TCG in Deutschland

SMS SEC Platform Security

2003-07-02

Thomas Rosteck
Senior Director Product Marketing
Infineon Technologies AG

Never stop thinking.

Infineon technologies

Never stop thinking

- **Mehr Sicherheit ... notwendig?**
- Standardization: TCPA - TCG
- Trusted Platform Module
- Marktausblick

Aufgaben von Sicherheit

Authentisierung	• Eindeutige Identifizierung von Personen und Systen • “Mit wem spreche ich?”
Datenintegrität	• Daten werden nicht manipuliert • “Sind das die Daten, die ich erwartet habe?”
Systemintegrität	• Das System wurde nicht verändert • “Ist mein PC immer noch unmanipuliert?”
Vertraulichkeit	• Verhindern von Abhören und Tracken • “Hört jemand zu? Überwacht mich jemand?”
Verfügbarkeit	• Verfügbarkeit von Daten: anytime, anywhere • “Habe ich Zugang?”

E-Commerce und Privatsphäre

Hacker, Sabotage
und Viren haben in 2002
einen Schaden von
40 Milliarden US$
erzeugt[1)]

"If electronic commerce is to live up to its full potential, consumers must have confidence in their ability to maintain their privacy, as well as other critical consumer protections."

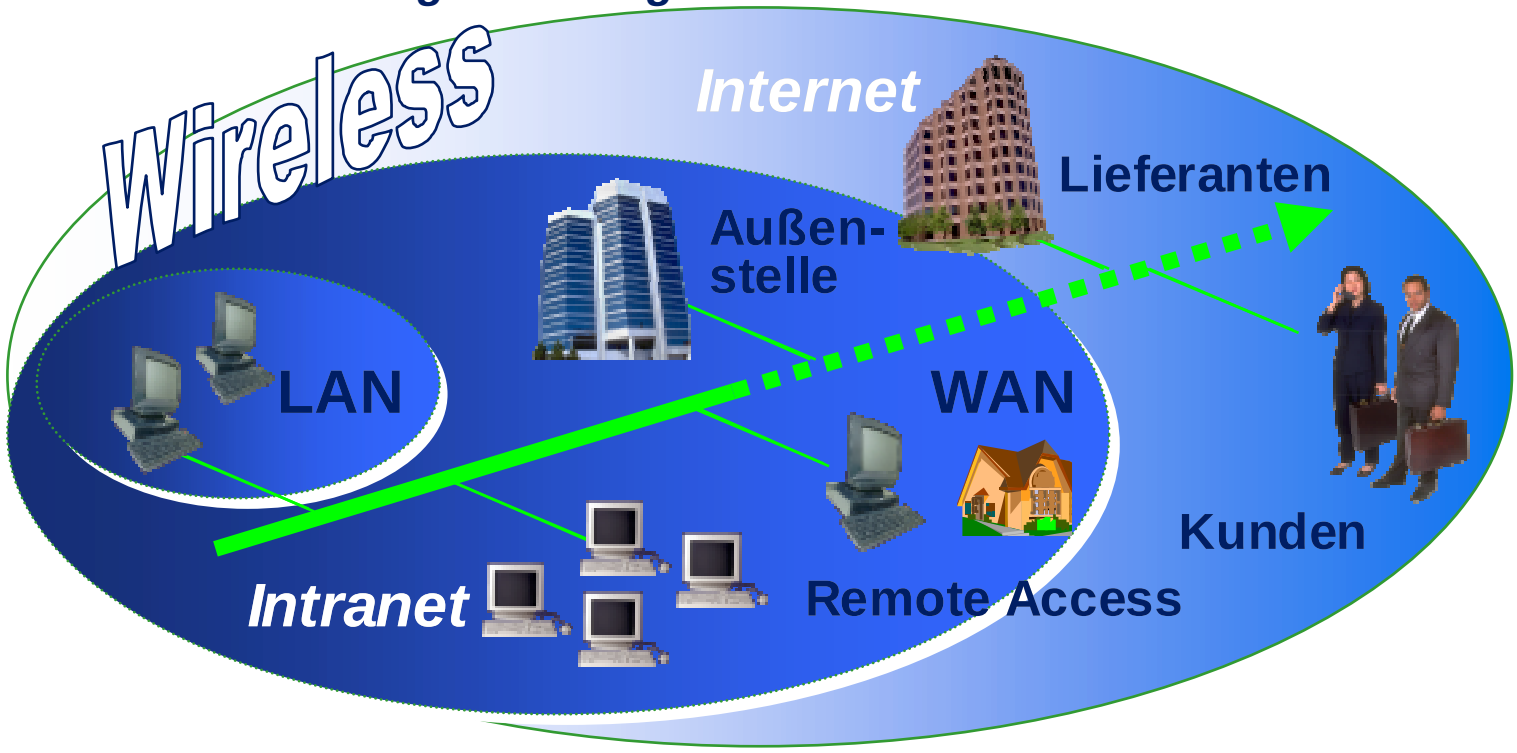
Gary Gensler
Under secretary for domestic finance
at the U.S. Treasury Department

Mehr als
58.000 Attacken
wurden in 2002 offiziell
berichtet[1)]

1) Quelle: mi2g, Focus 46/2002, see [8]

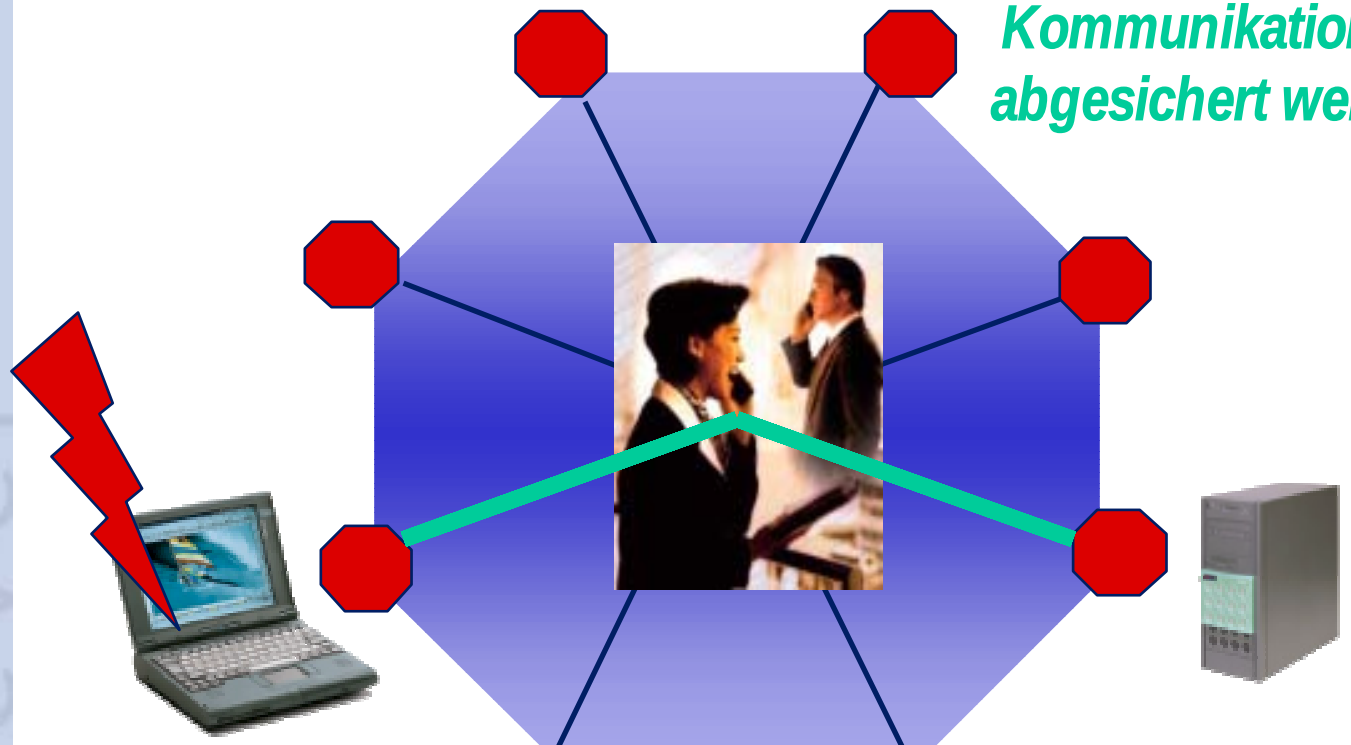
Grenzenloses Internet

Offene Netzwerke werden für die heutige Kommunikation und Geschäftsbeziehungen benötigt ...



... setzen aber ausreichenden Schutz für Informationen und IP vora

Das Hauptproblem in Kommunikation und Computing:
“Kann ich meinem Endgerät vertrauen?”



Kommunikation kann abgesichert werden ...

... die Angriffe erfolgen auf die Endgeräte

Viren, Trojaner, Würmer ...
Wie sichere ich meine digitale Identität

Angeblicher Millionen-Kauf: eBay-Kunde erstattet Anzeige

Die angebliche Ersteigerung unter anderem eines Grundstücks in Leipzig, eines Nobelautos, eines Ultraleichtflugzeuges, eines Bildes von Andy Warhol oder eines externen Herzschrittmachers durch einen Münchner Gärtner auf dem Online-Auktionshaus eBay stellt die Polizei vor Rätsel. Insgesamt 39 Artikel im Gesamtwert von rund **1,4 Millionen Euro** sind unter dem Namen des eBay-Nutzers ersteigert worden. Der 22-Jährige leugne die Kaufanträge über das Internet-Auktionshaus und sehe sich als Opfer eines unbekannten Computerkriminellen, bestätigte ein Polizeisprecher ...

Quelle: heise-online, 23.4.03

Silicon Based Security

is the Key

to Trust

in Tomorrow‘s Information Society.

Infineon technologies

Never stop thinking

- Mehr Sicherheit ... notwendig?
- **Standardization: TCPA - TCG**
- Trusted Platform Module
- Marktausblick

Trusted Computing
„Einfache“ Sicherheit

Ziel:
Vertrauen in Netze, Endgeräte und E-Business

Marktanforderung:

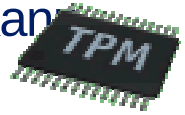
Sichere Lösungen in Applikationen mit geringer Sicherheitsexpertise

- **Einfach zu nutzende Sicherheit**
- **Standard für Sicherheit (plattformunabhängig)**
- **„TÜV“ für Sicherheitsprodukte**

Der Beginn:
Die Trusted Computing Platform Alliance (TCPA)

- 1999 gründeten Compaq, Hewlett Packard, IBM, Intel und Microsoft die

- Ziel: der ***Trusted Client***
  Das Endgerät (PC, Notebook, PDA, Handy) dem der Benutzer und der Kommunikationspartner bei Transaktionen und E-Commerce Applikationen **vertrauen** kann
  Basis: das Trusted Platform Module (TPM)



- Mehr als 200 Firmen entlang der Wertschöpfungskette traten der TCPA bei
- Der TCPA Standard V1.1b ist seit 2001 verfügbar und wird implementiert.
- Die TCPA hat mit der Gründung der TCG ihre Aktivitäten eingestellt

Die Fortsetzung:
Die Trusted Computing Group (TC

- **Die Trusted Computing Group wurde im April 2003 gegründet und ist der Nachfolger der TCPA, für die Spezifikationen von Trusted Computing**
- **Die TCG ist eine offene Industrie-Standard-Organisation**
  - Gegründet als Non-Profit Organisation
  - Offenes Mitgliedermodell mit unterschiedlichen Levels (Promoter, Contributor, Adopter)
  - AMD, HP, IBM, Intel und Microsoft als erstes Board of Directors
  - Supermajority voting
  - RAND Patentlizenzpolitik zwischen Mitgliedern
  - Logo-Programm geplant
- **Mehr Informationen: www.trustedcomputinggroup.org**

TCG-konforme Produkte sind bereits im Markt

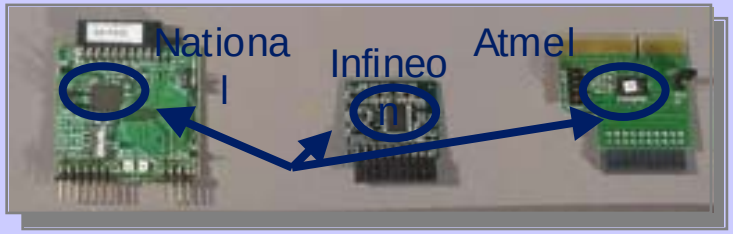
PCs / Notebooks

seit Mai 2002

Seit Mai 2003

Referenzdesigns

TPMs



Never stop thinking

- Mehr Sicherheit ... notwendig?
- Standardization: TCPA - TCG
- **Trusted Platform Module**
- Marktausblick

Das Trusted Platform Module (TPM)
Was macht es?

- Prüfen der System Integrität

  Wie ist der Status der Hardware und der Software?

- Authentisierung und attestieren des Sicherheitsstatus der Plattform

  Information für Benutzer und Kommunikationspartner (falls vom Benutzer autorisiert)

- Sichere Speicher

  für Schlüssel und andere Geheimnisse des Benutzers

- Volle Benutzerkontrolle

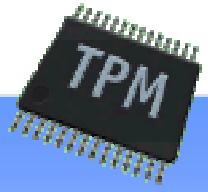
  Der Benutzer kontrolliert den Einsatz des TPM

Das Trusted Platform Module (TPM)
Was ist es?

- Ein Sicherheitscontroller
- fest mit dem Mainboard der Plattform verbunden
  (e.g. PC, Notebook, PDA, Handy, ...)
- aber ein separater Baustein (nicht im Hauptprozessor)
- mit der Fähigkeit logischen (=Software-) und physikalischen Angriffen zu widerstehen, um die Geheimnisse des Benutzers zu schützen
- sicherheitsevaluiert durch eine unabhängige Common Criteria Zertifizierung
- integriert in den Boot-Prozess und in das Betriebssystem

Die TPM Lösung

PC als Trusted Platform



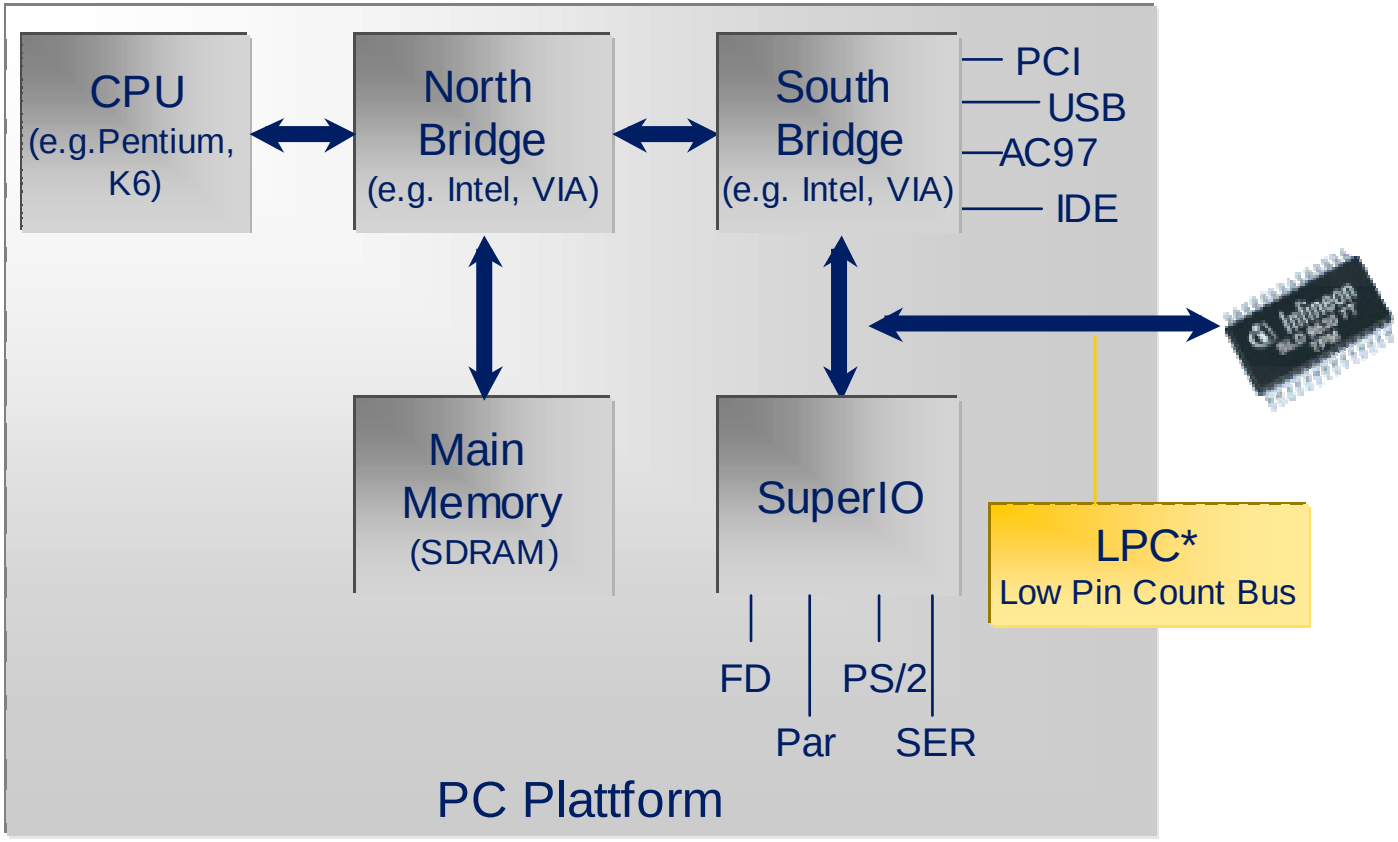
Verbunden mit dem LPC-Bus*

Integrierte Hardware Lösung auf dem Mainboard gemäß der TCG Spezifikation

Sicherer Speicher	*Kryptographie*	*Schlüsselerzeugung*	*SW Integration*
■ Geschützter Nicht-Flüchtiger Speicher	■ High-Performance RSA-Accelerator ■ Hash Accelerator (SHA-1)	■ True Random Number Generator	■ System Lösung - BIOS - Host SW (TSS)

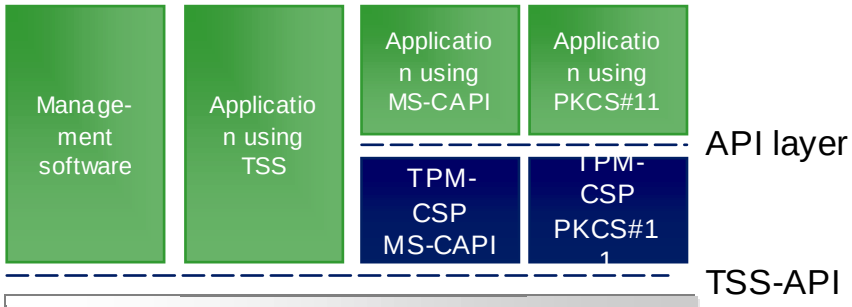
* definiert von Intel

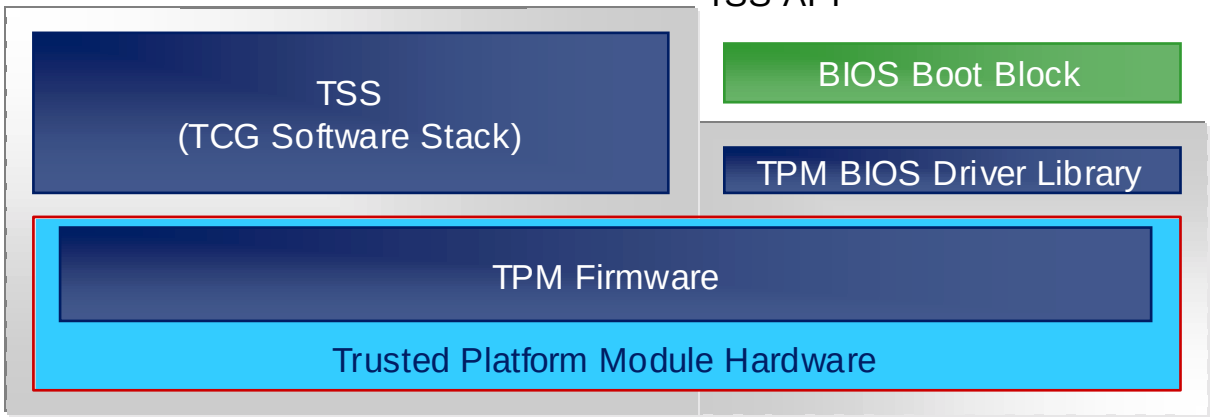
Mainboard-Architektur mit TPM



* definiert von Intel

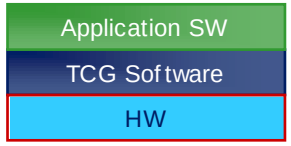
TPM Software Konfiguration





Beispiele für Applikationen:

- Datei-Verschlüsselung
- Secure Log-On
- Applikationen via MS-CAPI oder PKCS#11 (e.g. Outlook, Explorer, Netscape)
- PKI
- VPN



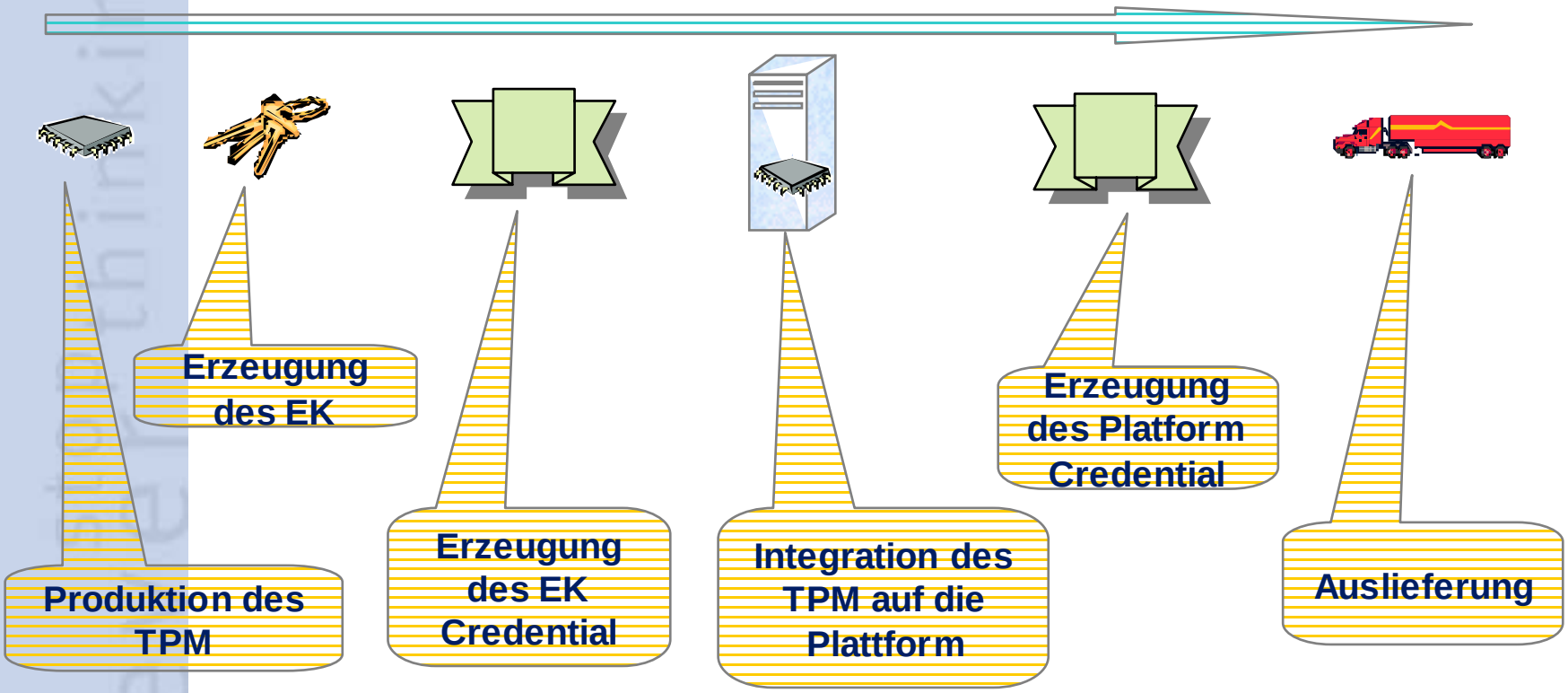
TCG =	Trusted Computing Group	CSP =	Crypto Service Provider
TSS =	TCG Software Stack	API =	Application Programming Interface
TPM =	Trusted Platform Module	MS-CAPI =	Microsoft Crypto Application Programming Interface

Secure Mobile Solutions

Zertifikate und Identitäten

- Endorsement Key Pair (EK)
  - Das EK ist ein eindeutiges Schlüsselpaar je TPM
  - Es trägt die digitale Unterschrift des TPM-Herstellers, der damit bestätigt, dass
    - es sich um ein Hardware-TPM handelt,
    - das gemäß TCG Spezifikation hergestellt wurde
    - Das TPM wird nicht für Authentisierung bei Services oder Digitalen Signaturen verwendet
- Attestation Identity Key Pair (AIK)
  - Es können beliebig viele Identitäten erzeugt werden
  - Das Vertrauen des EK wird auf die AIKs übergeben.
  - Diese haben keinen expliziten Link zum EK

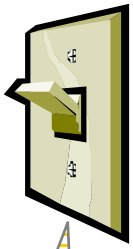
Trusted Platform
Fertigungsschritte



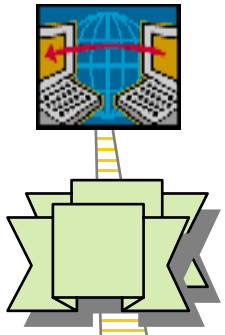
EK = Endorsement Key Pair / Eindeutiges Schlüsselpaar für ein TPM

Nutzung von Zertifikaten

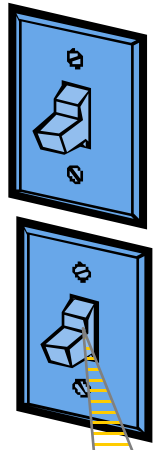
Erhalt der Trusted Platform



Der Owner aktiviert das TPM



Der Owner lässt das TPM AIKs erzeugen



Der Benutzer entscheidet, ob er das TPM benutzt

Anforderung eines Services unter Nutzung des AIK

AIK = Attestation Identity Key Pair / beliebig viele pro TPM

Infineon technologies

Never stop thinking

- Mehr Sicherheit ... notwendig?
- Standardization: TCPA - TCG
- Trusted Platform Module
- **Marktausblick**

Trusted Client
Das integrale Sicherheitskonzept

- **Der Trusted Client ist nicht nur der PC mit dem TPM - es ist das Gerät mit allen angeschlossenen Sicherheitskomponenten**

Plattform-Sicherheit in Netzen

More Information: **www.infineon.com/TPM**
www.silicon-trust.com

Danke für Ihre Aufmerksamkeit

Never stop thinking