Linux Powered Trusted Computing

DI Martin Pirker <martin.pirker@iaik.tugraz.at>
DI Thomas Winkler <thomas.winkler@iaik.tugraz.at>

Übersicht

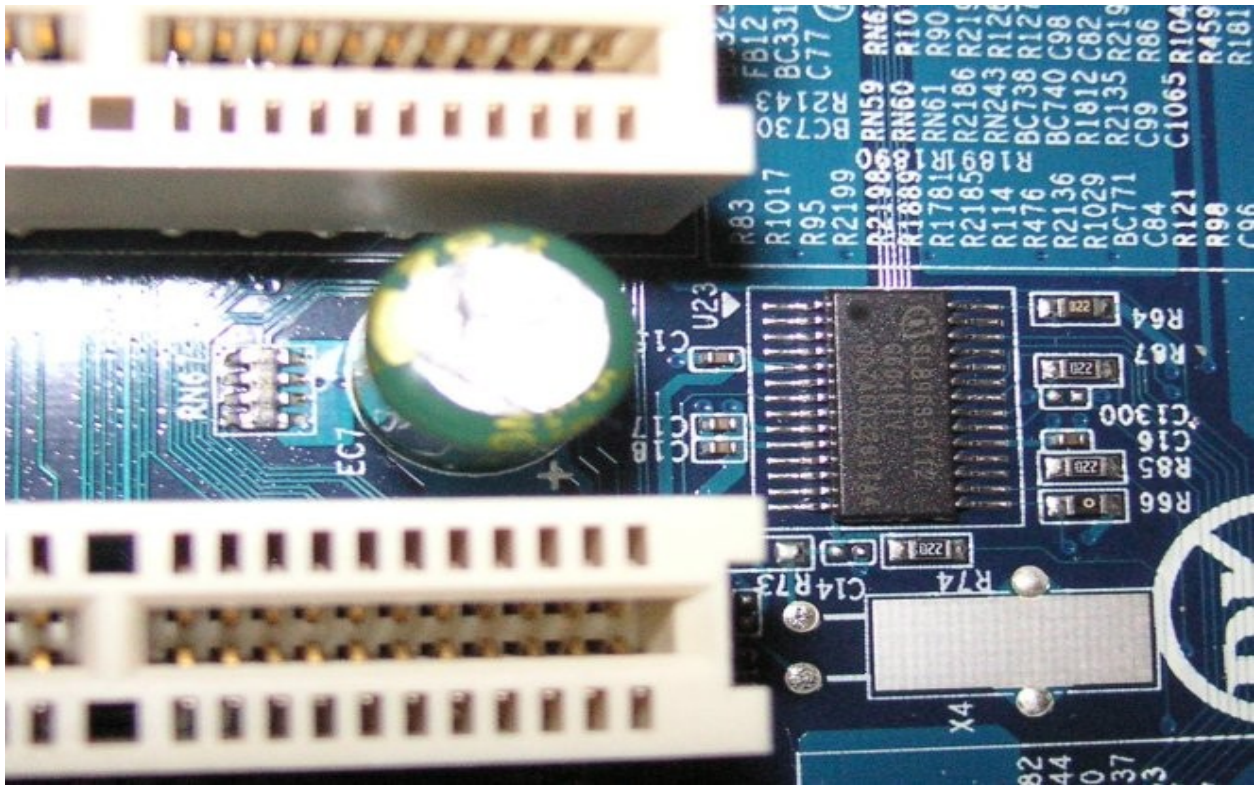
- Einführung und Motivation
- Trusted Computing - Geschichte
- TPM Chips: Hardware, Funktion und Anwendungen
- Chain of Trust
- Kryptografische Schlüssel und Schlüsselverwaltung
- Identitäten
- Attestierung
- Virtualisierung
- Stand der Dinge unter Linux: Treiber, Middleware, Anwendungen

Einführung

- einschlägige Medien voll mit Meldungen über Sicherheitsprobleme
- ständig neue Initiativen um diese Probleme zu lösen
- ein Ansatz: Trusted Computing von der Trusted Computing Group (TCG)
- bietet Möglichkeit festzustellen welche Software auf einem Computer ausgeführt wird
- soll Vertrauen in Computer erhöhen

Motivation (1/2)

- bis heute mehrere Millionen Rechner mit TPMs ausgeliefert
  - wer im Publikum hat schon ein TPM in seinem Rechner?
  - wer weiß was es kann und verwendet ihn?



Motivation (2/2)

- viele unklare und teilweise einseitige Medienberichte
- nächstes Microsoft Betriebssystem soll Trusted Computing unterstützen
- welche Perspektiven gibt es im Open Source Bereich?
- Ziele des Vortrags:
  - welche Technologien stecken hinter Trusted Computing?
  - verstehen der Wechselwirkungen und Konsequenzen
  - Anwendung(en) und Nutzen im Open Source Bereich

Trusted Computing - Organisation

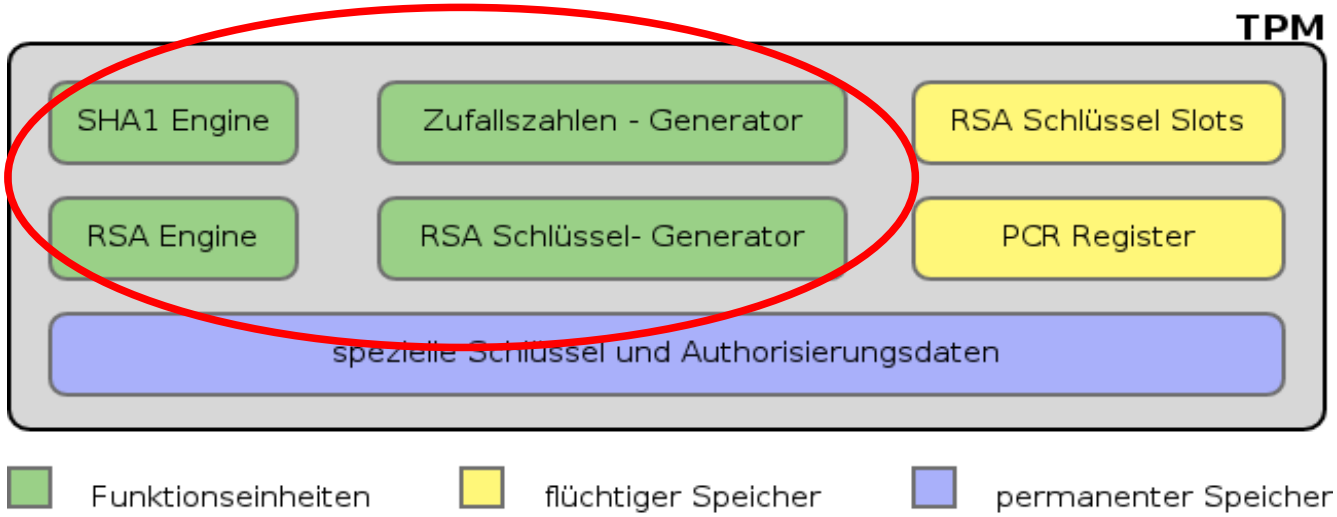
- ursprünglich: TCPA – Trusted Computing Platform Alliance
- jetzt: TCG – Trusted Computing Group
- Führungspositionen (Promotors):
  - AMD, HP, IBM, Infineon, Intel, Lenovo, Microsoft, Sun
- Abstufungen der Mitgliedschaft bis hin zu akademischen Beobachtern (z.B. IAIK)
- Non-Profit Organisation – Entwicklung globaler offener Industriestandards für:
  - Hardware
  - Softwarebibliotheken bzw. Protokolle
- Arbeitsgruppen zu Themenbereichen (TPM, TSS, Mobile, ...)

TPM Chip - Hardware

- TPM – Trusted Platform Module
- Kernstück von Trusted Computing
- Hardware weitaus schwerer manipulierbar als Software
- Low-Cost Device und kein Krypto-Beschleuniger
- auf neuen Motherboards aufgelötet – d.h. TPM ist fixer Bestandteil der Plattform und kann nicht entfernt werden
  - z.B. IBM Thinkpads, vermehrt auch in Desktop PCs zu finden
- bisher zwei Versionen von Chips: 1.1b und 1.2
- für viele Benutzer ist Sinn und Zweck nach wie vor unklar
- oftmals als “Panikreaktion” Deaktivierung des TPM im BIOS
- besser: verstehen der TPM Funktionen und Hintergründe

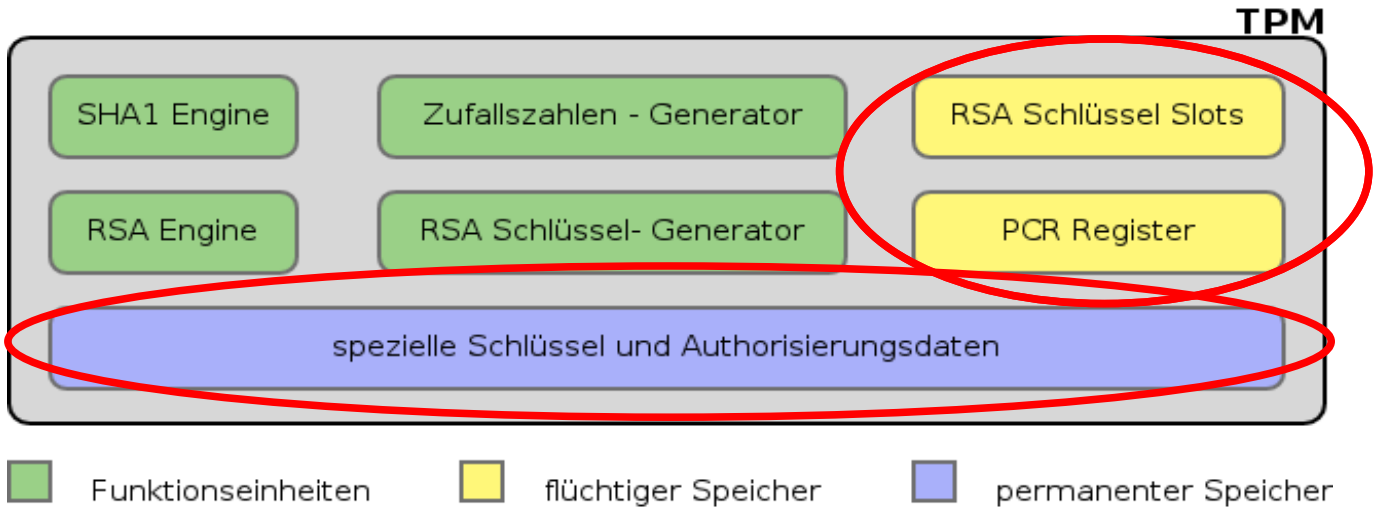
TPM Chip – Funktionen (1/2)

- Opt-In: Nutzer bestimmt ob er das TPM aktiviert
- Funktionseinheiten:
  - RSA Schlüsselerzeugung, Ent- und Verschlüsselung
  - SHA1 Hash Funktion
  - Zufallszahlen Generator
- Erkennung von Hardware Manipulation



TPM Chip – Funktionen (2/2)

- Speicher am TPM
  - PCRs – Platform Configuration Registers (Plattformintegrität)
  - temporärer Zwischenspeicher für RSA Schlüssel
  - permanenter Speicher für spezielle Schlüssel:
    - jedes TPM besitzt ein eindeutiges RSA Schlüsselpaar (Endorsement Key) dessen privater Teil das TPM nie verlässt. EK Erzeugung ist i.d.R. Teil des Herstellungsprozesses



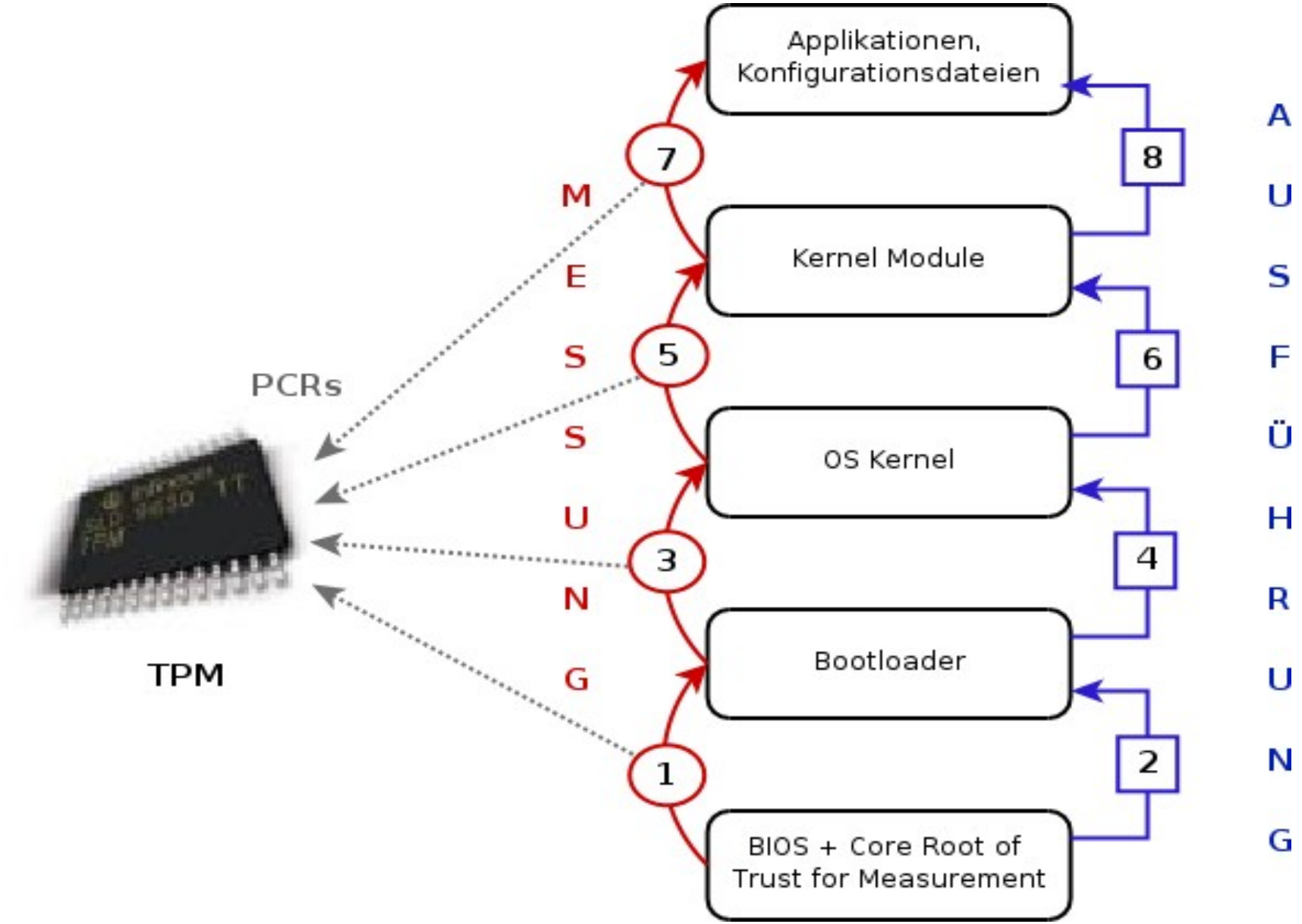
TPM Chip - Anwendungen

- Erzeugung von RSA Schlüsseln, ver- und entschlüsseln sowie signieren von Daten
- TPM gebundene Schlüssel können nicht (unverschlüsselt) aus dem TPM ausgelesen werden
  - Entschlüsselung der Daten ist folglich nur mit dem spezifischen TPM möglich
- Bindung an Systemzustand: Inhalte der PCRs werden bei der Verschlüsselung mit berücksichtigt.
  - Entschlüsselung nur dann möglich, wenn die Plattform im selben Zustand ist wie beim Verschlüsseln.
  - Schutz von Daten im Fall einer unerlaubten Manipulation am System

Chain of Trust und Trusted Boot (1/2)

- Ziel: Abbildung des Systemzustandes in PCRs
- mit PCRs kann man seinem Gegenüber beweisen, dass das System in einem wohlbekannten Zustand ist
- Benutzer wird nicht daran gehindert bestimmte Software auszuführen
- Ausführung wird aber protokolliert und kann nicht geleugnet werden
- CRTM – Core Root of Trust for Measurement (BIOS)
- Messung (und Protokollierung) der nächsten Komponenten bevor diese die Kontrolle bekommen

Chain of Trust und Trusted Boot (2/2)

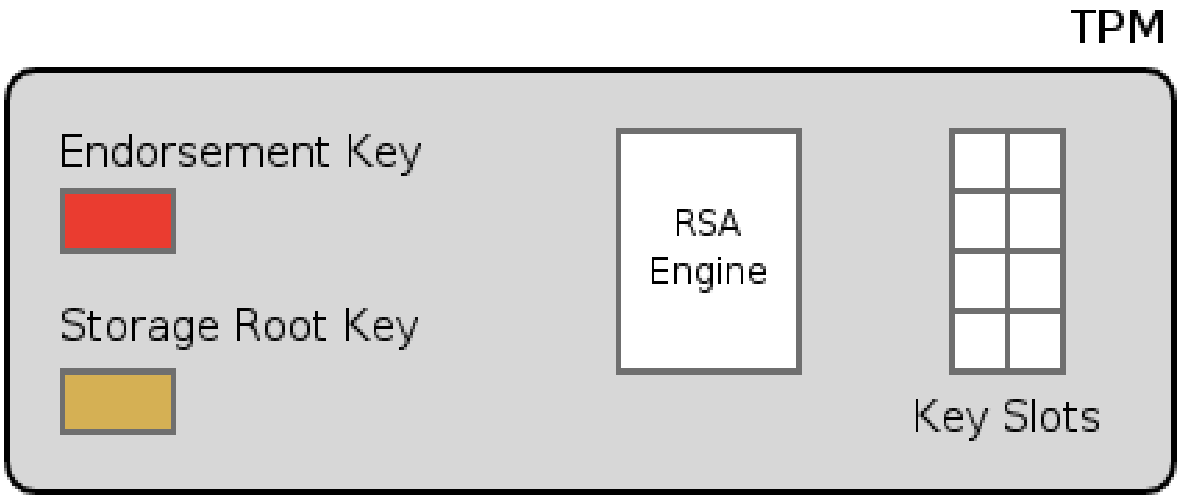


Kryptographische Schlüssel

- Endorsement Key (EK)
  - untrennbar mit dem TPM verbunden
- Storage Root Key (SRK)
  - steht an der Spitze einer Schlüssel-Hierarchie
- Storage Keys und Signing Keys
  - migrierbare und nicht migrierbare Schlüssel
- TPM hat nur beschränkten internen Speicher
  - Keys außer EK und SRK werden nicht dauerhaft im TPM gespeichert, sondern in einem vom TSS verwalteten (Key Cache Manager) externen Speicher
  - die Schlüssel verlassen das TPM nur in verschlüsseltem Zustand

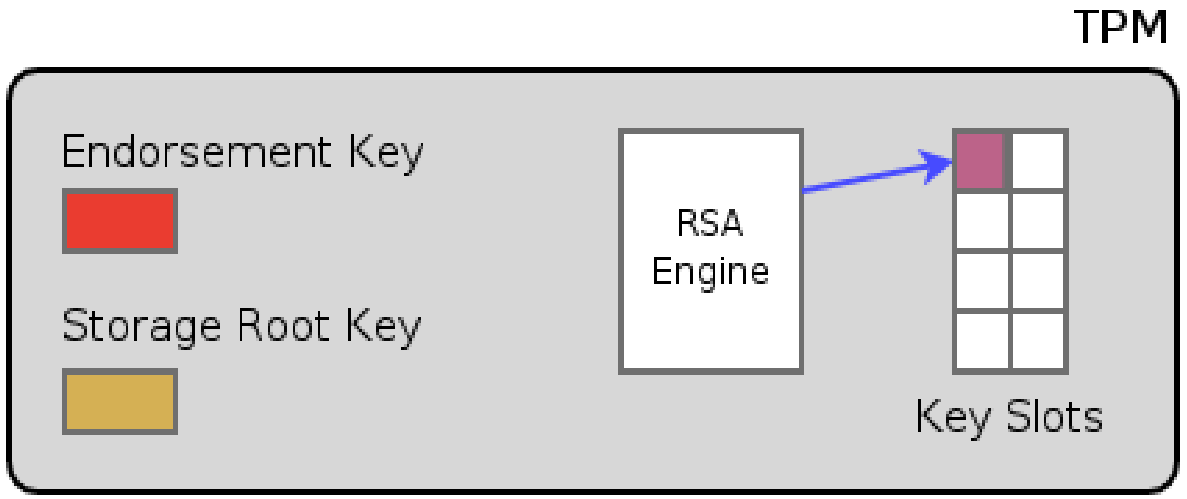
Schlüsselerzeugung (1/2)

- Endorsement Key und Storage Root Key sind als einzige Schlüssel fix im TPM gespeichert
- Key Slots können dynamisch mit Schlüsseln geladen werden



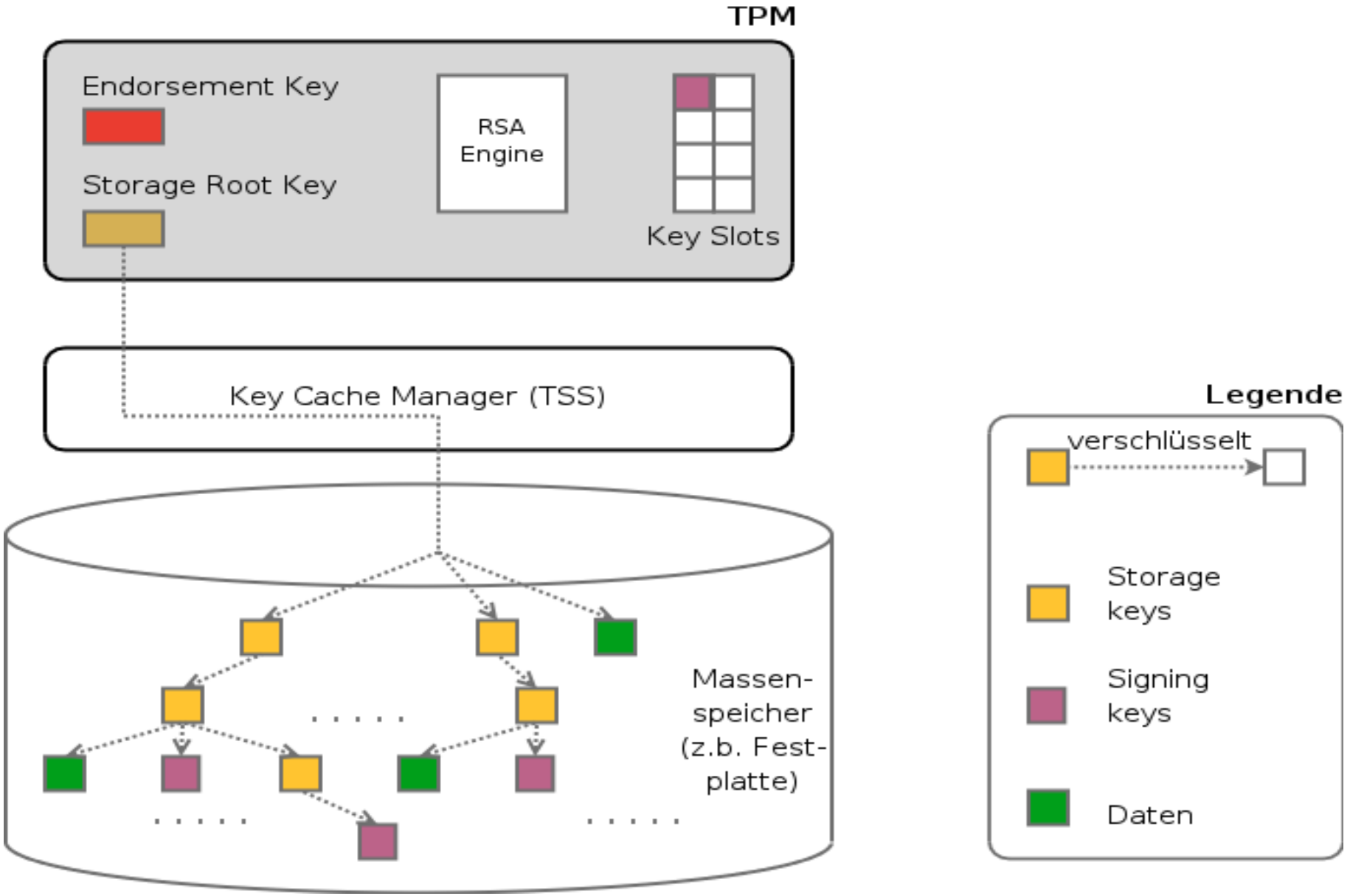
Schlüsselerzeugung (2/2)

- RSA Engine erzeugt neues Schlüsselpaar
  - es muss ein Parent Key angegeben werden
- Anzahl der Key Slots ist begrenzt => Schlüssel müssen aus TPM ausgelagert werden

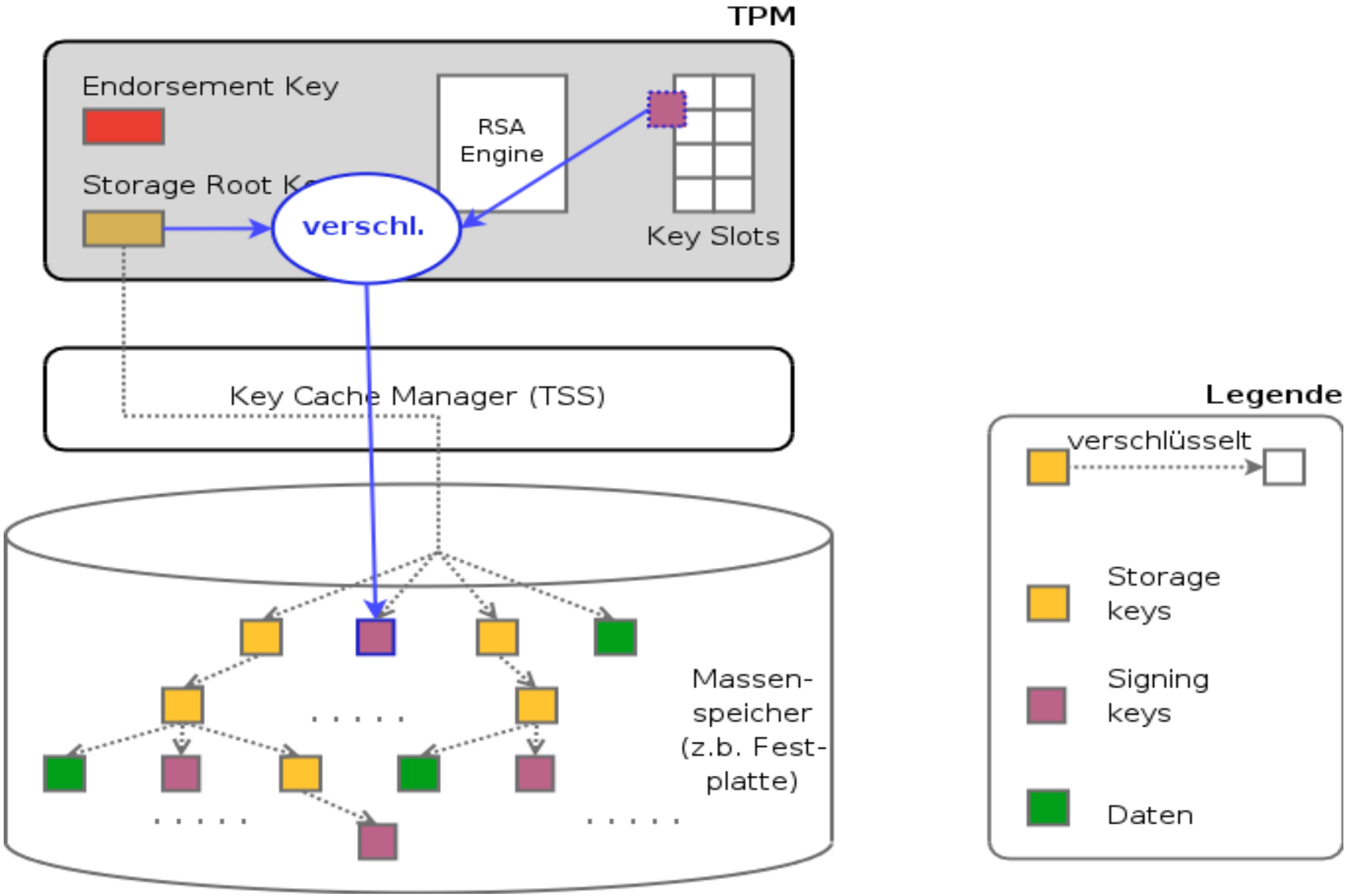


- wenn Schlüssel aus TPM exportiert wird, dann nur in verschlüsseltem Zustand (mit Elternschlüssel verschlüsselt)

Schlüsselverwaltung (1/2)



Schlüsselverwaltung (2/2)



Identitäten

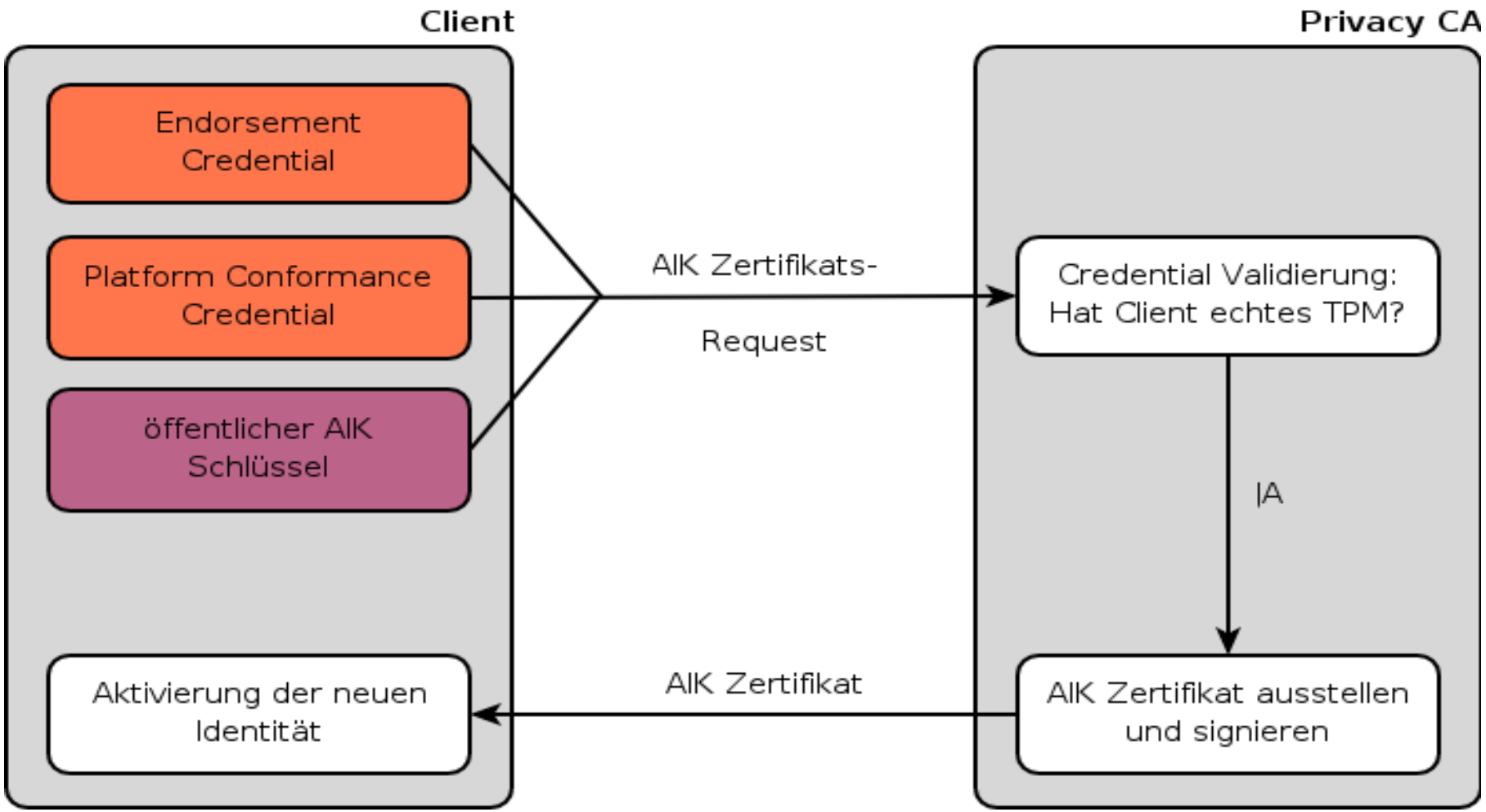
- Endorsement Key Problematik
  - identifiziert das TPM und damit oft zugleich den Benutzer
  - bleibt über die gesamte TPM Lebenszeit gleich
- zum Schutz der Privatsphäre: Erzeugung mehrerer, verschiedener Identitäten
- AIK – Attestation Identity Key
  - TPM erzeugtes RSA Schlüsselpaar
  - hat keinen direkten Bezug mehr zum EK
  - ein Benutzer kann viele AIKs haben – damit sind seine Aktivitäten nicht mehr einfach auf ihn zurückführbar
  - besseren Schutz der Privatsphäre der Nutzer
  - AIK Zertifikat: bescheinigt, dass hinter einem AIK Schlüsselpaar tatsächlich ein TPM steht

Identitätserzeugung (1/2)

- Privacy Certificate Authority
  - stellt AIK Zertifikate aus
  - Antragsteller muss beweisen, dass er ein TPM besitzt
    - Endorsement Credential: Zertifikat mit öffentlichem EK; vom TPM Hersteller
    - Platform Conformance Credential: Zertifikat für TPM/Plattform; vom Plattform Hersteller
  - wenn Credentials OK: Privacy CA stellt AIK Zertifikat aus
- Privacy CA Kritikpunkte
  - Vertrauen in Privacy CA (kennt Zuordnung zw. EK und AIKs)
  - Skalierbarkeit
- Alternative ab Version 1.2: Direct Anonymous Attestation

Identitätserzeugung (2/2)

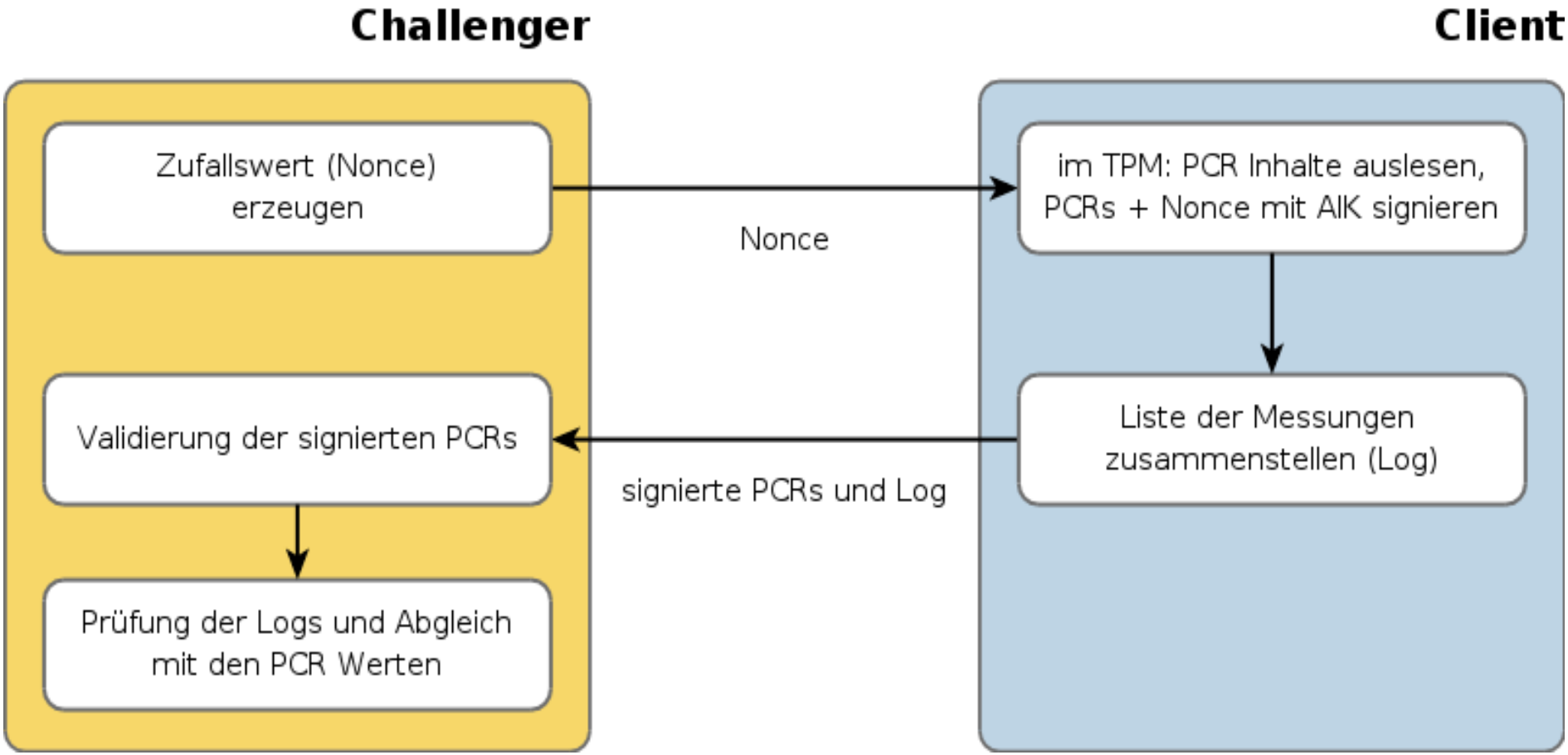
- Client erzeugt neues AIK Schlüsselpaar und will AIK Zertifikat



Attestierung (1/2)

- Ziel: eine Gegenstelle (z.B. eine Bank) will sicher sein, dass auf dem Client keine unerwünschten Programme laufen (Schadsoftware, Keylogger, ...)
- Plattform darf jeden Zustand annehmen (d.h. der Benutzer darf tun und lassen was er will) aber man soll Systemzustand nicht leugnen können (z.B. dass bestimmte Applikation läuft/gelaufen ist)
- PCRs bilden den Zustand der Plattform ab
  PCR[i] <- SHA1(i | PCR[i] | new data)
- PCRs sind im TPM und können nicht manipuliert werden (werden nur bei (Re-)Boot der Plattform zurückgesetzt)

Attestierung (2/2)



Zertifikate

- Datenblock mit
  - Aussteller
  - Inhaber
  - public key
  - Zusatzinformationen
    - Gültigkeitsdauer, Verwendungszweck, ...
  - Signatur des Ausstellers (“diese Informationen sind wahr“)
- TC Erweiterungen
  - Key stammt aus TPM
  - Sicherheitslevels

Public Key Infrastructure (PKI)

- Problem: Zertifikat alleine ist nur eine „Behauptung“
- Gültigkeitsüberprüfung benötigt Infrastruktur
  - noch keine TC spezifische vorhanden
- Gültigkeitszeitraum (trivial)
- Aussteller lokalisieren
  - Beweiskette zum Aussteller aufbauen
- verschiedene Aussteller haben verschiedene Zertifizierungspolitiken (kosten auch verschieden viel)
- Revozierung
  - Liste vs. online Abfrage
- alle Zusätze richtig und für den Einsatzzweck gültig

Virtualisierung

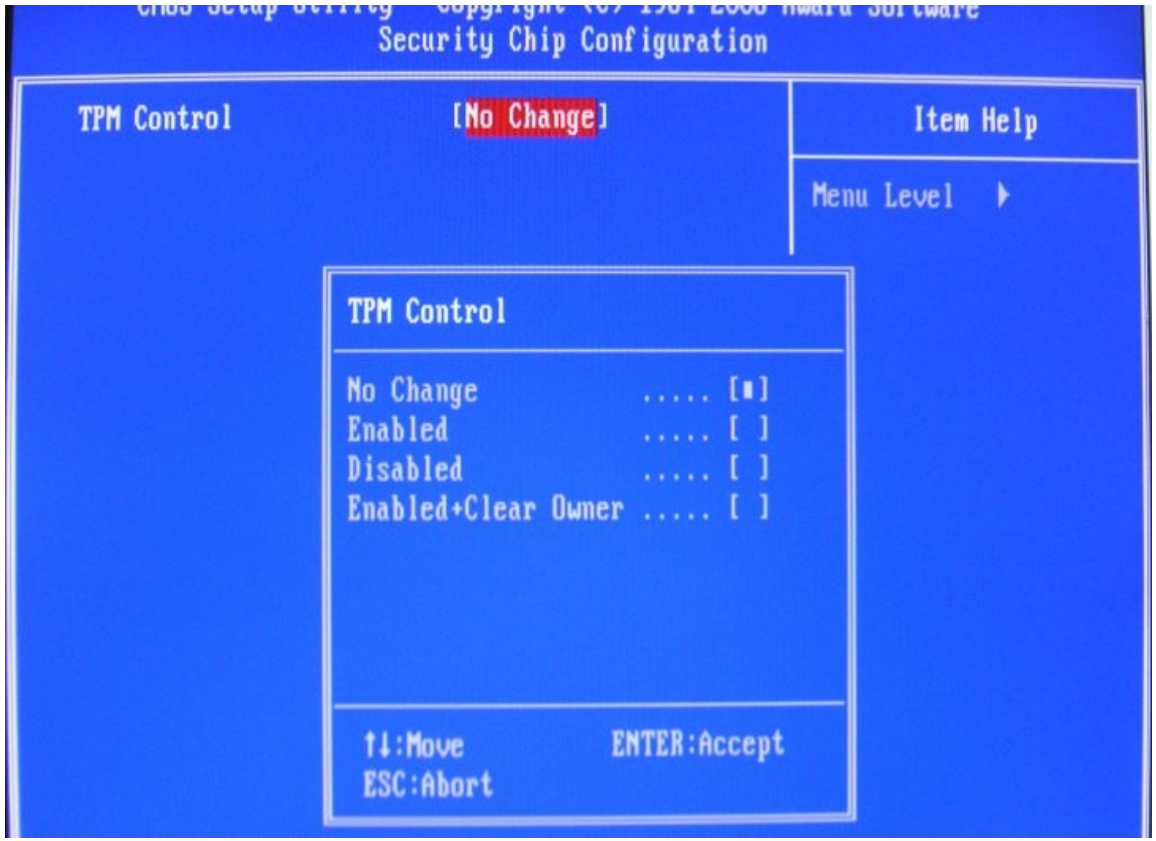
- Messung eines gesamten General Purpose OS ist zu aufwändig
- Idee: mehrere spezialisierte, kleine Systeme die auf einer Virtualisierungs-Schicht („Hypervisor“) laufen
- leichter messbar
- sichere und unsichere Systeme gleichzeitig nebeneinander
- Ansätze basierend auf XEN und dem L4 Microkernel
- kommende CPU Generation bietet Hardware Unterstützung für Virtualisierung
- Herausforderung: TPM Virtualisierung

Software - Schichten

- ein TPM benötigt mehrere Software Komponenten um sinnvoll genutzt werden zu können.
- bereits heute eine Reihe von Open Source Komponenten für Trusted Computing verfügbar
- treibende Kräfte: Universitäre Forschung und einige Firmen (z.B. IBM)

BIOS

- Trusted Computing unterstützendes BIOS
  - Kontrollfunktionen für Nutzer
  - Zukunft: Messung Bootloader



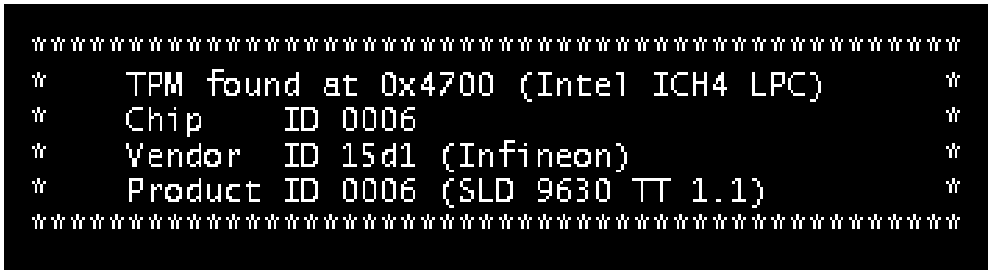
Bootloader

- Trusted Grub
  - modifizierte GRUB Version um Chain of Trust zu realisieren
  - stützt sich auf BIOS um TPM anzusprechen
  - misst nächste Stufe (Kernel) in PCR

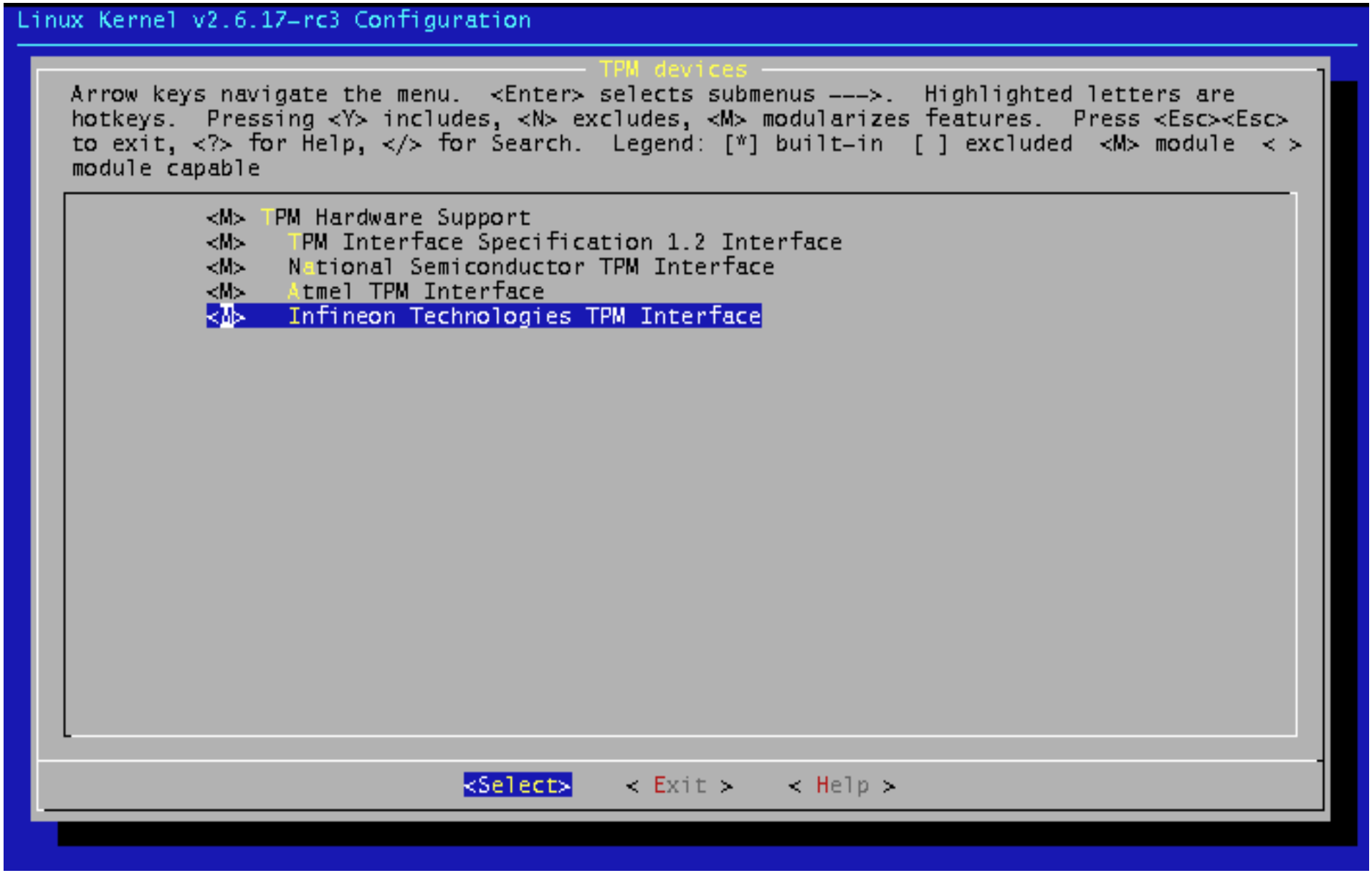
  - http://www.prosecco.rub.de/trusted_grub_details.html
  - http://trousers.sourceforge.net/grub.html

TPM Treiber (1/2)

- Kernel Treiber
  - in aktuellen 2.6er Kernels enthalten:
    - Infineon
    - Atmel
    - National Semiconductors
  - TIS Treiber – generischer Treiber für 1.2 TPMs (ab Ver. 2.6.17)
  - Alternative wenn man kein TPM hat: TPM Emulator
    - http://tpm-emulator.berlios.de
    - nicht ganz vollständing aber genug Funktionalität (1.1b) sodass man selbst experimentieren und testen kann



TPM Treiber (2/2)



Software - Middleware

- libTpm
  - direkter Zugriff auf /dev/tpm
  - erlaubt direkt Befehle (Byte Sequenzen) an das TPM zu schicken
- TrouSerS – TCG Software Stack von IBM
  - implementiert TSS Spec 1.1b (C API)
  - relativ vollständig, noch mit „Kinderkrankheiten“
  - sowohl mit TPM Emulator als auch Hardware TPM verwendbar
  - http://trousers.sourceforge.net/

TCG Software Stack

- TPM Treiber (Kernel)
- TSS stellt TPM Funktionalität als Service (Daemon) bereit
- verwaltet parallelen Zugriff durch Applikationen auf das TPM
- Applikationen verwenden oberste TSS Schicht (TSPI) für Zugriff auf TSS
- API auf C Ebene von TCG spezifiziert

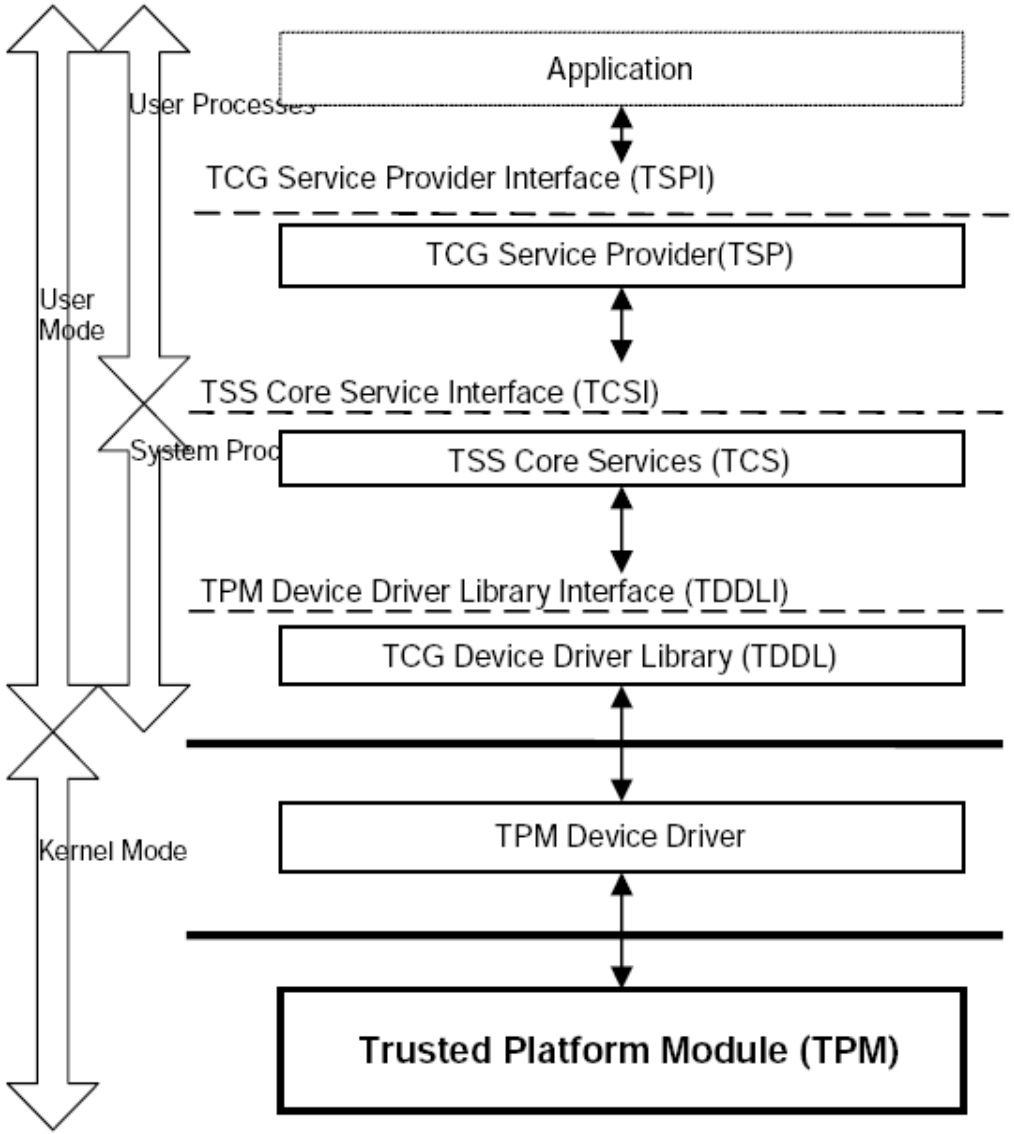


image © 2004 by Trusted Computing Group
TCG Specification: Architecture Overview, p. 26

Software - Anwendungen

- Trusted Java
  - setzt auf TSS auf (z.B. TrouSerS)
  - macht TPM/TSS Funktionalität von Java aus zugänglich
  - basiert auf Version 1.1b
  - noch in Entwicklung
  - http://trustedjava.sourceforge.net/
- viele Einzelprojekte
  - TPM Anbindung für OpenSSL und SSH
  - PKCS#11 Anbindung
  - Integrity Measurement Architecture (IMA)
  - Trusted grml

Was tut sich sonst?

- EU Projekt OpenTC
- Ziel: Schaffung einer offenen Trusted Computing Infrastruktur auf Linux Basis
- Vorteil: Jeder kann die Technologie studieren und sich eine eigene Meinung über Trusted Computing bilden
- über OpenTC:
  - http://www.opentc.net
  - europaweit über 20 Projektpartner (Firmen und Unis)
  - 3,5 Jahre Laufzeit
  - offene Auseinandersetzung mit Trusted Computing

Weiterführende Literatur

- Trusted Computing Group:
  http://www.trustedcomputinggroup.org

  speziell für Einstieg/Überblick: Architecture Overview
  https://www.trustedcomputinggroup.org/specs/IWG/TCG_1_0_Architecture_Overview.pdf

- Trusted Computing and Linux:
  ftp://www6.software.ibm.com/software/developer/library/os-ltc-security/ratliff-05.pdf

- Trusted Computing für Linux:
  Stand der Dinge (Linux Magazin 04/2006)
  http://www.linux-magazin.de/Artikel/ausgabe/2006/04/tcpa/tcpa.html

- Clarifying Missinformation on TCPA
  http://www.research.ibm.com/gsal/tcpa/tcpa_rebuttal.pdf

- Google is your friend...

Zusammenfassung

- Trusted Computing kommt (bzw. ist schon da)
- ignorieren ist unproduktiv und hilft nicht weiter
- Auseinandersetzung mit der Technologie
- mit freien Softwarebausteinen Erfahrung sammeln
- Anwendungsszenarien ausloten
- Kontakte knüpfen, Dialog führen
- selbst Code schreiben (Sourceforge Projekte...)

... Entwicklung mitgestalten!

Letzte Folie!

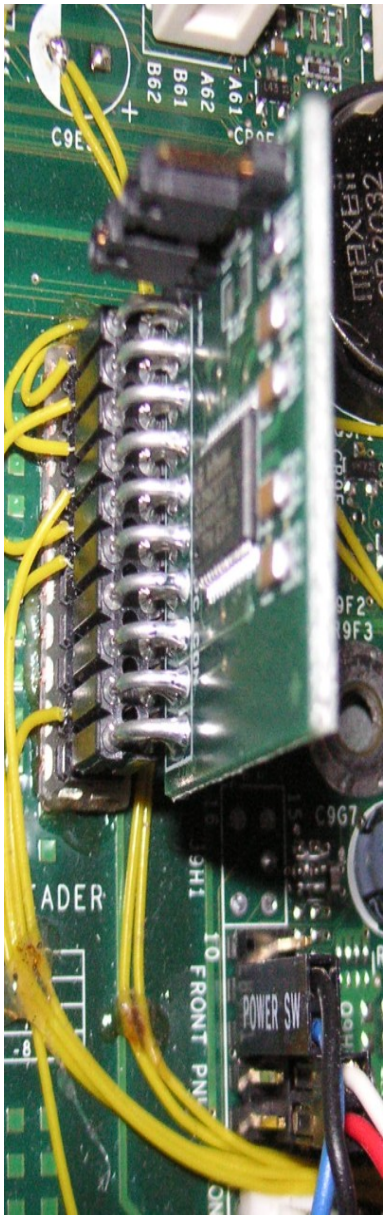
- Kontakt:

  Trusted Computing @ IAIK TU Graz

  web: http://iaik.tugraz.at

  mail: iaik_open_tc@iaik.tugraz.at

- Fragen?



Vielen Dank für die Aufmerksamkeit!

OpenTC Project Details

- The Open_TC project is co-financed by the EC.
  contract no: IST-027635

- If you need further information, please visit our website www.opentc.net or contact the coordinator:

  Technikon Forschungs- und Planungsgesellschaft mbH
  Richard-Wagner-Strasse 7, 9500 Villach, AUSTRIA
  Tel. +43 4242 23355 0
  Fax. +43 4242 23355 77
  Email coordination@opentc.net