Trusted Platform Module

Die Hardware der Trusted Computing Initiative

Jörg Holfeld

s7207040@inf.tu-dresden.de

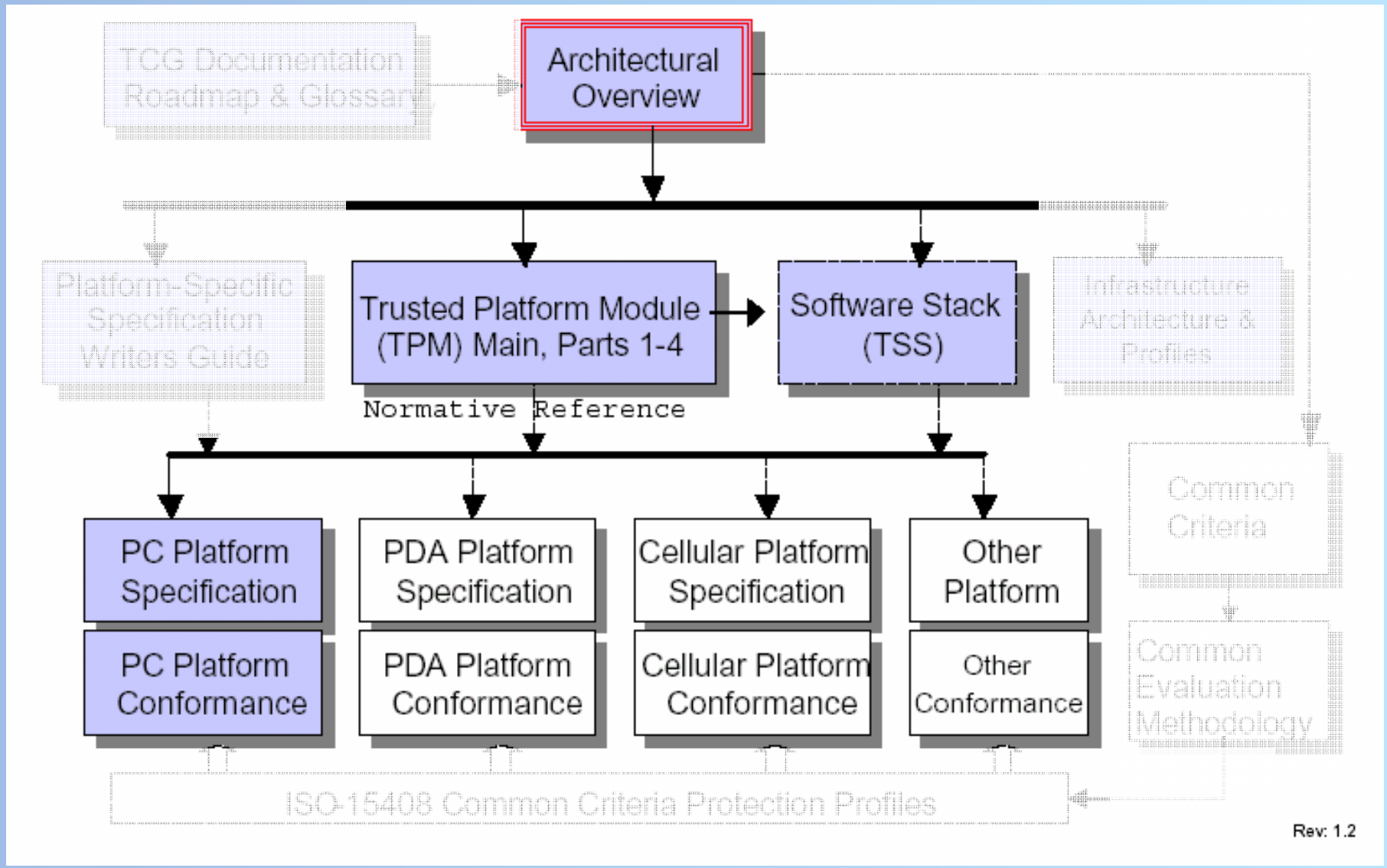
Struktur des Vortrags

- Einführung
  - Was ist die TCG bzw. TPM?
  - Ziele
- Die Hardware
  - Integration in Systeme
  - Aufbau des Trusted Platform Module
  - Funktionen
  - Beispiele
- Die Software
  - Treibermodell
  - Szenarien
- Abschluss
  - Bewertung
  - Diskussion

Trusted Computing Group

- Standardisierungsgremium der Computerindustrie:
  - Sicherheitstechnologie
  - vertrauenswürdiges Computing plattformübergreifend:
    - definieren
    - entwickeln
    - publizieren
  - 1999 TCPA (Trusted Computing Platform Alliance)
  - 2003 Trusted Computing Group
  - AMD, Atmel, Fujitsu, HP, IBM, Infineon, Intel
    National Semiconductor, Microsoft und viele weitere

Architekturübersicht



Trusted Platform Module

- passiver Chip, „Fritz Chip“
  - fest eingebaute Smartcard
  - nicht an Benutzer gebunden, sondern an System
    - Desktop, Server, Notebook
    - PDA´s
    - Mobilfunkgeräte
    - Peripherie
- Aufgaben:
  - Überprüfen von Systemkomponenten und Erkennen von Manipulationen
  - Identifizierung und Authentifizierung
  - Zugriffsschutz

Trusted Platform Module

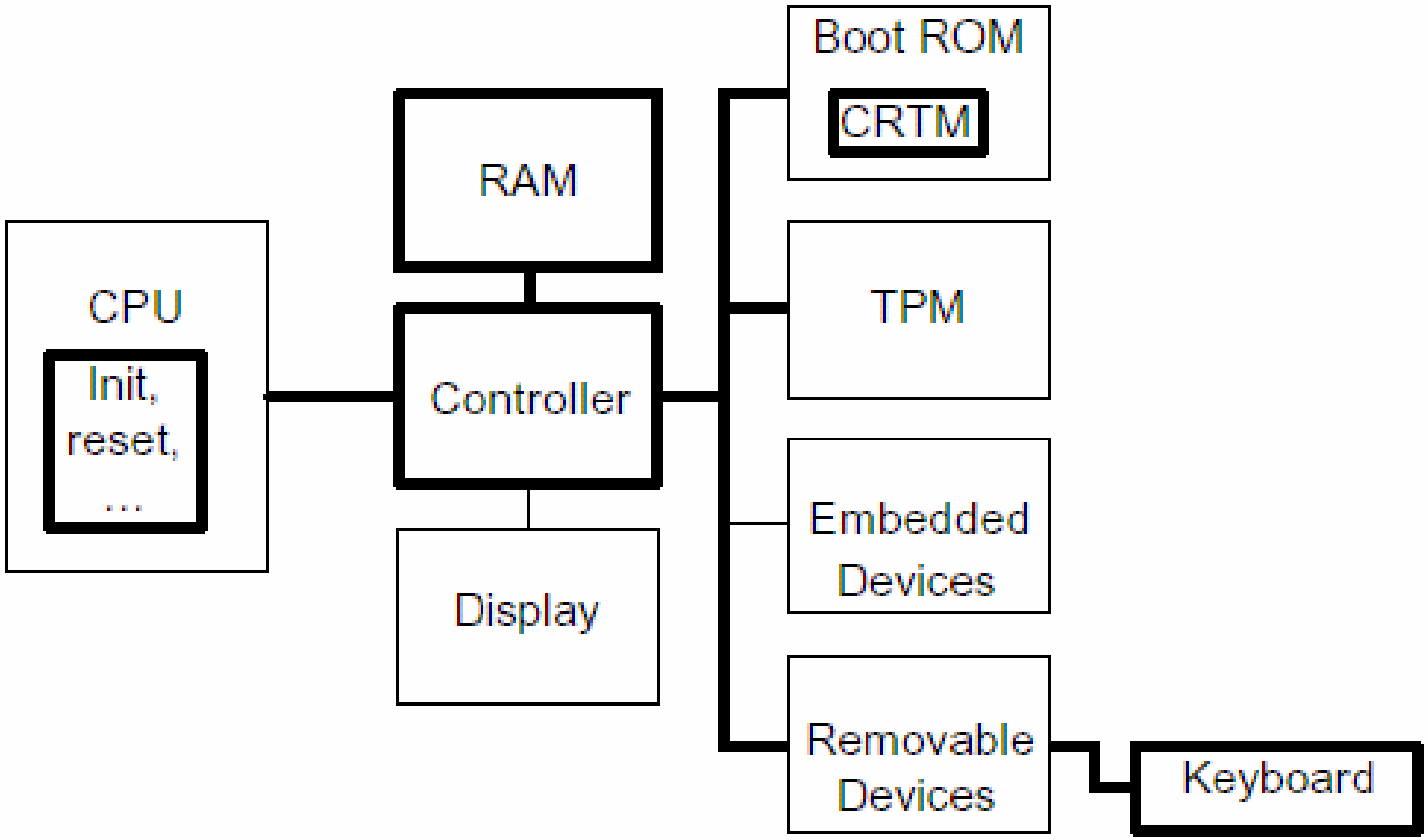


Figure 4:b – Bold indicates part of Trusted Building Block components of a trusted platform

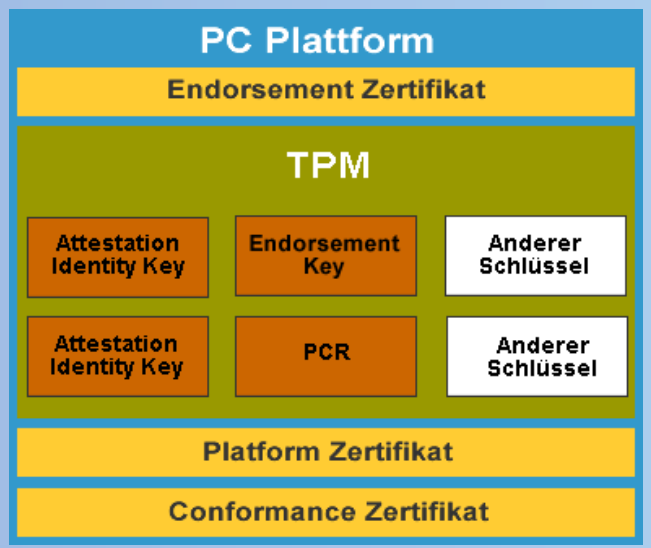
Ziele

- Zugriff
  - einfache Bedienung durch integrierte Technik
  - E-Commerce
  - Mobilität
  - Integration von Mehrwertdiensten
- Schutz
  - Administration
  - Begrenzen und Absichern
    - z.B. Speicherbereiche
    - z.B. Schlüsselerzeugung
  - Datenschutz und Kontrolle

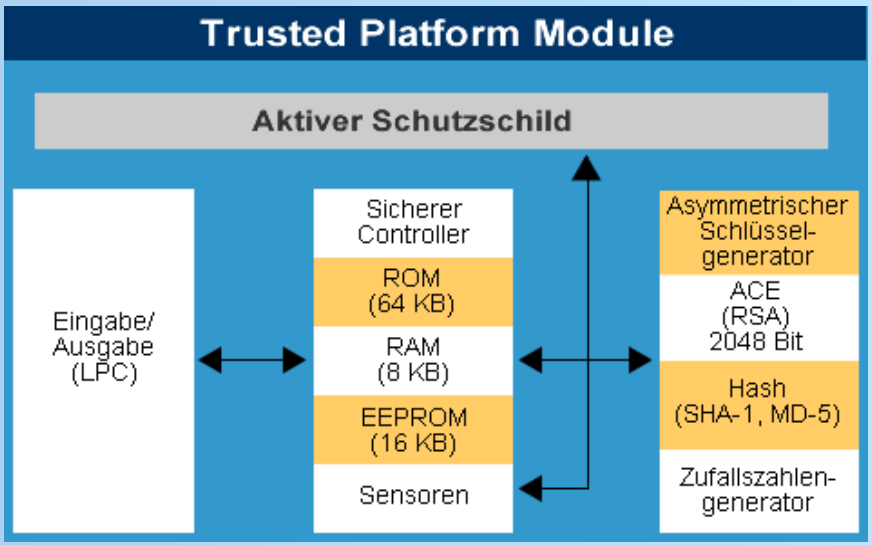
- Plattform-Authentifikation -> gegenüber OS und Software
- Benutzer-Authentifikation -> geheime ID´s und Passwörter
- Email
- Digitale Signaturen verwalten
- Daten- und Dateischutz

Architektursichten

- Zertifikate



- Funktionen



Zertifikate

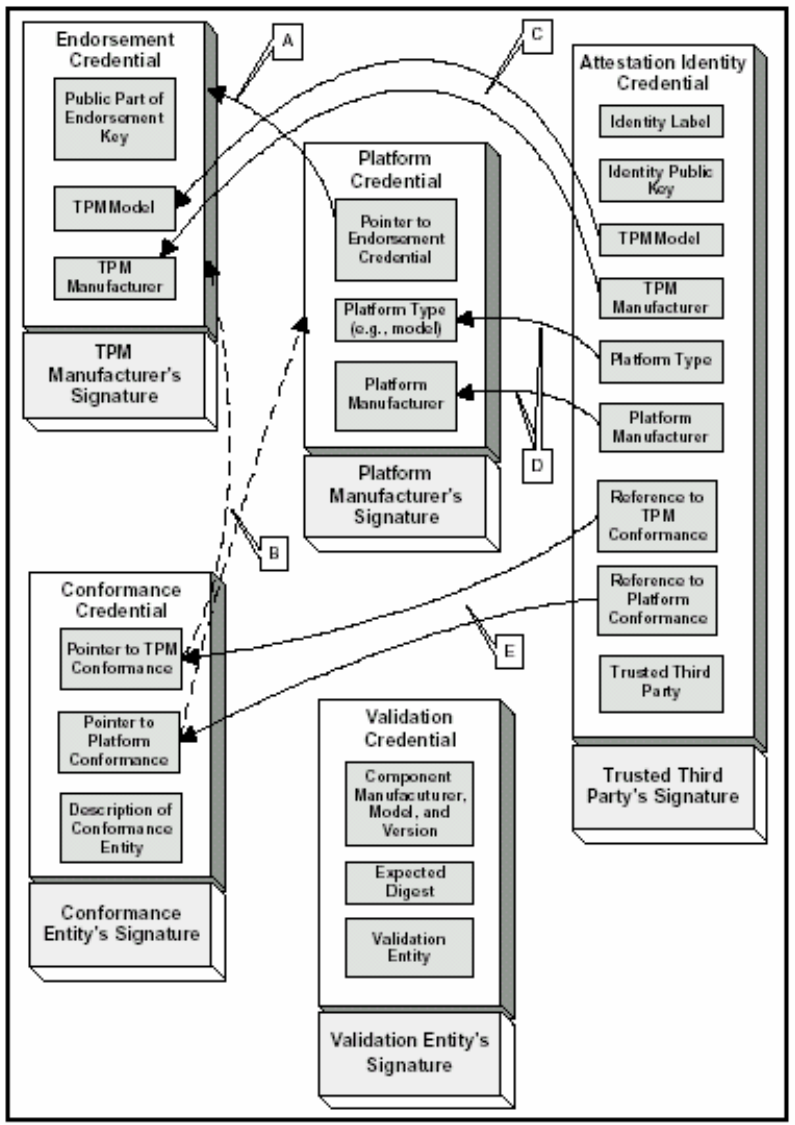


Figure 4:e - Diagram of Credentials and their Relationships.

- Endorsment Zertifikat
  - bestätigt Echtheit des TPM
  - 2048 Bit Schlüssellänge
  - Ableitung zum Attestation Identiy Key
- Platform Zertifikat
  - alle Komponenten
- Conformance Zertifikat
  - TPM-Chipdesign und Implementation
- Validation Zertifikat
  - einzelne Komponenten

➢ Zertifikate dienen dem Nachweis der Spezifikation im Auslieferungs- und Herstellungszustand

Root of Trust for Storage

- Storage Root Key
  - erzeugt Baumstruktur gültiger Schlüssel
  - Root of Trust for Storage

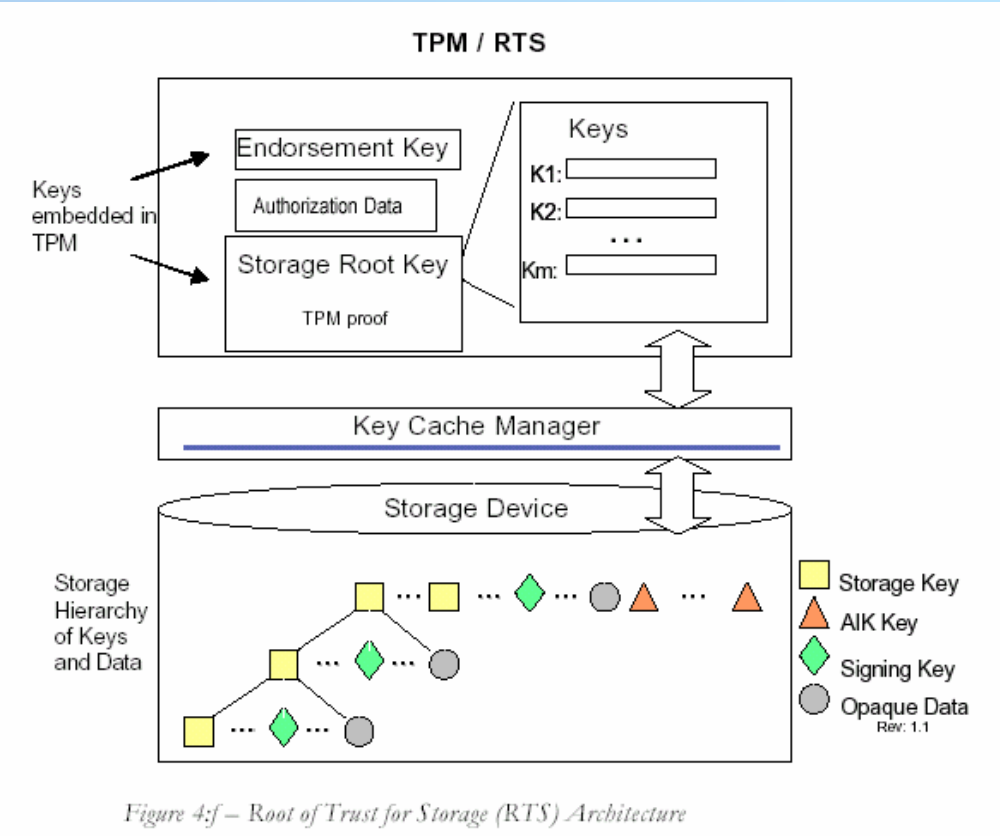


Figure 4:f – Root of Trust for Storage (RTS) Architecture

Komponenten des TPM

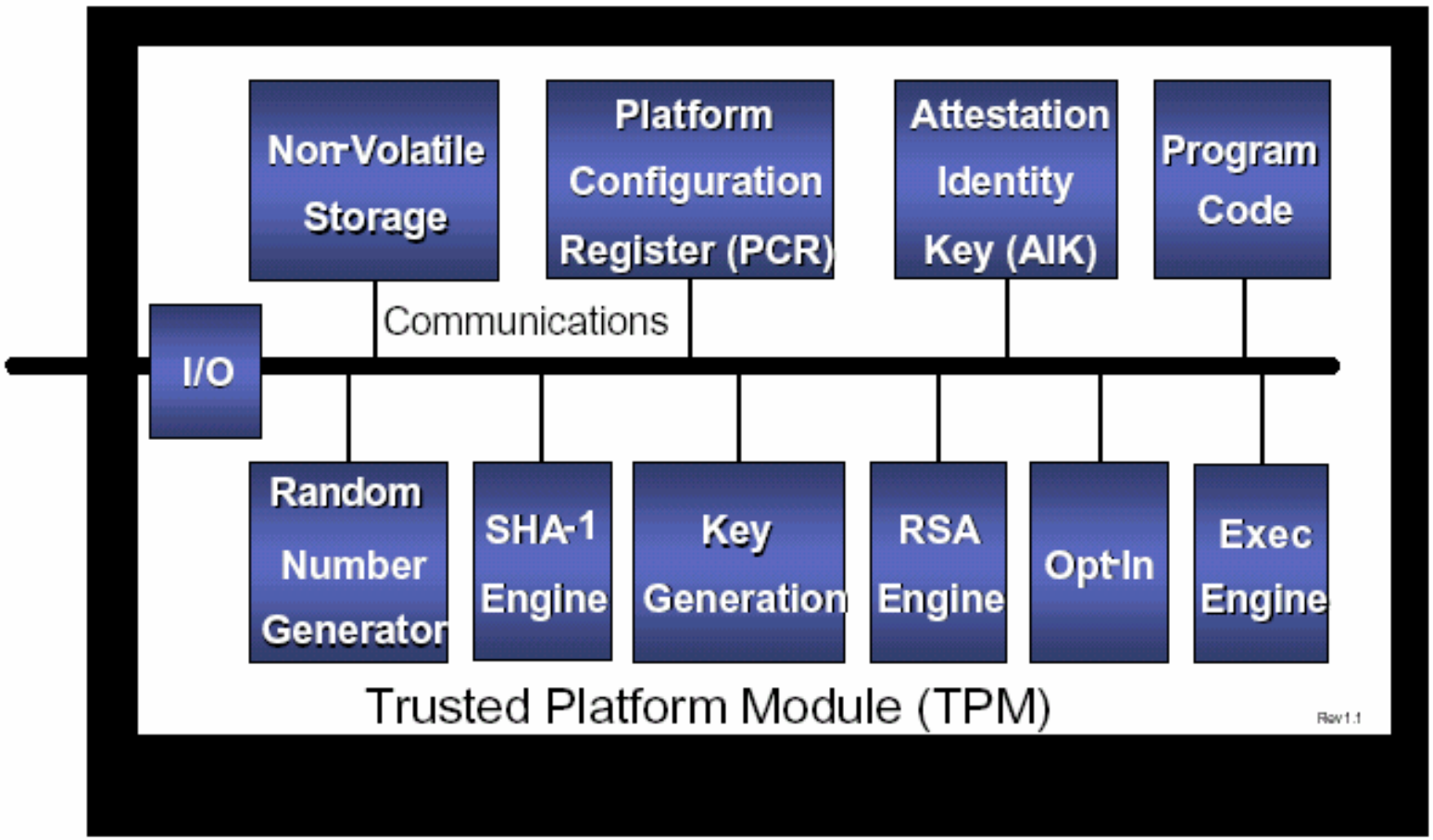
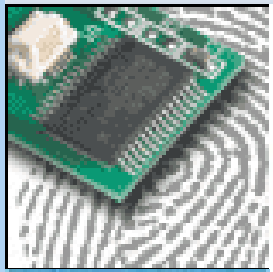
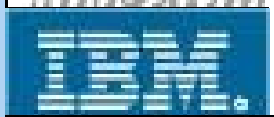


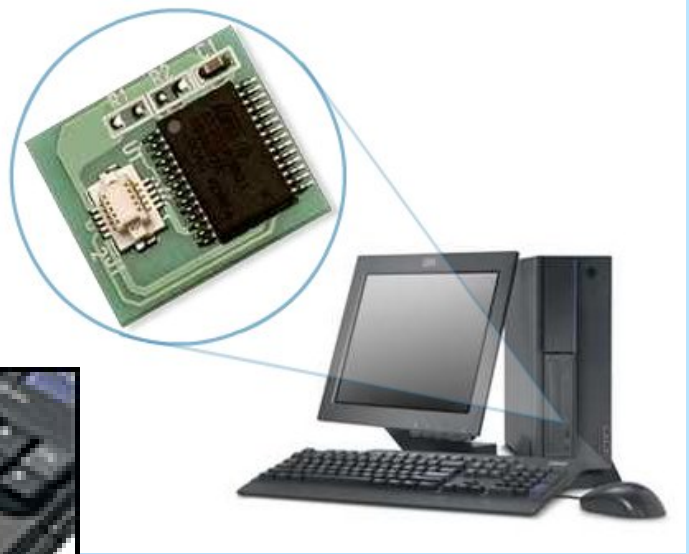
Figure 4:g – TPM Component Architecture

Beispiele

- Chips von Infineon, Broadcom, Atmel
- Chipsätze von Intel (865, 875, 915 …)
- Systeme von IBM (Thinkpad), Acer, HP, Toshiba
- medizinische Geräte
- Multimedia Plattformen, Spielekonsolen
- Intel: LaGrande
- ARM: TrustZone







➢ http://www.tonymcfadden.net/tpmvendors.htm

TSS

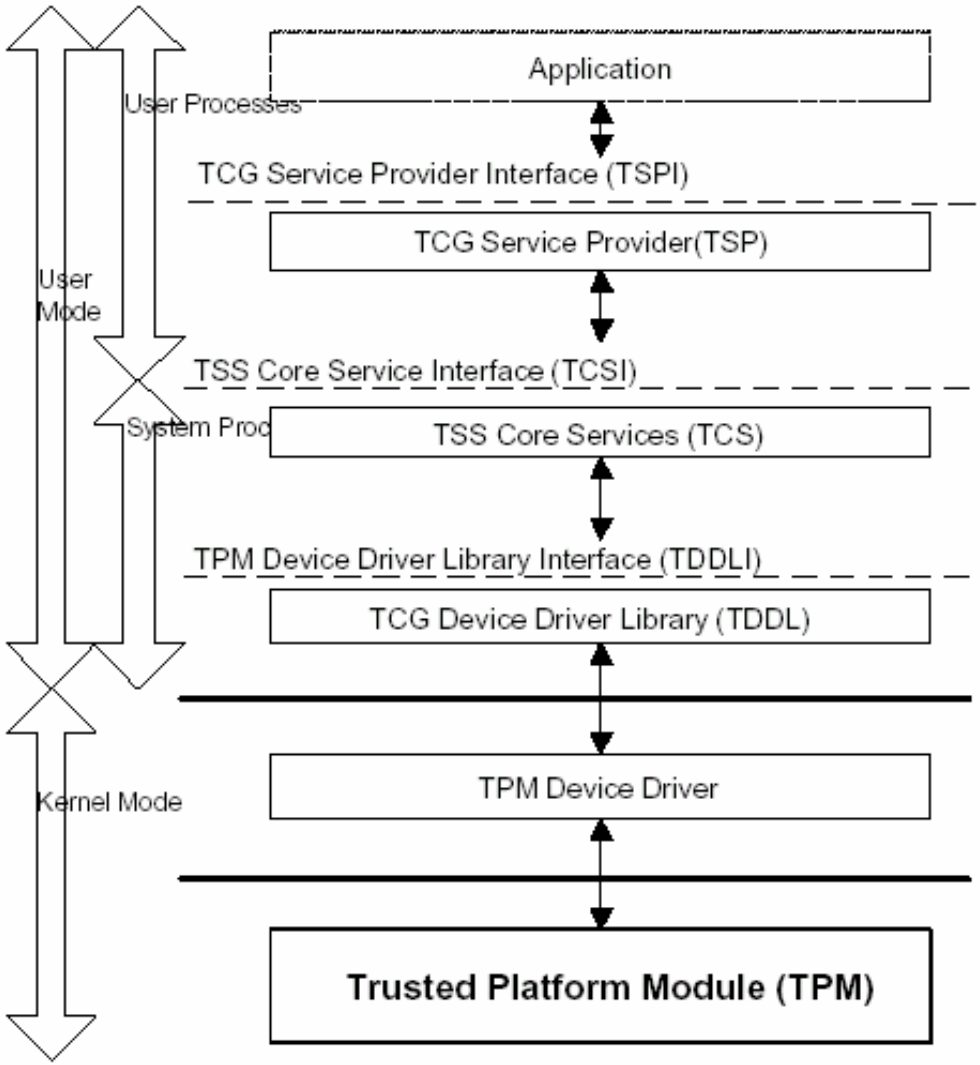
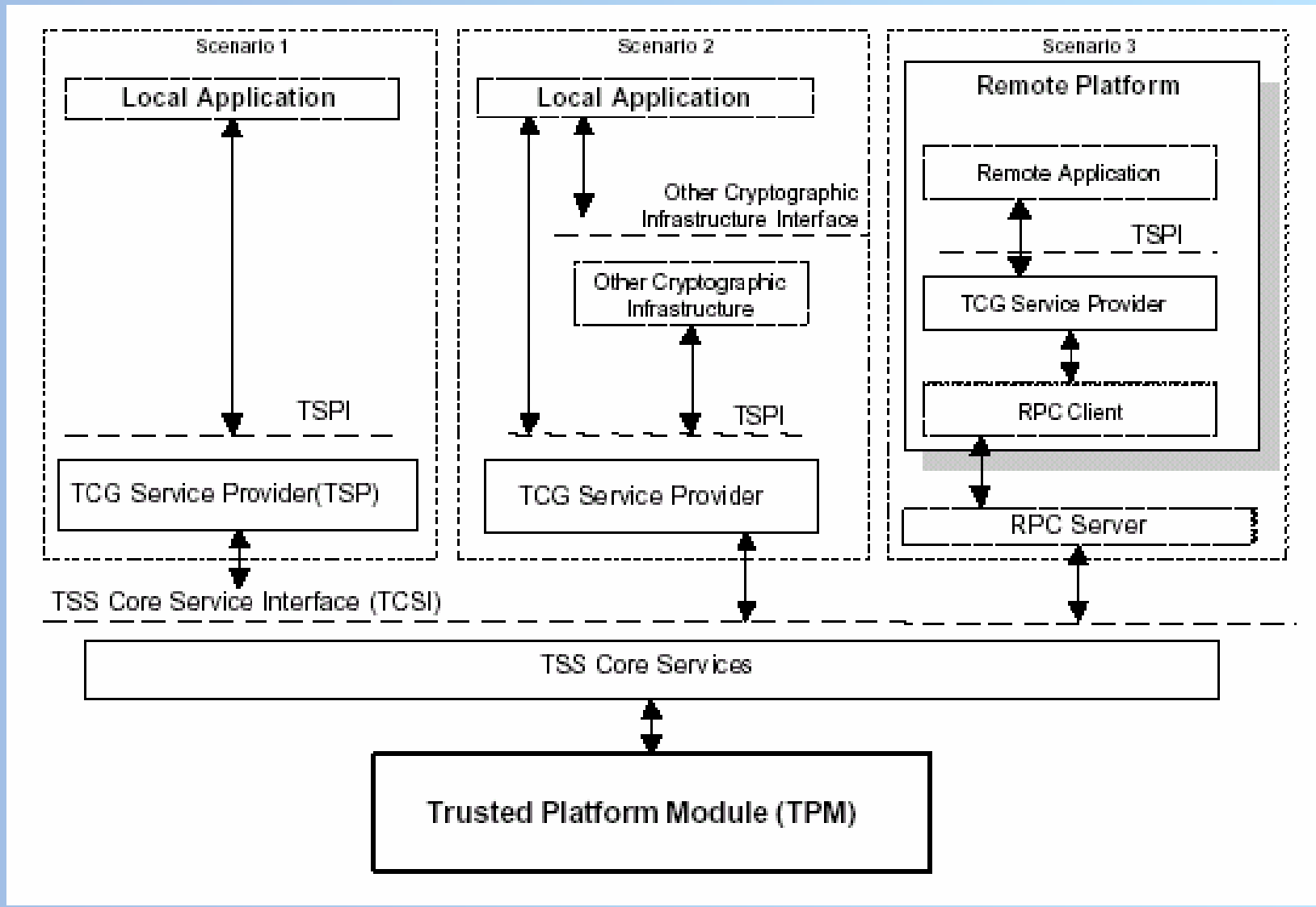


Figure 4:i – TCG Software Layering.

- Trusted Software Stack
  - Schnittstelle zum TPM
  - unabhängige Ebenen

- TDD
  - TPM Treiber vom Hersteller
- TDDL
  - Bibliothek, die Treiberfunktionen zur Verfügung stellt
- TCS
  - verwaltet kritische Zugriffe auf Hardware
- TSP
  - Schnittstelle zum Anwender

Szenarien


Scenario 1
Local Application
TSPI
TCG Service Provider(TSP)
Scenario 2
Local Application
Other Cryptographic Infrastructure Interface
Other Cryptographic Infrastructure
TSPI
TCG Service Provider
Scenario 3
Remote Platform
Remote Application
TSPI
TCG Service Provider
RPC Client
RPC Server
TSS Core Service Interface (TCSI)
TSS Core Services
Trusted Platform Module (TPM)

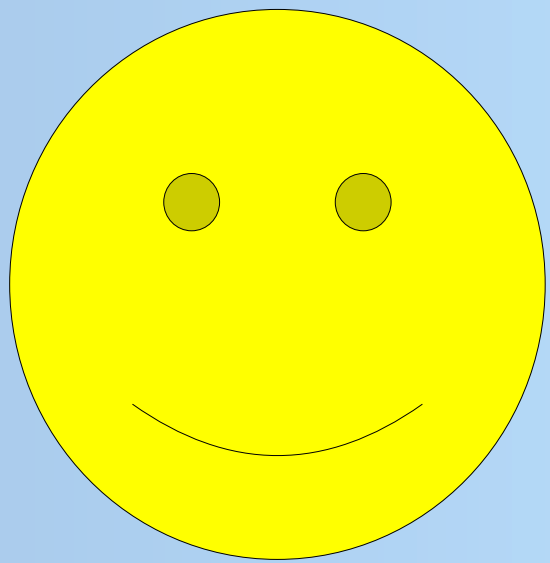
Chancen und Risiken

- Neue Software-Lizenzmodelle
- Stärkere Kundenbindung
- Digital Rights Management
- E-Commerce

- Verhindert direkte Kommunikation zwischen Anwendungen
- Teil des Systems an TCG, die es als vertrauenswürdig einstuft
- Dokumente altern

Fragen und Anregungen

Vielen Dank für Ihre Aufmerksamkeit !



Was ist Ihre Meinung zum Trusted Computing?

Literatur

- https://www.trustedcomputinggroup.org/home
  - *Die Spezifikation als Download (Rev 1.2)*
- http://www.bsi.de/sichere_plattformen/trustcomp/index.htm
  - *Anschauliche Informationsseite des Bundesamtes für Sicherheit in der Informationstechnik*
- http://de.wikipedia.org/wiki/Trusted_Platform_Module
  - *Eine kurze Begriffsklärung zum Trusted Platform Module*
- http://www.infineon.com/cgi/ecrm.dll/ecrm/scripts/prod_ov.jsp?oid=29049&cat_oid=-9313
  - *Daten zum TPM von Infineon*
- http://www.tonymcfadden.net/tpmvendors.html
  - *Übersicht der TPM Hersteller und Implementierungen*
- http://moon.hipjoint.de/tcpa-palladium-faq-de.html
  - FAQ von Ross Anderson (University of Cambridge)

Trusted Platform Lifecycle

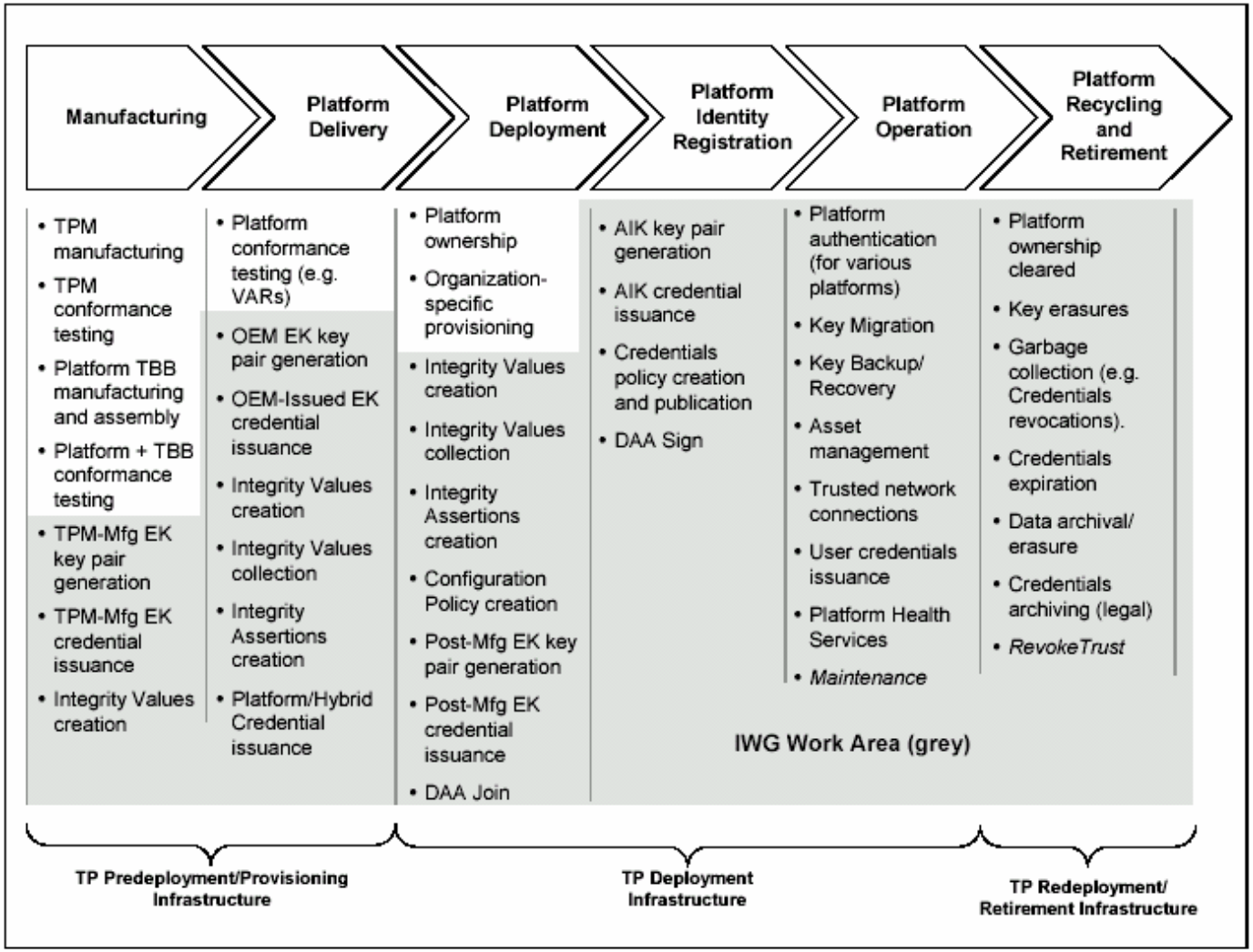


Figure 3: The Trusted Platforms Lifecycle