



**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Trusted Computing → Security Platform - Turaya

Prof. Dr. (TU NN)

Norbert Pohlmann

Institute for Internet Security - if(is)
University of Applied Sciences Gelsenkirchen
<http://www.internet-sicherheit.de>

if(is)
internet security.

- **Aim and outcomes of this lecture**
- **Motivation/Approach/EMSCB Project**
- **Idea/Architecture**
- **Application Scenarios**
- **Summary**

- **Aim and outcomes of this lecture**
- Motivation / Approach / EMSCB Project
- Idea / Architecture
- Application Scenarios
- Summary

Security Platform - Turaya

→ Aims and outcomes of this lecture

Aims

- To introduce the topic Security Platform Turaya
- To explore the general idea of a Security Platform Turaya
- To analyze the goals of a Security Platform Turaya
- To assess the concerns of a Security Platform Turaya

At the end of this lecture you will be able to:

- Understand the basic idea of a Security Platform Turaya.
- Know something about the approach of a Security Platform Turaya.
- Understand the need for a Security Platform Turaya.

- Aim and outcomes of this lecture
- **Motivation / Approach / EMSCB Project**
- Idea / Architecture
- Application Scenarios
- Summary

Security Platform - Turaya

→ Motivation

What we need is trustworthy IT that is achievable by means of a **security platform**

- which **solves the security problems** of existing computer systems or **greatly restricts the harmful effects** of e.g. viruses, worms, trojans, phishing, exploits, SW updates
- which **guarantees the trustworthy processing of information** on one's own and on external computer systems
- which **supports the use of existing operating systems**
- which offers **transparent security** or **transparent trustworthiness**

What we need is **increased trustworthiness** through the **conception** and **development** of a **trustworthy, fair and open security platform**.

Trustworthiness

- Comprehensible architecture, low level of complexity of the technology
- Transparent implementation and **trustworthy execution**
- Functions that guarantee trustworthiness: sealing, attestation, secure (trusted) boot

Fairness

- The enforcement of rights requires the **agreement of all parties**.
- The security platform **can be used, but does not have to be**.
- User (data protection), Organisations (secure handling of important data), External bodies (copyrights and licences)

Openness

- Creation of an open standard to improve interoperability.
- Turaya can be used by all operating systems and platforms. (Desktop, SmartPhone, PDAs, embedded systems)
- Open to all partners - no discrimination against individual suppliers/users

Security Platform - Turaya

→ The EMSCB-Project



Consortium manager

Ruhr-University-Bochum
eurobits



Institute for
System architecture



Institute for
Internet Security



Strategic industrial partners:



Security Platform - Turaya

→ Milestones / Applications

- **Turaya.Crypt**
- **Turaya.VPN**
- **Turaya.FairDRM**
A simple fair DRM system
- **Turaya.ERM**
Partner SAP
Policy-based document management
- **Turaya.Embsys**
Partner Bosch/Blaupunkt
use of the platform in embedded systems (multimedia)



- Aim and outcomes of this lecture
- Motivation / Approach / EMSCB Project
- **Idea / Architecture**
- Application Scenarios
- Summary

Security Platform - Turaya

→ Basic Idea

- Trusted Computing needs a security platform!
- The security platform requires special attributes such as:
 - **Trustworthiness**
 - **Fairness**
 - **Openness**
- With the security platform Turaya we enable Trusted Computing to be "open" within the meaning of our attributes.

Security Platform - Turaya

→ Architecture and Technology 1/3

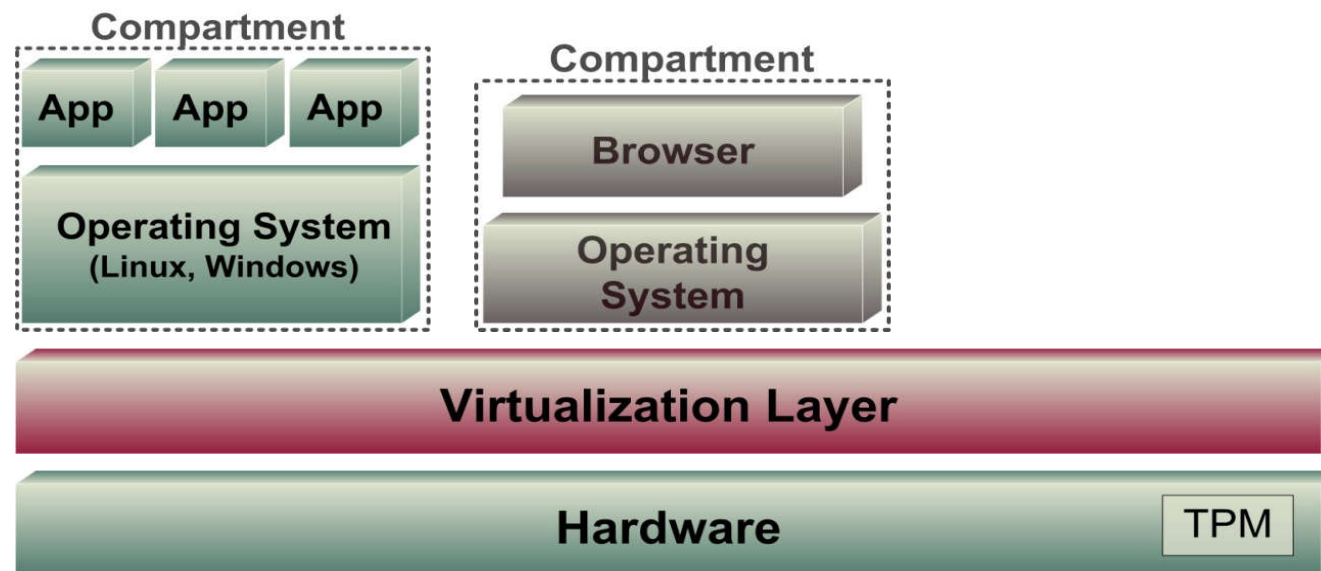
- ***Conventional hardware***
 - CPU / hardware devices
- ***TPM***
 - Highest level of protection through hardware-based security
- ***Use the advantages of Trusted Computing technology***



Security Platform - Turaya

→ Architecture and Technology 2/3

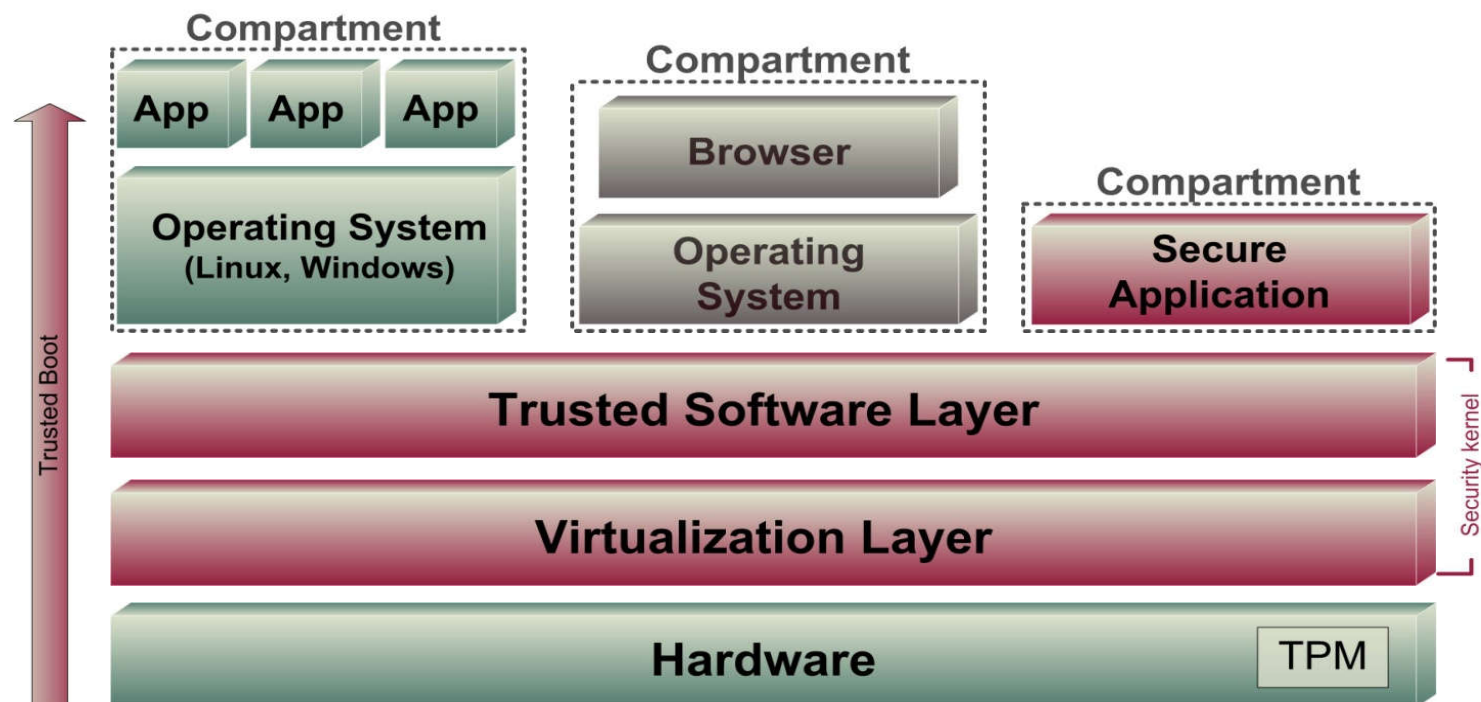
- **Virtualization layer for the purposes of isolation...**
 - Protect applications
 - Protect user data
 - Protect against the manipulation of an application (e.g. browser)
- **... through modern virtualization technologies**
 - Micro-kernel architecture
 - Use of existing components in compartments



Security Platform - Turaya

→ Architecture and Technology 3/3

- **Security Platform (Trusted Software Layer)**
 - Authentication of individual compartments
 - Binding of data to individual compartments
 - Trusted Path
 - Between user & application / application & smartcard
 - Secure policy enforcement



Security Platform - Turaya

→ Architecture in detail - overview

■ *Application Layer*

- legacy operating systems
- Secure applications

■ *Trusted Software Layer*

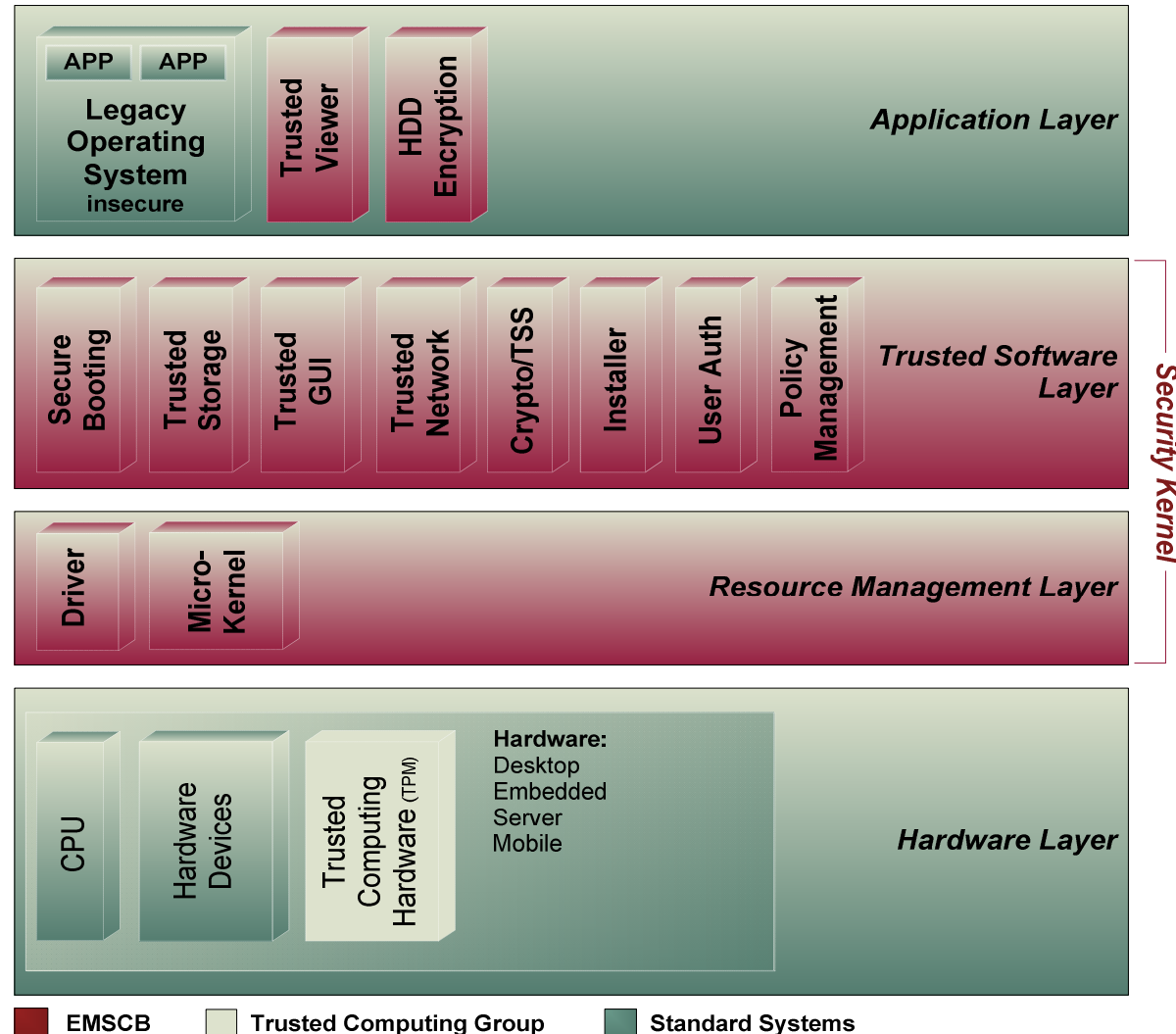
- Security services
- Application management
- Sec. policy management

■ *Resource Management Layer*

- Mikro-kernel / HW sharing
- **Policy enforcement**

■ *Hardware Layer*

- CPU
- TC technology



Security Kernel

Security Platform - Turaya

→ Architecture in detail – secure apps

- **Trusted Viewer**
 - Provides a trustworthy document viewer working with the principle of **What-you-see-is-what-you-get**.
 - Applications can store documents in a certain fashion, only enabling the **Trusted Viewer** to open and display these documents.
 - Output, displayed by the **Trusted Viewer**, cannot be overlaid by a different application.
- **Device Encryption**
 - By the means of **Device Encryption** block orientated devices (hard drive, memory sticks, CD/DVDs) can be encrypted.
 - The **Device Encryption** is transparent to the user depending on the used configuration.

Security Platform - Turaya

→ Architecture in detail – services (1/3)

- **Trusted Storage (Manager)**
 - The **Trusted Storage Manager** provides a trustworthy storage space, which can be used by processes, to store data securely and with a full level on integrity.
 - Data can be bound to a certain configuration (measurements within the **PCRs**), a certain user, or a certain application.
 - The **Trusted Storage Manager** also provides the attribute defined as „freshness“. This allows the detection and prevention of replay attacks.
- **Trusted GUI**
 - Manages the in- and output devices of the user (mouse, keyboard, graphics adaptor, ...).
 - Provides a secure path (**trusted path**) between the input of the keyboard up to the secure application, ensuring that no input can be detoured or intercept keyboard data.



Security Platform - Turaya

→ Architecture in detail – services (2/3)

- **Trusted Network**
 - Provides a trustworthy network interface, which verifies the network components and if necessary bans the connection.
- **Crypto/TSS**
 - Forms a centralized contact point for all applications, which need functions of the TSS.
- **Installer**
 - Presents the Loader of the system.
 - It installs and runs services from within the TCB as well as applications of the user.
 - Manages all running processes and offers a trustworthy entity to identify processes.

Security Platform - Turaya

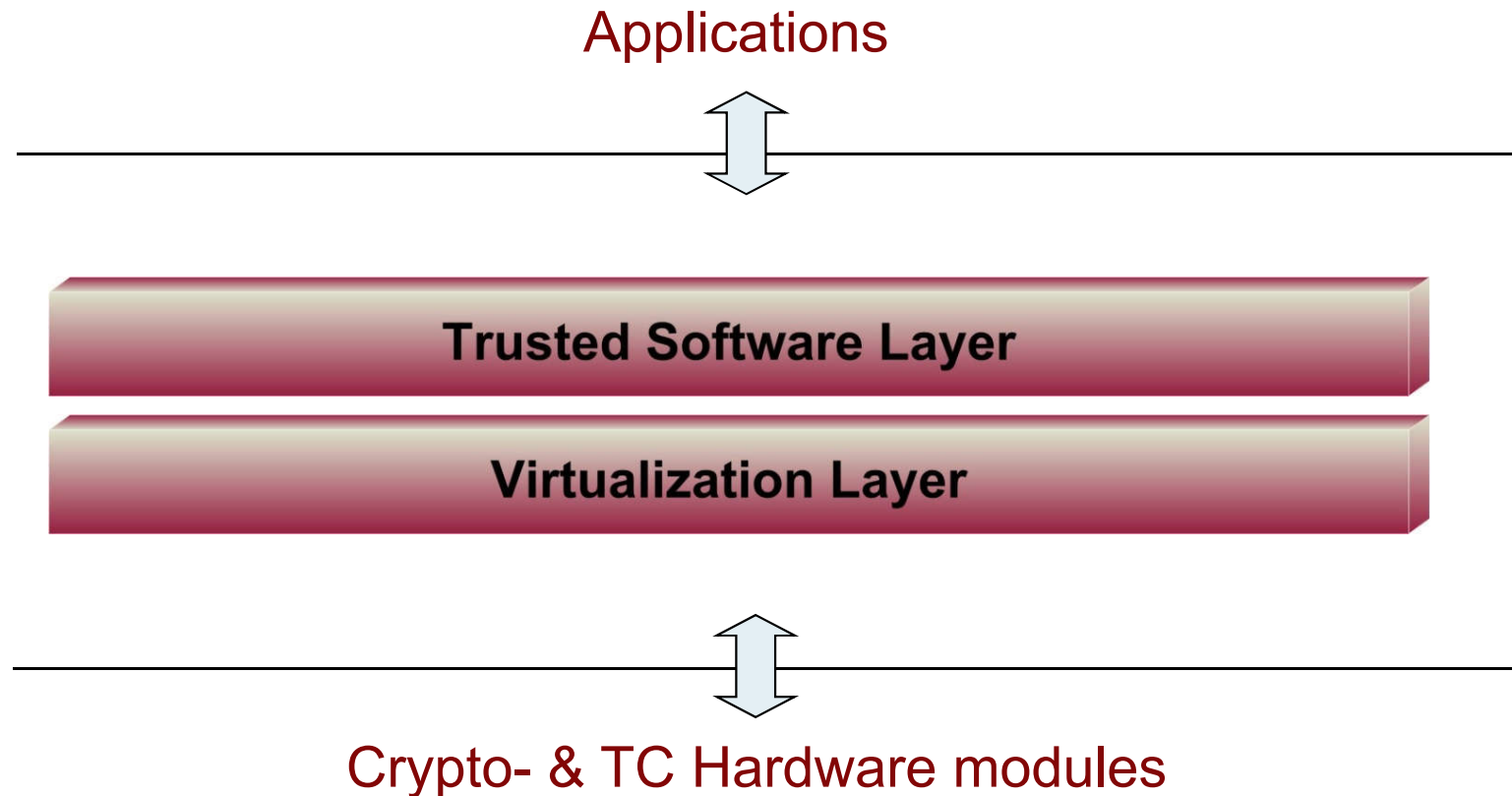
→ Architecture in detail – services (3/3)

- **User Auth**
 - Presents the user management for the users of the system and offers this service to the other applications.
 - Applications can use the service to conduct user authentication.
 - This enables the binding of data to a certain user.

- **Policy Management**
 - This service ensures that policies are enforced.
 - Data, that needs to be processed by observing certain policies, is binded encrypted to the **Policy Management**.
 - The policy is checked by the **Policy Management**, before the data can be processed.

Security Platform - Turaya

→ Architecture in detail: hardware module



Examples (with different functions)
TPM, Intel TXT, AMD Presidio, ARM Trustzone
Smartcards, IBM4758

Security Platform - Turaya

→ Additional Properties

- ***Minimalisation***
 - Error avoidance through the **modularity** and **low level of complexity**
- ***Openness:***
 - Design, source code, documentation, standards
- ***A simple application***
 - Standardized management interface for all compartments
 - Small support requirement
 - High level of stability
- ***Compatibility & Interoperability***
 - Different operating systems and versions are possible in parallel
 - The security services are independent of the respective operating system

- Aim and outcomes of this lecture
- Motivation/Approach/EMSCB Project
- Idea/Architecture
- **Application Scenarios**
- Summary

Security Platform - Turaya

→ Application Scenarios

- ***Financial Field***
 - Secure online banking
 - Secure communication
- ***Public Authorities and Companies***
 - Secure processes / communication / applications
 - eGovernment, ePassport, eVoting, health card
 - Qualified signature, secure middleware
 - Enterprise rights management (content / document protection)
- ***Content Providers / Commercial Sale***
 - eCommerce
 - Digital Rights Management (DRM)
- ***Secure Client Server Models***
 - External employees, secure supply chain, company communication
- ***Security in Embedded Systems***
 - Mobile devices, automotive

Security Platform - Turaya

→ Pilot: Turaya.ERM (1/2)

Fair Enterprise Rights Management (ERM)

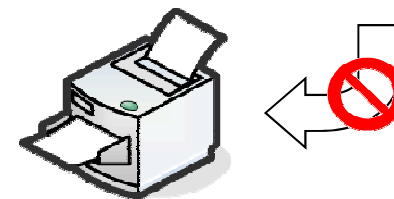
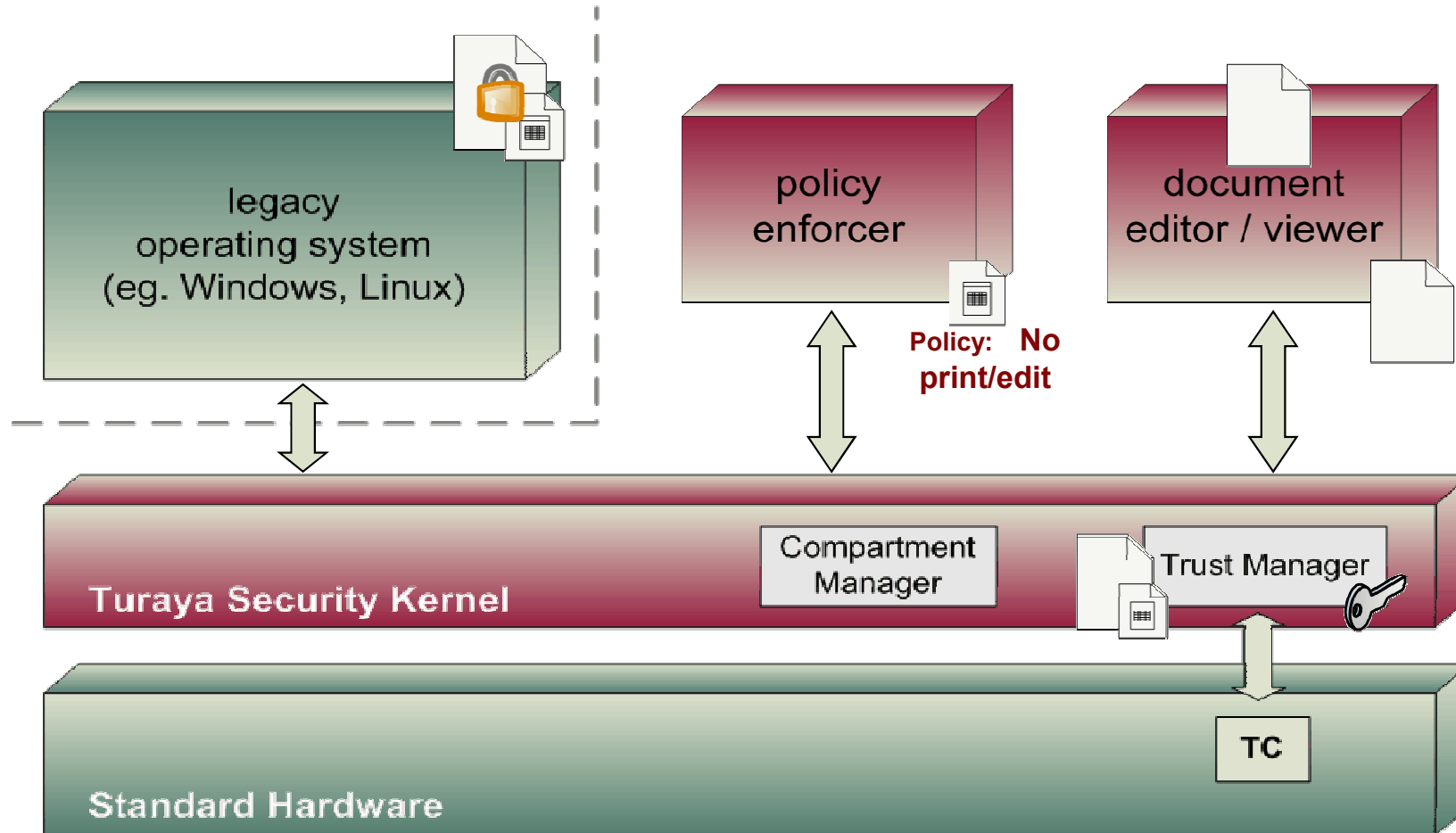
- **Open** Security Platform which gives **equal** consideration to the requirements of the **content provider** and the **content consumer**
- Runs in **parallel** to the conventional operating system
- Independently of conventional operating systems

Properties and services

- License negotiations
- License transfer
- Protection of user data

Security Platform - Turaya

→ Pilot: Turaya.ERM (2/2)



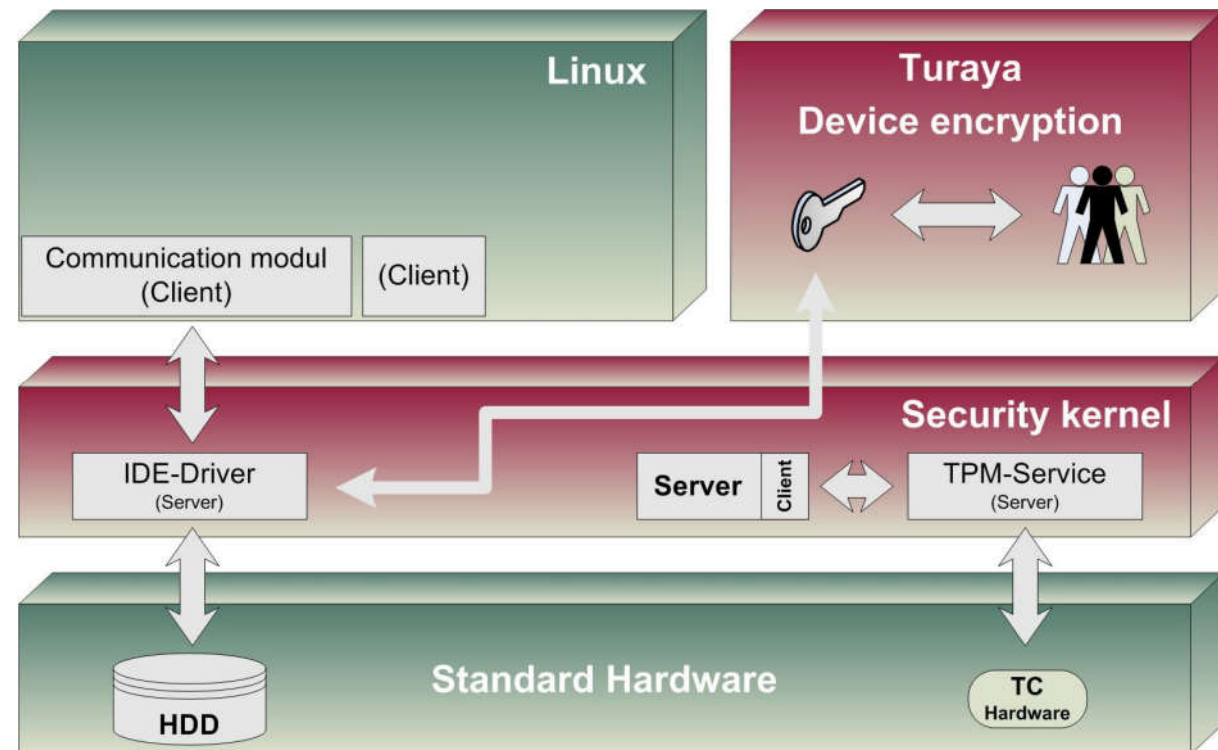
Architektur und Technologie

→ Turaya.Crypt

- **Transfer of data** between Linux und the evacuated IDE driver
- **IDE driver** communicates with the device encryption
- **Authentication of the user**, cryptographic keys and functions are isolated from Linux
- **Encryption is transparent** to the user and the legacy operating system

Supported devices

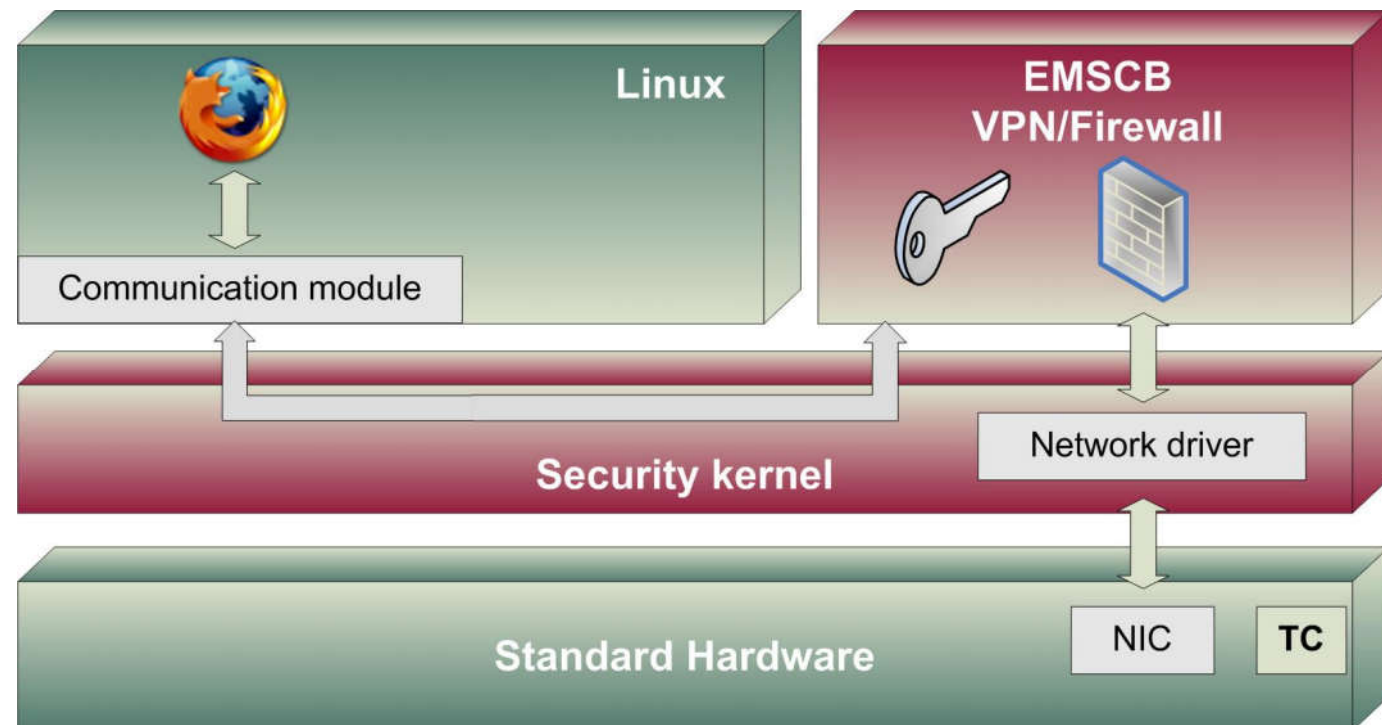
- Hard drives
- USB memory sticks
- CDR/DVDs



Architektur und Technologie

→ Turaya.VPN

- ***Isolated from the legacy operating system :***
 - Network device drivers
 - Client software for VPNs and keys as well as certificates
 - Firewall and firewall policies
- ***Encryption is transparent to the user and the legacy operating system***



Usage scenarios

→ ERM?



- ***Enterprise Rights Management***
 - Approach for the management of the flow of information of sensitive documents.
 - Access privileges for documents with mandatory enforcement
 - Provided with a policy label (xml) on a technical level most of the time
- ***New protection approach***
 - „Link security“ \leftrightarrow „object security“
 - So far the transport of the data has been secured ((VPN, PGP, ...))
- ***Problems of current ERM systems***
 - Systems are as secure as the underlying operating systems
 - No trustworthiness of the computer systems can be attested

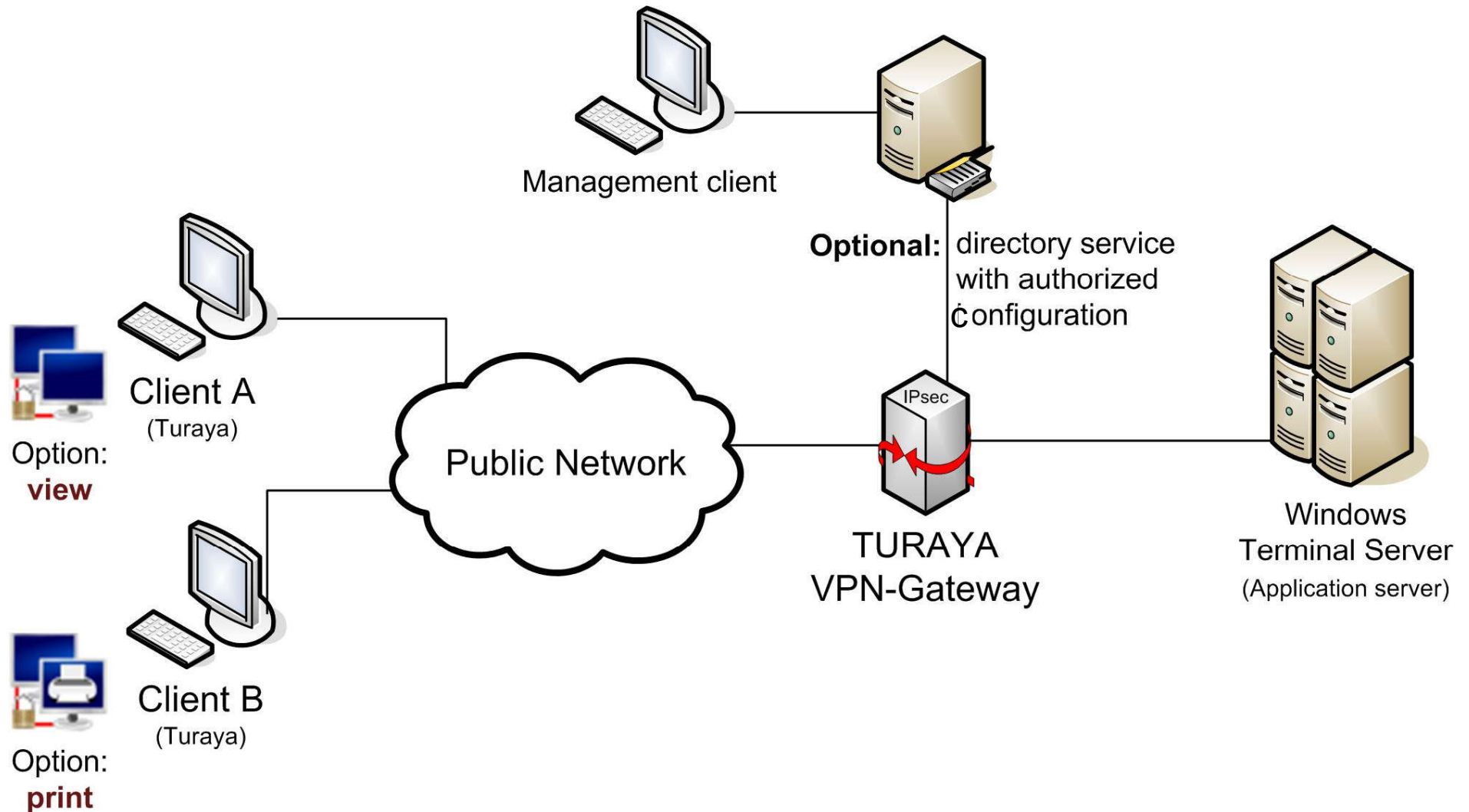
Usage scenarios

→ What does a trustworthy ERM have to achieve?

- ***Document life cycle protection:***
 - The guaranteed enforcement of document specific access and processing policies across platforms and company borders and through the entire life cycle of a document: from creation to destruction.
- ***Verifiability of the IT systems handling the data :***
 - Only IT systems, which can attest their trustworthiness, can access the protected documents.
- ***Trustworthiness of the IT systems handling the data:***
 - Trustworthy IT system are those, which on the one side enable the processing of data along policies in a functional manner and on the other side offer an inherent higher level of protection against external manipulation.

Usage scenarios

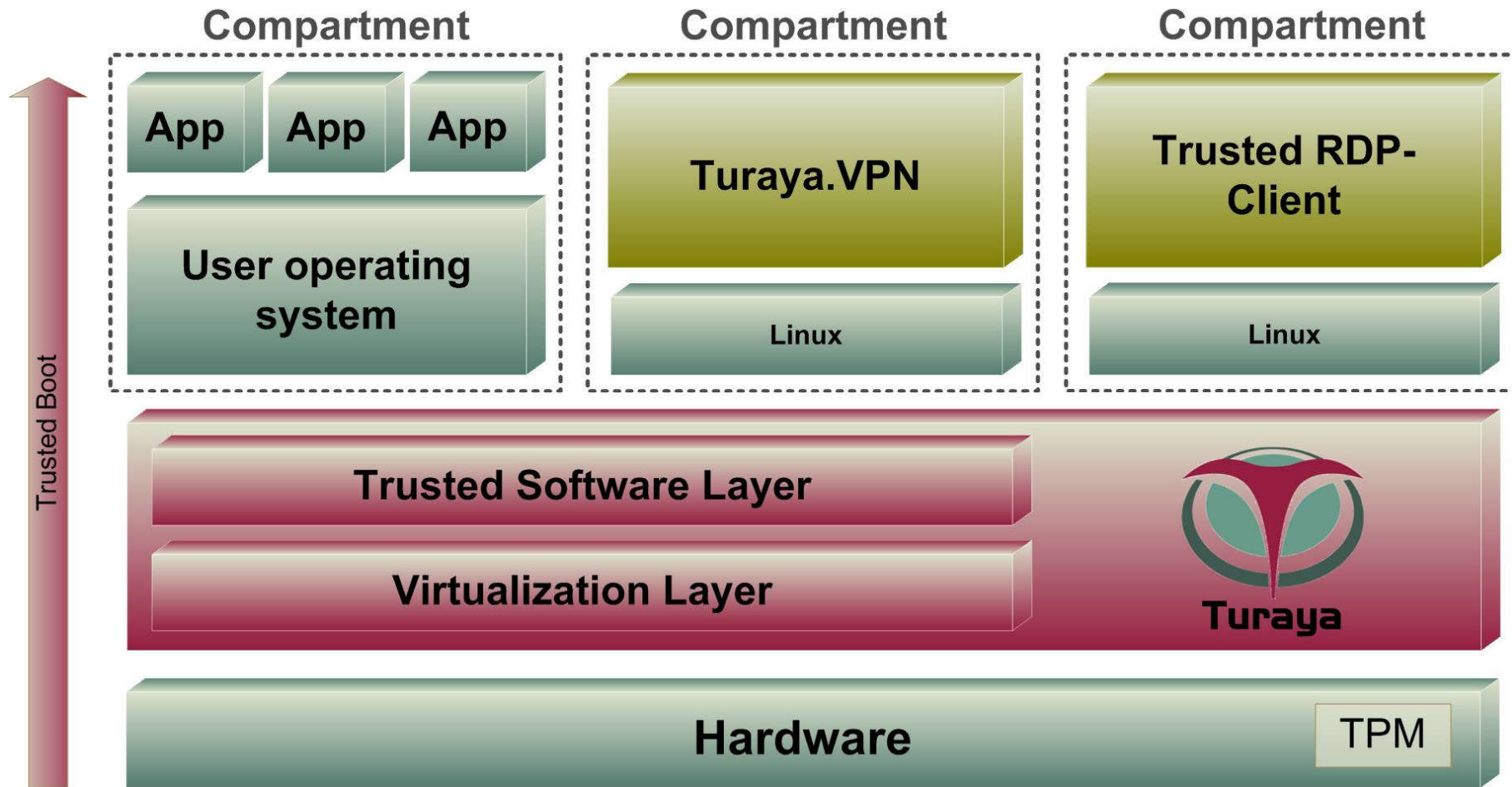
→ Overview Turaya.WTS



WTS: Windows Terminal Server

Usage scenarios

→ Architecture Turaya.WTS



RDP: Remote Desktop Protocol

- Aim and outcomes of this lecture
- Motivation/Approach/EMSCB Project
- Idea/Architecture
- Application Scenarios
- **Summary**

Security Platform - Turaya

→ Summary

- The security platform Turaya enables the trustworthy, fair and open use of Trusted Computing technology.
 - The security platform Turaya is freely available.
 - Turaya is one of the leading developments in the field of TC.
 - Important industrial partners are developing interesting pilot applications together with the EMSCB team utilizing the Turaya security platform.
- **Trusted Computing will spread anyway, but without a security platform like Turaya to an extent over which the user has little influence!**



**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Trusted Computing → Security Platform - Turaya

Thank you for your attention!
Questions?

Prof. Dr. (TU NN)

Norbert Pohlmann

Institute for Internet Security - if(is)
University of Applied Sciences Gelsenkirchen
<http://www.internet-sicherheit.de>

if(is)
internet security.

Security Platform - Turaya

→ Literature

- [1] N. Pohlmann, A.-R. Sadeghi, C. Stüble: "European Multilateral Secure Computing Base", DuD Datenschutz und Datensicherheit – Recht und Sicherheit in Informationsverarbeitung und Kommunikation, Vieweg Verlag, 09/2004
- [2] M. Linnemann, N. Pohlmann: "An Airbag for the Operating System – A Pipedream?", ENISA Quarterly Vol. 3, No. 3, July-Sept 2007 (see link)

Links:

Institute for Internet Security:

<http://www.internet-sicherheit.de/forschung/aktuelle-projekte/trusted-computing/>

ENISA

http://www.enisa.europa.eu/doc/pdf/publications/enisa_quarterly_09_07.pdf