

# Trusted Computing - Die Sicherheitsplattform Turaya

→ Grundlagen, Aufbau und Anwendungen

**Gianfranco Ricci**

**Andreas Speier**

Institut für Internet-Sicherheit

Fachhochschule Gelsenkirchen

[www.internet-sicherheit.de](http://www.internet-sicherheit.de)

# Agenda

- **Problemstellung & Trusted Computing**
- **Sicherheitsplattform Turaya**
- **Anwendungsbeispiele**
- **Fazit**

# Agenda

- ***Problemstellung & Trusted Computing***
- **Sicherheitsplattform Turaya**
- **Anwendungsbeispiele**
- **Fazit**

# Trusted Computing

## → Idee und Funktionen (1/3)

### ■ *Idee*

→ Zusammenwirken von **vertrauenswürdigen Hardware- und Software-Sicherheitsmechanismen**

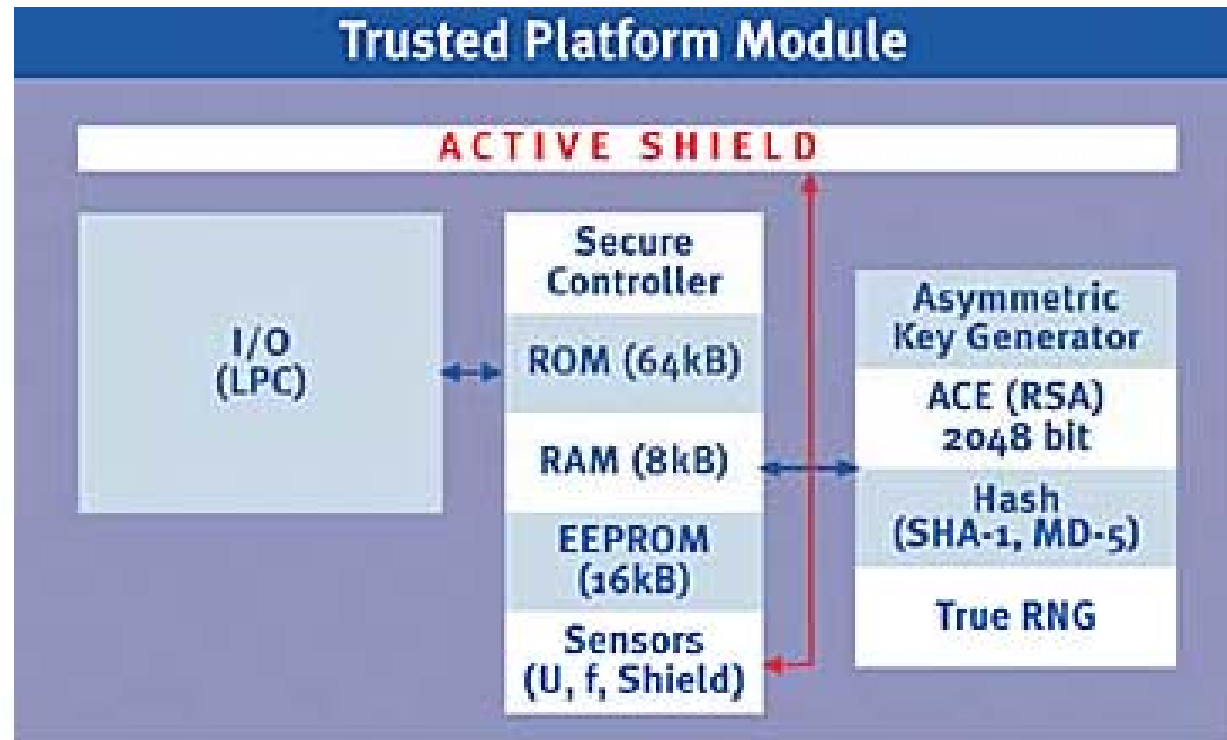
- Manipulationssichere Hardwarekomponente
- Überprüfung der **Integrität und Authentizität** von Rechnersystemen
- Sicherheit beim **Aufbewahren und Übertragen** von Daten
- Schutz vor **Malware** (Viren, Würmer, Trojaner, ...)#

→ **Verhält sich ein Rechnersystem für eine spezielle Aufgabe jedes mal so wie es erwartet wird, dann gilt das Rechnersystem als vertrauenswürdig.**

# Trusted Computing

## → Trusted Platform Module (TPM)

### ■ Funktionen des TPMs



### ■ TPM Hersteller

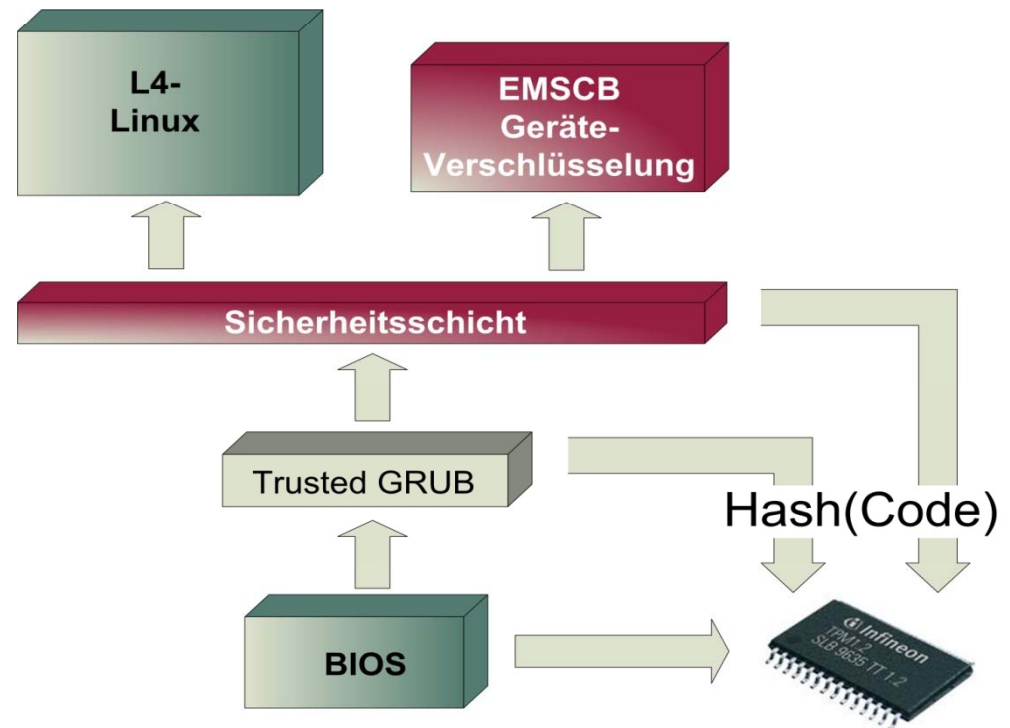
- Infineon
- Atmel
- ST Microelectronics
- National Semiconductor
- Sinosun

# Trusted Computing

## → Trusted Grub und Trusted Boot

### ■ *Vertrauenswürdiger Bootvorgang durch angepassten Bootloader*

- Integritätsmessung aller Programmdateien vor Ausführung
- Ablegen der Integritätswerte in Registern des Trusted Platform Modules (TPM)#
- Bildet die Wurzel der Sicherheitsplattform



- **Überprüfbares Booten**
  - Systemkonfiguration kann mittels eines TPMs überprüft werden
- **Sealing (Versiegeln)**
  - Binden von kryptographischen Schlüsseln an ein IT-System und /oder eine bestimmte Softwarekonfiguration
- **Attestation (Attestierung)**
  - Aktuelle Softwarekonfiguration des IT-Systems wird dargestellt
- **Remote Attestation**
  - Erkennung manipulierter IT-Systeme im Netzwerk
  - Kommunikation nur mit vertrauenswürdigen IT-Systemen
- **Sicherer Speicher**
  - Speicherung kryptographischer Schlüssel im Hardwaremodul
  - Erzeugung sicherer kryptographischer Schlüssel

### ***Gegenüber herkömmlichen Systemen bietet Trusted Computing***

- mehr Sicherheit und
- höhere Vertrauenswürdigkeit

### ***durch***

- Authentifizierung eines Systems
  - Überprüfbarkeit der Integrität eines Systems
  - Darstellbarkeit der Authentizität und Integrität
  - den nachweisbaren Bootvorgang ("Trusted Boot")#
- 
- ***Entscheidend ist die richtige Anwendung der Technologie***
  - ***Trusted Computing hat Grenzen, die es zu lösen gilt***

# Agenda

- **Problemstellung & Trusted Computing**
- ***Sicherheitsplattform Turaya***
- **Anwendungsbeispiele**
- **Fazit**

# Die Sicherheitsplattform Turaya

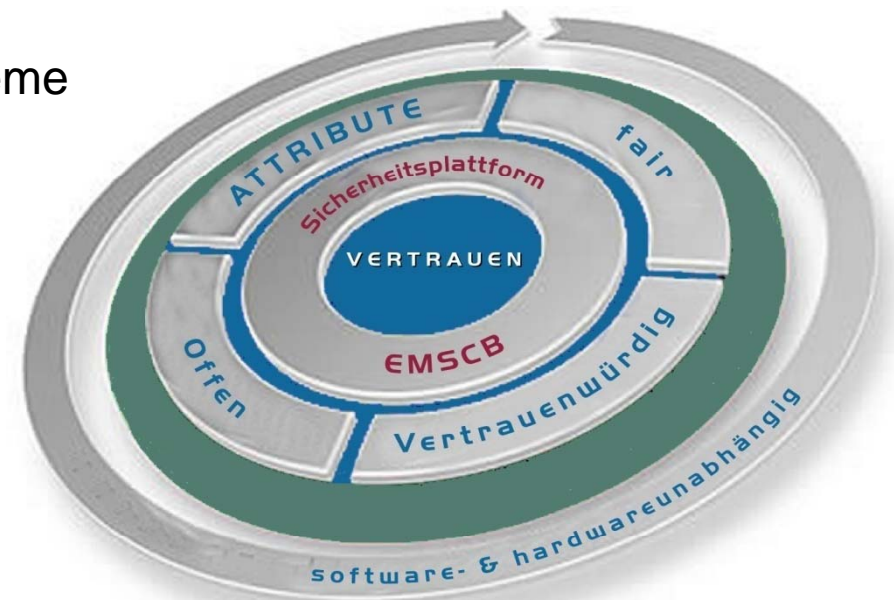
## → Motivation

### *Eigenschaften einer Sicherheitsplattform*

- **Sicherheitsprobleme** existierender Rechnerplattformen **lösen**
- **Schädliche** Auswirkungen von Viren, Würmern & Co. **stark einschränken**
- **Sensible Informationen** auf **eigenen** und **fremden** Rechnersystemen **garantiert** vertrauenswürdig verarbeiten
- Unterstützung **existierender** Betriebssysteme

### *Besondere Attribute:*

- **Vertrauenswürdig**
- **Fair**
- **Offen**



# Die Sicherheitsplattform Turaya

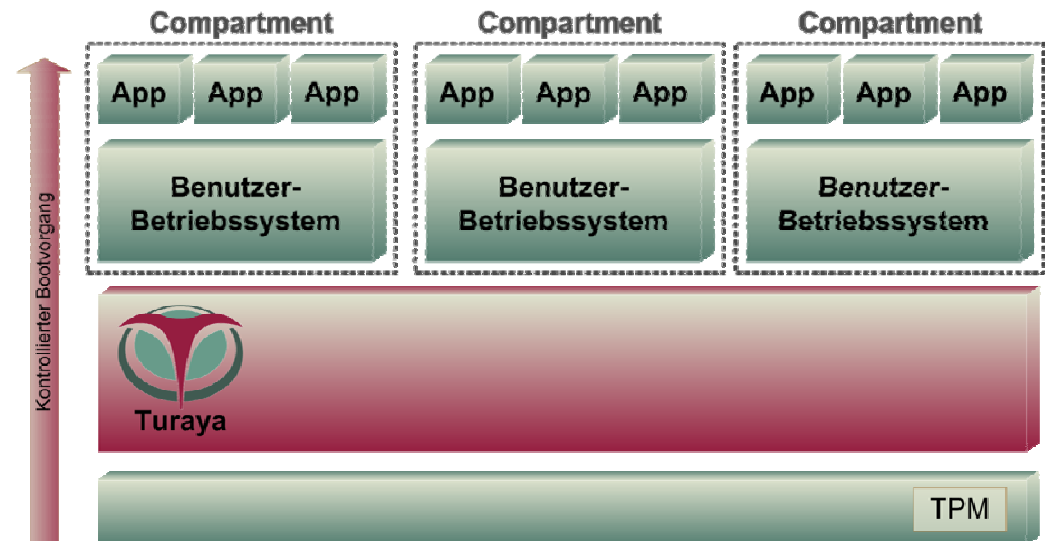
## → Attribute

- **Vertrauenswürdig**
  - Nachvollziehbare Architektur, geringe Komplexität
  - Transparente Implementierung, **vertrauenswürdige Realisierung**
  - TC-Funktionen, um **Vertrauenswürdigkeit** zu garantieren
- **Fair**
  - Durchsetzen von Rechten verlangt **Zustimmung aller Parteien**
  - Benutzer (Datenschutz), Organisationen (sichere Behandlung von wichtigen Daten), externe Instanzen (Urheberrechte, Lizenzen)
  - Die Plattform **kann, muss aber nicht** genutzt werden
- **Offen**
  - Schaffung eines offenen Standards zur Erhöhung der Interoperabilität
  - Für alle Betriebssysteme und Plattformen nutzbar (Desktop, SmartPhone, PDA, Embedded Systems usw.)#
  - Offen für Partner, keine Diskriminierung einzelner Anbieter / Anwender

# Die Sicherheitsplattform Turaya

## → Aufbau

- **Sicherheitskern (Trusted Software Layer)**
  - **Authentifikation** einzelner Compartments
  - **Binden von Daten** an einzelne Compartments
  - **Trusted Path**
    - Zwischen Anwender & Applikation / Applikation & Smartcard
  - **Sicheres Policy Enforcement**
  - **Schutz der Applikationen**
  - **Schutz der Anwenderdaten**
  - **Schutz vor Manipulationen** einer Applikation



# Die Sicherheitsplattform Turaya

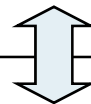
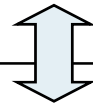
## → Kerntechnologien

- ***Virtualisierung***
  - z.B. Kontrolle des Datenflusses durch eine Sicherheitsschicht
- ***Starke Isolation***
  - Sicherheitskritische Vorgänge werden separiert (Compartments)#
- ***Minimalisierung***
  - Fehlervermeidung durch **Modularität** und **geringe Komplexität**
- ***Trusted Computing Technologie***
  - Überprüfbare hardwarebasierte Sicherheit

# Die Sicherheitsplattform Turaya

→ Offenheit / Kompatibilität

## Konkrete Anwendungen



## Krypto- und TC-Hardwaremodule

Beispiele (mit unterschiedlicher Funktion)#  
TPM, Intel TXT, AMD Presidio, ARM Trustzone  
Smartcards, IBM4758

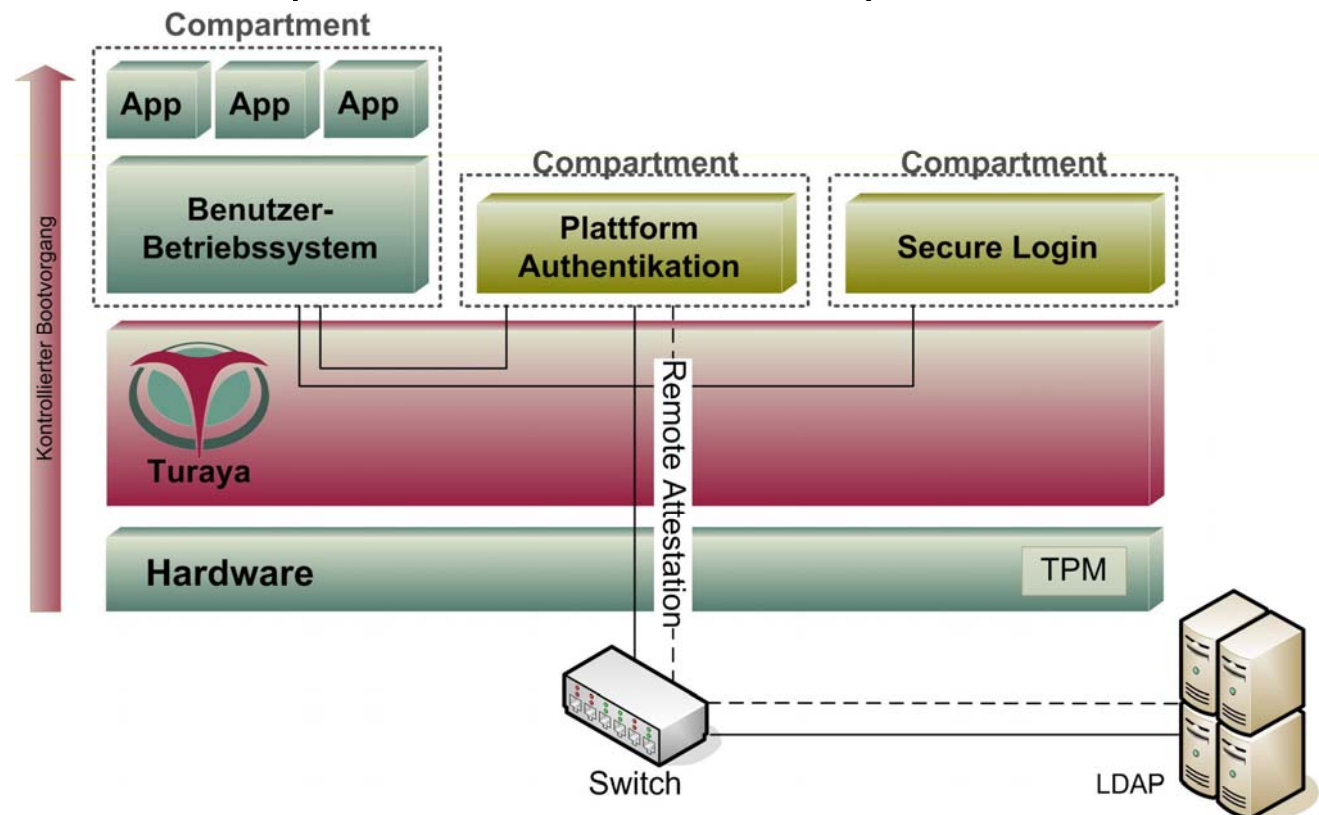
# Agenda

- **Problemstellung & Trusted Computing**
- **Sicherheitsplattform Turaya**
- ***Anwendungsbeispiele***
- **Fazit**

# Anwendungsbeispiele

## → Turaya.SecAuth

- **Keine Eingabe** von sensiblen Daten im **unsicheren** Kompartiment
- **Eingabe** von Benutzerdaten im gemessenen **sicheren** Kompartiment
- Sichere Kommunikation der Compartments über die Turaya Sicherheitsschicht

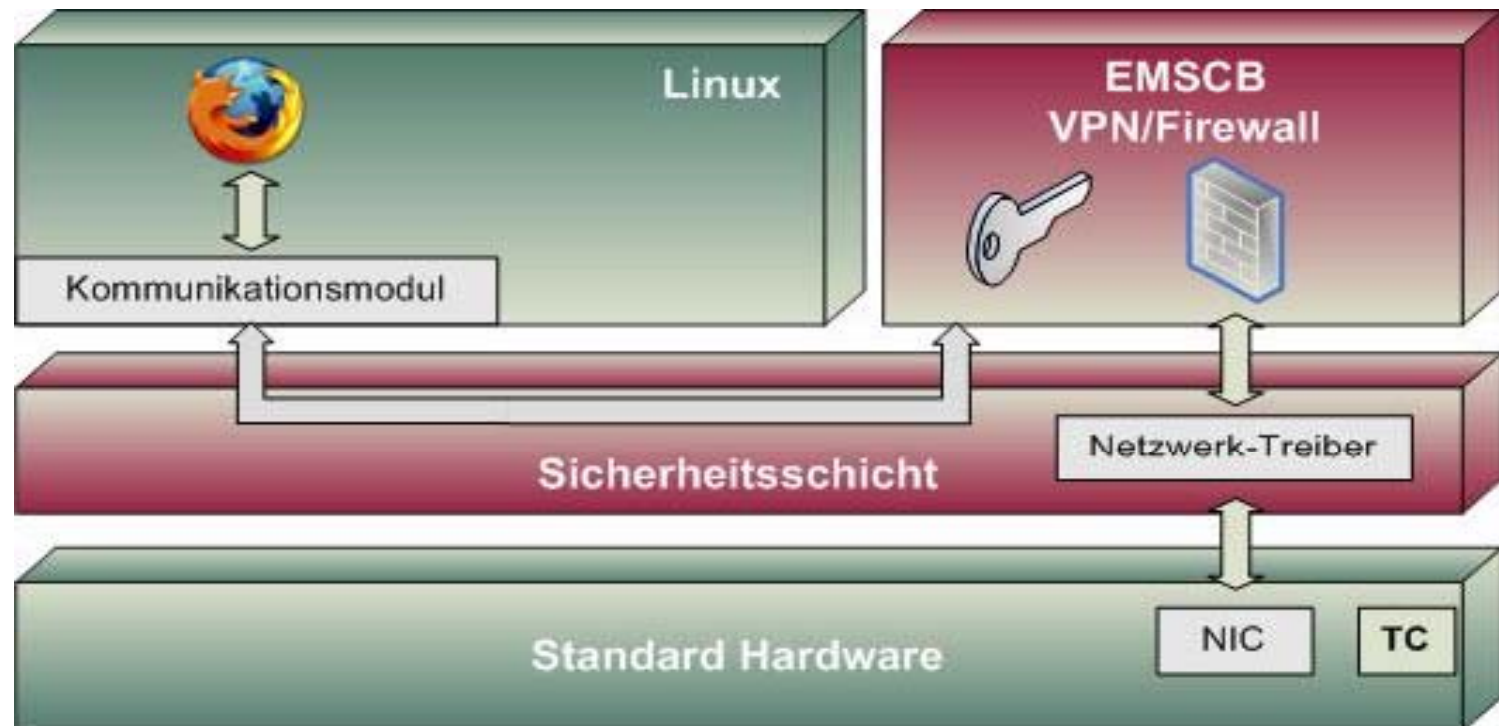


# Anwendungsbeispiele

## → Turaya.VPN

### ■ **Ziele - Isolation vom Standard-Betriebssystem:**

- Netzwerk-Treiber
- VPN-Client und Zertifikate/Schlüssel
- Firewall und Firewall-Policy
- ...



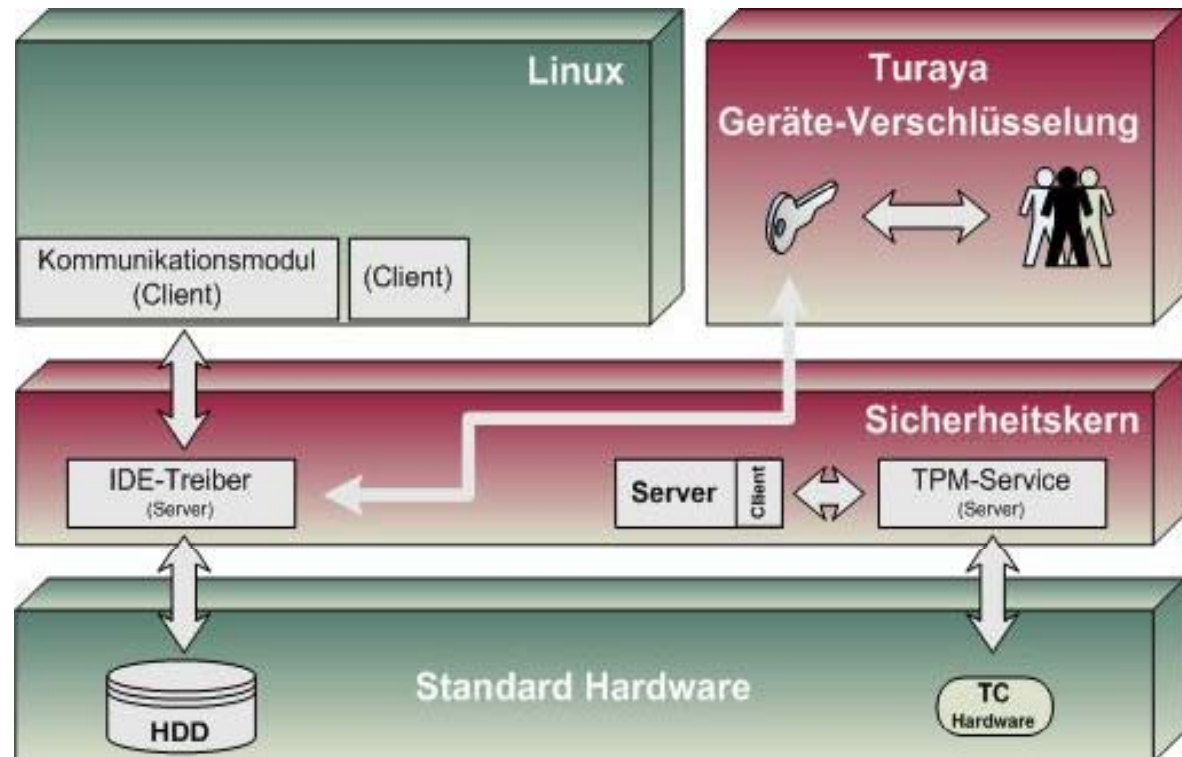
# Anwendungsbeispiele

## → Turaya.Crypt

- **Benutzerauthentifikation**, kryptographische Schlüssel und Operationen sind vom **Linux-Betriebssystem isoliert**
- **Verschlüsselung transparent** für Nutzer und Standard-Betriebssystem

### ■ **Unterstützte Geräte**

- Festplatten
- USB Memory Sticks
- CDR/DVD-Medien
- ...



# Anwendungsbeispiele

## → Anwendungsszenarien und -Branchen

- ***Finanzbereich***
  - Sicheres Online-Banking
  - Sichere Kommunikation
- ***Behörden und Unternehmen***
  - Sichere Prozesse / Kommunikation / Applikationen
  - eGovernment, ePass, eVoting, Gesundheitskarte
  - Qualifizierte Signatur, sichere Middleware
  - Enterprise Rights Management (Content- / Dokumentenschutz)#
- ***Inhalteanbieter / kommerzieller Verkauf***
  - eCommerce
  - DRM (Schutz digitaler Güter)#
- ***Sichere Client-Server-Modelle***
  - Externe Mitarbeiter, sichere Supply Chain, Firmenkommunikation
- ***Sicherheit in Embedded Systems***
  - Mobile Geräte, Automotive

# Agenda

- **Problemstellung & Trusted Computing**
- **Sicherheitsplattform Turaya**
- **Anwendungsbeispiele**
- ***Fazit***

## ***Turaya / Trusted Computing:***

- Die Sicherheitsplattform ermöglicht den vertrauenswürdigen Einsatz der Trusted-Computing-Technologie
- Die Turaya-Sicherheitsplattform ist frei verfügbar (Open Source)
- Turaya ist eine der führenden Entwicklungen im Bereich TC

## ***Schließen Sie sich uns an:***

- Profitieren Sie vom direkten Dialog mit der IT-Security-Spitzenforschung
- Beeinflussen Sie die nächsten Entwicklungen



# **Turaya & Trusted Computing zum Schutz von Daten, Kommunikation, Privatsphäre, Urheberrecht.**

[www.internet-sicherheit.de](http://www.internet-sicherheit.de)  
[www.turaya.de](http://www.turaya.de)