Neues zum Thema Trusted Computing

Wilhelm Dolle
Director Information Technology
interActive Systems GmbH

12. Workshop des DFN CERT
„Sicherheit in vernetzten Systemen“
02./03. März 2005, Hamburg

Agenda

- Spezifikationen der Trusted Computing Group (TCG)
- Funktionen des Trusted Platform Module (TPM)
- Chancen – Potentieller Sicherheitsgewinn durch Trusted Computing
- Risiken
- Betriebssystem-, Hard- und Softwareunterstützung
- Forderungen von Kritikern

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

- **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 $/Jahr, kein Stimmrecht)
  - Seit Mitte 2004: „Industry Liaison Program“ (kein Stimmrecht und NDA)
- **Ziel: Entwicklung und Support von offenen Industriestandards für „Trusted Computing“ auf verschiedenen Plattformen (PC‘s, Server, Handys und PDA‘s)**

iAS

DFN CERT

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)

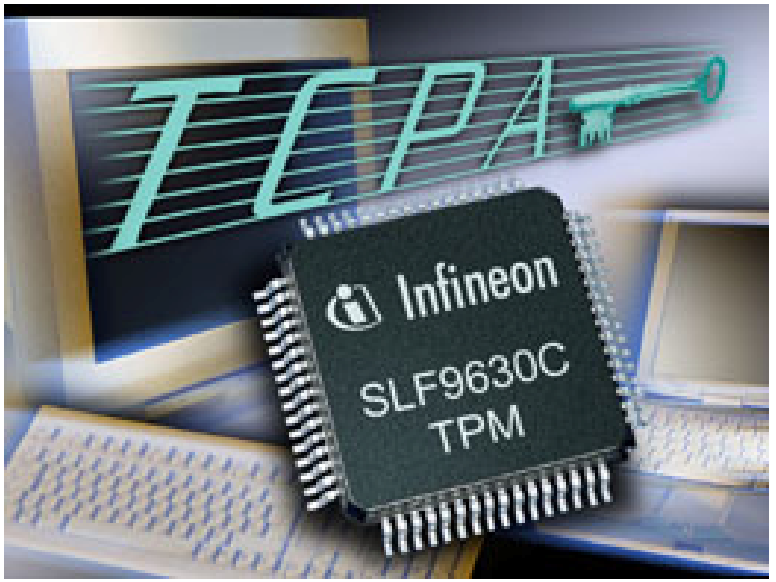
- TCG TPM Specification Version 1.2 (November 2003)
  - Design Principles
  - Structures of the TPM
  - TPM Commands

iAS

DFN CERT

TPM (Trusted Platform Module)

- **Nach US-Senator Fritz Hollings benannter Prozessor „Fritz Chip“**
- **Chip auf Motherboard**



- **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		

Aktivieren und Löschen des TPM

- **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

Designpunkte der TCPA-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“

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
- **Vergleich zu Smart-Cards**
  - TPM authentifiziert Plattform
  - Smart-Card authentifiziert Benutzer

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)

- **TPM nach 1.1b Spezifikation erhältlich von**
  - Atmel, Infineon, National Semiconductor
- **Konforme Systeme werden unter anderem ausgeliefert von**
  - IBM (ThinkPad Notebooks, NetVista Desktops), HP
- **Über 16 Millionen Motherboards mit TPM (1.1b) ausgeliefert (Embedded Security Subsystem 2.0)**
- **Zukünftig unter anderem**
  - TPM integriert in I/O-Chip mit Ports für Tastatur, Maus, Drucker, Floppy, RS-232 (National Semiconductor)
  - Frühjahr 2005: Trusted-Mode Keyboard Controller (Intel, MS)
  - Herbst 2005: USB-Security-Extension (Intel, MS)
  - TPM in CPU (Intel)

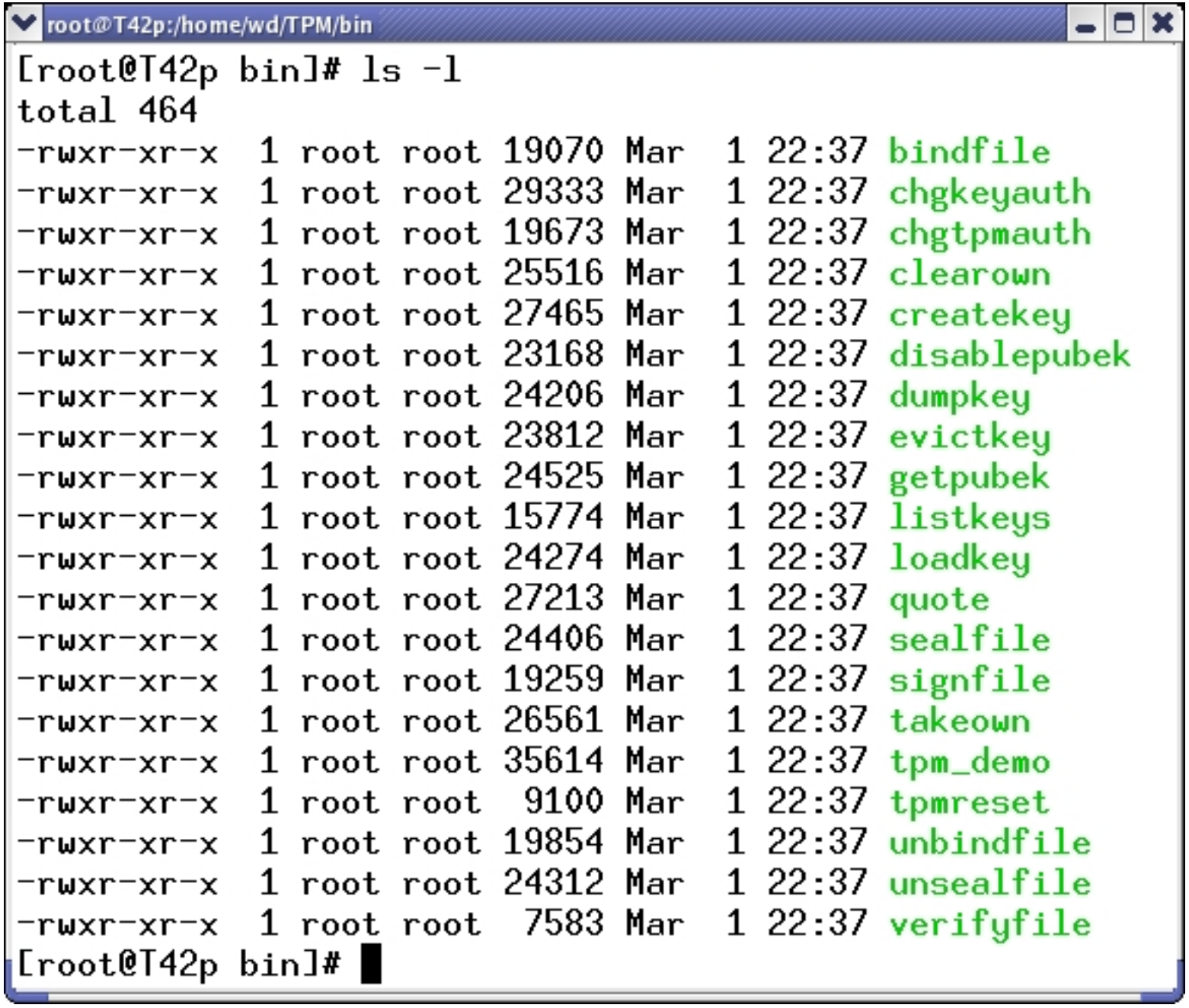
Palladium / NGSCB (Next Generation Secure Computing Base)

- **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 einen Benutzer- und Kernel-Modus
  - Nexus im Kernel-Modus in der RHS
- **WinHEC 2004**
  - LHS bleibt nahezu unverändert
  - RHS wird komplett überarbeitet
  - Compartment-Modelle?
- **Womit überrascht uns Microsoft in 2005?**
- **Microsoft Longhorn angekündigt für 2006**

Status Quo (Software)

- **Kommerzielle Applikationen mit Support**
  - RSA, Checkpoint, Verisign, ...
- **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)

Linux: Befehle



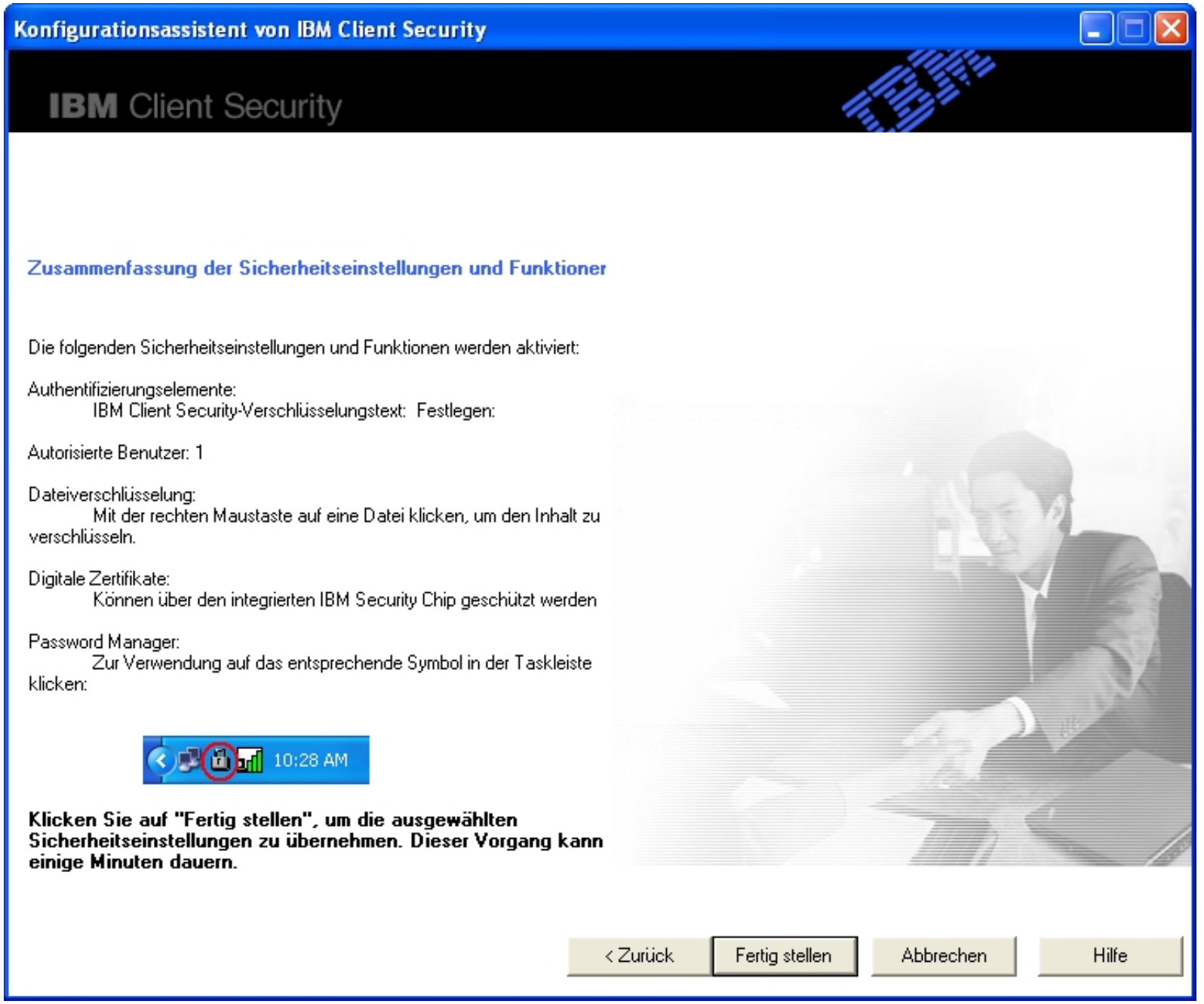
Linux: Inhalt eines TPM-Chips (PCR)

root@tcpa:~/TPM/examples - Shell - Konsole

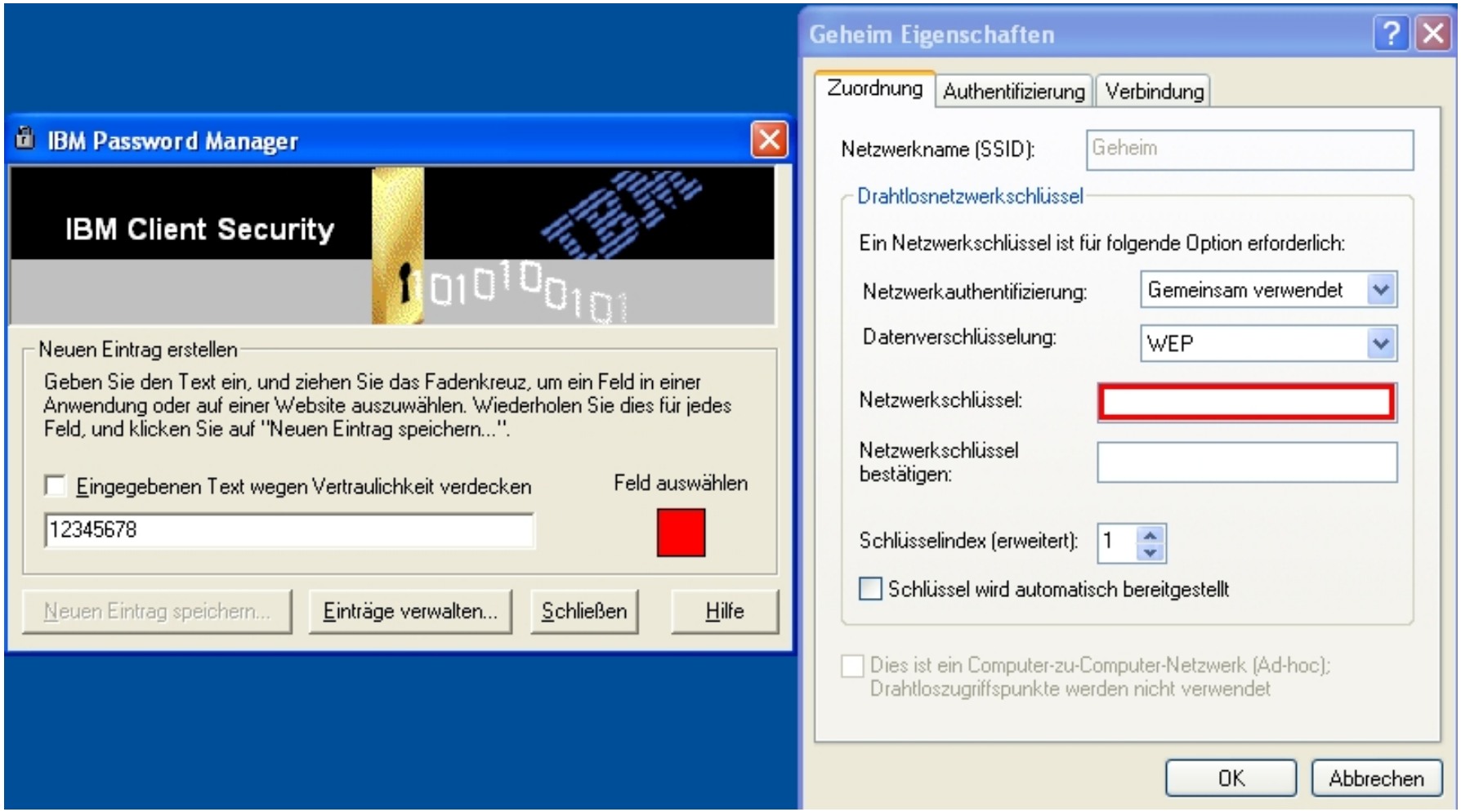
Session Edit View Bookmarks Settings Help

```
[root@tcpa examples]# ./tcpa_demo
TPM successfully reset
TPM version 1.1.0.6
16 PCR registers are available
PCR-00: C5 09 63 65 C1 94 E1 03 DC C7 A6 5F C6 B8 89 B7 47 9D 80 05
PCR-01: 67 53 1E F3 50 CE 1D AB BE 27 2B 77 2C 8B 3A 37 81 2D E1 DE
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: AE 18 0F 64 3B BA 3A 78 41 7D 6B B5 10 68 52 AE 2A D6 4B BA
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 00
PCR-09: 00 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 00
PCR-11: 00 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 00
PCR-13: 00 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 00
PCR-15: 00 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@tcpa examples]#
```

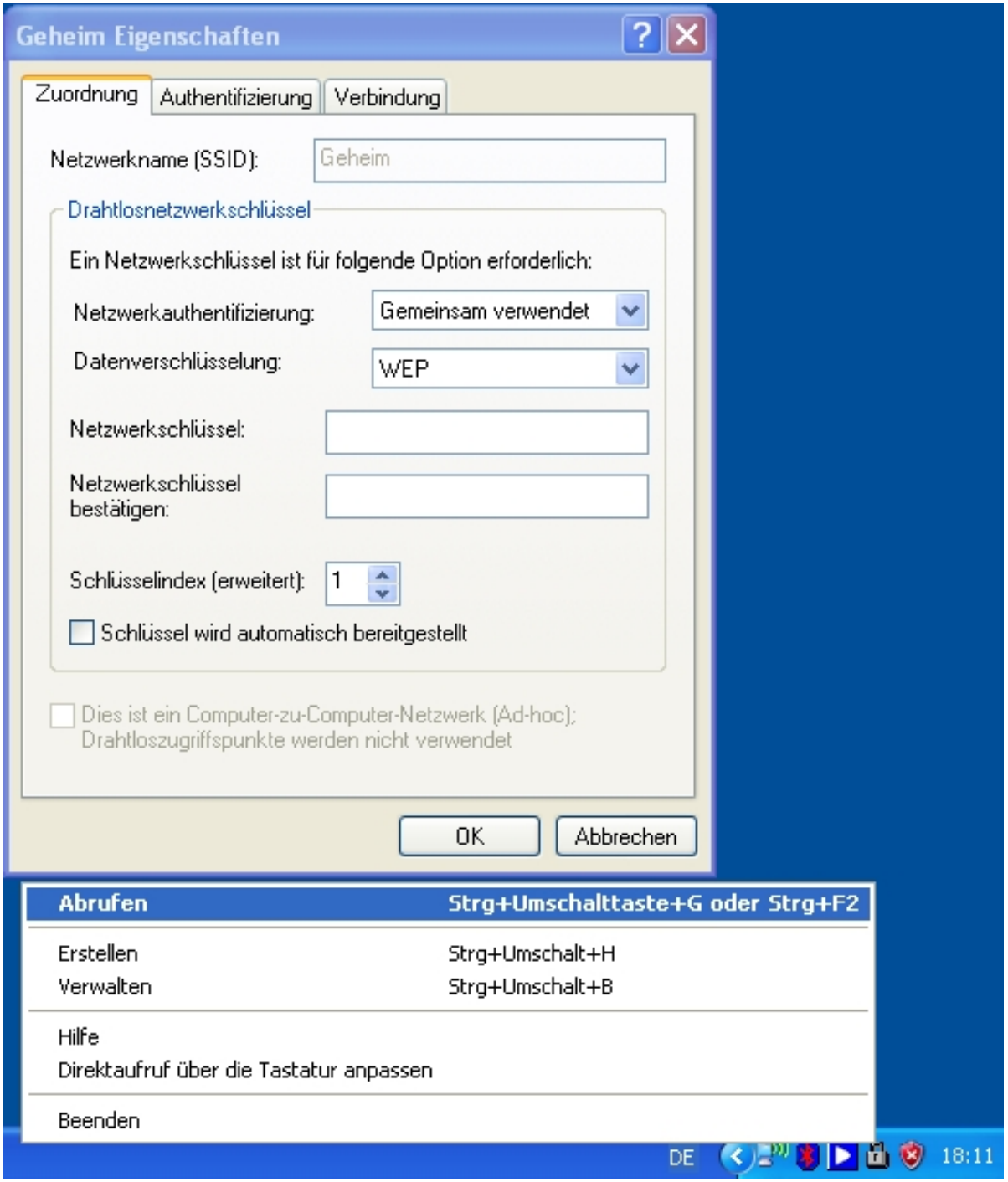
IBM Client Security



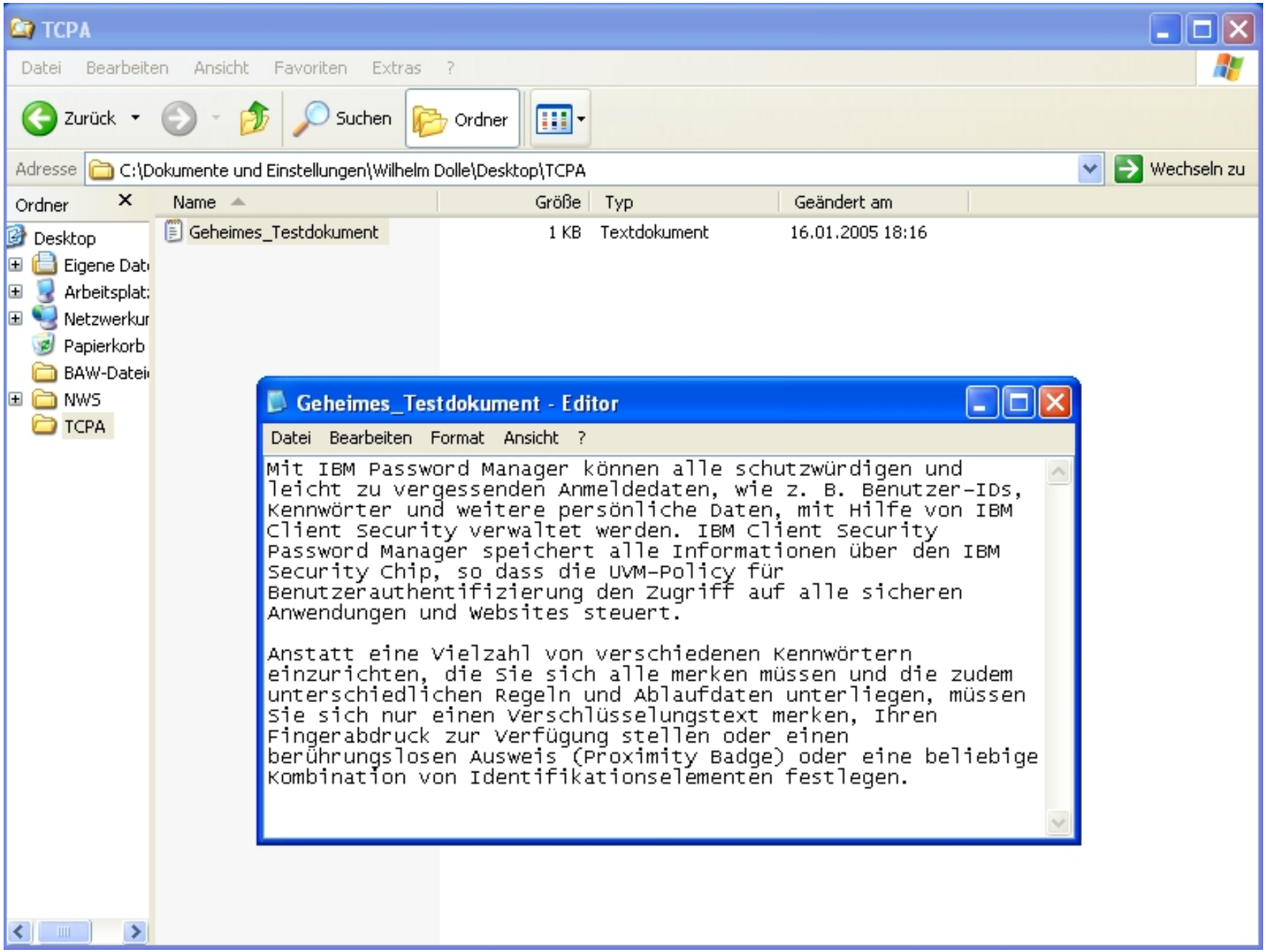
IBM Password Manager (Capture)



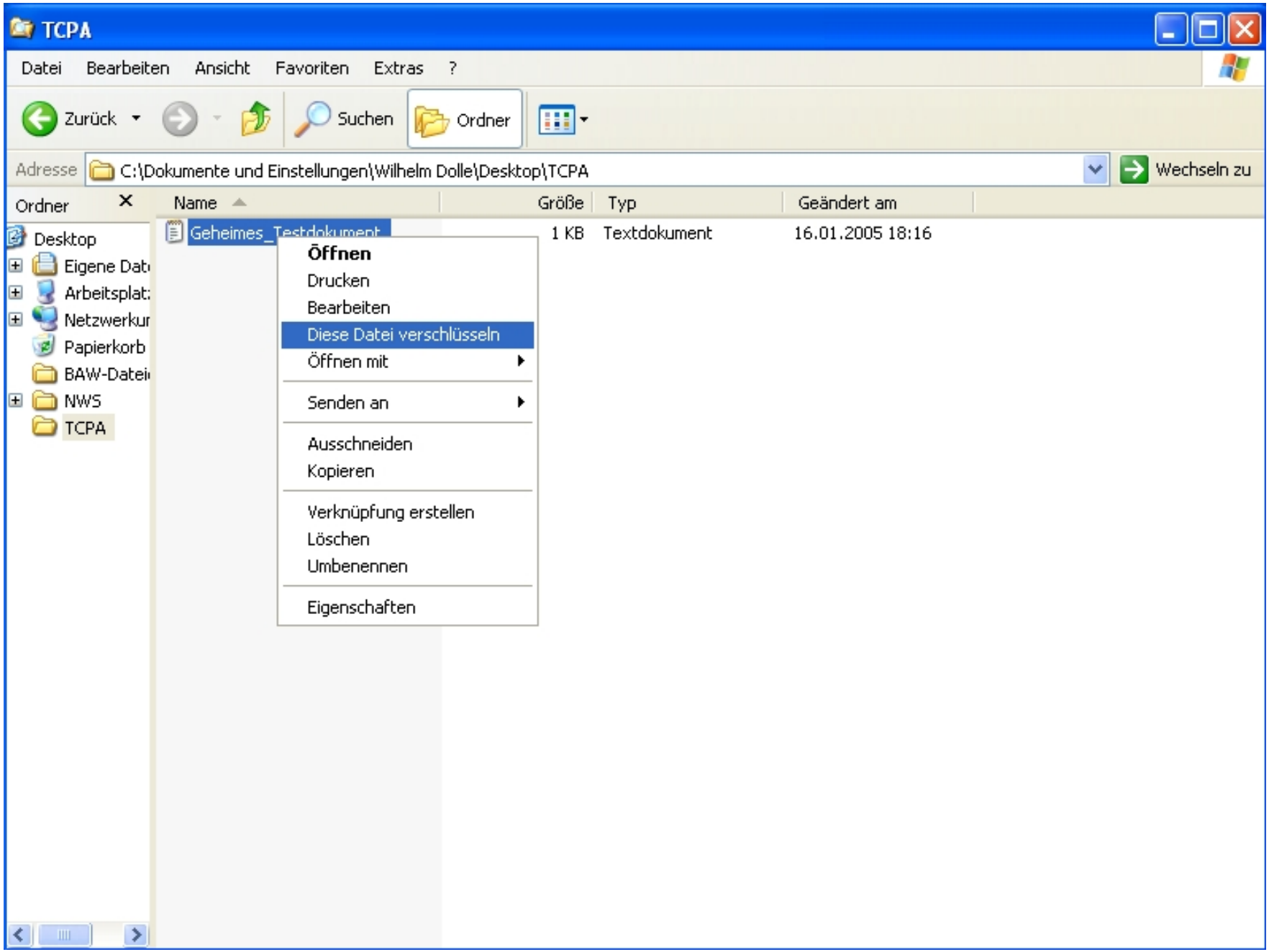
IBM Password Manager (Paste)



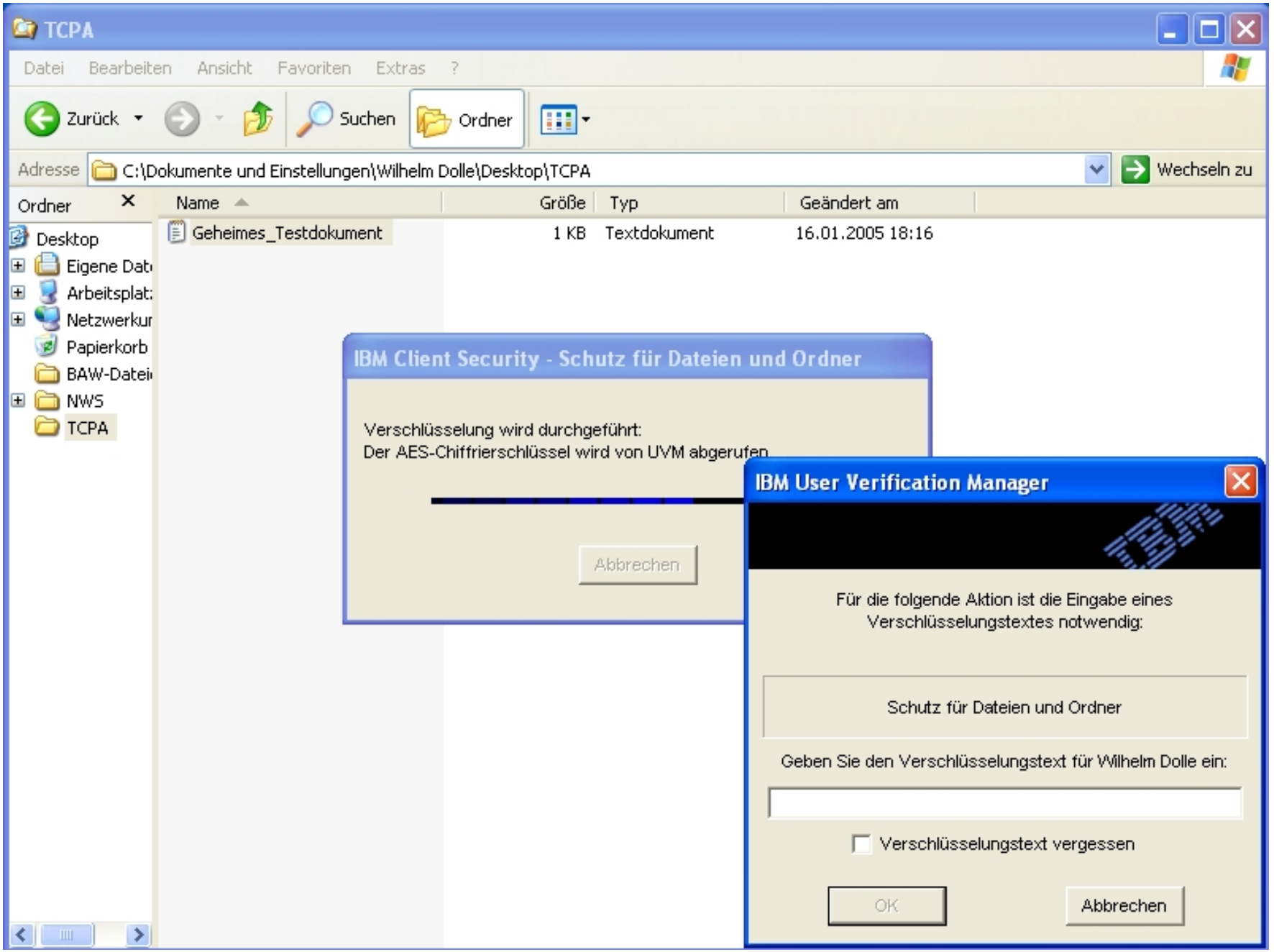
IBM Client Security (Dateiverschlüsselung)



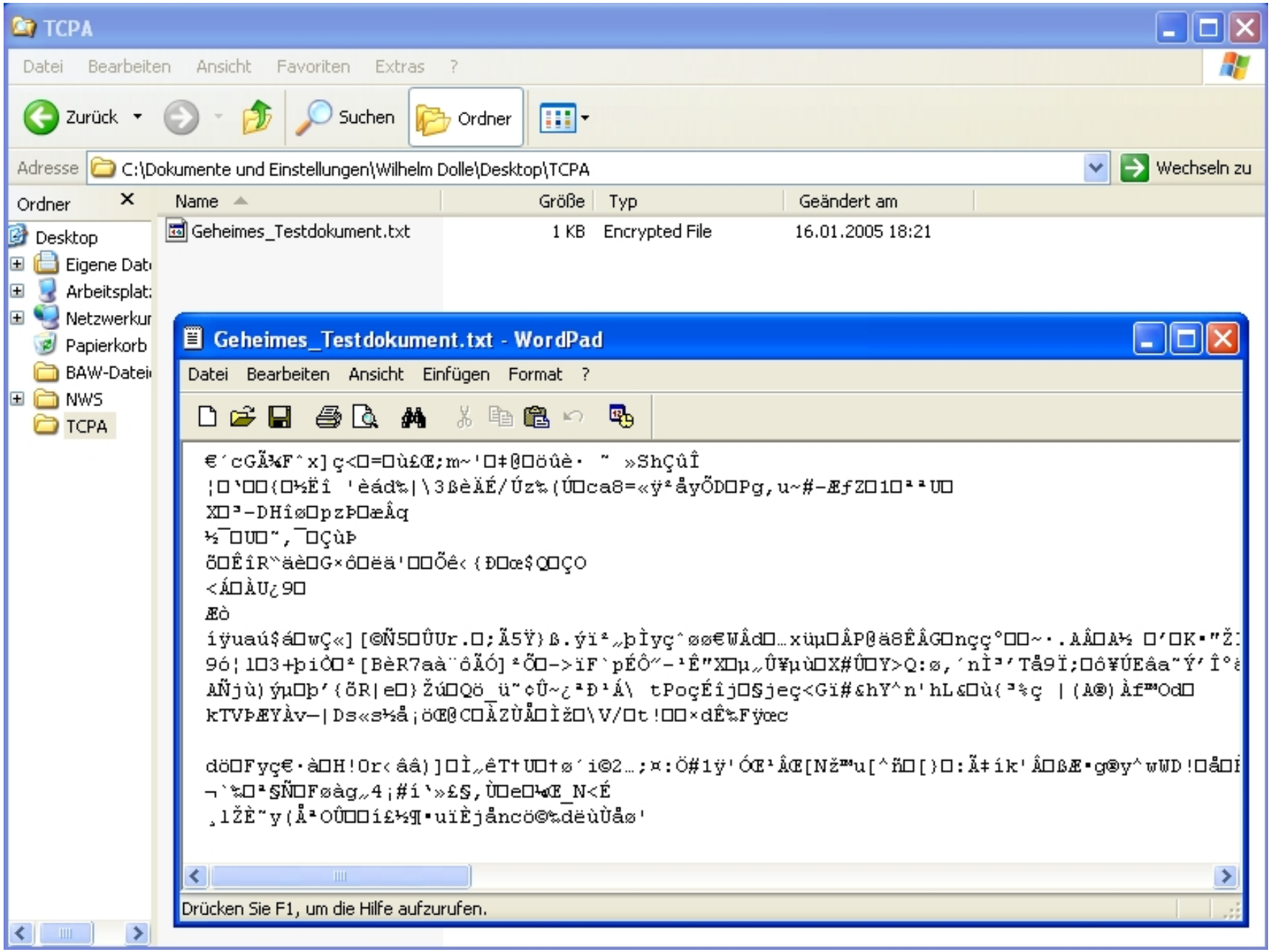
IBM Client Security (Dateiverschlüsselung)



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?)**

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