

gefördert durch das



Bundesministerium  
für Wirtschaft  
und Technologie

## Die Sicherheitsplattform Turaya

→ Trusted Computing hat eine  
vertrauenswürdige Plattform

### **Ammar Alkassar**

Sirrix AG security technologies  
[www.sirrix.de](http://www.sirrix.de)

### **Markus Linnemann**

Institut für Internet-Sicherheit  
Fachhochschule Gelsenkirchen  
[www.internet-sicherheit.de](http://www.internet-sicherheit.de)



Ruhr-Universität Bochum



Fachhochschule  
Gelsenkirchen



TECHNISCHE  
UNIVERSITÄT  
DRESDEN



Sirrix AG  
security technologies

escrypt  
Embedded Security

# EMSCB

European Multilaterally Secure Computing Base  
[www.emscb.org](http://www.emscb.org)

# Agenda

---

- ◉ **Motivation**
- ◉ **Mission**
- ◉ **Architektur und Technologie**
- ◉ **Anwendungen**
- ◉ **EMSCB-Projekt**
- ◉ **Kompetenzzentrum**
- ◉ **Fazit**



# Motivation

## → Probleme herkömmlicher Systeme auf einen Blick

- ◉ **Kein Trusted Path**
  - Malware kann sensitive Daten bei Eingabe mitlesen
- ◉ **Keine Anwendungs-Authentifikation**
  - Benutzer können echte Anwendungen nicht von Trojanern unterscheiden
- ◉ **Keine strenge Isolation**
  - Anwendungen können auf Daten anderer Anwendungen zugreifen
- ◉ **Kein sicheres Booten**
  - Benutzer können Manipulationen des Betriebssystems nicht erkennen
- ◉ **Unsichere Anzeige**
  - Bspw. Phishing-Angriffe

# Motivation

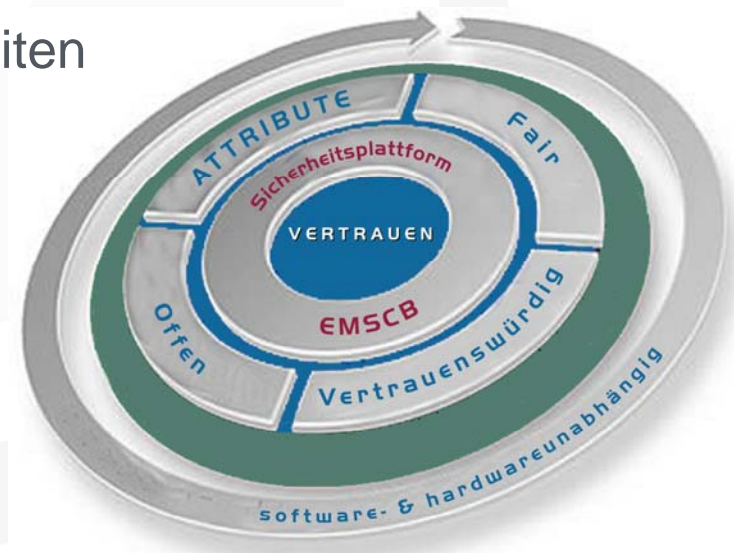
## → Der Ansatz

### **Eigenschaften einer Sicherheitsplattform**

- Grundsätzliche **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**



# Mission

## → 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

# Mission

## → Projekt EMSCB


---

*Mit Hilfe einer vertrauenswürdigen, fairen und offenen Sicherheitsplattform neue Möglichkeiten für innovative Geschäftsmodelle und kreative Anwendungen schaffen.*

# Architektur und Technologie

## → Funktionsweise der sicheren Plattform Turaya 1/3

- ◉ **Herkömmliche Hardware**
  - CPU / Hardware Devices
- ◉ **TPM**
  - Höchster Schutz durch hardwarebasierte Sicherheit
- ◉ **Vorteile der Trusted-Computing-Technologie nutzen**



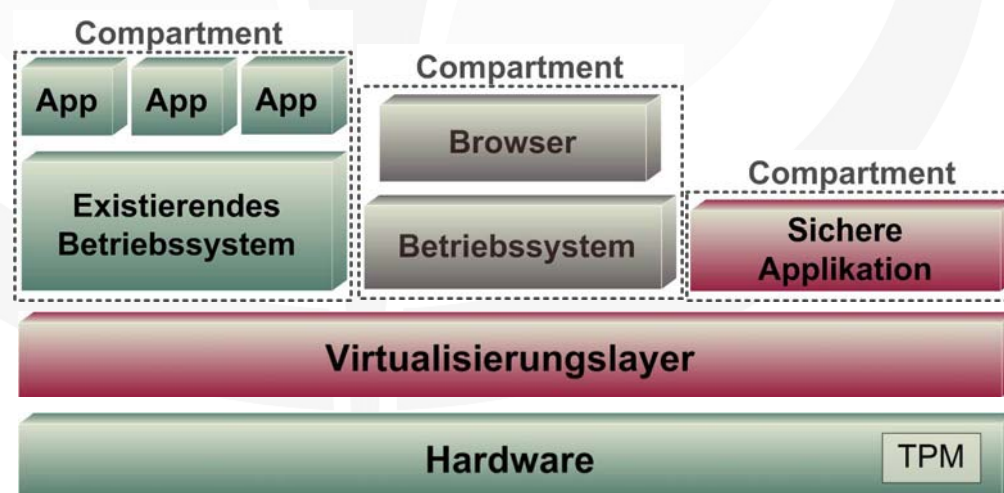
Hardware

TPM

# Architektur und Technologie

## → Funktionsweise der sicheren Plattform Turaya 2/3

- ◉ **Virtualisierungslayer zur Isolation ...**
  - Schutz der Applikationen
  - Schutz der Anwenderdaten
  - Schutz vor Manipulationen einer Applikation (bspw.: Browser)
- ◉ **... mittels moderner Virtualisierungstechniken**
  - Mikrokern-Architektur
  - Verwendbarkeit existierender Komponenten in Compartments

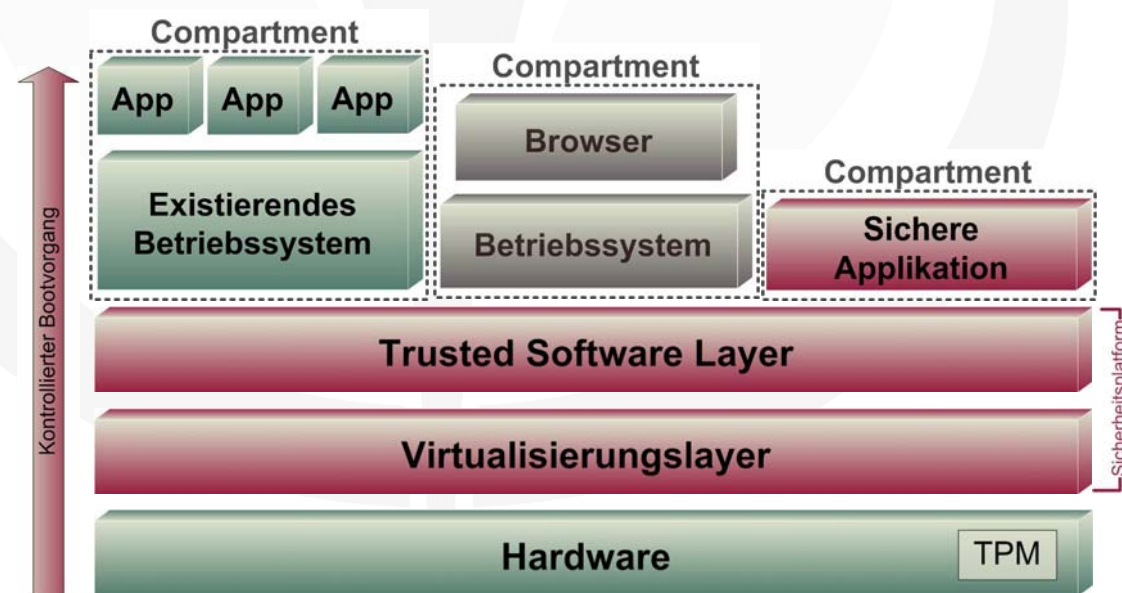


# Architektur und Technologie

## → Funktionsweise der sicheren Plattform Turaya 3/3

### ○ **Sicherheitskern (Trusted Software Layer)**

- **Authentifikation** einzelner Compartments
- **Binden von Daten** an einzelne Compartments
- **Trusted Path**
  - Zwischen Anwender & Applikation / Applikation & Smartcard
- **Sicheres Policy Enforcement**



# Architektur und Technologie

## → Sicherheitsarchitektur

### **Isolierte Compartments**

- Existierendes Betriebssystem
- Anwendungen wie: DRM, Signatur, Home Banking

### **Trusted Software Layer**

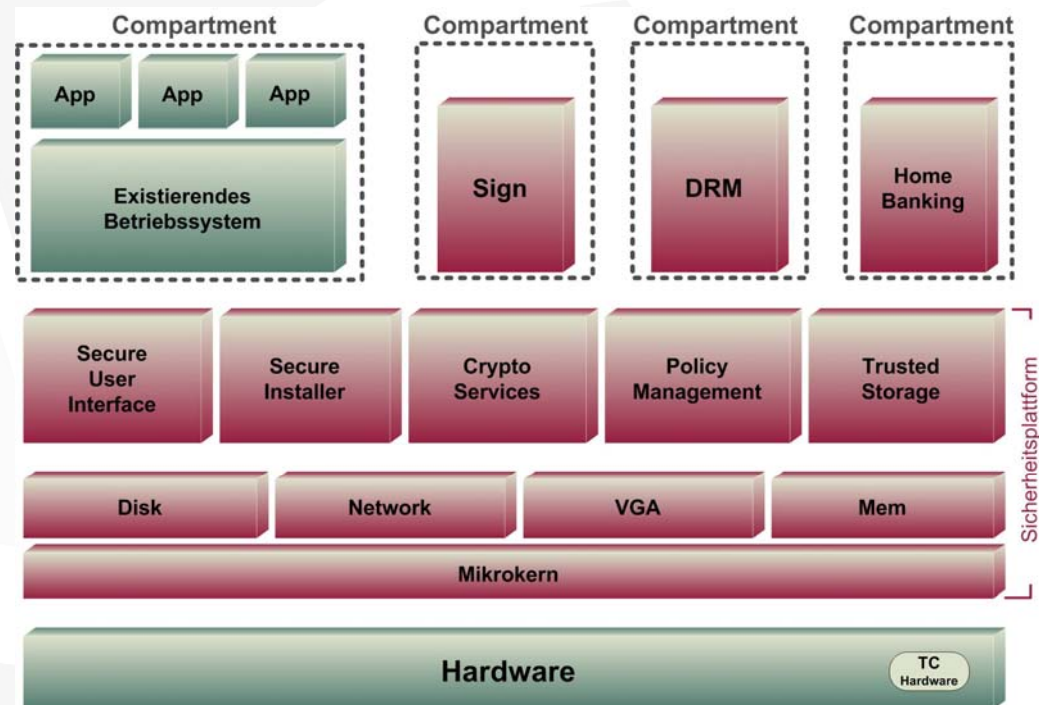
- Basis-Sicherheitsdienste
- Compartment Management
- TC Support

### **Virtualisierungslayer**

- Policy Enforcement
- Gerätetreiber

### **Hardware**

- CPU
- Trusted-Computing-Technologie



# Architektur und Technologie

→ Offenheit / Kompatibilität

Konkrete Anwendungen



Trusted Software Layer

Virtualisierungslayer



Krypto- und TC-Hardwaremodule

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

# Architektur und Technologie

## → 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 Hardware-basierte Sicherheit

# Architektur und Technologie

## → Eigenschaften

---

- ◉ **Offenheit:**
  - Design, Sourcecode, Dokumentation, Standards
- ◉ **Mehrseitige Sicherheit:**
  - Die Interessen/Rechte aller Beteiligten werden berücksichtigt und durchgesetzt → **Policy Enforcement**
- ◉ **Einfache Anwendung**
  - Einheitliches Managementinterface für alle Compartments
  - Wenig Supportaufwand
  - Hohe Stabilität
- ◉ **Kompatibilität & Interoperabilität**
  - Verschiedene Betriebssysteme und -versionen parallel möglich
  - Sicherheitsdienste sind unabhängig vom jeweiligen Betriebssystem

# Anwendungen

## → 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

# EMSCB-Projekt

## → Meilensteine / Applikationen

- **Turaya.Crypt**  
→ fertiggestellt
- **Turaya.VPN**  
→ fertiggestellt
- **Turaya.FairDRM**  
→ Testphase  
Einfaches faires DRM System
- **Turaya.ERM**  
→ Ende 2007 - **Partner SAP**  
Policybasiertes Dokumentenmanagement-System
- **Turaya (embsys)**  
→ Ende 2007 - **Partner Bosch/Blaupunkt**  
Multimedialer Einsatz der Plattform in eingebetteten Systemen



# EMSCB-Projekt

## → Konsortium Übersicht



# EMSCB-Projekt

## → Turaya - "Die Marke"

### ◉ **Das Projekt**

- Bezeichnung des Teams
- Angelegt auf 3 Jahre Förderung
- Förderung durch BMWi
- Zeitraum: 14.03.05 – 14.03.08

EMSCB

### ◉ **Das Produkt / Die Ergebnisse**

- Produktname / Technologienname
- Technologie: Sicherheitsplattform Turaya
- Konvention: Turaya.Produktname
  - Bsp. Turaya.Crypt



EMSCB

European Multilaterally Secure Computing Base

# Kompetenzzentrum

## → Ihr Ansprechpartner

---

- ◉ **Trusted Computing Kompetenzzentrum**
  - Die Basis für die Entwicklung der **Turaya-Technologie**
  - Gebündeltes "**Know-how**" der IT-Sicherheitsexperten
- ◉ **Aufgabe**
  - Weiterentwicklung und Pflege der **Turaya-Technologie**
- ◉ **Leistungen**
  - Beratung für Unternehmen und Organisationen
  - Entwicklung anwenderspezifischer Lösungen für mehr IT-Sicherheit
- ◉ **Ziel**
  - Das Streben nach **strategischen Kooperationen** mit Partnern für innovative Anwendungen zur Etablierung der **Vertrauenswürdigkeit von IT-Systemen**

# Fazit

---

## ***Turaya:***

- ◉ Die Sicherheitsplattform ermöglicht den vertrauenswürdigen Einsatz der Trusted-Computing-Technologie
- ◉ Die Turaya-Sicherheitsplattform ist frei verfügbar
- ◉ Turaya ist eine der führenden Entwicklungen im Bereich TC
- ◉ Bedeutende Industriepartner erarbeiten mit dem EMSCB-Team Pilotanwendungen.

→ **Trusted Computing verbreitet sich ohnehin, doch ohne Turaya in einem vom Anwender wenig beeinflussbarem Umfang!**

## → ***Schließen Sie sich uns an:***

- Profitieren Sie vom direkten Dialog mit der IT-Security-Spitzenforschung
- Beeinflussen Sie die nächsten Entwicklungen
- Nutzen Sie die Chance für Ihr Unternehmen

gefördert durch das



Bundesministerium  
für Wirtschaft  
und Technologie

# Kommen sie auf die sichere Seite!

## Werden sie Partner des EMSCB-Projekts

[www.emscb.de](http://www.emscb.de)

### **Ammar Alkassar**

Sirrix AG security technologies  
[www.sirrix.de](http://www.sirrix.de)

### **Markus Linnemann**

Institut für Internet-Sicherheit  
Fachhochschule Gelsenkirchen  
[www.internet-sicherheit.de](http://www.internet-sicherheit.de)

# EMSCB

European Multilaterally Secure Computing Base  
[www.emscb.org](http://www.emscb.org)