Konzepte und Technik des Trusted Computing der TCPA / TCG

Wilhelm Dolle
Director Information Technology
interActive Systems GmbH

Vorlesung „Sicherheit in Rechnernetzen“
Prof. Dr. Bettina Schnor, Universität Potsdam
08. Juni 2005, Potsdam

Agenda

- Einführung
- Trusted Computing Konzepte der TCG / TCPA
- Funktionen des Trusted Platform Module (TPM)
- Chancen und Risiken
- Status Quo der Unterstützung durch Hard- und Software
- Forschungsprojekte

Ausgangssituation: Warum Trusted Computing?

- **Herkömmliche Sicherheitskonzepte sind unzureichend**
- **Beispiel Speicherschutz**
  - Muss durch Speicherverwaltungseinheit (MMU) der Hardware (CPU) unterstützt werden
  - Betriebssystem muss Aufteilen des Hauptspeichers und damit die Trennung von laufenden Prozessen unterstützen
  - Trotzdem können Hardwarekomponenten wie DMA-Geräte direkt und unter Umgehung der Sicherheitskontrollen der CPU lesend und schreibend auf den Speicher zugreifen
- **Aufeinander abgestimmte Hardware-, Firmware- und Software-Sicherheitskonzepte werden benötigt**
  - Einheitliche Schnittstellen zu Betriebssystemen und Anwendungen

Trusted Computing Platform Alliance (TCPA)

- **1999 von Microsoft, Intel, IBM, Compaq und HP gegründetes Hersteller-Konsortium**
- **2003 über 200 Mitglieder (u.a. Infineon, Siemens, RSA, Nokia)**
- **Einstimmige Entscheidungsfindung**
- **Erste Veröffentlichung der Spezifikationen in Version 0.9 im August 2000**
- **Ziel: Hard- und Softwarestandards zu spezifizieren, um das Vertrauen (Trust) in Computerplattformen zu erhöhen**
  - Plattform: Motherboard, CPU, und weitere Geräte und Chips
  - Vertrauen: Komponenten agieren so wie erwartet

Trusted Computing Group (TCG)

- **Von AMD, IBM, 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 $ bzw. 1.000$/Jahr, kein Stimmrecht)
  - Juni 2005: 7 Promotor, 70 Contributor, 30 Adopter
  - Seit Mitte 2004: „Industry Liaison Program“ (kein Stimmrecht und NDA)
- **Ziel: Entwicklung und Support von offenen Industriestandards für „Trusted Computing“ auf verschiedenen Plattformen**
  - Plattform: PC‘s, Server, Laptops, Mobiltelefone und PDA‘s

TCG-Architektur

- **Hardware**
  - Trusted Platform Module (TPM)
- **Hardware oder Firmware**
  - Root of Trust for Measuring Integrity Metrics (RTM)
  - Kann auch vollständig durch das TPM implementiert werden
- **Software**
  - Trusted Software Stack (TSS)
- **TCG-Subsystem aus TPM, RTM und TSS stellt Betriebssystemen vertrauenswürdige Dienste und Mechanismen zur Verfügung**
- **Hier wichtige Spezifikationen**
  - TCG TPM Main Specification (alte Version 1.1b)
  - TCG TPM Specification Version 1.2 (November 2003)

Designziele der TCG-Architektur

- **Authentifizierung der Systemkonfiguration (Sicheres Booten)**
- **Schutz kryptographischer Schlüssel (Speichern in Hardware)**
- **Remote Platform Attestation**
- **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“

TPM (Trusted Platform Module)

- **Nach US-Senator Fritz Hollings (macht sich sehr für DRM stark) auch „Fritz Chip“ genannt**
- **Chip auf Motherboard (geplant ist aber auch eine Integration in CPUs)**

- **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 … RSA Key Slot-9
Hash (SHA-1)	Storage Root Key (2048 Bit)	PCR-0 … 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 (EK)**
  - 2.048 Bit RSA Schlüsselpaar
  - Beim Herstellungsprozess im TPM generiert oder in dieses geschrieben
  - Nicht lösch- oder änderbar (ab TPM 1.2 Löschen möglich)
  - Privater Teil verlässt das TPM nie
  - Öffentlicher Teil kann zur „attestation“ dienen
  - Öffentlicher Teil zur Verschlüsselung von sensitiven Daten die an den Chip gesendet werden (zum Beispiel beim „Besitz übernehmen“)
  - Öffentlicher Schlüssel aus Sicht der Privatsphäre kritisch (siehe Seriennummern von Intel-Prozessoren) -> AIKs

- **Attestation Identity Keys (AIK)**
  - Mit EK signierte pseudonyme Schlüssel (beliebig viele)
  - Bestätigt Vorhandensein und Konfiguration des TPM (z.B. PCRs) ohne den EK (öffentlicher Teil) selbst herauszugeben
  - Signierte AIK werden mit EK-Zertifikat nur an vertrauens-würdige Zertifizierungstellen (Privacy CA) herausgegeben

TPM – Nicht flüchtiger Speicher

- **Storage Root Key (SRK)**
  - 2.048 Bit RSA Schlüsselpaar
  - Initial ist dieser Speicherplatz leer
  - Wird beim „Besitz übernehmen“ generiert
  - Schlüssel verlässt den Chip nie
  - Kann vom Systembesitzer gelöscht werden
  - Bildet die Wurzel einer Schlüsselhierarchie
  - Dient zum Verschlüsseln (wrap) von privaten Schlüsseln der ersten Hierarchiestufe die außerhalb des Chips gespeichert werden, sowie beim Entschlüsseln dieser privaten Schlüssel wenn sie wieder in den Chip geladen werden

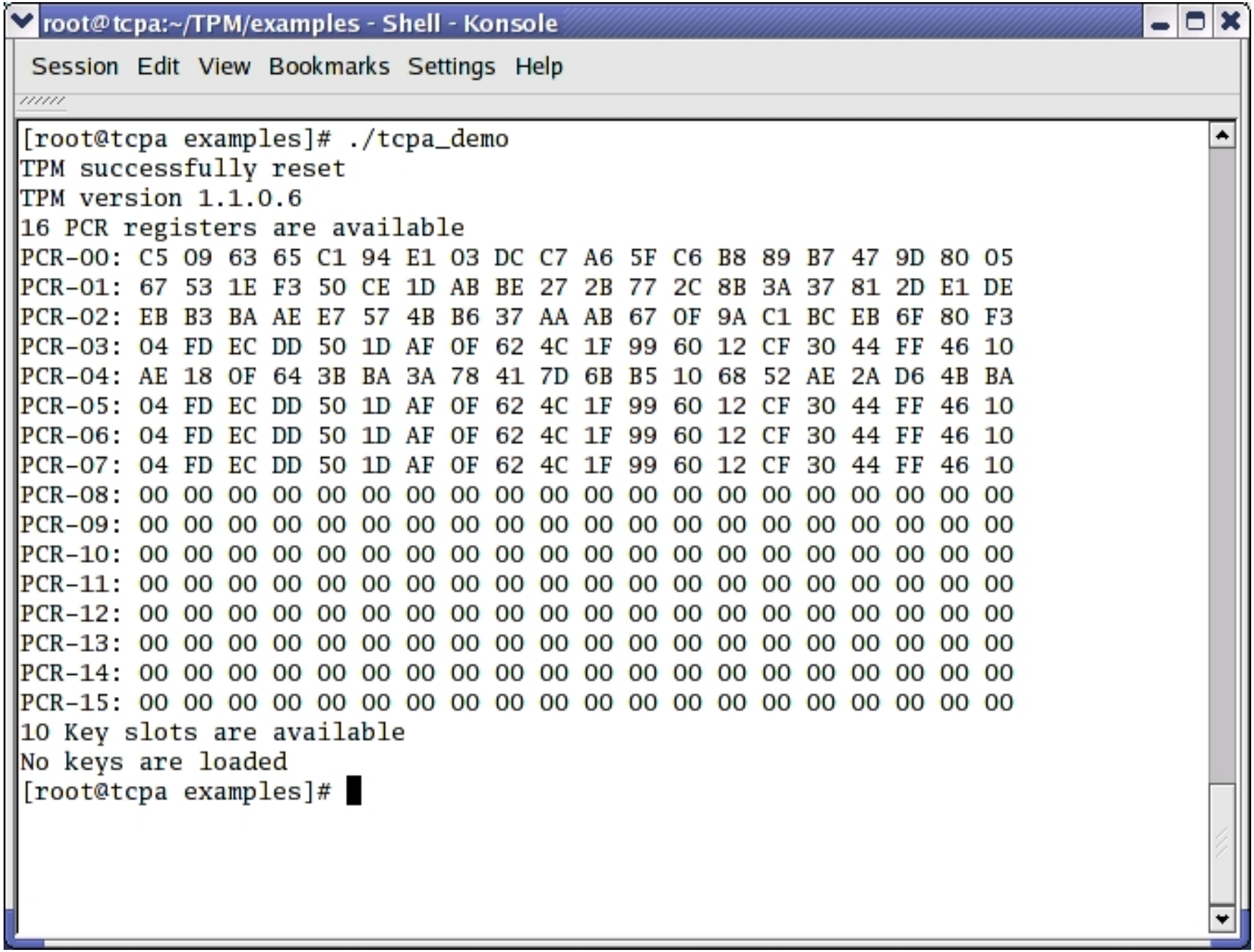
- **Owner Authorization**
  - 160 Bit Schlüssel den der Besitzer mit dem Chip teilt (SHA-1 Hash des angegebenen Passworts mit EK verschlüsselt)
  - Wird beim „Besitz übernehmen“ in den Chip geladen
  - Autorisierung von sensitiven Benutzerbefehlen

TPM – Flüchtiger Speicher I

- **Zehn Plätze für temporäre RSA Schlüssel**
  - Extern gespeicherte Schlüssel können hier in den Chip geladen (nach Eingabe des Passworts) und genutzt werden
  - Können hinausgeworfen (evicted) werden um Platz zu schaffen

- **16 Plätze für PCR‘s (Platform Configuration Register)**
  - 160 Bit ermittelte Hash-Werte der Integritätsmessungen
  - Folge von Integritätswerten: $PCR_i=HASH(PCR_{i-1},Wert)$
  - Zugriff nur im Rahmen von Sicherheitsdiensten
  - 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
  - Ab TPM Version 1.2 für PC-Platfform 24 Register vorgesehen

Inhalt eines TPM-Chips (PCR) - Linux



TPM – Flüchtiger Speicher II

- **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 mindestens 20 Byte große Speicherplätze (Data Integrity Register)**

Aktivieren und Löschen des TPM durchs BIOS

- **BIOS gibt TPM beim Einschalten des Rechners ein Startkommando (drei Möglichkeiten)**
  - TPM deaktivieren (kann bis zum 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

Chancen

- **Sicherer Hardwarespeicher**
  - verhindert u.a. Off-Line-Angriffe auf Geheimnisse
- **Sicheres Booten**
  - TPM als sicherer Hardware-Anker (Root of Trust)
  - Chain of Trust beim Boot-Prozess
- **Digital Rights Management (DRM)**
  - Mit Hardware-Anker sicherer als ausschließlich in Software (bzw. Betriebssystem)
- **Vergleich zu Smart-Cards**
  - TPM authentifiziert Plattform
  - Smart-Card authentifiziert Benutzer

Exkurs: Digital Rights Management (DRM)

- **Ziel von DRM-Systemen**
  - Abgrenzung zum reinen Kopierschutz (lediglich das Verhindern von illegaler Vervielfältigung)
  - DRMS erlauben dem Rechteinhaber digitaler Inhalte zusätzlich ein Rechtemodell gegenüber dem Rechteverwerter durchzusetzen

- **Rechtemodelle können beinhalten**
  - Wiedergaberechte (Anhören, Ansehen, Ausdrucken, ...)
  - Transportrechte (Kopieren, Vermieten, Weitergeben, ...)
  - Derivativrechte (Extrahieren, Editieren, Einbinden, ...)
  - Dienstrechte (Sicherung, Caching, Integritätssicherung, ...)

- **Geschäftsmodelle (Kombinationen möglich)**
  - Zeitlich befristete Nutzung
  - Mengenabhängige Nutzung (n Wiedergaben / Aufrufe)
  - Geräteabhängige Nutzung
  - Gebrauchsorientierte Nutzung (n Minuten wiedergegeben)

Risiken

- **Remote Platform Attestation**
  - wirklich (komplette) Softwareumgebung preisgeben?
- **Sealing, Zensur, DRM, … (TCG ist „Policy Neutral“)**
- **Open Source Software / Patente**
- **Gefahr von (nicht entdeckbaren) Hintertüren**
  - Ron Rivest: „… renting out a part of your PC to people you may not trust.“
- **Migration / Backup der Schlüssel (bzw. Daten)?**
- **„ungeeignete“ Kryptographie**

„ungeeignete“ Kryptographie

- **Februar 2005: erfolgreicher Angriff auf SHA-1**
  - SHA-1 bildet Hash-Werte mit 160 Bit
  - Für Kollision „nur“ noch 2^{69} statt 2^{80} Nachrichten überprüfen (Faktor 2048, 2^{11})
  - Existierende signierte Nachrichten und selbst erstellte Dokumente sind sicher

- **2004er Empfehlungen BSI / RegTP (Regulierungs-behörde für Telekommunikation und Post)**
  - SHA-1 und RIPEMD-160 sind bis 2009 geeignet
  - SHA-256, SHA-384 und SHA-512 gewähren ein langfristiges Sicherheitsniveau (mindestens bis 2009)
  - Bei RSA für langfristiges Sicherheitsniveau 2048 Bit empfohlen (Mindestwert bis Ende 2009 sind 1536 Bit)

Status Quo (Hardware)

- **Über 16 Millionen Motherboards mit TPM (1.1b) ausgeliefert**
  - STMicroelectronics und Amtel fertigt bereits 1.2er TPMs
  - Infineon kündigt 1.2er TPMs für Juli 2005 an
- **Verfügbare Komponenten (Beispiele)**
  - Hauptsächlich Komplettrechner oder Motherboards für Unternehmenskunden (u.a. von IBM, HP, Fujitsu-Siemens)
  - Bei IBM (1.1b) als Embedded Security Subsystem 2.0
  - Gigabit-Ethernet-Controller von Broadcom (1.1b)
  - Von Intel bereits neue Chipsätze und Motherboards mit TPM 1.2 erhältlich
- **Angekündigt unter anderem**
  - TPM integriert in I/O-Chip mit Ports für Tastatur, Maus, Drucker, Floppy, RS-232 (National Semiconductor)
  - Trusted-Mode Keyboard Controller (Intel, MS)
  - USB-Security-Extension (Intel, MS)
  - TPM in CPU (Intel – LaGrande Technology)

Microsofts Palladium bzw. NGSCB (Next Generation Secure Computing Base)

- **Vorschlag 2003**
  - Windows in Quadranten aufteilen
  - Left Hand Site (LHS) – ungesicherte Windowsumgebung
  - Right Hand Site (RHS) – Anwendungen im Trusted Mode
  - LHS und RHS haben jeweils Benutzer- und Kernel-Modus
  - Nexus im Kernel-Modus in der RHS

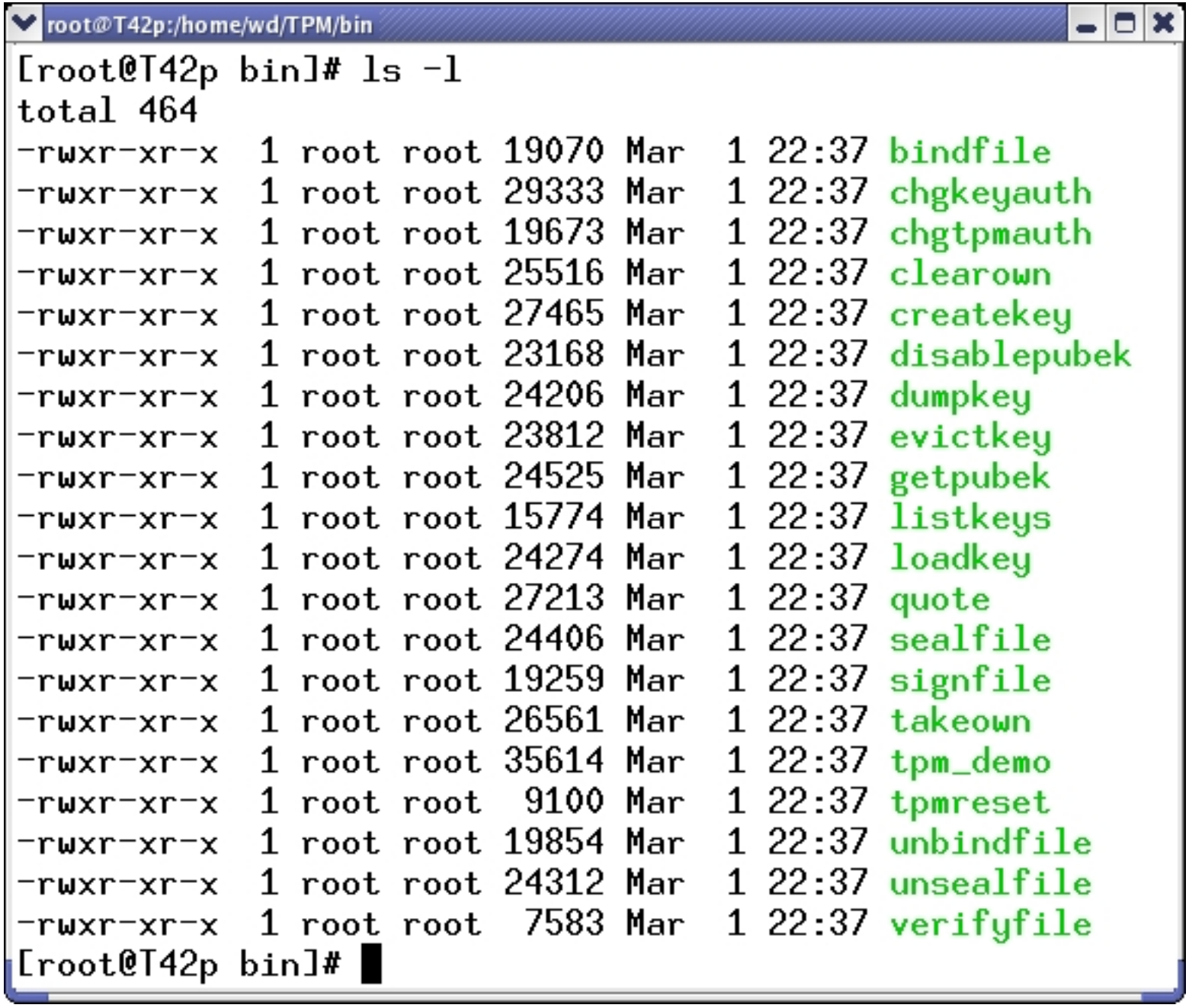
- **Ankündigungen auf der WinHEC 2004**
  - LHS nahezu unverändert, RHS wird komplett überarbeitet
  - Compartments (abgeschottete virtuelle Systeme parallel zum Hauptbetriebssystem)

- **Ankündigungen auf der WinHEC 2005**
  - Secure Startup – Full Volume Encryption in Longhorn mit 1.2er TPM

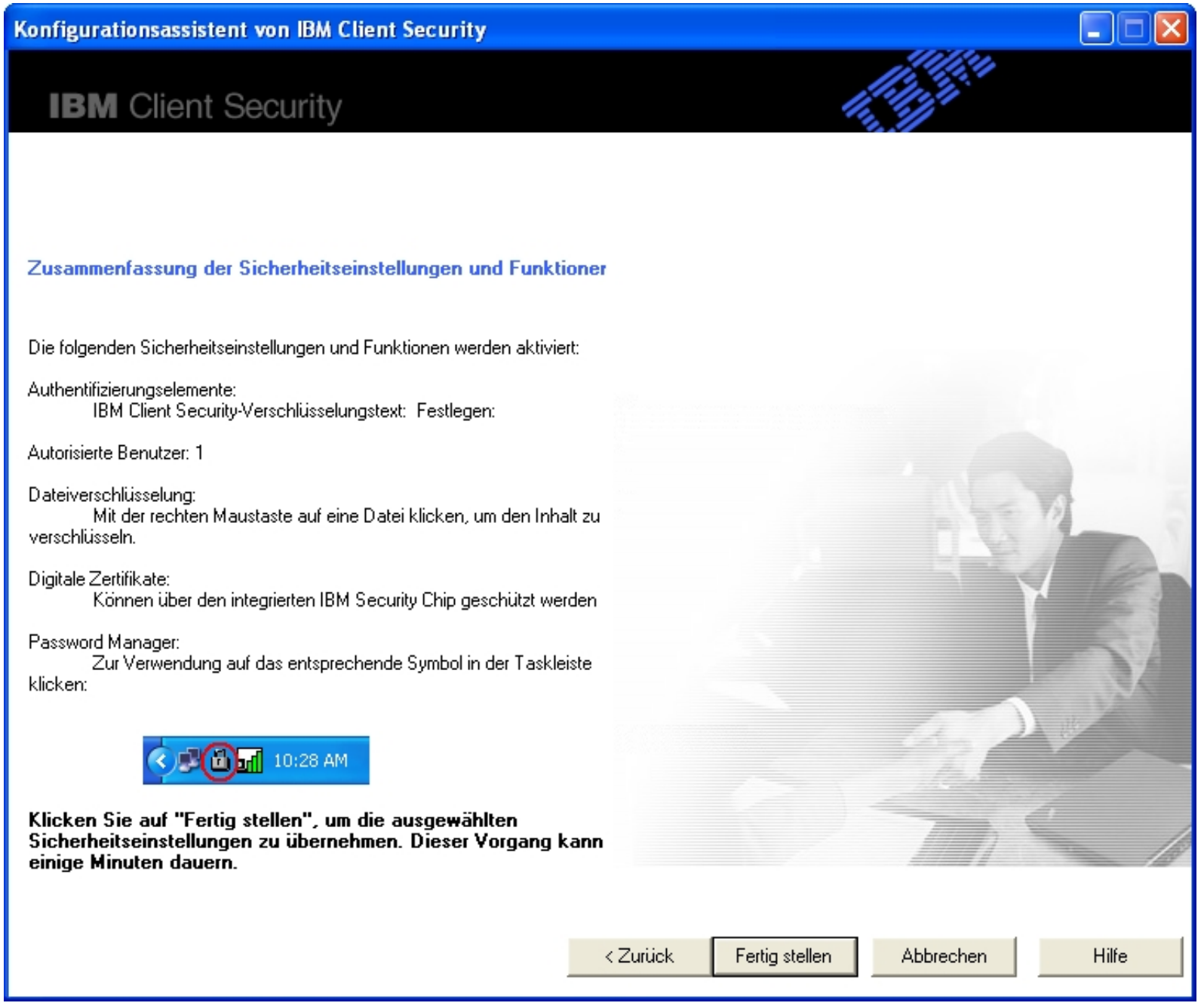
Status Quo (Software)

- **Kommerzielle Applikationen mit TPM-Support (Beispiele)**
  - Utimaco SafeGuard (Laufwerksverschlüsselung)
  - Check Point VPN-1 SecureClient
  - Adobe Acrobat 6.0 (Verschlüsselung bzw. Zugriffskontrolle von PDF-Dokumenten - DRM-Lösung)
- **Software von IBM**
  - Windows: verändertes Login, rudimentäre Verschlüsselungswerkzeuge
  - Linux-Testpaket (samt Quellen) mit Kernel-Modul, Bibliothek, API und Beispielprogrammen
  - tcgLinux: TPM-based Linux Run-time Attesttation
- **Forschungsprojekte**
  - Enforcer Linux Security Module
  - PERSEUS
  - European Multilateral Secure Computing Base (EMSCB)

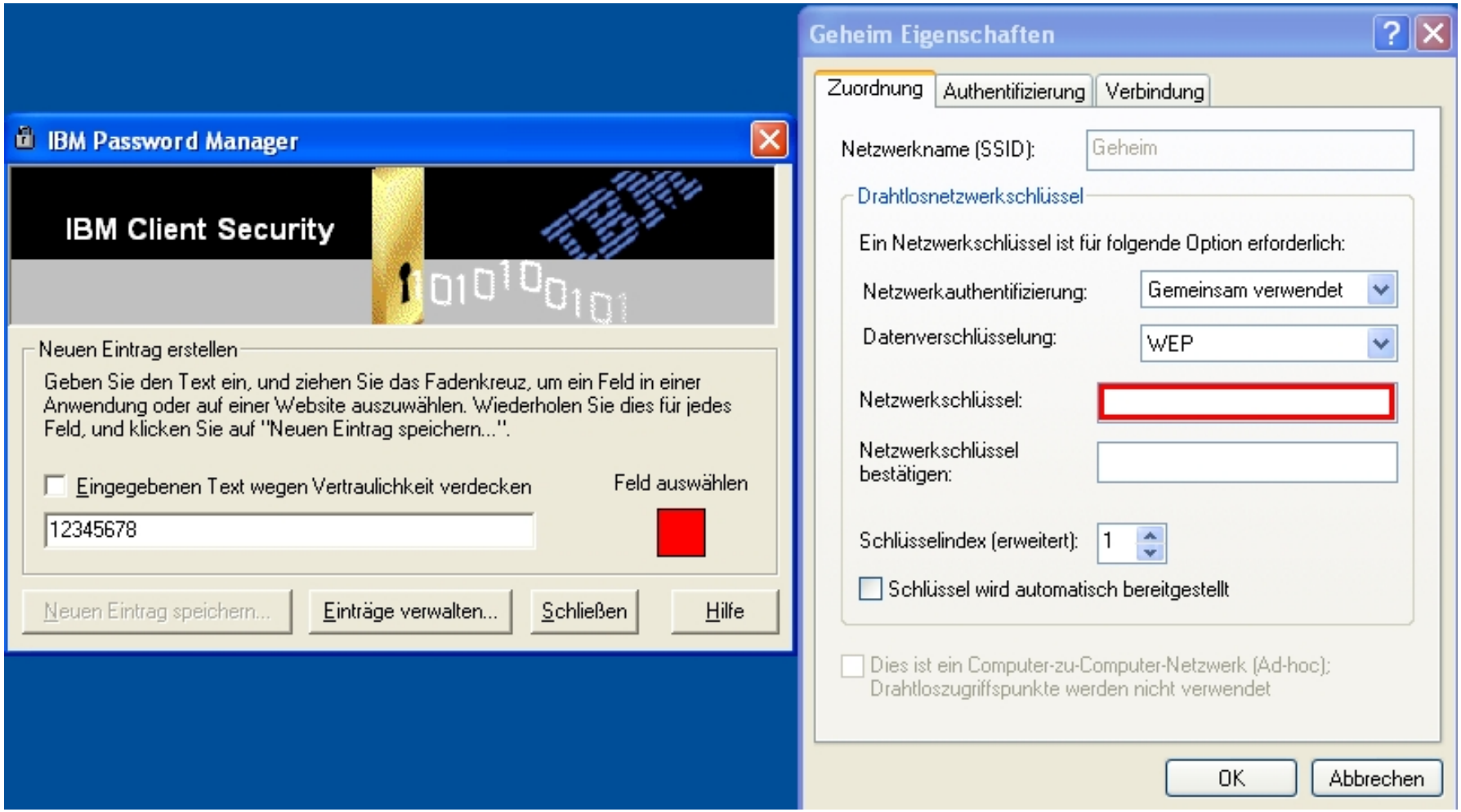
IBM Linux-Paket - Befehle



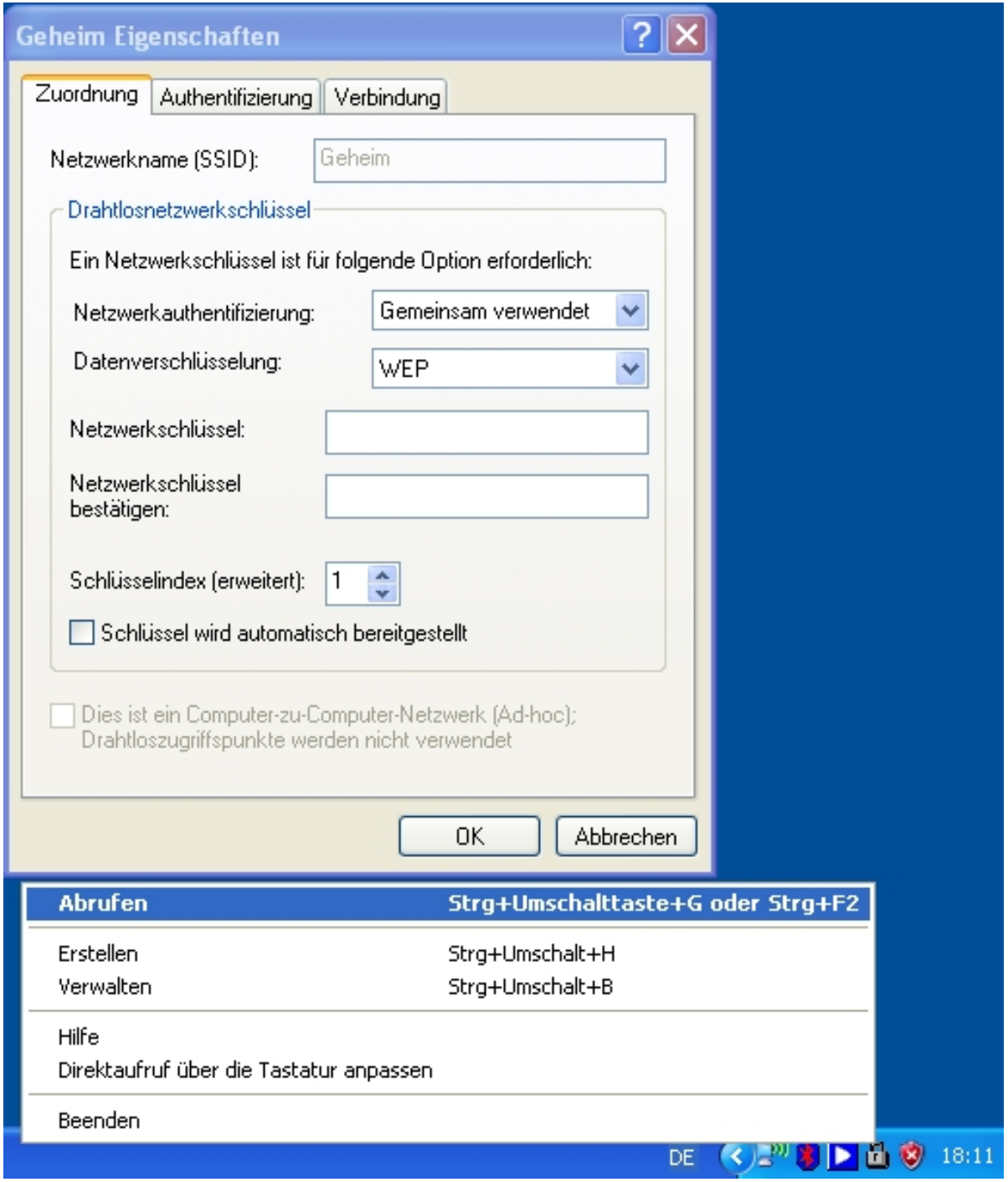
IBM Client Security



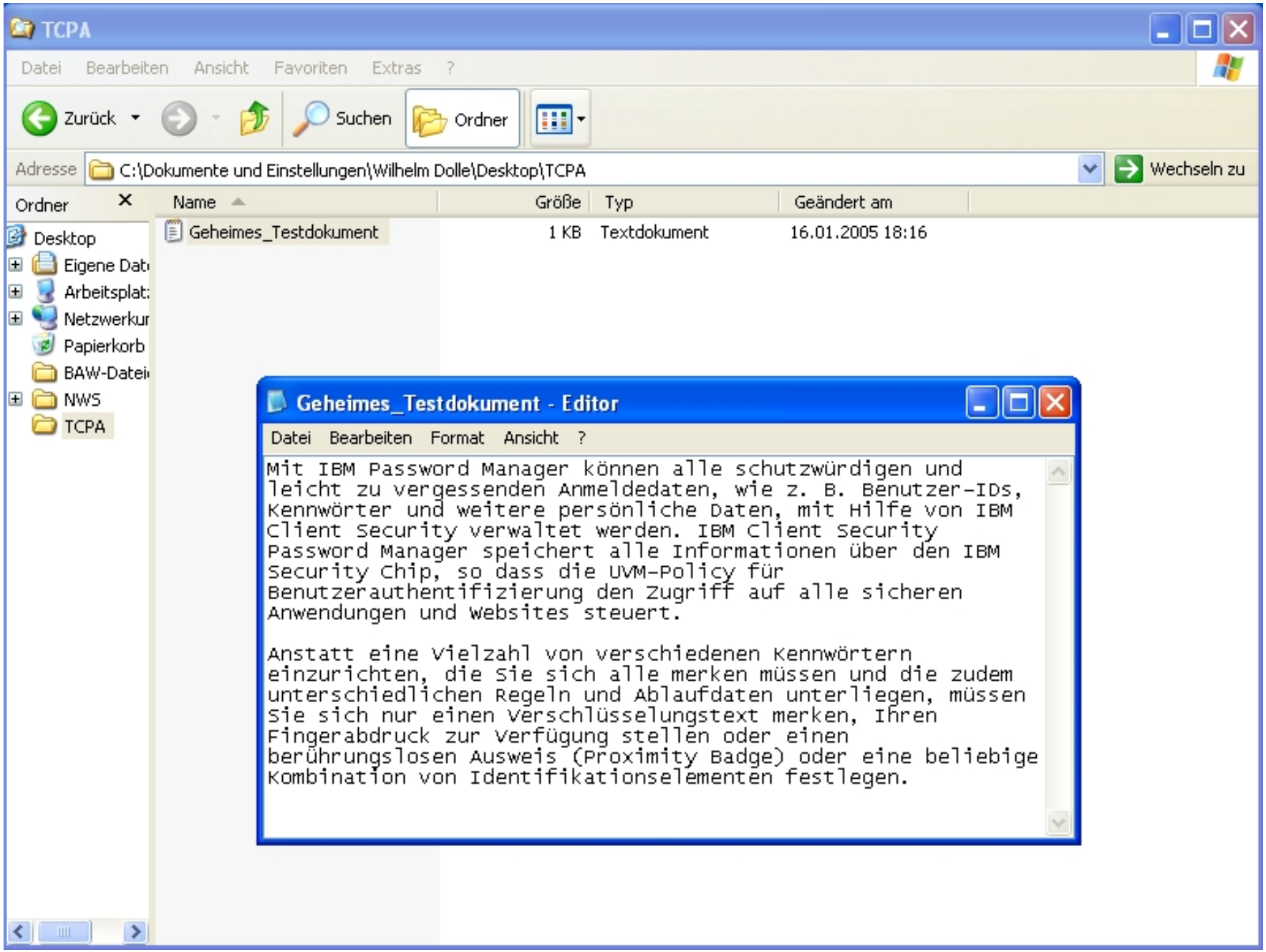
IBM Password Manager (Capture)



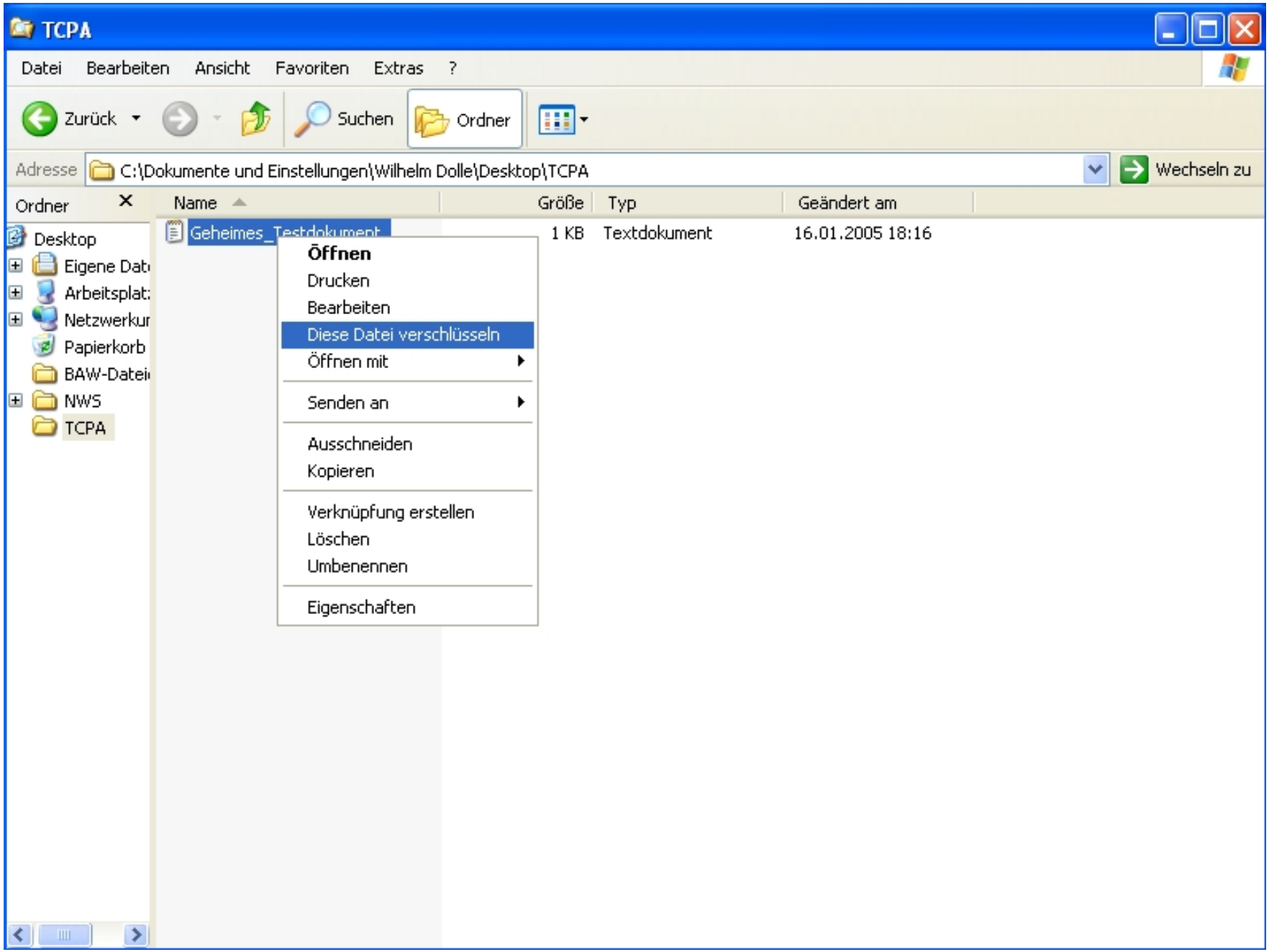
IBM Password Manager (Paste)



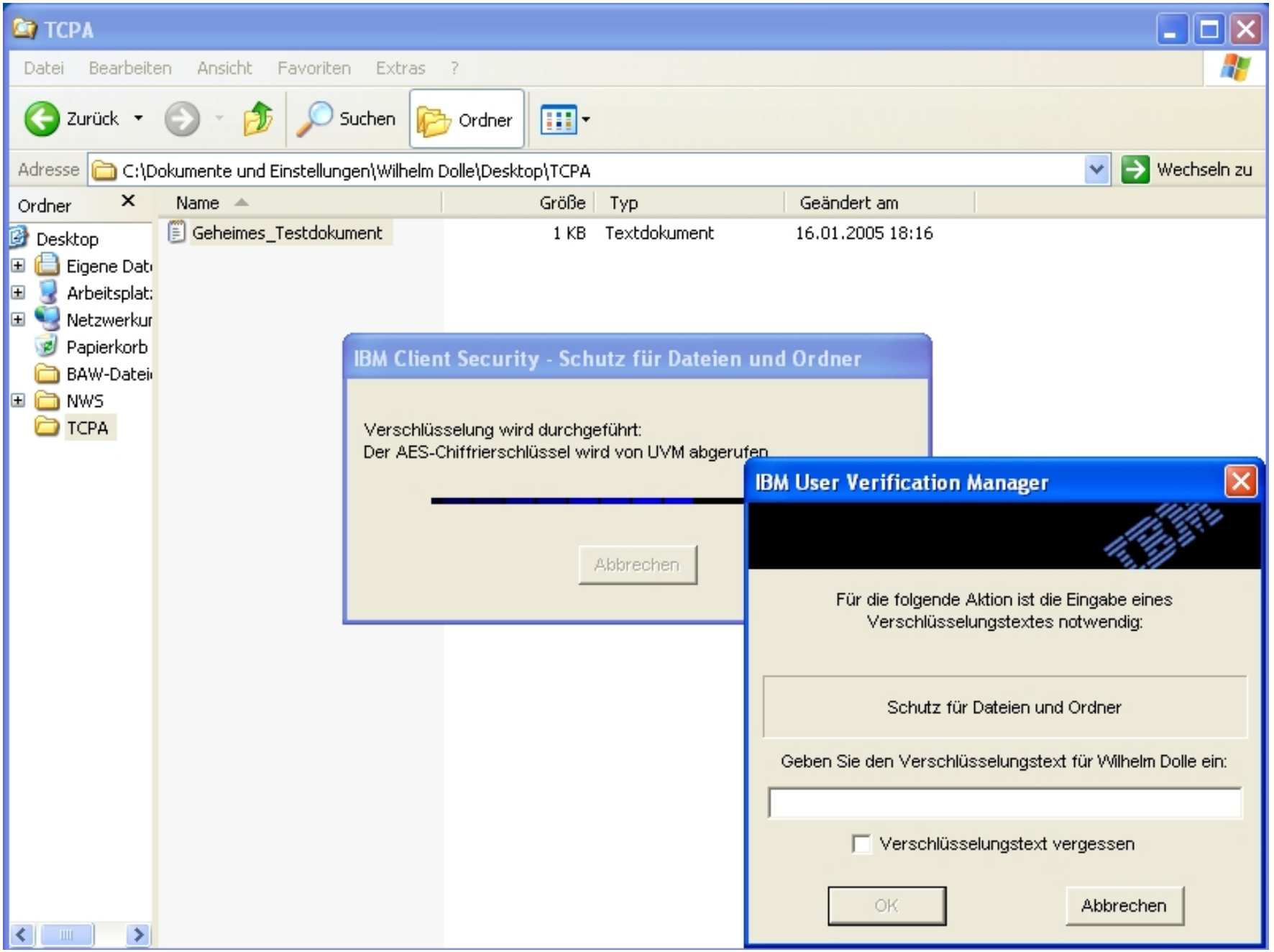
IBM Client Security (Dateiverschlüsselung)



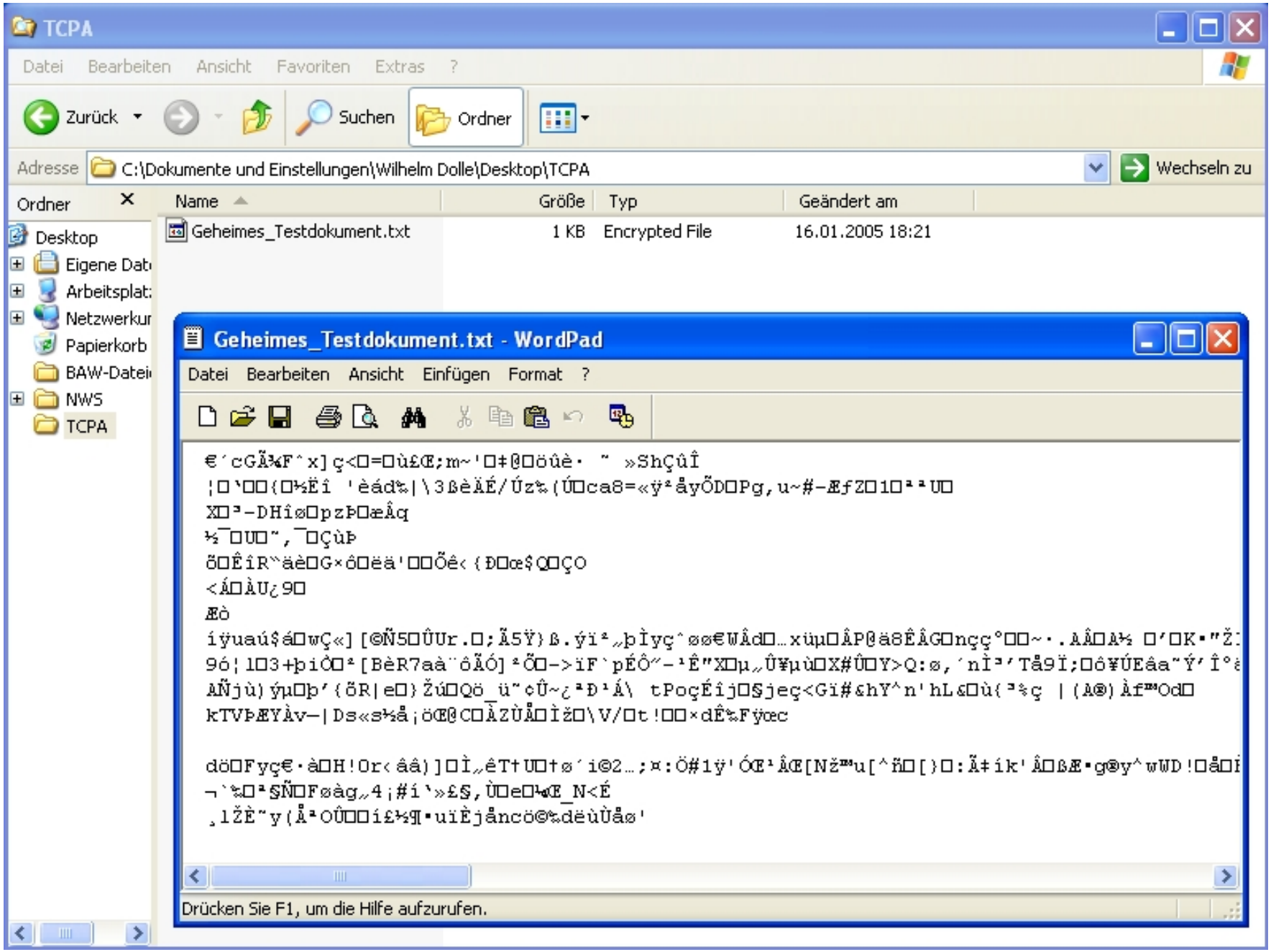
IBM Client Security (Dateiverschlüsselung)



IBM Client Security (Dateiverschlüsselung)



IBM Client Security (Dateiverschlüsselung)



Weitere Projekte (I)

- **IBM tcgLinux – TPM-based Linux Run-time Attesttation**
  - Erweitert Integritätsprüfung vom Boot-Prozess auf alle geladenen Programme bzw. Konfigurationsdateien
  - Anfragendes System benötigt Hash-Wert-Datenbank

- **Enforcer Linux Security Module**
  - Linux Security Module (LSM)
  - Baut auf den IBM-Treibern für Linux auf
  - Gleicht beim Lesen / Laden von sensiblen Daten / Programmen Hash-Werte mit einer Datenbank ab
  - Datenbank signiert und versiegelt
  - Modifizierter LILO überprüft Kernel Image und Master Boot Record

Weitere Projekte (II)

- **PERSEUS**
  - Security-Softwareschicht kontrolliert zu Schutz von sensiblen Anwendungen und Daten kritische Hardware-Ressourcen (auch das TPM)
  - Baut auf L4-Microkernel auf
  - Codebasis von PERSEUS maximal 100.000 Zeilen
- **European Multilateral Secure Computing Base (EMSCB)**
  - Vorschlag für eine offene Computing Platform
  - Soll PERSEUS, TPM und herkömmliche Betriebssysteme kombinieren

Forderungen von Kritikern

- **Endorsement Key austauschbar**
  - Bereits in TPM Spezifikationen 1.2 enthalten
  - Für kleine Organisationen nicht sinnvoll einsetzbar
- **Direct Anonymous Attestation**
  - Bereits in TPM Spezifikationen 1.2 enthalten
  - Beliebig viele anonyme Zertifikate
  - Unlinkbarkeit
- **Vollständige Kontrolle über alle TPM-Schlüssel (CCC)**
- **Owner Override (EFF)**
- **Internationale und unabhängige Kontrolle des TPMs muss möglich sein (CPU-Integration?)**

Fazit

- Rechteinhaber können über wirksames (hardware-basierendes) DRM Inhalte in digitaler Form veröffentlichen (und vermarkten)
- Anwender werden DRM nur einsetzen (und dafür bezahlen) wenn es einfach und sicher zu benutzen ist
- Interessen des Anwenders vs. Interessen der Industrie (wer hat die Kontrolle über Inhalte und Hardware?)
- Die Verbreitungsfreiheit von Wissen könnte durch DRM (bzw. die TCG-Konzepte) eingeschränkt werden
- Es lohnt sich die Entwicklung bezüglich TCG / DRM im Auge zu behalten

Offene Fragen?

Vielen Dank für die Aufmerksamkeit!

Wilhelm Dolle, CISA, CISSP, BSI IT-Grundschutz-Auditor
Director Information Technology

iAS interActive Systems GmbH
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