

---

**Identitäten in elektronischen Geschäftsprozessen**  
**Fraunhofer SIT, 20. September 2006**

**Welche Rolle spielt die TCG für Identity Management?**



**Alexander W. Koehler, CEO, ICT Economic Impact**

- Zum Workshop: Identitäten in elektronische Geschäftsprozessen
- Es sollen die Ziele aus unternehmensübergreifenden Geschäftsprozessen erreicht und ein Beitrag zur Investitionssicherheit bei der Implementierung von Identity Management-Lösungen geleistet werden.
- Ziele sind etwa
  - - Steigerung der Produktivität und Senkung der Kosten
  - - Verbesserung von IT Services  
(ausreichende Zugriffs- und Zugangssicherung)
  - - Einhaltung bestehender Regularien
- Trusted Computing und Identity Management
  - Anwendungsszenarien für Trusted Identity
  - **Welche Rolle spielt die TCG für Identity Management?**

- Workshop Agenda
  - Behauptung
    - TCG ist die Grundlage für den Umgang mit Identitäten
  - Beleg: Maßnahmen
  - Das Gremium TCG
  - Beleg: Implementierungen
  - Zusammenfassung
  
- *Definitionen:*
  - *Identitäten: Benutzer bezogene Identitäten*
  - *Berechtigungsnachweise: Credentials. Beinhaltet: kryptografische Schlüssel, Passphrasen, Authentifizierungstoken, Cookies etc.)*
  - *CMD: Converged Mobile Devices (Handy & PDA)*
  - *TCG: Trusted Computing Group<sup>TM</sup>*
  - *TPM: Trusted Platform Module*

- Es geht um den Umgang mit Identitäten
  - Technik
  - Mensch
- Realisierung: Grundlagen
- Realisierung: Produkte
  
- Allgemeine Prinzipien zur Konstruktion sicherer Systeme\*
  - Erlaubnisprinzip
  - Vollständigkeit
  - Prinzip der minimalen Rechte
  - Akzeptanz
  - Offener Entwurf
  - Bester Platz im Design

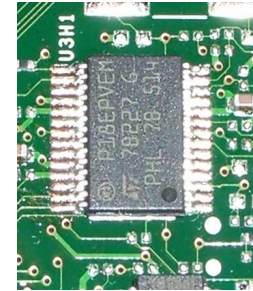
\* Saltzer and Schroeder, IEEE, March 1975

- Identity Management ist ein Konzept
  
- Identitäten sind bewegliche Objekte
  - Ihre Existenzberechtigung entsteht dadurch, daß diese an
    - einem anderen Ort
    - zu einem anderen Zeitpunkt
    - außerhalb der eigenen Organisation
    - in einer anderen technischen Umgebung
  - verwendet / abgefragt werden
  
- Mit TCG-Technologie wird dabei sichergestellt, daß
  - dies in einer möglichst sicheren Umgebung geschieht
  - Berechtigungsnachweise, die zum Schutz von Identitäten eingesetzt werden, hochwertig geschützt sind
    - am Ursprungs- und am Zielspeicherort
    - während der Verarbeitung
    - auf dem Übertragungsweg

- Behauptung
  - TCG ist die Grundlage für den Umgang mit Identitäten
    - Sicher
    - Akzeptiert
    - Unternehmensfähig
    - Ökonomisch
  
- Belegt mit 8 konkreten Maßnahmen
  
- Belegt mit konkreten Implementierungen

## ➤ 8 Maßnahmen

## Qualität der Schlüsselgenerierung



Echter Zufallszahlengenerator

- Konstante Qualität: Systemsoftware und Applikationen
- Massenhafte Verbreitung → Massenhafte Verfügbarkeit qualitativ hochwertiger Schlüssel



➤ TPM: Zufallszahlengenerator (TRNG)

### Speicherung von Schlüsseln, geschützt durch Hardware, und damit vor Softwareangriffen geschützt

- Alle Anwendungen, die schützenswerte Berechtigungsnachweise, also insbesondere Identitäten, verwenden profitieren von TCG.
- Identitäten werden verschlüsselt gespeichert. Die Schlüssel sind durch Hardware (TPM) geschützt
  - an den Endpunkten der Kommunikation Client←→Client
- Identitäten werden verschlüsselt übertragen. Die Schlüssel sind durch Hardware (TPM) geschützt



- TPM: Hardware Schutz
- TCG: Definition der Root of Trust for Storage (RTS)

## Maßnahme 3

---



### Exponieren von Identitäten (Berechtigungs nachweisen), im laufenden Betrieb

- Aktuelles Hardware Design
  - Arbeitsintensive Sicherheitsaufgaben: CPU
- Konsequenz
  - Der Integritätsstatus ist
    - permanent zu überwachen
    - nicht manipulierbar zu hinterlegen
    - abzufragen, bevor empfindliche Komponenten exponiert werden
- Verwertung des Integritätsstatus zwecks Entscheidung
  - Lokal
  - Domäne
  - Remote



### Trusted Network Connect

- TPM stellt sicheren Speicherplatz für Messwerte bereit
- TCG definiert Protokolle

### Exponieren von Identitäten (Berechtigungsnachweisen) während des Bootvorgangs

- Absicherung des Boot Prozesses
  - Maßnahme: Schritt weises Öffnen des BS nachdem Prüfpunkte unter Nachweis der korrekten Messwerte passiert werden durften
  
- Status:
  - Weltweit verbreitetes PC-Design: BIOS und Betriebssystem
  
- Ergebnis: Mit hoher Wahrscheinlichkeit ist sichergestellt, daß die bereitgestellte Arbeitsumgebung integer ist
  - Identitäten können exponiert werden

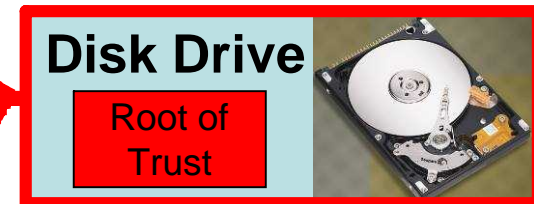
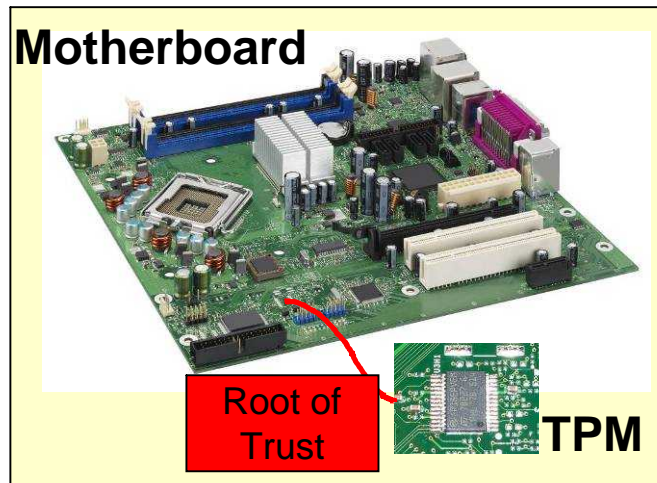


- TCG definiert Schnittstellen zu BIOS und OS
- TPM ist Sicherheitsanker für Messwerte (RTM)

# Maßnahme 5

## Sichere Kommunikation mit Komponenten innerhalb und außerhalb des PCs: Festplatten

- Speicherort für Identitäten
- Transportmedium für Identitäten
- Archivierung



### Secure Communications

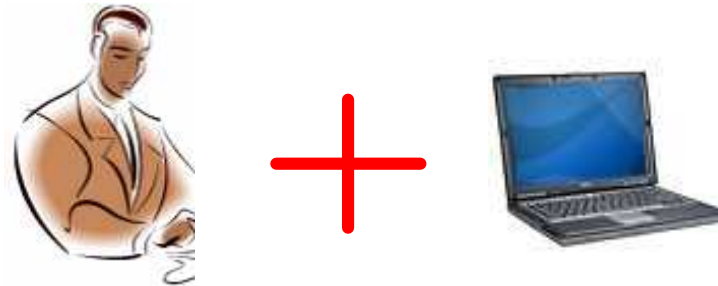
**TRUSTED SEND**  
(Protocol ID = 0 .....)  
**TRUSTED RECEIVE**  
(Device Credential, ....)



➤ TCG definiert die Inhalte der Protokolle (Payload)

## Maschinenidentität

- Der Besitzer verleiht dem PC eine Maschinenidentität
- Am Ende des Lebenszyklus wird diese gelöscht
  
- Mehrfaktor-Authentifizierung
- Zusätzliche Absicherung von Identitäten
  - Phishing



- TPM: Maschinenidentität

### Identitäten in CMDs

- Grundsätzlich gleiche Schutzmechanismen wie bei PCs unter Berücksichtigung
  - BS-Design Spezifika
  - Hardware
  
- Spezifische Anwendungen:
  - Robuste DRM Implementierung
  - SIMLock / Personalisierung der Geräte
  - Sicherer Kanal zwischen den Geräten und dem UICC
  - Mobiles Ticketing / Mobiles Bezahlen
  
- Unterschied gegenüber PC und TPM:
  - Mehrfache MTMs pro Gerät ← → Mehrfache Stakeholder



➤ Industriestandard Mobile Trusted Module (MTM)

Sicherung von Berechtigungsnachweisen, welche Identitäten schützen

Wiederherstellung von Berechtigungsnachweisen, welche Identitäten schützen

Erfassung aller möglichen Szenarien

- Ausfall von Hardware
  - TPM
  - Motherboard
  - Festplatte
- Übertragung von einem PC auf einen weiteren
  - Richtlinien
- Automatisiert durchführbar, auch für große PC-Bestände



➤ Definition Sicherungs- und Wiederherstellungsmaßnahmen

- Behauptung
  - TCG ist die Grundlage für den Umgang mit Identitäten
    - Sicher
    - Akzeptiert
    - Unternehmensfähig
    - Ökonomisch

➤ **Belegt mit 8 konkreten Maßnahmen**

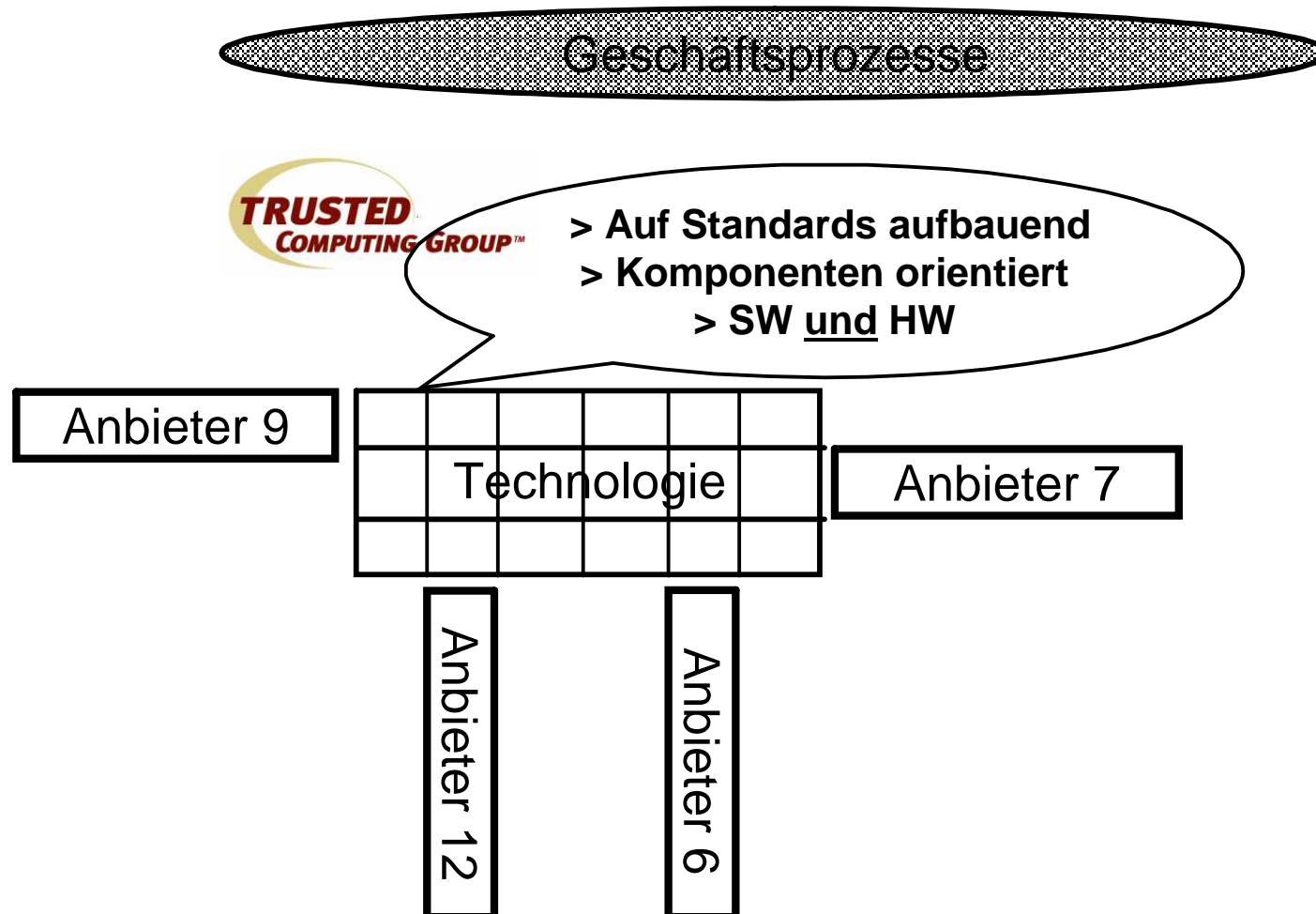
➤ Belegt mit konkreten Implementierungen



- Die Trusted Computing Group™ (TCG) ist ein Standardisierungsgremium, bestehend aus Computer- und Geräteherstellern, Softwarehäusern und anderen Firmen, deren Geschäftszweck damit verbunden ist, die Sicherheit von Computersystemen und Netzen Plattform und Geräte übergreifend zu verbessern.
- Gegründet: 2003; 140 Mitgliedsfirmen und Institutionen (2006).
- Die Aufgabe der TCG ist es, offene, Hersteller unabhängige Spezifikationen für einen Industriestandard zu Computereinheiten und Softwareschnittstellen über eine Vielzahl von Plattformen hinweg zu entwickeln.

# Trusted Computing Group™

In 2003 wurden die Grundlagen für eine IT-Sicherheit gelegt, die es erlaubt, Prozess orientierte **Strukturen** auf Produkt**strukturen** abzubilden: Sicherheitsarchitektur.



## Das Ecosystem TCG™



- Ein **Ecosystem** ist eine Zusammenstellung von Organisationen (Firmen, Institutionen), welche sich ergänzen und im Zusammenspiel eine komplette Lösung oder Industrie bilden.
  - Struktur und Arbeitsteilung: Welche Funktionen werden **wo** (im BS, in der Applikation, Ebene/Schicht, etc.) und **wie** (Software, Hardware) optimal (Sicherheit, Wirtschaftlichkeit) und von **wem** (Kernkompetenz) realisiert.
  - Standard
  - Modularität
  - Flexibilität
    - Investitionssicherheit für Anwender

**TCG: Das Rahmenwerk für IT-Sicherheit in einer vernetzten Welt**

## ➤ Implementierungen

## Brute Force-Attacken auf Kerberos-Pakete

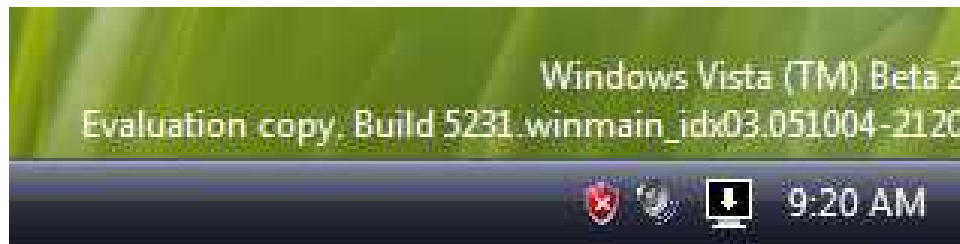


- Alternative Problemlösungen
  - IPsec
  - Smartcard basierter Windows™ Log-On
    - PIN: Zugriff auf privaten Schlüssel
  - TPM
    - Biometrie: Zugriff auf private Schlüssel

\* Quelle: Windows IT Pro 7/2006

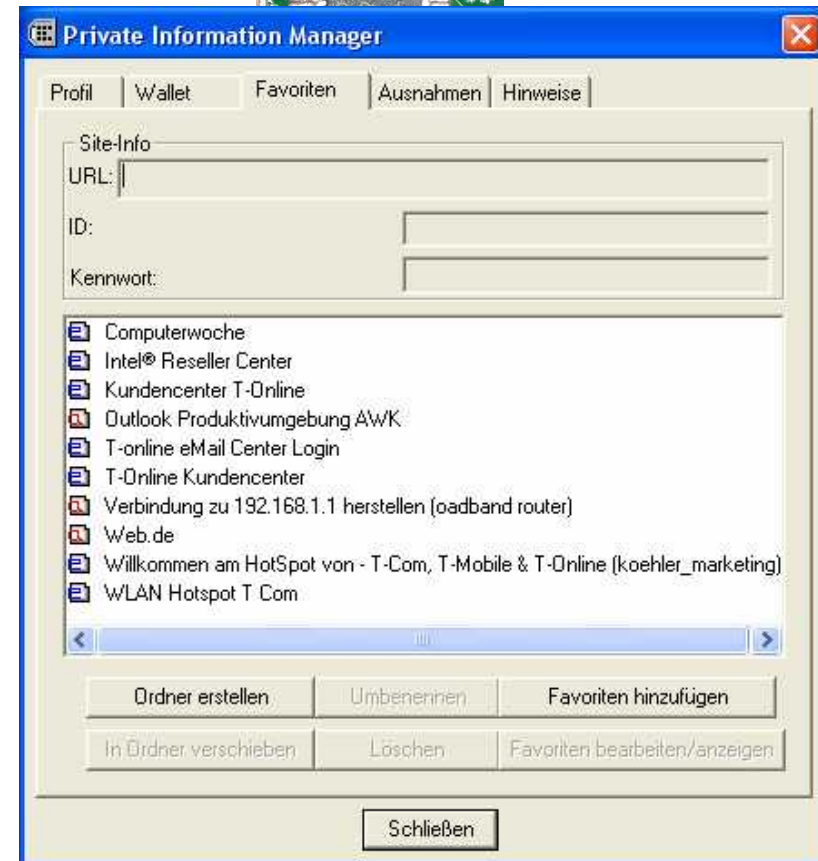
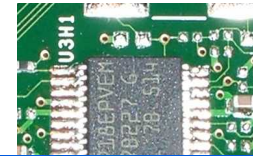
### Exponieren von Identitäten (Berechtigungsnachweisen) während des Bootvorgangs

- Umfassender Schutz des BIOS und Betriebssystems
  - Während des Bootens werden Identitäten schrittweise im Zuge von Integritätsmessungen verfügbar gemacht: TPM
  - Übergang „BIOS → OS → Betrieb“ durch TCG-Prozess *Secure Boot* kontrolliert
  - Microsoft® Vista™ Bitlocker: Start aus verschlüsseltem Laufwerk C:\ heraus
- Finaler Zustand
  - CPU führt Aufgaben unter Verwendung von Identitäten erst dann durch, wenn von einer integrieren Plattform ausgegangen werden kann



# Implementierung C

- Schutz von Identitäten durch Hardware
- Benutzt den TPM um sicher Passwörter, Benutzernamen und persönliche Daten zu speichern
- Anmeldung an Webseiten
  - Web Forms
  - Neu aufkommende Anmelde-Daten werden automatisch erkannt und erfasst
- Anmeldung an Applikationen mit gleichem Funktionsumfang
- Vielzahl von Identitäten sicher und produktiv handhabbar

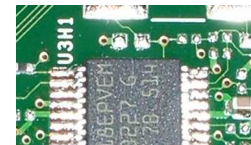


**EMBASSY®** Private Information Manager \*

\* Produkt der Wave Systems Corp.

## Authentifizierung im Zusammenspiel mit TPM

- Hohes Sicherheitsniveau: wie Smartcard
  - Anstelle von <PIN> tritt <Biometrie>
    - Vollständigkeitsprinzip
      - Praktikabel
    - Benutzerfreundlich
      - Notebook: eingebaut
    - Ökonomisch



**EMBASSY® Security Center \***



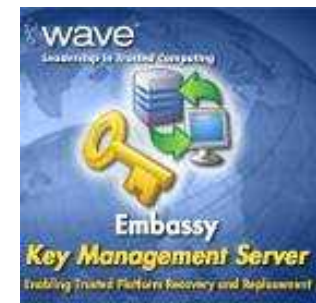
\* Produkt der Wave Systems Corp.

## Sicherung und Wiederherstellung von Berechtigungsnachweisen, welche Identitäten schützen

- Erfassung aller möglichen Szenarien
  - Ausfall von Hardware
    - TPM
    - Motherboard
    - Festplatte
  - Übertragung von einem PC auf einen weiteren
  - Richtlinien
  - Automatisiert durchführbar, auch für große PC-Bestände
- Der KTM archiviert und stellt alle migrierbaren Schlüssel, so auch diejenigen, die von Applikationen verwendet werden, wieder her



**EMBASSY® Key Transfer Manager \***  
**EMBASSY® Key Management Server \***



\* Produkte der Wave Systems Corp.

## Virtual Private Network

- VPN als Service für mittelständische Unternehmen
  - Bereitsstellung des Servers
  - EAP/TLS Authentifizierung: Zertifikate
  - Notebooks
    - Keine zusätzliche Hardware
    - Verwendung vorhandener Infrastrukturen
  
- Implementierung
  - TPM bestückte Notebooks mit Fingerabdruckleser
  - **EMBASSY**<sup>®</sup> Security Center \*: Biometrie
  - **EMBASSY**<sup>®</sup> KMS\*: Sicherung und Wiederherstellung der Zertifikate

\* Produkt der Wave Systems Corp.

- Behauptung
  - TCG ist die Grundlage für den Umgang mit Identitäten
    - Sicher
    - Akzeptiert
    - Unternehmensfähig
    - Ökonomisch



➤ **Belegt mit 8 konkreten Maßnahmen**

➤ **Belegt mit konkreten Implementierungen**

- **TCG ist die Grundlage für den Umgang mit Identitäten**
  - **Sicher**
  - **Akzeptiert**
  - **Unternehmensfähig**
  - **Ökonomisch**



[alexander.koehler@ict-economic-impact.de](mailto:alexander.koehler@ict-economic-impact.de)  
[www.ict-economic-impact.com](http://www.ict-economic-impact.com)