



Trusted Computing

Modul D3.2

Referent: Dr. Jörg Cosfeld

Trusted Computing

Um was handelt es sich?

Trusted Computing

Um was handelt es sich?

Erlangen der Kenntnisse über

- **Authenticated Boot**
- **Attestation**
- **Binding**
- **Sealing**

Trusted Computing

Um was handelt es sich?

Erlangen der Kenntnisse über

- **Authenticated Boot**
- **Attestation**
- **Binding**
- **Sealing**

Aber auch Kenntnisse über:
Kernelarchitekturen

Trusted Computing

Definition: Ein System ist trusted wenn es sich berechenbar und absehbar verhält.

Trusted Computing

Definition: Ein System ist trusted wenn es sich berechenbar und absehbar verhält.



Trusted Computing

Definition: Ein System ist trusted wenn es sich berechenbar und absehbar verhält.

Wie kann man sowas checken?

Der User vertraut seinen eigenen Erfahrungen mit dem System.

oder

Der User vertraut jemanden der Ihm das System als berechenbar zertifiziert.

Trusted Computing

Definition: Ein System ist trusted wenn es sich berechenbar und absehbar verhält.

Wie kann man sowas checken?

Der User vertraut seinen eigenen Erfahrungen mit dem System.

Trusted Computing Group (TCG):
Industriekonsortium bestehend aus den
führenden IT-Firmen
(Hewlett-Packard, IBM, Intel, AMD,
Microsoft, Sony, Sun, Infineon, ...)

TRUSTED[®]
COMPUTING
GROUP

Trusted Computing

Definition: Ein System ist trusted wenn es sich berechenbar und absehbar verhält.



Ziele:

Entwicklung **offener Spezifikationen** für **trusted Systems**

Ohne massive Einschnitte.

Trusted Computing

Definition: Ein System ist trusted wenn es sich berechenbar und absehbar verhält.



Ziele:

Entwicklung **offener Spezifikationen** für **trusted Systems**

Ohne massive Einschnitte.

Manipulationssichere Komponenten in Hardware.

Trusted Computing

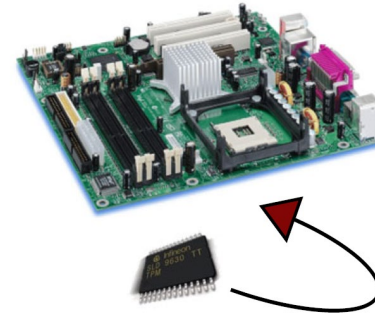
Definition: Ein System ist trusted wenn es sich berechenbar und absehbar verhält.

Wie setzt man diese Ziele um?

Trusted Platform Modules



TPM

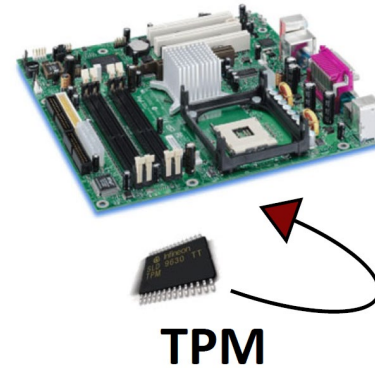


Trusted Computing

Definition: Ein System ist trusted wenn es sich berechenbar und absehbar verhält.

Wie setzt man diese Ziele um?

- Einbau eines TP-Moduls
- Zufallsgenerator – erzeugt kryptografische Schlüssel

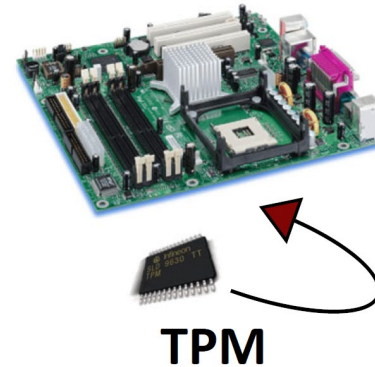


Trusted Computing

Definition: Ein System ist trusted wenn es sich berechenbar und absehbar verhält.

Wie setzt man diese Ziele um?

- Einbau eines TP-Moduls
- Zufallsgenerator – erzeugt kryptografische Schlüssel
- Kopplung an Speicher der Systemkonfiguration

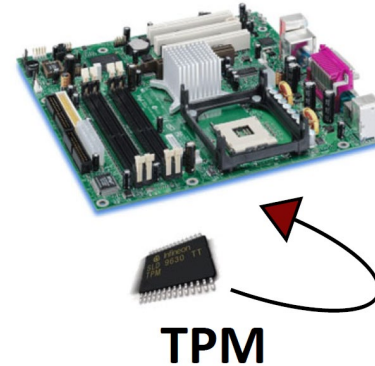


Trusted Computing

Definition: Ein System ist trusted wenn es sich berechenbar und absehbar verhält.

Wie setzt man diese Ziele um?

- Einbau eines TP-Moduls
- Zufallsgenerator – erzeugt kryptografische Schlüssel
- **Platform Configuration Register (PCR)**

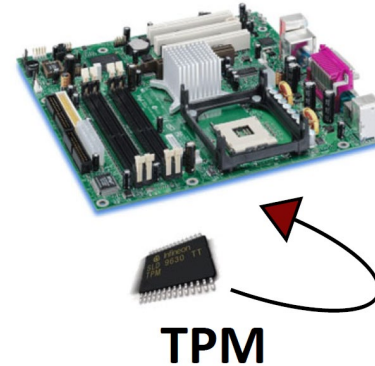


Trusted Computing

Definition: Ein System ist trusted wenn es sich berechenbar und absehbar verhält.

Wie setzt man diese Ziele um?

- Einbau eines TP-Moduls
- Zufallsgenerator – erzeugt kryptografische Schlüssel
- **Platform Configuration Register (PCR)**



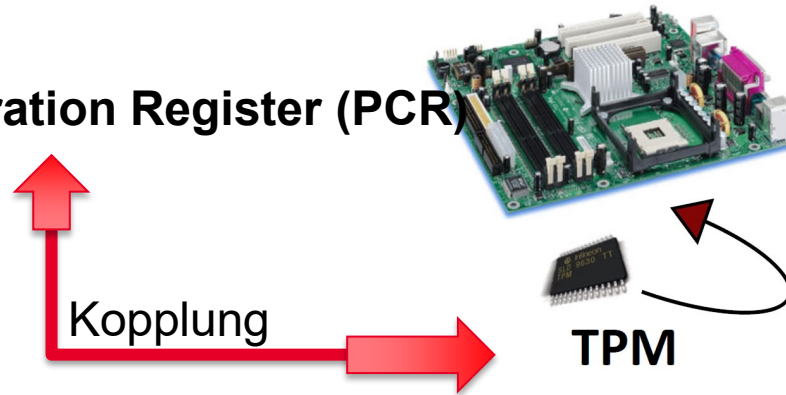
Sitzt auf den Main-Board Ihres PCs

Trusted Computing

Definition: Ein System ist trusted wenn es sich berechenbar und absehbar verhält.

Wie setzt man diese Ziele um?

- **Platform Configuration Register (PCR)**



Trusted Computing

Definition: Ein System ist trusted wenn es sich berechenbar und absehbar verhält.

Wie setzt man diese Ziele um?

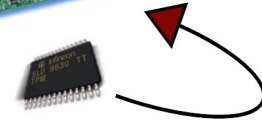
- **Platform Configuration Register (PCR)**

Sealing

Errechnete Schlüssel werden auf
PCR angepasst.

Kopplung

TPM

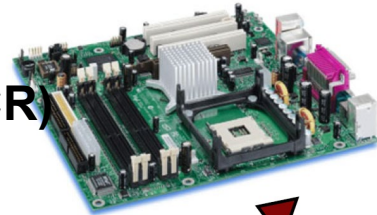


Trusted Computing

Definition: Ein System ist trusted wenn es sich berechenbar und absehbar verhält.

Wie setzt man diese Ziele um?

- **Platform Configuration Register (PCR)**



Sealing

Lassen sich nicht aufbrechen.

Kopplung

TPM



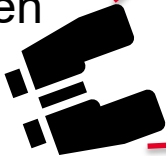
Trusted Computing

Definition: Ein System ist trusted wenn es sich berechenbar und absehbar verhält.

Wie setzt man diese Ziele um?

- Platform Configuration Register (PCR)

Unternehmen



Kopplung



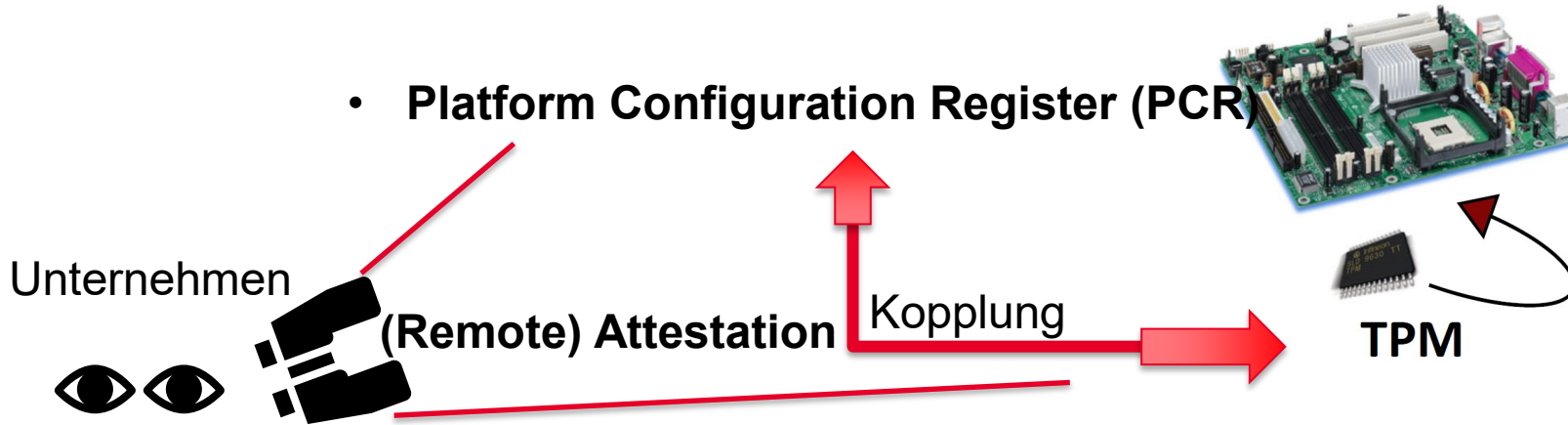
TPM

Trusted Computing

Definition: Ein System ist trusted wenn es sich berechenbar und absehbar verhält.

Wie setzt man diese Ziele um?

- Platform Configuration Register (PCR)

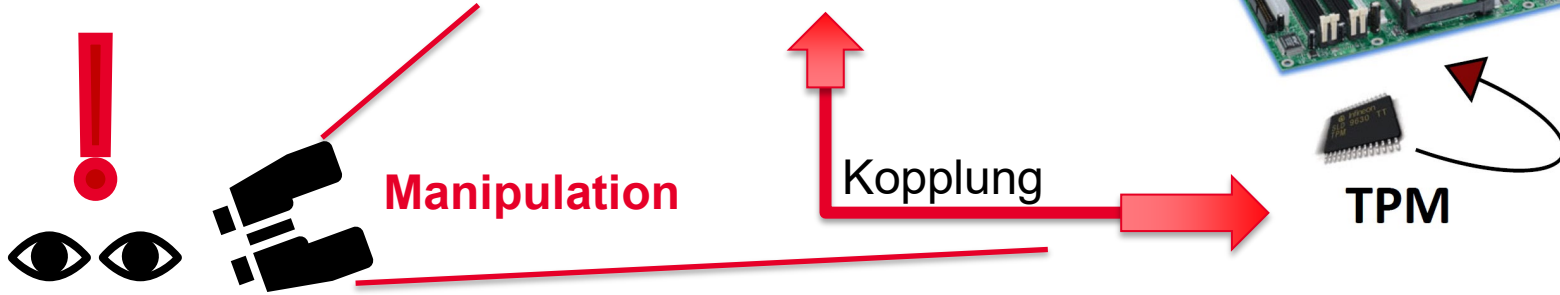


Trusted Computing

Definition: Ein System ist trusted wenn es sich berechenbar und absehbar verhält.

Wie setzt man diese Ziele um?

- Platform Configuration Register (PCR)

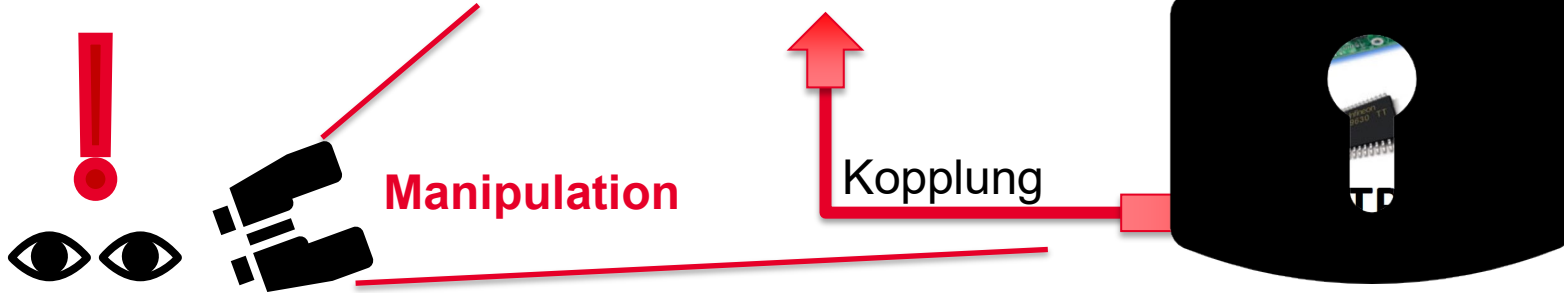


Trusted Computing

Definition: Ein System ist trusted wenn es sich berechenbar und absehbar verhält.

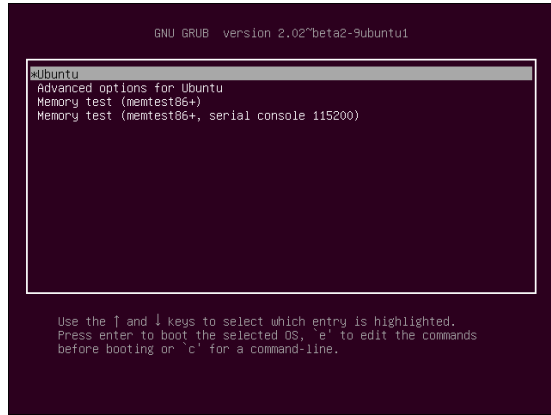
Sperrt den PC aus der Ferne.

- Platform Configuration Register (PCR)



Trusted Computing

Definition: Ein System ist trusted wenn es sich berechenbar und absehbar verhält.



Kopplung an
Bootloader.

Configuration Register (PCR)



TPM

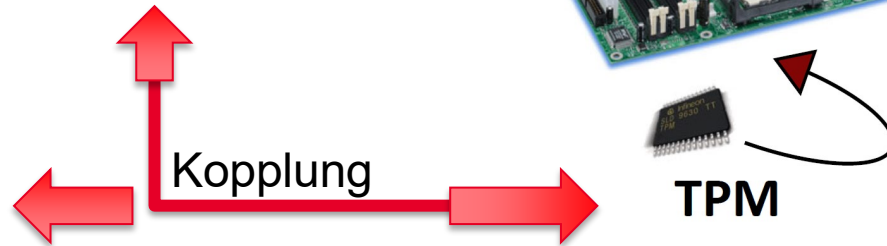
Trusted Computing

Definition: Ein System ist trusted wenn es sich berechenbar und absehbar verhält.

- Platform Configuration Register (PCR)

Authenticated Boot

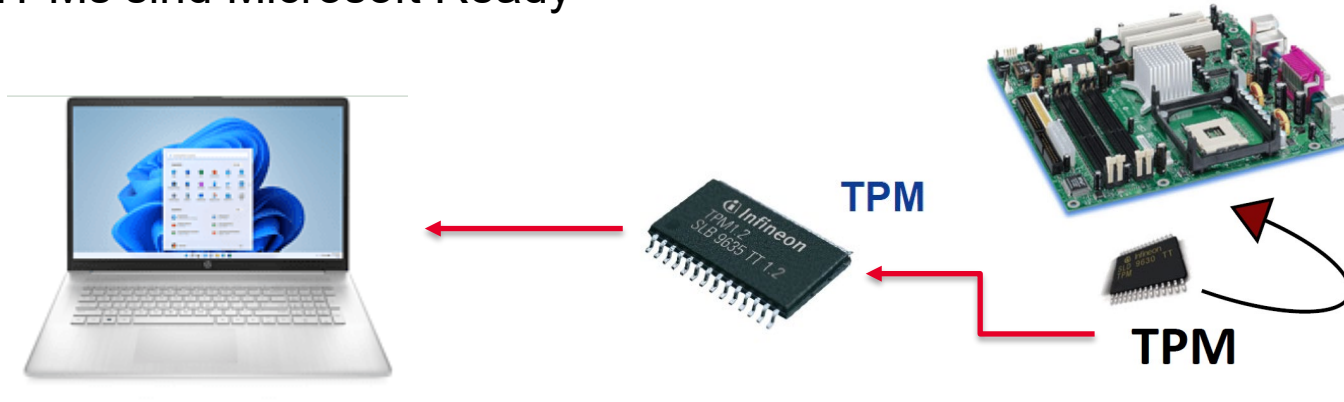
Kopplung an
Bootloader.



Trusted Computing

Definition: Ein System ist trusted wenn es sich berechenbar und absehbar verhält.

- TPMs sind Microsoft Ready



Trusted Computing

Implementierung einer TPM in
das Unternehmen

Möglichkeit 1



Airbag – „bitte lass es
nicht zu dulle
schmerzen“

Trusted Computing

Implementierung einer TPM in
das Unternehmen

Möglichkeit 2



ESP – greift ein,
Schaden wird im besten
Fall verhindert.

Trusted Computing

Implementierung einer TPM in
das Unternehmen

Möglichkeit 2



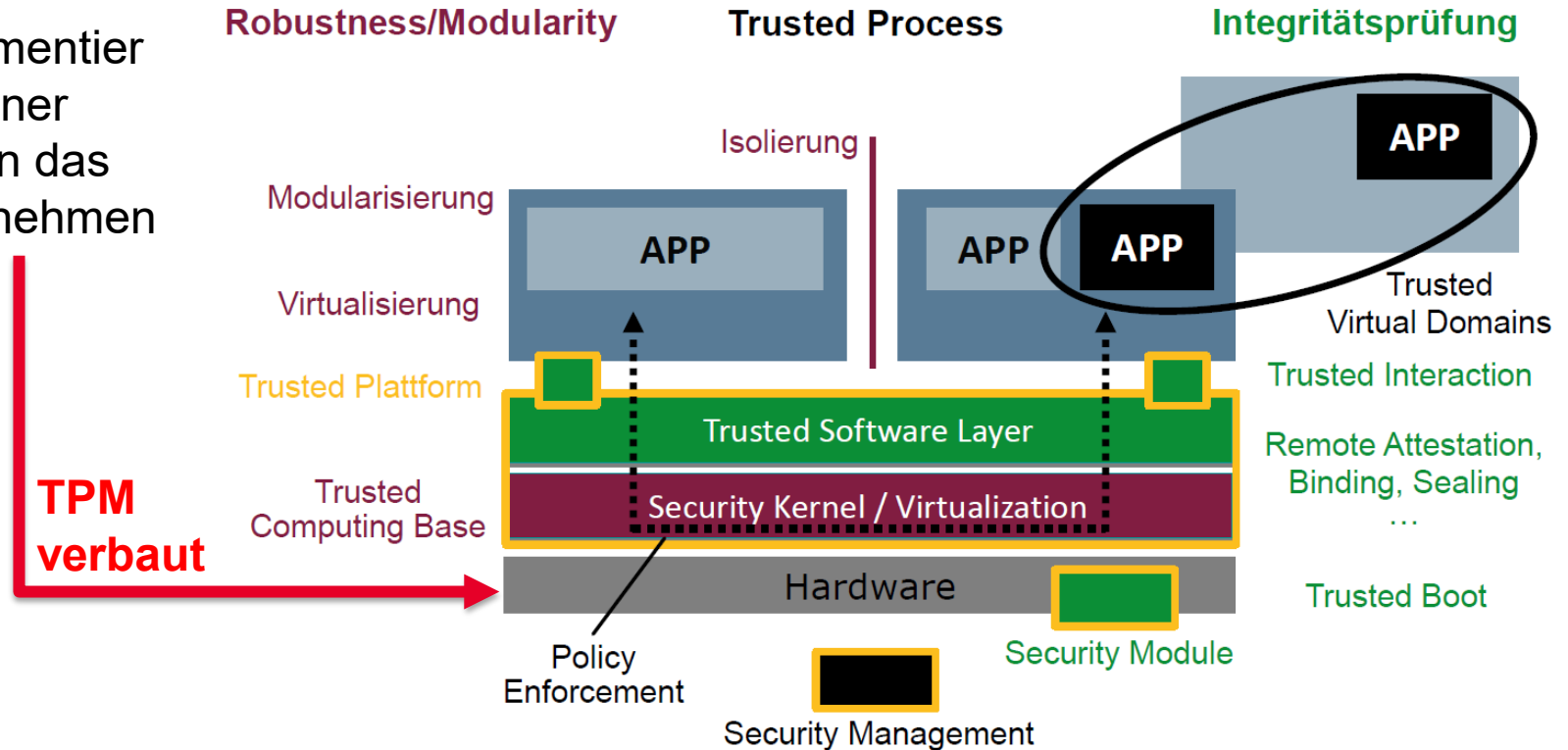
ESP – greift ein,
Schaden wird im besten
Fall verhindert.

**TPM orientiert
sich hier
dran.**

Wir wollen einen Unfall
verhinder!

Trusted Computing

Implementierung einer TPM in das Unternehmen



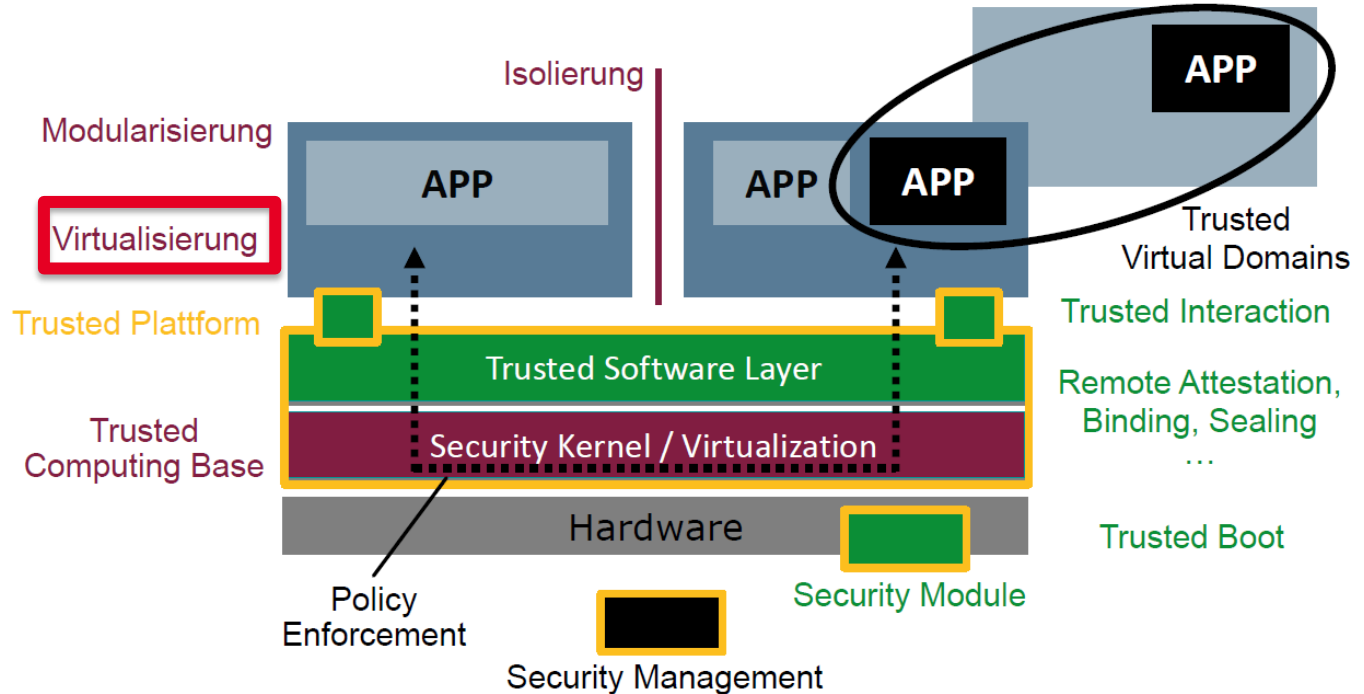
Trusted Computing

- Virtualisierung auf dem Endgerät
- Fehler treten in einer Sandbox auf
- Reset auf stabilen Zustand sehr schnell möglich

Robustness/Modularity

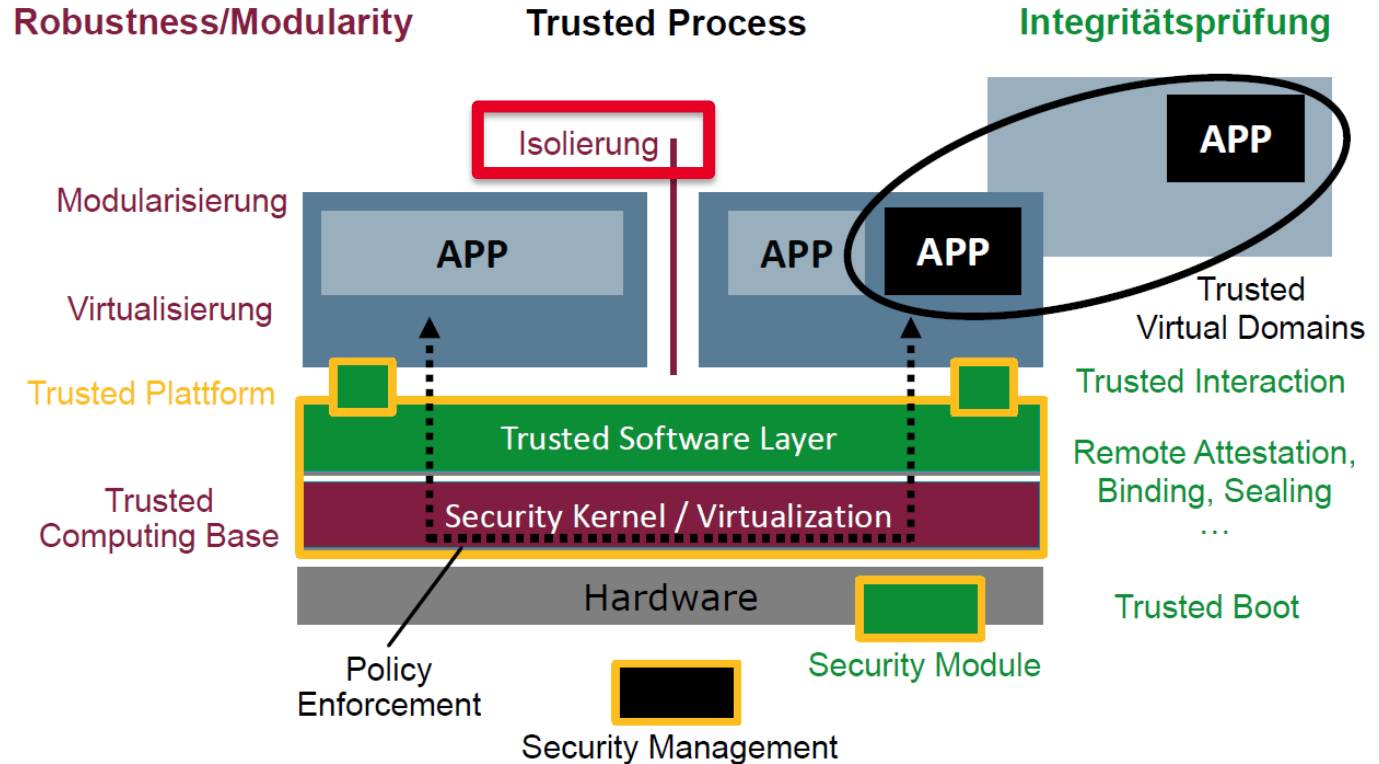
Trusted Process

Integritätsprüfung



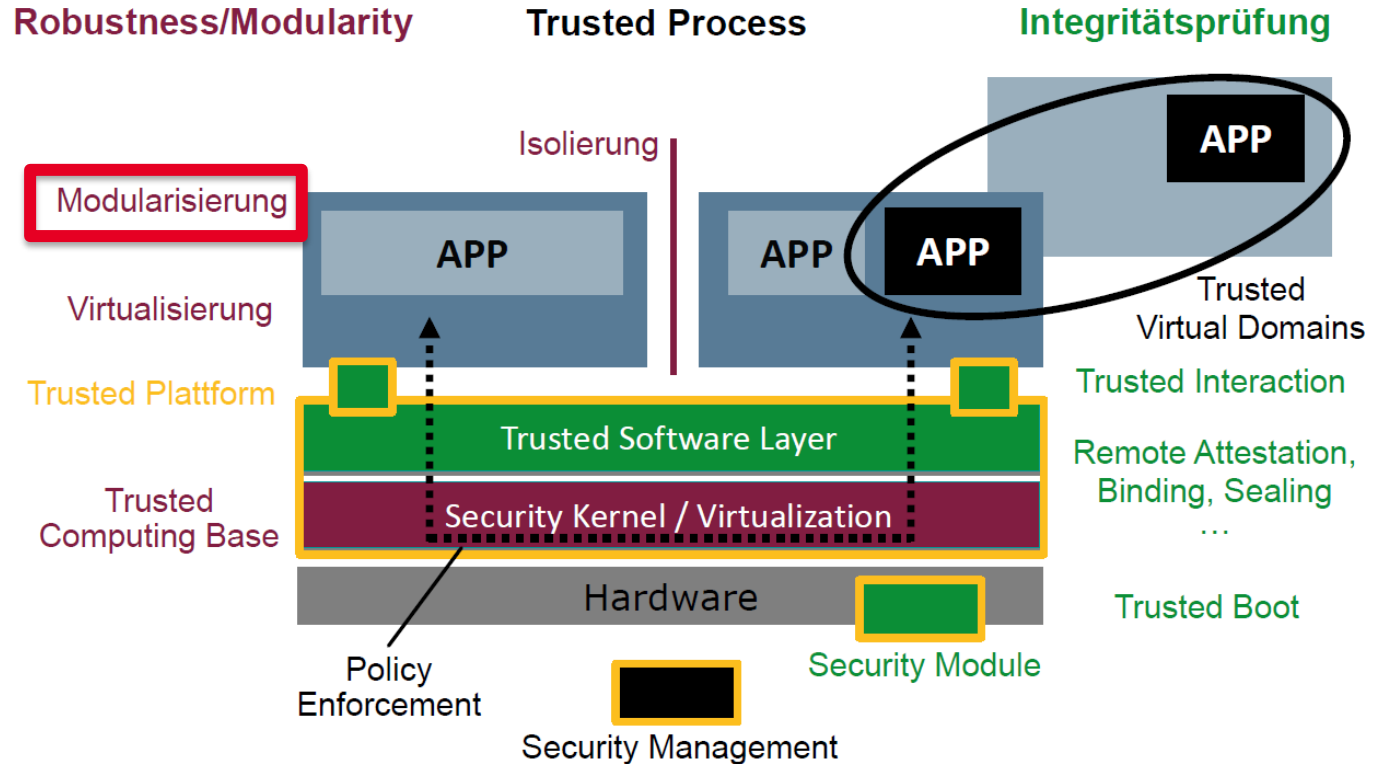
Trusted Computing

- Virtualisierte Umgebungen lassen sich schnell isolieren
- Wie wird isoliert?
- Verbot der Kommunikation
- Verschlüsselung der Daten auf VM



Trusted Computing

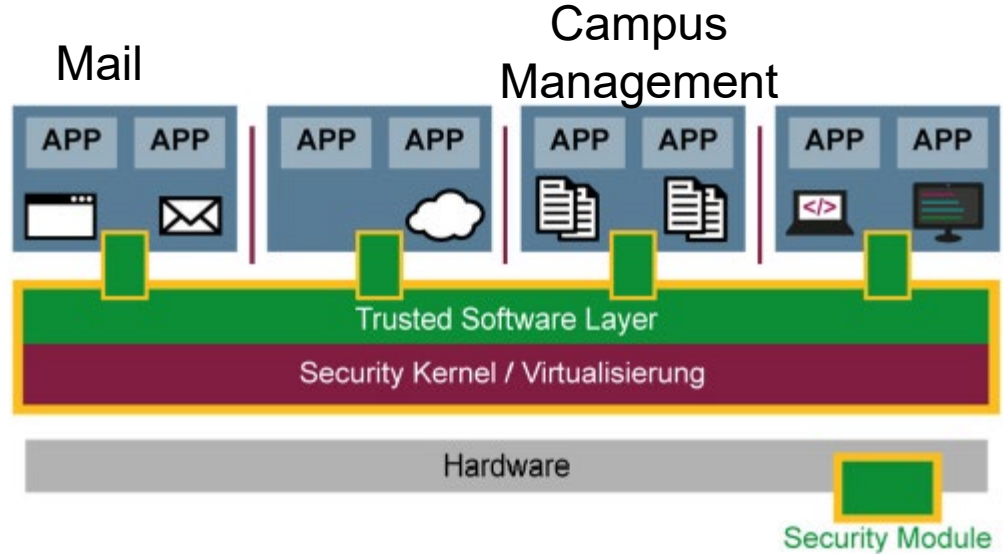
- Bildung von modularen VM Pools
- Campus Management VMs laufen in einem Pool
- Office Pakete laufen in einer davon getrennten Umgebung



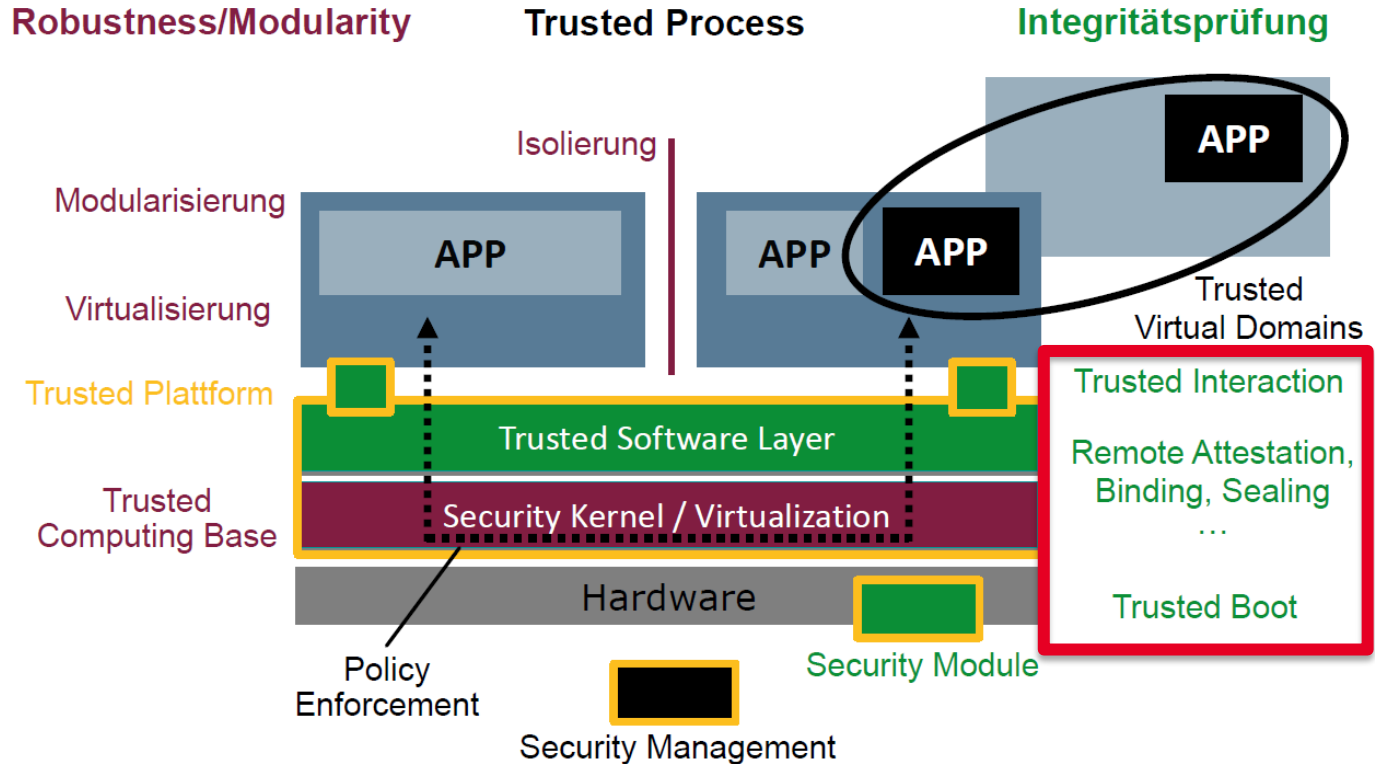
Trusted Computing

- Bildung von modularen VM Pools
- Campus Management VMs laufen in einem Pool
- Office Pakete laufen in einer davon getrennten Umgebung

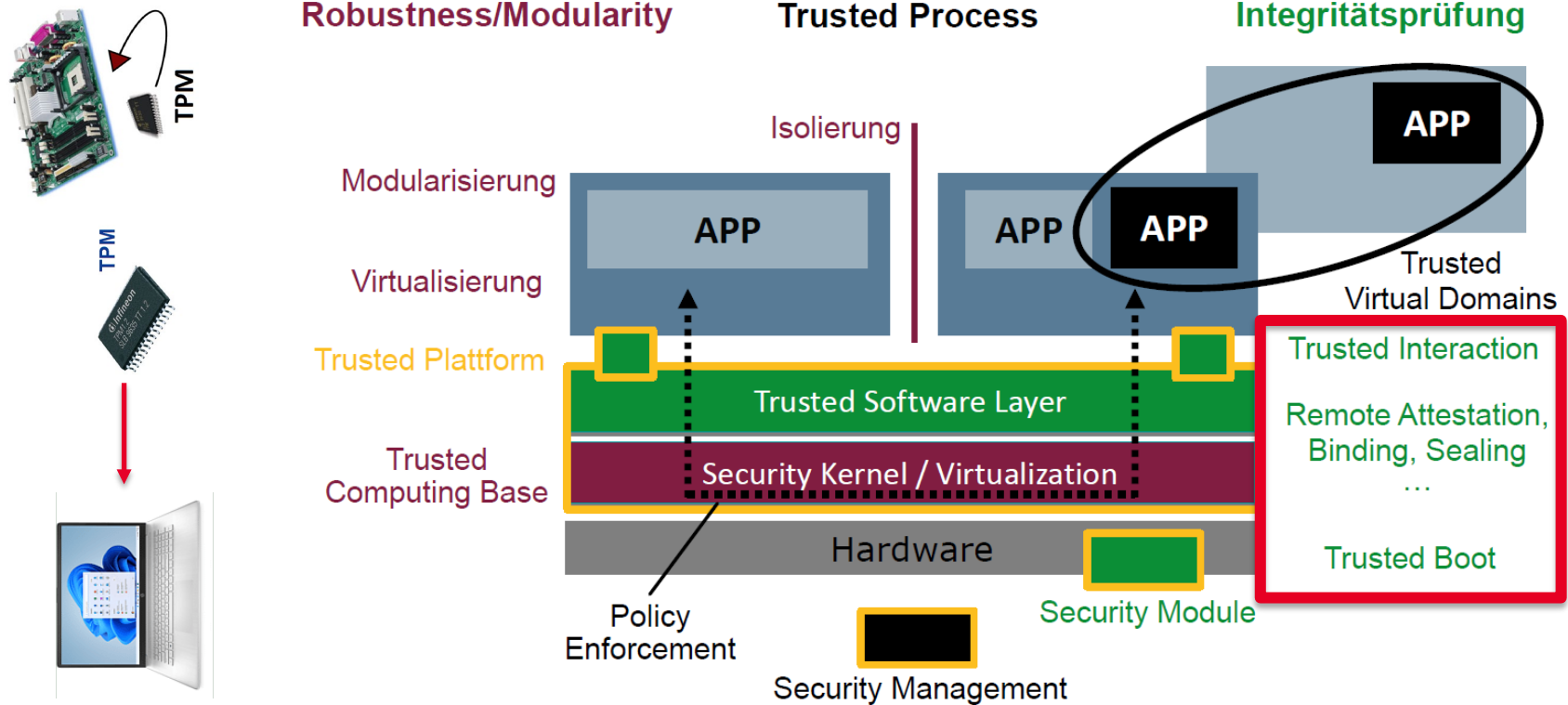
Modularisierung



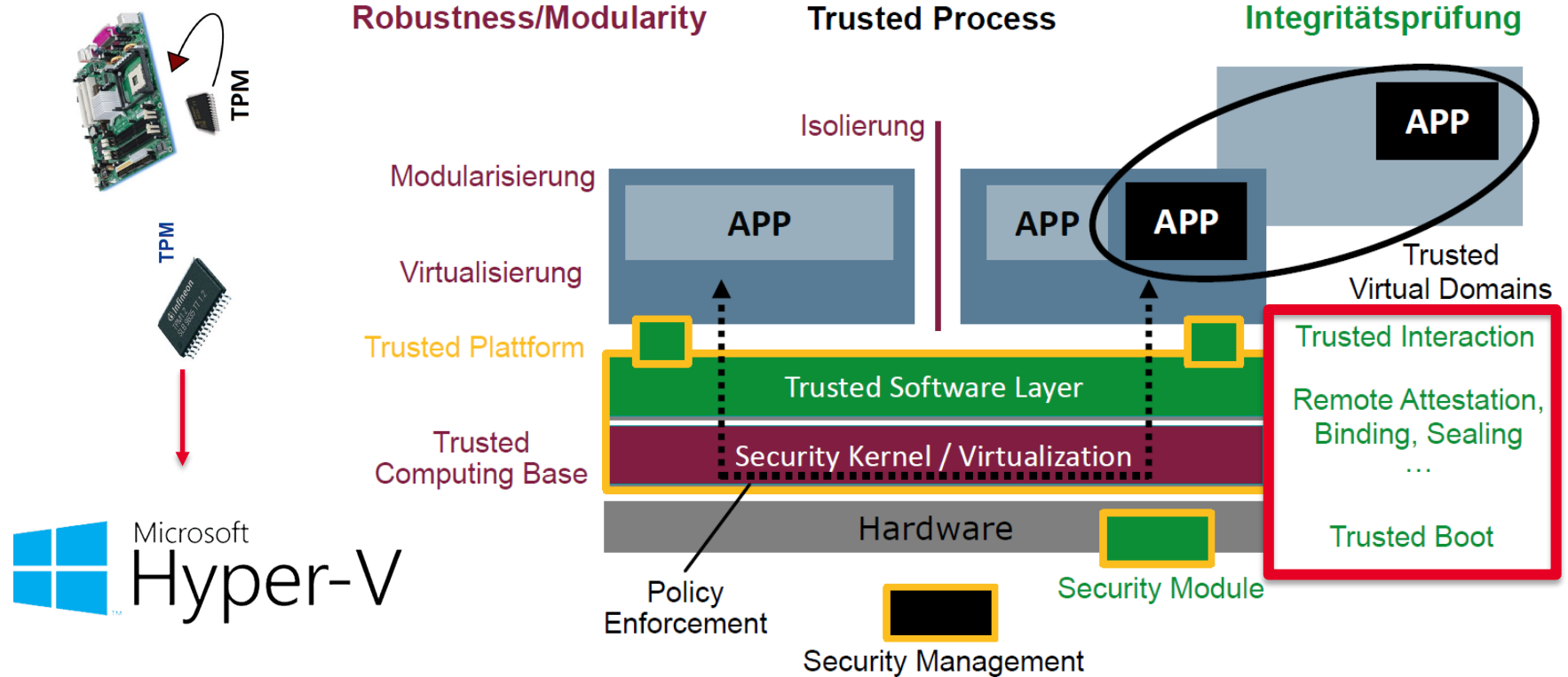
Trusted Computing



Trusted Computing

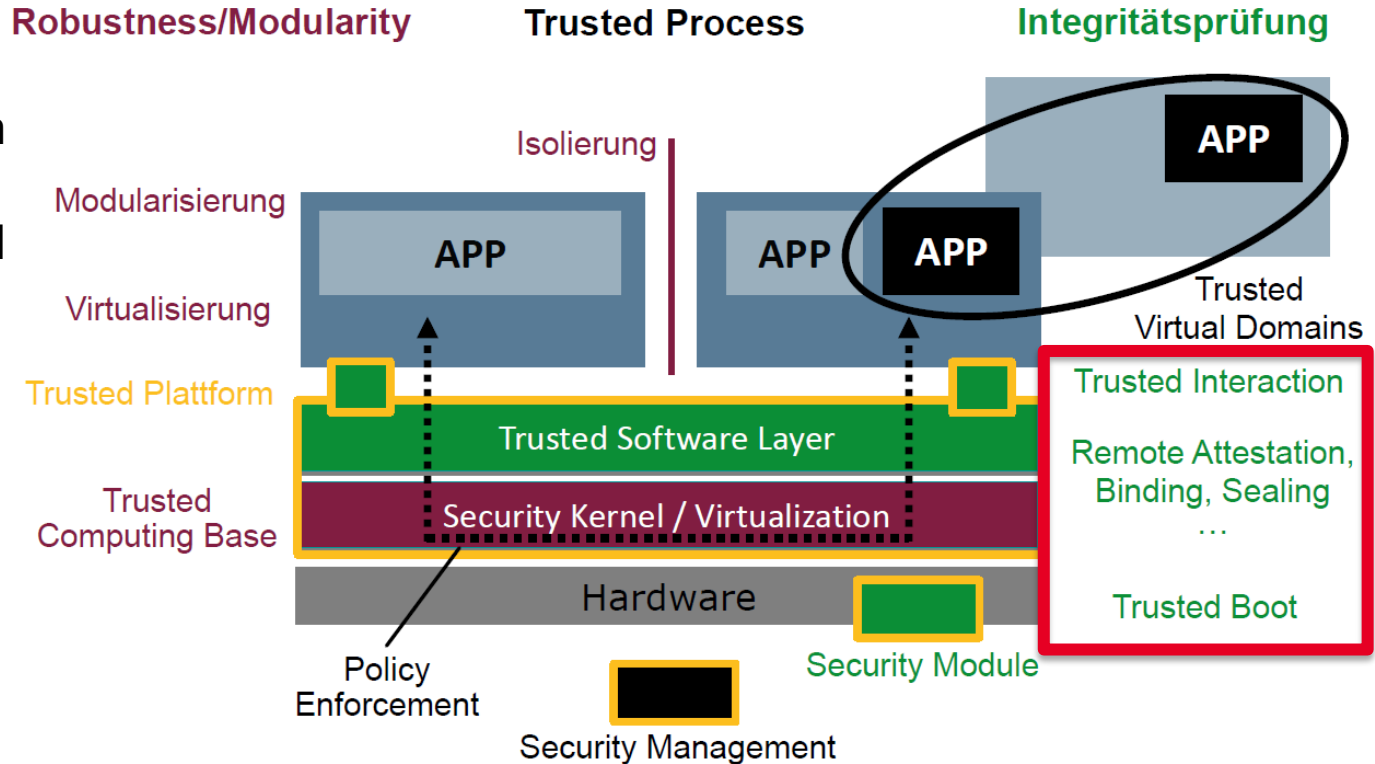


Trusted Computing

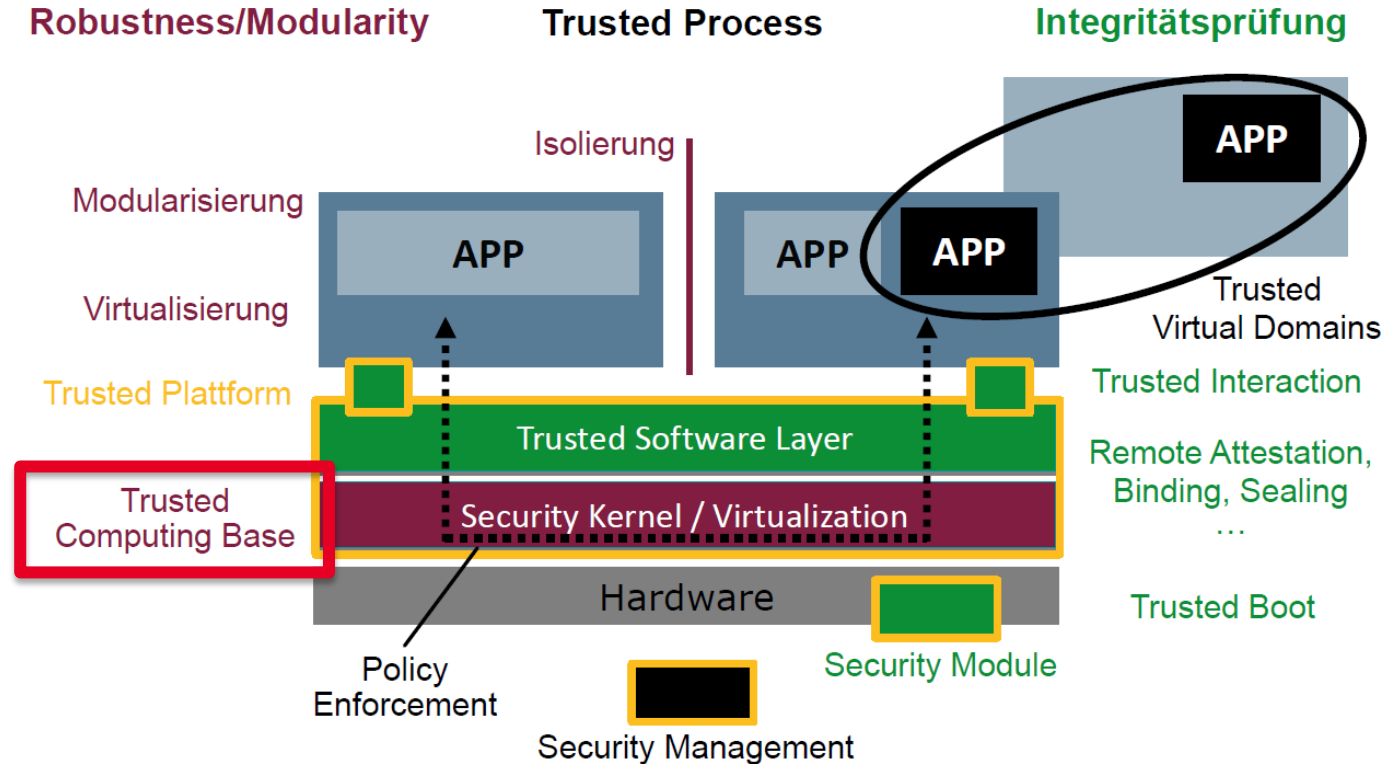


Trusted Computing

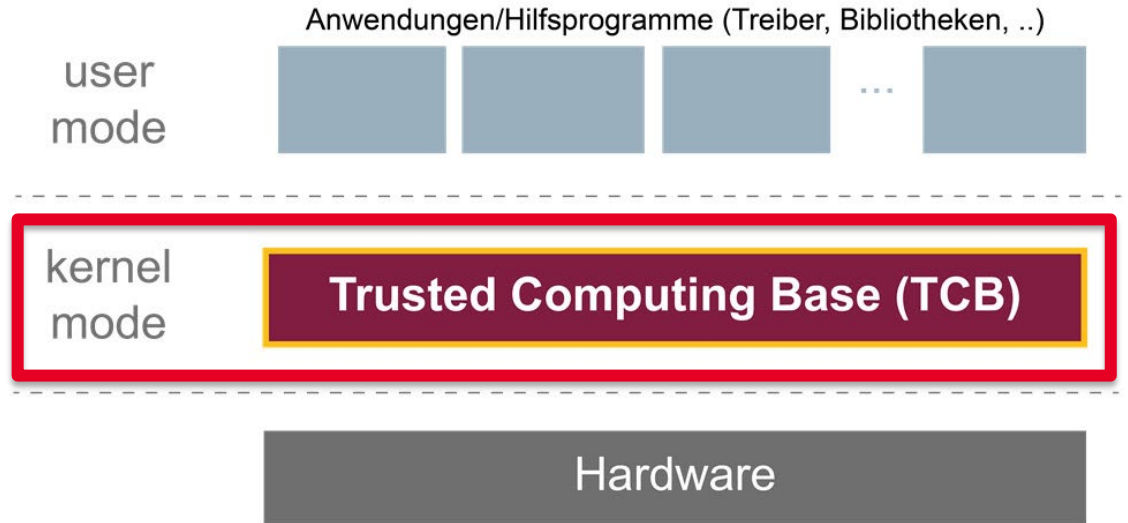
- VM Boot nur in einem bekannten und sicheren Zustand.



Trusted Computing



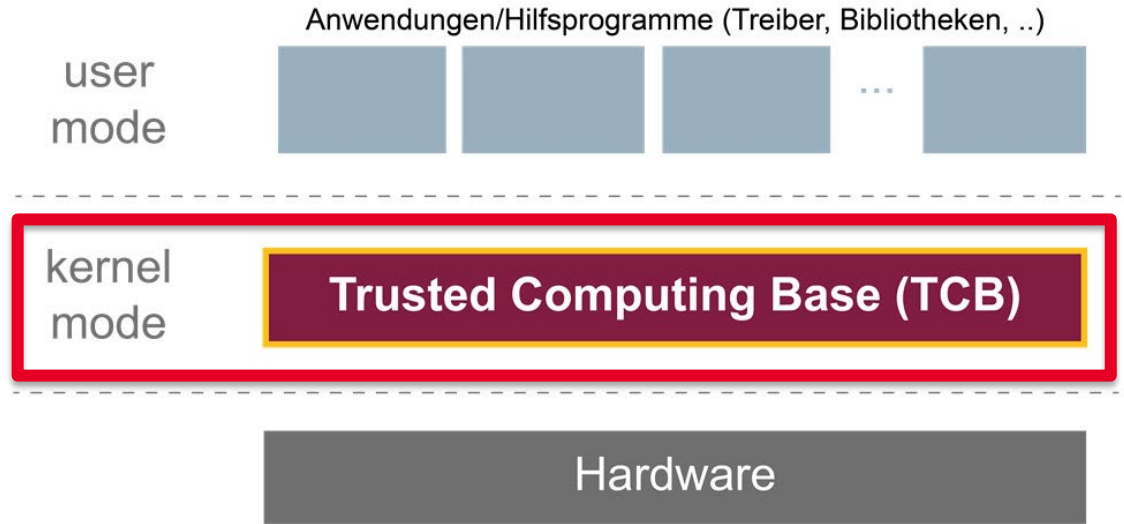
Trusted Computing



Trusted Computing

Sicherheitsfundament
jeder Organisation

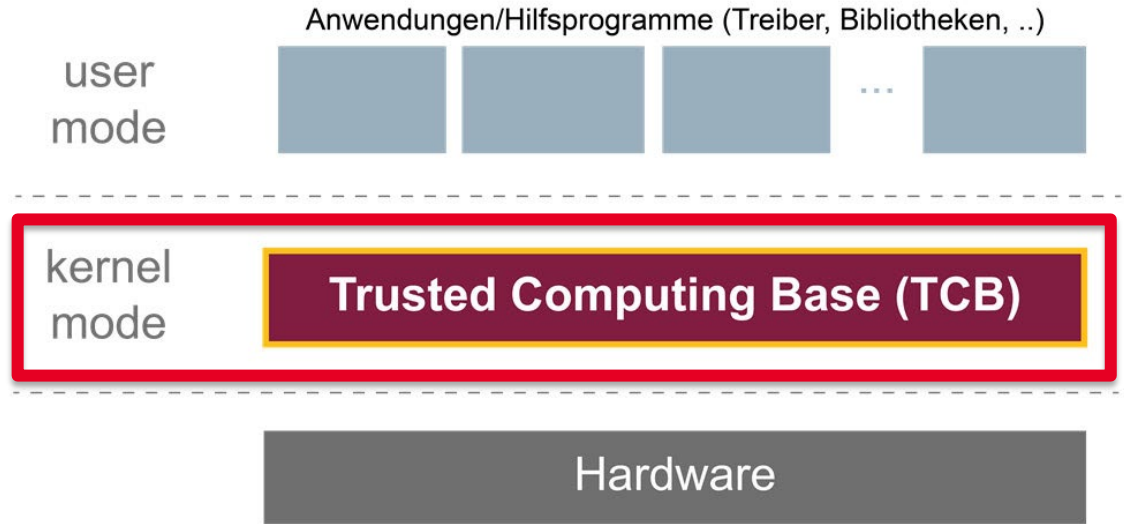
- Wenn Basis
kompromittiert ist der
Schaden groß
- Schwachstelle im TCB
Alles ist angreifbar



Trusted Computing

Sicherheitsfundament
jeder Organisation

- Wenn Basis
kompromittiert ist der
Schaden groß
- Schwachstelle im TCB
Alles ist angreifbar
- **Meist mehr als 20.000
Zeilen an Code**

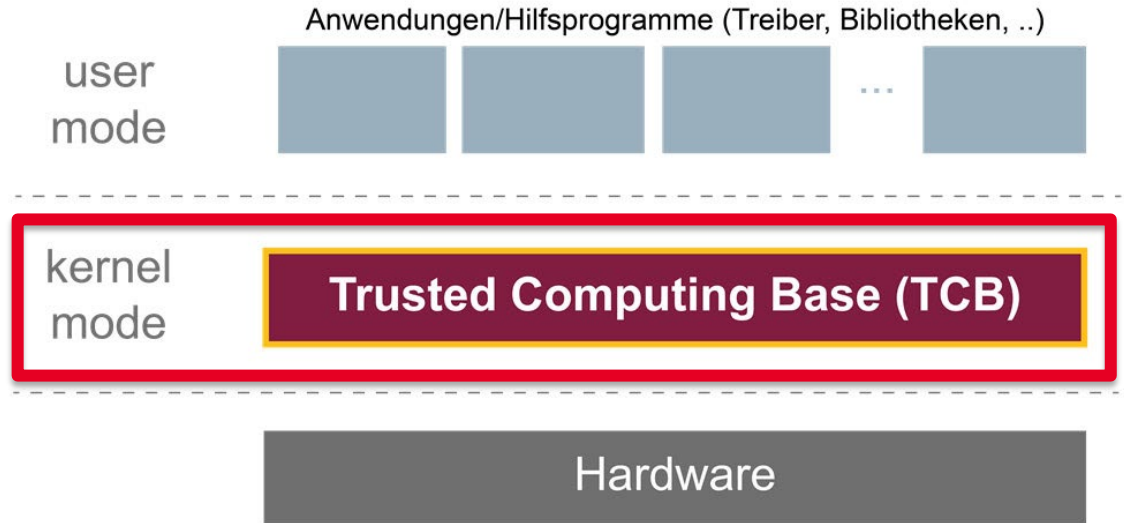


Trusted Computing



Sicherheitsfundament
jeder Organisation

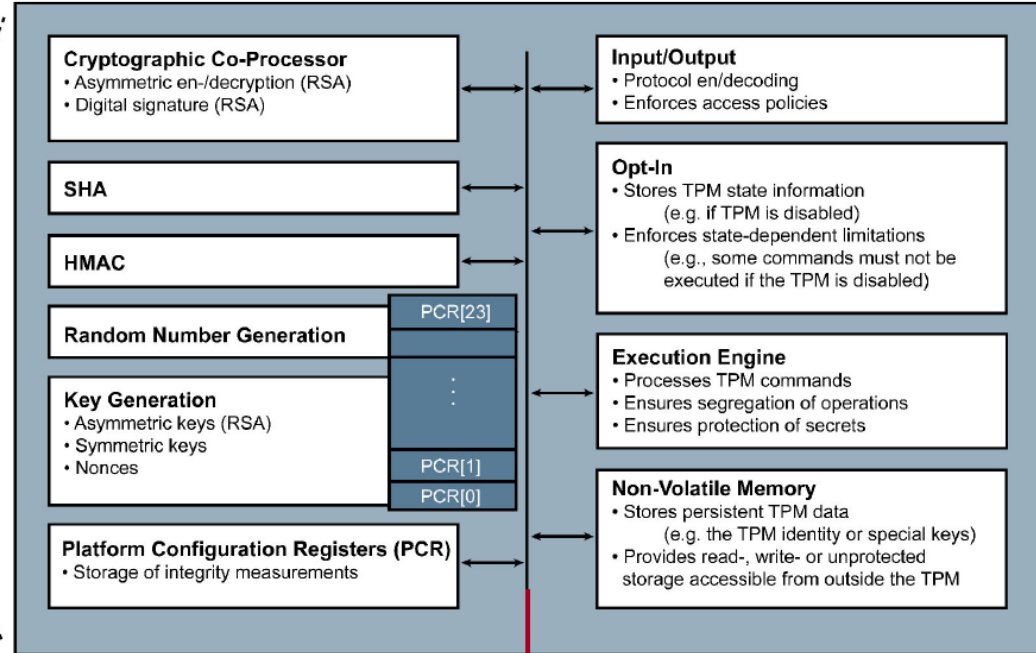
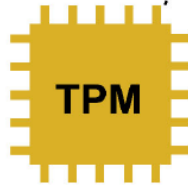
- Wenn Basis
kompromittiert ist der
Schaden groß
- Schwachstelle im TCB
Alles ist angreifbar
- **Meist mehr als 20.000
Zeilen an Code**



Trusted Computing

Basisfunktionen

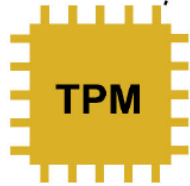
TPM Revisited



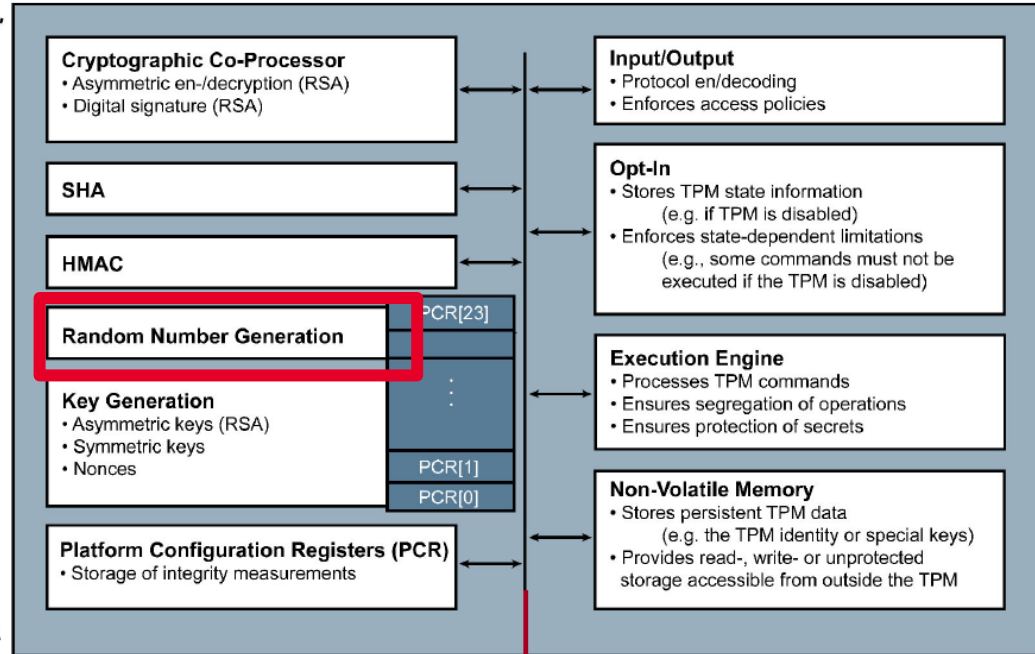
Sealing — Attestation

Trusted Computing

TPM Revisited



Basisfunktionen

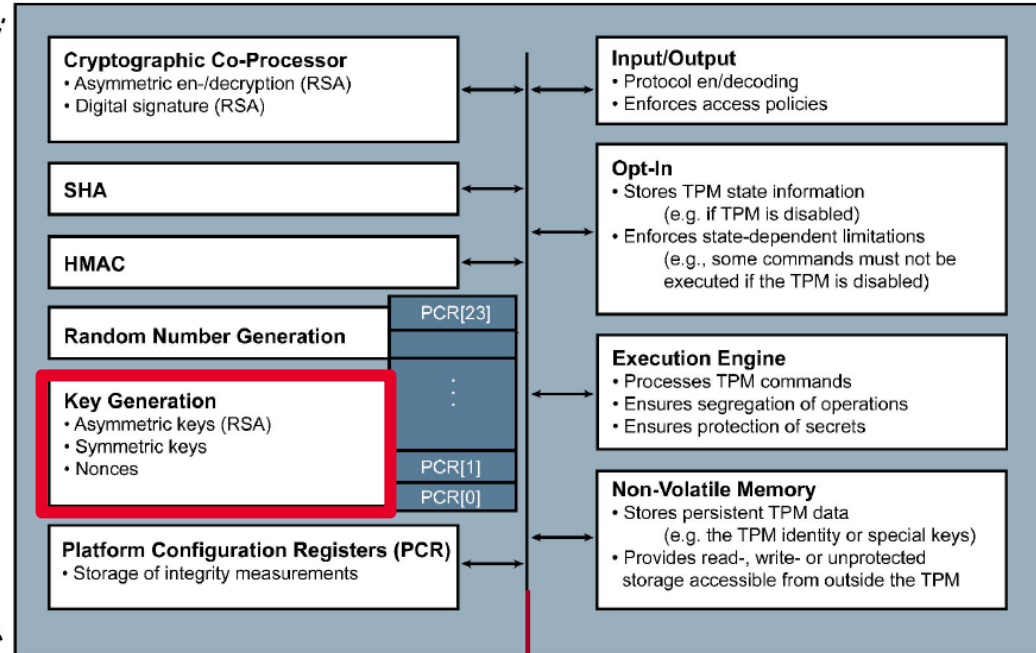
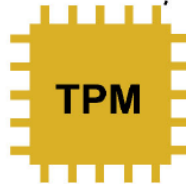


Sealing — Attestation

Trusted Computing

Basisfunktionen

TPM Revisited

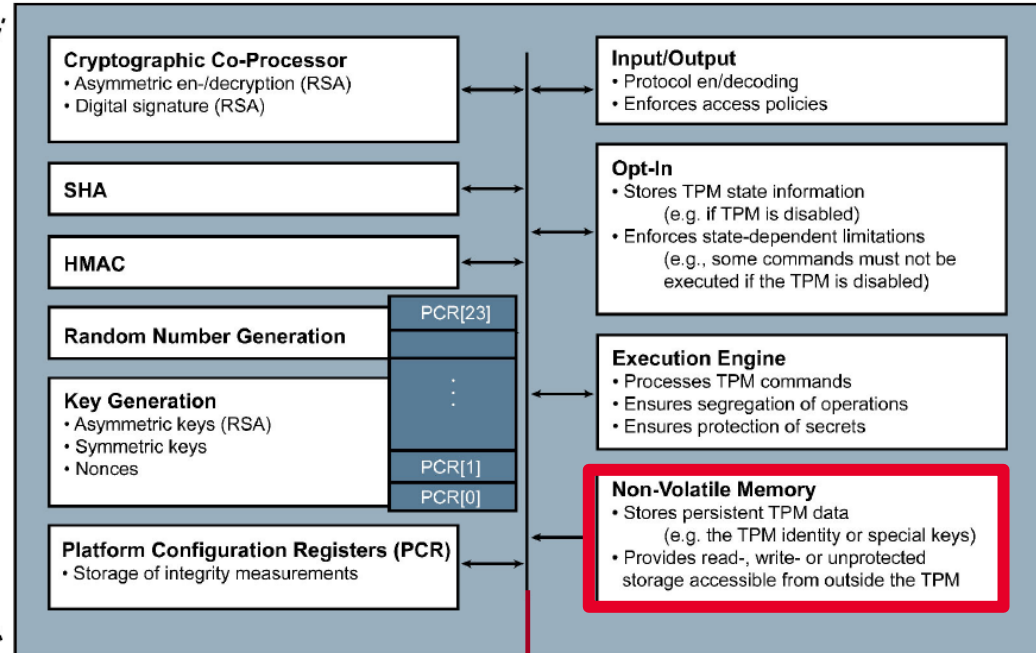
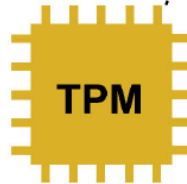


Sealing — Attestation

Trusted Computing

Basisfunktionen

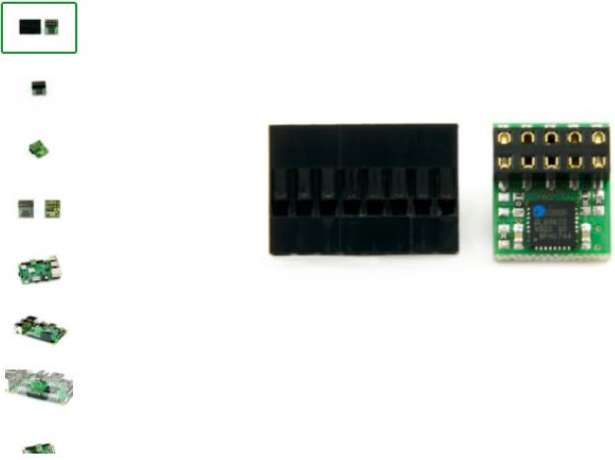
TPM Revisited



Sealing — Attestation

Trusted Computing

TPM Kosten - Raspberry Pi



LetsTrust TPM for Raspberry Pi

LETSTRUST
★★★★★ 11 Reviews

SKU: p-letstrust
MPN: p-letstrust
EAN / Barcode: 0700729578049
Lieferfrist: Sofort versandfertig, Lieferfrist 1-2 Tage

Preis: **25,00 €**
Inkl. Steuern **Versand** wird an der Kasse berechnet

Lager: ● **Auf Lager**

Menge:

In den Warenkorb legen **Jetzt kaufen**

Beschreibung

Trusted Computing

Core Root of Trust for Measurement - CRTM

- Eine trusted **Computing Umgebung** braucht eine **Basis** des **Vertrauens**
- Basis Root of Trust

TRUSTED[®]
COMPUTING
GROUP

Trusted Computing

Core Root of Trust for Measurement - CRTM

- Eine trusted **Computing Umgebung** braucht eine **Basis** des **Vertrauens**
- Basis Root of Trust
- CRTM nimmt eine Messung über einzelne Systemzustände vor.
- Umfasst Hard und Software
- Ergebnisse werden an den PCR geliefert und gespeichert

TRUSTED[®]
COMPUTING
GROUP

Trusted Computing

Idee des transitiven Vertrauen

Entity E_0

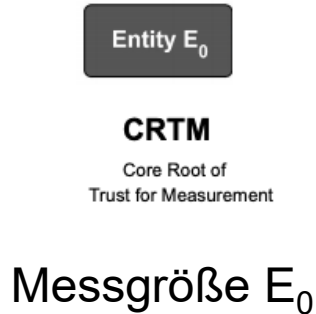
CRTM

Core Root of
Trust for Measurement

Messgröße E_0

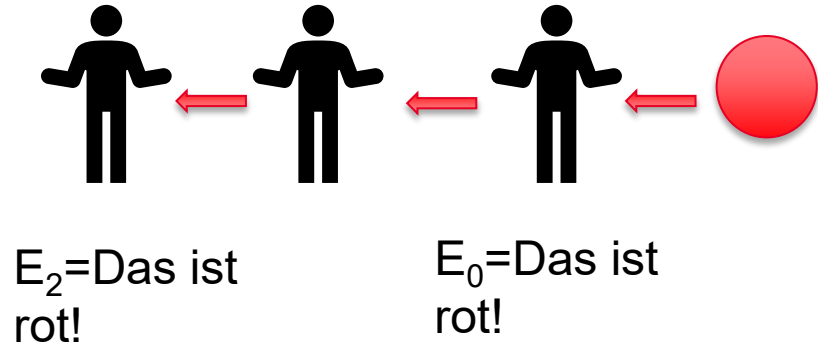
Trusted Computing

Idee des transitiven Vertrauen



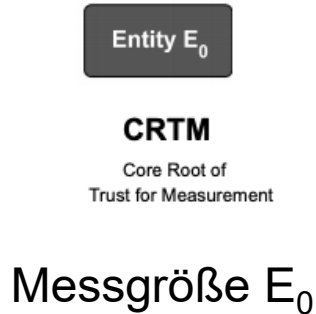
Was wollen wir erreichen?

Eine Trust-Chain.



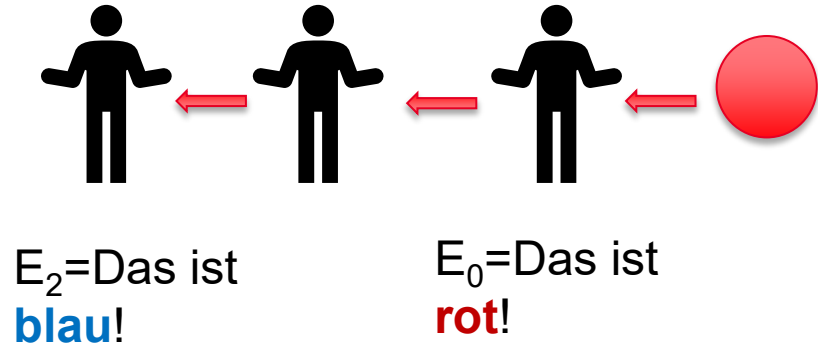
Trusted Computing

Idee des transitiven Vertrauen



Was wollen wir erreichen?

Eine Trust-Chain.



Trusted Computing

Idee des transitiven Vertrauen

Entity E_0

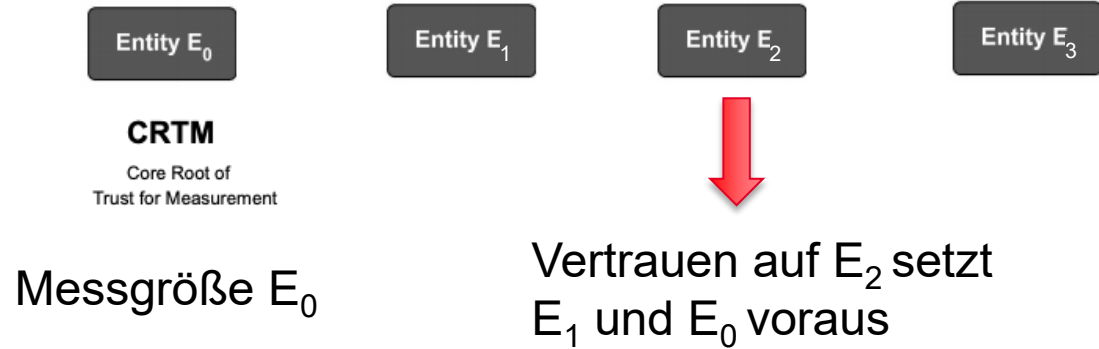
CRTM

Core Root of
Trust for Measurement

Messgröße E_0

Trusted Computing

Idee des transitiven Vertrauen



Trusted Computing

Authenticated Boot

Transitiven Vertrauen oder der Boot wird abgebrochen.

- **Ablauf:**

Berechnung des Hashwertes und Schreiben in ein PCR-Register

- Vertrauenswürdige CRTM Software → BIOS
- BIOS → Boot Loaders, Hardwarezustand (Mainboard, ROM-Konfigu. ...)
- Boot Loader → Betriebssystem
- Betriebssystem → Anwendung

Trusted Computing

Authenticated Boot

Transitiven Vertrauen oder der Boot wird abgebrochen.

Werte können auch aus der Ferne kontrolliert werden.

■ Ablauf:

Berechnung des Hashwertes und Schreiben in ein PCR-Register

- Vertrauenswürdige CRTM Software → BIOS
- BIOS → Boot Loaders, Hardwarezustand (Mainboard, ROM-Konfigu. ...)
- Boot Loader → Betriebssystem
- Betriebssystem → Anwendung

Trusted Computing

Authenticated Boot

Transitiven Vertrauen oder der Boot wird abgebrochen.

Werte können auch aus der Ferne kontrolliert werden.

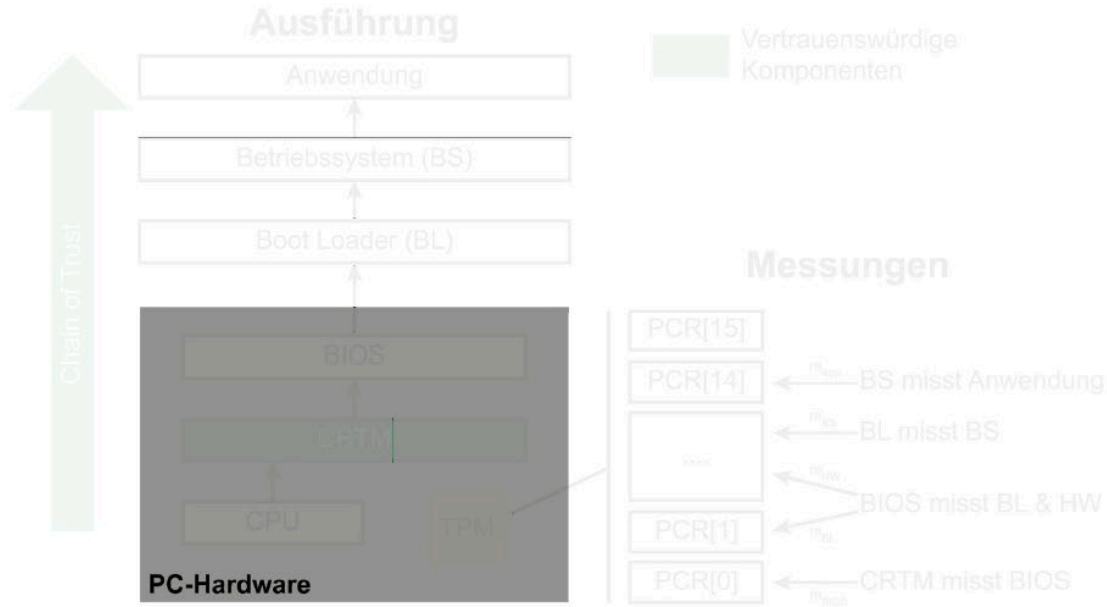
■ Ablauf:

Berechnung des Hashwertes und Schreiben in ein PCR-Register

- Vertrauenswürdige CRTM Software → BIOS
- BIOS → Boot Loaders, Hardwarezustand (Mainboard, ROM-Konfigu. ...)
- Boot Loader → Betriebssystem
- Betriebssystem → Anwendung

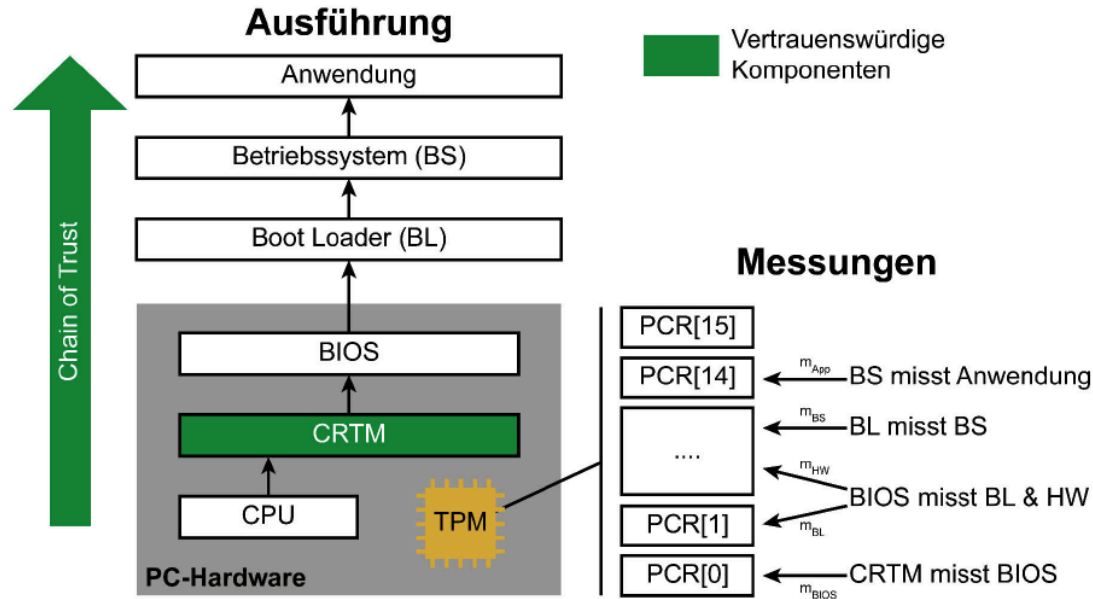
Trusted Computing

Authenticated Boot



Trusted Computing

Authenticated Boot



Trusted Computing

Authenticated Boot – Sealing

Eingabe Parameter

daten

{unverschlüsselte Daten}

Ausgabe Parameter

cipher

{verschlüsselte Daten}

cryptedKEY

{verschlüsselter Schlüssel}

TPM Interne Funktionen und Daten

encrypt (key, daten)

{symmetrischer Verschlüsselungsalgorithmus „AES“}

H (daten)

{One-Way-Hashfunktion „SHA-256“}

genKey()

{Schlüsselerzeugung}

SRK

{Storage Root Key}

PCRs

{PCR-0, PCR-1, ...} z.B. aktuell abgespeicherte PCR-Werte

plainKEY = genKEY ()

cipher = encrypt (plainKEY, (daten // H (daten // PCR-0 // ... // PCR-x))

cryptedKEY = encrypt (SRK, plainKEY // H (plainKEY))

Trusted Computing

Authenticated Boot - Sealing

Eingabe Parameter

<i>cipher</i>	<i>{verschlüsselte Daten}</i>
<i>cryptedKEY</i>	<i>{verschlüsselter Schlüssel}</i>

Ausgabe Parameter

<i>daten</i>	<i>{unverschlüsselte Daten}</i>
--------------	---------------------------------

TPM Interne Funktionen und Daten

<i>decrypt (key, daten)</i>	<i>{symmetrischer Verschlüsselungsalgorithmus „AES“}</i>
<i>H (daten)</i>	<i>{One-Way-Hashfunktion „SHA-256“}</i>
<i>checkPCRs (Hash-Value)</i>	<i>{vergleicht PCRs-Inhalte mit Hash-Value}</i>
<i>SRK</i>	<i>{Storage Root Key}</i>
<i>PCRs</i>	<i>{PCR-0, PCR-1, ...}</i>

plainKEY = decrypt (SRK, cryptedKEY)

daten // H (daten // PCR-0 // ... // PCR-x) = decrypt (plainKEY, cipher)

if (checkPCRs (Hash-Value))

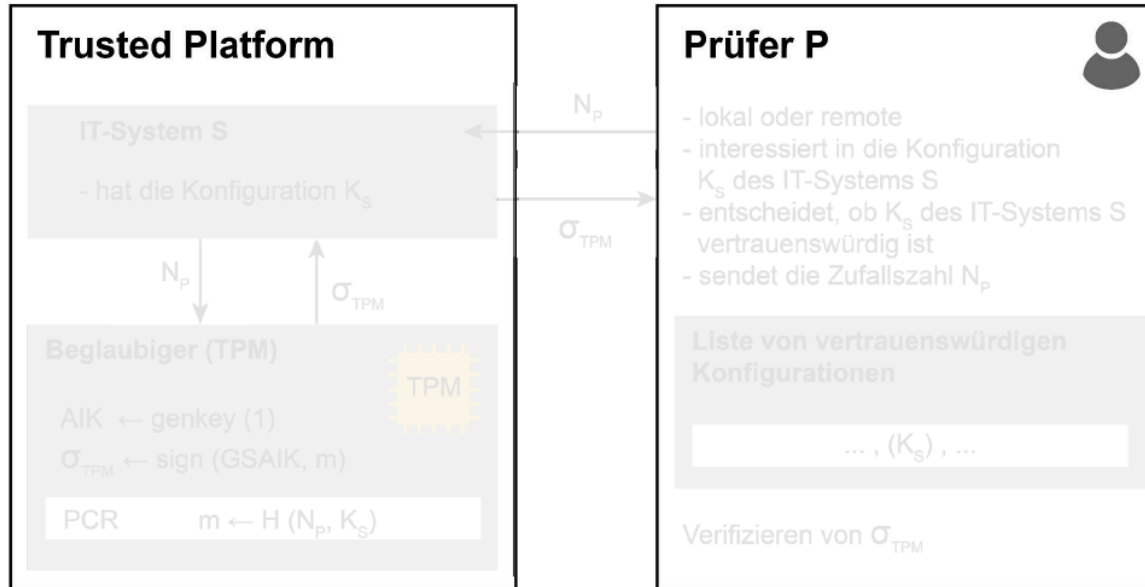
return daten

else

return ERROR

Trusted Computing

Authenticated Boot – Remote Attestation



Trusted Computing

Authenticated Boot – Remote Attestation

