkPad und IBM Linux-Experimentalpaket (Schlüsselerzeugung)



# IBM R32 ThinkPad und IBM Linux-Experimentalpaket (geladener Schlüssel)



# Palladium/NGSCB (Next Generation Secure Computing Base)

- Geschützter Speicherbereich (Curtained Memory) um NGSCB-Applikationen vor potentiellen Schadprogrammen abzuschirmen
- Sicherer Speicherbereich (Sealed Storage) zur sicheren Ablage von sensiblen Daten
- Abgesicherte Ein- und Ausgaben (Trusted I/O)
- Software Authentifizierung (Attestation)

- Soll auf TCG-Spezifikationen Version 1.2 aufbauen

- Sicherheitskritische (und DRM) Komponenten werden in einen Nexus zusammengefasst und in eine sichere Hardwareumgebung ausgelagert

- Microsoft definiert den Nexus als sicher und packt hier eine Menge Funktionalität rein

# Palladium/NGSCB Versprechungen

- Benutzer bekommen volle Kontrolle darüber ob sie NGSCB nutzen wollen
- Sämtliche heutige Software ist weiter nutzbar
- Programmierschnittstellen für NGSCB werden veröffentlicht und dokumentiert
- Microsoft-Nexus wird zur Evaluierung zur Verfügung stehen
- Keine Zertifizierung von NGSCB-Software nötig
- Besserer Schutz der Privatsphäre der Benutzer als bei heutigen PCs

# Wahrheit und Spekulation? Forderungen?

- Marktanteile: TCG = Palladium = DRM?
- Patente und freie Weitergabe von Code/Daten: GPL und TCG vereinbar?
- Marktschranken durch Kosten und Wissen?
- Datenschutz / Privatsphäre?
- Vollständige Kontrolle über alle Schlüssel im TPM (CCC)
- Owner Override bei physikalischer Anwesenheit (EFF)

# Fragen?

## Vielen Dank für die Aufmerksamkeit!

**Wilhelm Dolle**
**Director Information Technology**

**iAS interActive Systems**
**Gesellschaft fuer interaktive Medien mbH**
**Dieffenbachstrasse 33c**
**D-10967 Berlin**

**phone** +49-(0)30-69004-100
**fax** +49-(0)30-69004-101
**mail** wilhelm.dolle@interActive-Systems.de
**web** http://www.interActive-Systems.de