

# 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 integrierter 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)

The logo for the Trusted Computing Group (TCG) features the letters 'TCG' in a bold, red, sans-serif font. The letters are set against a background of horizontal white lines that create a sense of motion or depth, as if the text is floating or moving through a digital space.

- 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

## TCG

- **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 TCGA-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 sensiblen 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)



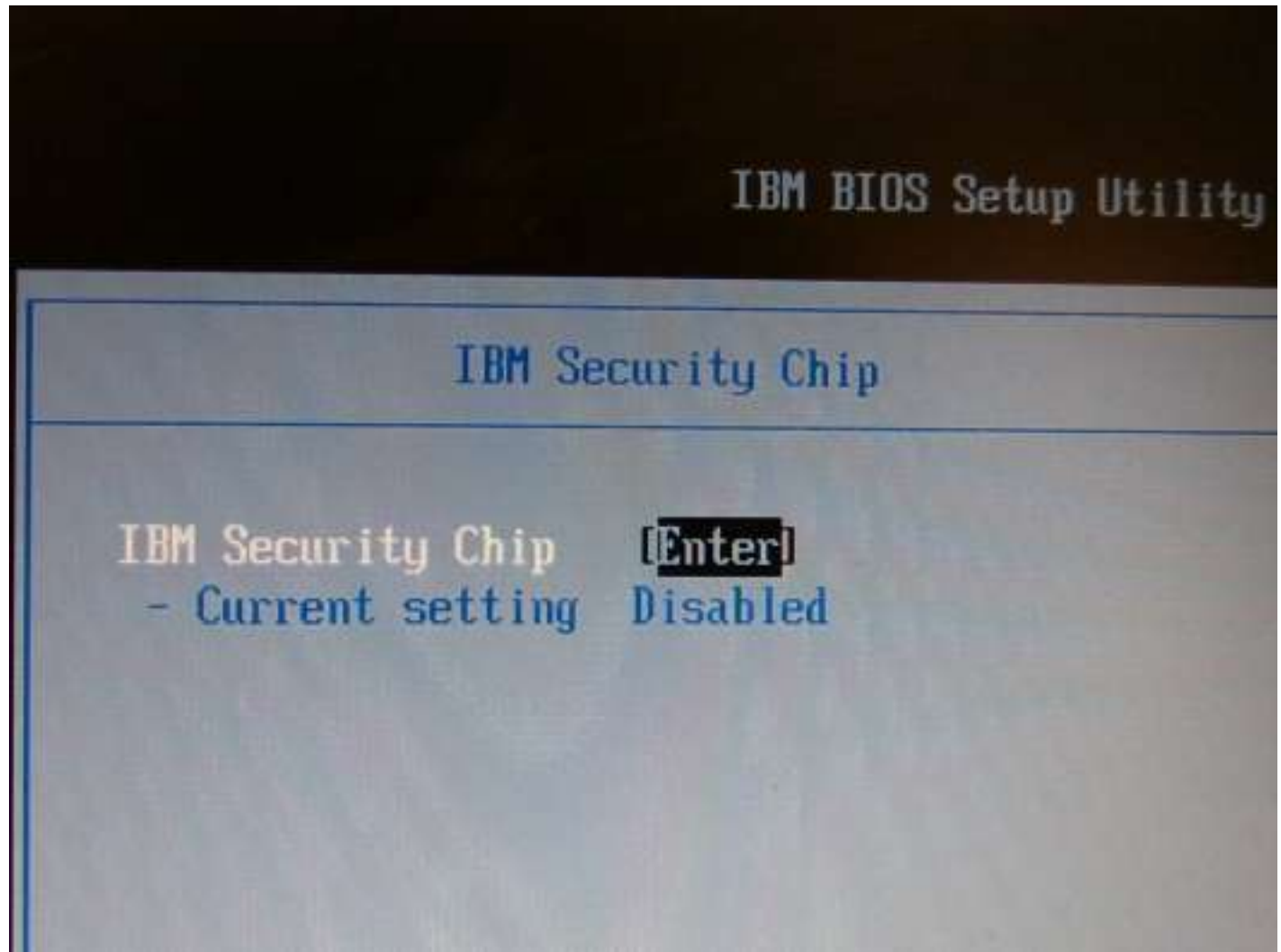
# Neu in TCG TPM 1.2

- **Direct Anonymous Attestation (DAA)**
  - ✗ Anonyme Attestierung der Identität ohne Zugriff auf eine Drittinstantz ("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)?**

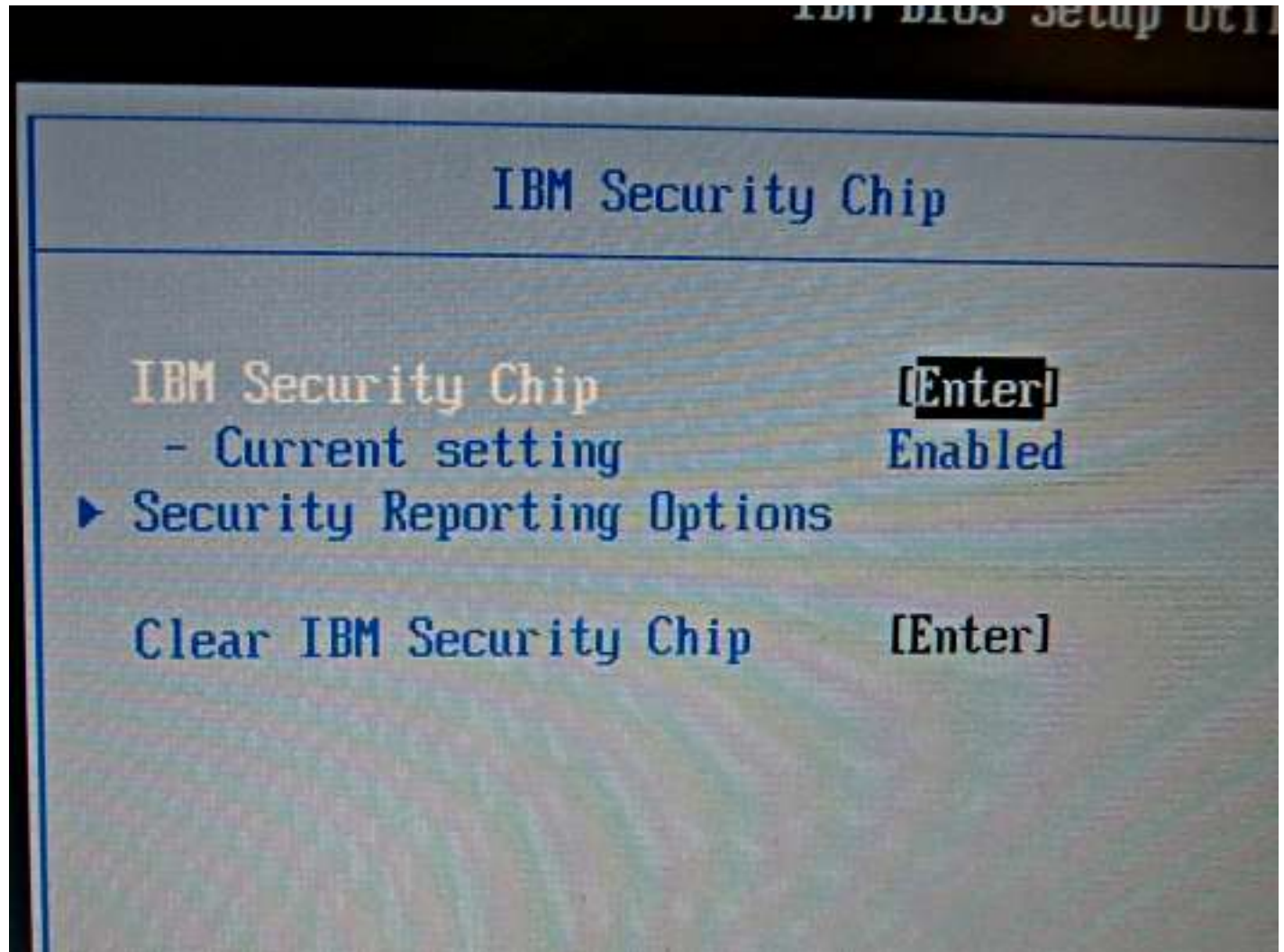
# Aktivieren und Löschen des TPM

- **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)

```
xterm
root@zeus:/tcpa/TPM/examples$./tcpa_demo
TPM successfully reset
TPM version 1.1.0.6
16 PCR registers are available
PCR-00: BA C0 5E 35 C9 05 05 38 20 D6 1A D7 44 11 BF DF 79 30 C7 5F
PCR-01: 3B BE 04 CD B4 CF 16 23 4A 91 2B 35 55 65 9E 73 05 58 AC F0
PCR-02: EB B3 BA AE E7 57 4B B6 37 AA AB 67 0F 9A C1 BC EB 6F 80 F3
PCR-03: 04 FD EC DD 50 1D AF 0F 62 4C 1F 99 60 12 CF 30 44 FF 46 10
PCR-04: 67 80 2B CF DE 65 2A 5B 72 BF EA AC 99 DE 5F FD 48 DC DA 93
PCR-05: 04 FD EC DD 50 1D AF 0F 62 4C 1F 99 60 12 CF 30 44 FF 46 10
PCR-06: 04 FD EC DD 50 1D AF 0F 62 4C 1F 99 60 12 CF 30 44 FF 46 10
PCR-07: 04 FD EC DD 50 1D AF 0F 62 4C 1F 99 60 12 CF 30 44 FF 46 10
PCR-08: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-09: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-11: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-12: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-13: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-14: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-15: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
10 Key slots are available
No keys are loaded
root@zeus:/tcpa/TPM/examples$
```

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

```
xterm
root@zeus:/tcpa/TPM/examples$echo "Testdaten aaaaaaffffffxxxxxx" > test.txt
root@zeus:/tcpa/TPM/examples$./sealfile 40000000 srk_password data_password test.
txt test.enc
root@zeus:/tcpa/TPM/examples$
```



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

```
xterm
root@zeus:/tcpa/TPM/examples$echo "Testdaten aaaaaaffffffxxxxxx" > test.txt
root@zeus:/tcpa/TPM/examples$./sealfile 40000000 srk_password data_password test.
txt test.enc
root@zeus:/tcpa/TPM/examples$cat test.enc
++t, [eVÈÈgÙt-Sò0_r-P4ÈQ#eVÈÈgÙt-Sò0_r-P4ÈQ#N#èüf(°~² iQçšyozD"%ÉY2t+e0:]À1ááóá'πē
ÙÂ!!   èz)šulâBÛc!!xzÈgò5ap*#öq-É/!!žYî À1
+eJü±/iŠKÛ{ih!!opßö
      ú([BÈ!!òXk]òé|vöÜ_îfdš:±ö_e)_!!â|tX!!T!!
sö_JÉ_òÉÄ_!!_!_@6W8!!91F80š_60% 'V#1;2f1;2f
```

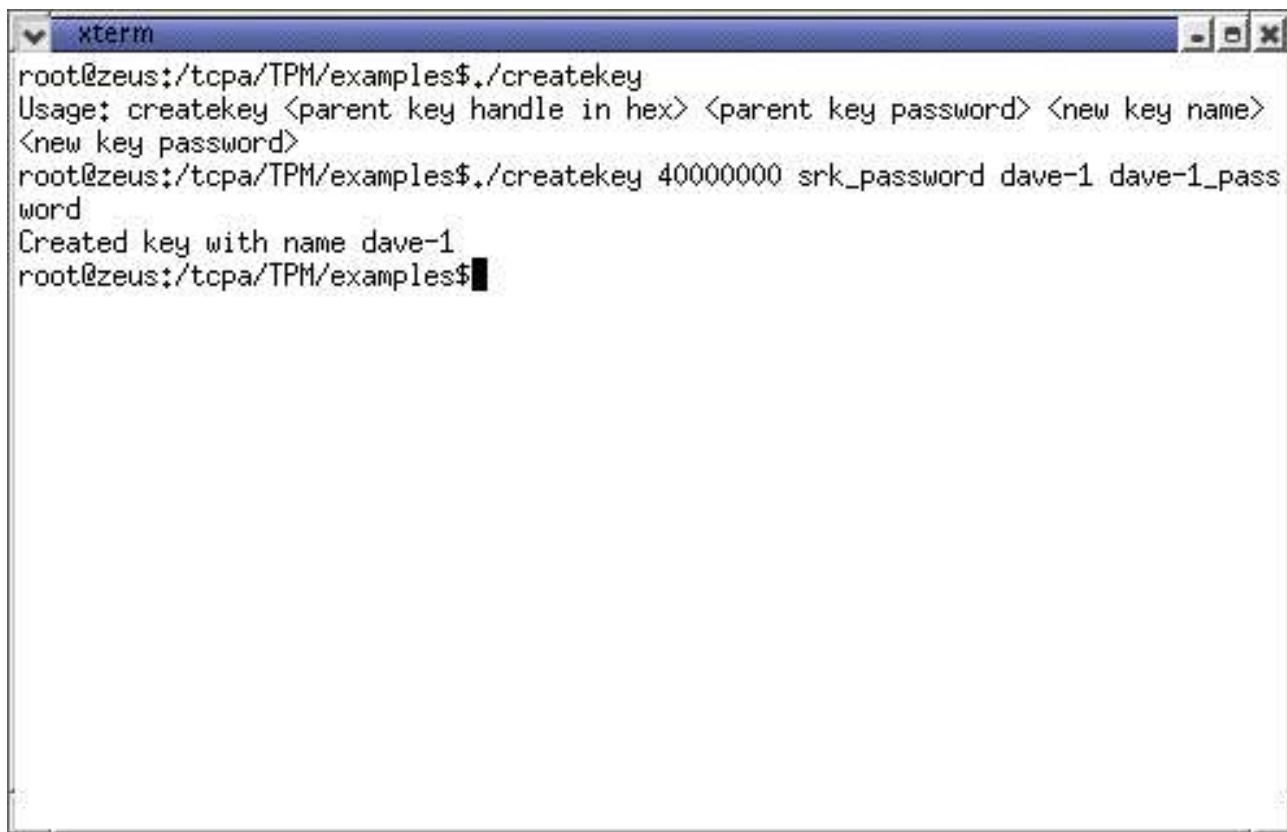
# IBM R32 ThinkPad und IBM Linux-Experimentalpaket (Sealfile)

```
xterm
00000000 01 01 00 06 00 00 00 2C 00 02 7F 00 65 56 C8 C8 .....eV..
00000010 8E FD DB 06 AD 53 F2 D8 10 72 AD DE 34 CB 51 A2 .....S...r..4.Q.
00000020 65 56 C8 C8 8E FD DB 06 AD 53 F2 D8 10 72 AD DE eV.....S...r..
00000030 34 CB 51 A2 00 00 01 00 4E C3 4D 02 89 74 52 A6 4.Q.....N.M..tR.
00000040 A4 F2 B5 D9 1A BE 7D AD 58 CA 82 65 4D 94 E8 B4 .....}.X..eM...
00000050 5A F6 F0 D3 EF 46 AC BE 31 D8 11 85 D6 48 B4 9C Z....F..1....H..
00000060 59 85 79 A7 DA 76 20 0D B1 92 8D DC 26 3F 12 14 Y.y..v .....&?.
00000070 CD FB 98 86 5D 2B 7A 9C 7A 68 41 7A 7D 5D 19 33 ....]+z.zhAz}].3
00000080 F1 15 2F CA 86 49 48 1B 62 C4 A6 8A B8 8A 80 08 ../.IH.b.....
00000090 A7 3A 01 87 7C 13 12 66 AB A6 ED 8E B5 7E 9D 9F ..l..f.....~..
000000A0 9A A9 C7 EE E3 45 EC FC 10 98 59 AD F4 C2 C8 EA .....E....Y....
000000B0 81 59 3E C6 0B 10 99 FC 03 8E 06 D7 F6 AE 2A ED .Y>.....*.
000000C0 AC 9E 66 4D ED C6 3C E9 F5 8F 6F 84 E0 62 78 23 ..fM.<...o..bx#
000000D0 AD 0B D7 DA 23 82 ED B7 5B 3B 04 FE 6C C3 3B 2C ....#[;:1.;,
000000E0 27 7D 7E F5 B4 68 7F 77 2F 55 C9 5E 63 30 D6 74 '}~..h,w/U.^c0.t
000000F0 10 8D 29 B5 E9 4B 6E 09 A5 7E 5F 33 9D 3E E6 A5 ..)..Kn..^_3.>..
00000100 D1 BB 1A DA C2 30 C9 13 F5 07 8B 68 D5 A7 3F 8A .....0.....h..?.
00000110 E5 83 3A E9 A1 0A DF AE E8 81 CE 4D 79 EB 4B 40 ..:.....My.K@
00000120 79 40 DF FB 8C 24 0A F4 55 E0 86 D8 25 6F B6 81 y@...$.U...%o..
00000130 00 11 FC AB 5E 74 BD 8A .....^t..
00000140
00000150
--- test.enc -----0x0/0x138-----
```

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

```
xterm
root@zeus:/tcpa/TPM/examples$ ./unsealfile
Usage: unsealfile <key handle in hex> <key password> <data password> <input file>
<outputfile>
root@zeus:/tcpa/TPM/examples$ ./unsealfile 40000000 srk_password data_password te
st.enc test.out
root@zeus:/tcpa/TPM/examples$ cat test.out
Testdaten aaaaaaffffffxxxxxx
root@zeus:/tcpa/TPM/examples$
```

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



```
xterm
root@zeus:/tcpa/TPM/examples$./createkey
Usage: createkey <parent key handle in hex> <parent key password> <new key name>
<new key password>
root@zeus:/tcpa/TPM/examples$./createkey 40000000 srk_password dave-1 dave-1_pass
word
Created key with name dave-1
root@zeus:/tcpa/TPM/examples$
```

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

```
xterm
root@zeus:/tcpa/TPM/examples$./tcpa_demo
TPM successfully reset
TPM version 1.1.0.6
16 PCR registers are available
PCR-00: BA C0 5E 35 C9 05 05 38 20 D6 1A D7 44 11 BF DF 79 30 C7 5F
PCR-01: 3B BE 04 CD B4 CF 16 23 4A 91 2B 35 55 65 9E 73 05 58 AC F0
PCR-02: EB B3 BA AE E7 57 4B B6 37 AA AB 67 0F 9A C1 BC EB 6F 80 F3
PCR-03: 04 FD EC DD 50 1D AF 0F 62 4C 1F 99 60 12 CF 30 44 FF 46 10
PCR-04: 67 80 2B CF DE 65 2A 5B 72 BF EA AC 99 DE 5F FD 48 DC DA 93
PCR-05: 04 FD EC DD 50 1D AF 0F 62 4C 1F 99 60 12 CF 30 44 FF 46 10
PCR-06: 04 FD EC DD 50 1D AF 0F 62 4C 1F 99 60 12 CF 30 44 FF 46 10
PCR-07: 04 FD EC DD 50 1D AF 0F 62 4C 1F 99 60 12 CF 30 44 FF 46 10
PCR-08: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-09: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-11: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-12: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-13: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-14: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-15: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
10 Key slots are available
Key Handle B11B00 loaded
root@zeus:/tcpa/TPM/examples$
```

# **Palladium/NGSCB**

## **(Next Generation Secure Computing Base)**

- **Geschützter Speicherbereich (Curtained Memory) um NGSCB-Applikationen vor potentiellen Schadprogrammen abzusichern**
- **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](mailto:wilhelm.dolle@interActive-Systems.de)  
web <http://www.interActive-Systems.de>**