# TCPA
# Trusted Computing

Ausarbeitung im Rahmen des Moduls
„Softwaresystementwicklung“ im WS 2003/2004
an der Carl-Von-Ossietzky Universität, Oldenburg

Klaus Krogmann

2. Februar 2004

# Inhaltsverzeichnis

# 1 Abstract

Trusted Computing der TCG (Trusted Computing Group) soll die Grundlage für eine zukünftige Generation von Computern sein. Ziel ist der Schutz von Dokumenten und geheimen Informationen. Auf Basis einer veränderten Hardwareplattform, in dessen Zentrum das TPM (Trusted Platform Module) steht, soll eine neue Generation von Betriebssystemen aufsetzen. Microsoft nennt seine Bemühungen um ein sicheres Betriebssystem NGSCB.

Dem Anwender steht eine Menge neuer Hardware bevor, die dem Schutz von Daten auf allen Ebenen der Architektur dienen wird. Daneben steht aber auch die Befürchtung, dass der Nutzer die Kontrolle über seinen eigenen Rechner und die darin gespeicherten Schlüssel verliert, und DRM (Digital Rights Management) allgegenwärtig die Rechte der PC-Benutzer einschränkt - so abgesichert, dass die Schutzsysteme nicht mehr ausgehebelt werden können; vorausgesetz, dass alle Implementierungen korrekt durchgeführt wurden.

# 2 Einleitung

Wenige Themen der aktuellen Entwicklung aus dem Bereich des Computers, könnten in den kommenden Jahren das Verhalten von Nutzern und die Möglichkeiten der Industrie so verändern, wie „Trusted Computing“. So ist es wenig verwunderlich, dass dieses Thema auch Einzug in das politische Geschehen genommen hat und heftig von beiden Seiten diskutiert wird. Befürworter eines neuen Sicherheitskonzepts für Computer, dass endlich das Heilmittel für alle virengeplagten PC-Nutzer, die um ihre Datensicherheit besorgt sind, sein soll, stoßen auf erbitterten Widerstand von Seiten der Open-Source-Gemeinde und Verfechtern der Freiheit des PC-Besitzers.

In der Tat könnte „Trusted Computing“ nicht nur dem Endanwender Sicherheit bringen, sondern vor allem einer Medienindustrie, die sich mit sinkenden Umsätzen bei CDs und in Kinos konfrontiert sieht und auf die Einführung von sicheren DRM-Systemen hofft. Möglich wären Szenarien, in denen man einen Film eben nur mit *einem* Gerät sehen kann - für jedes andere Abspielgerät würde der Nutzer erneut zur Kasse gebeten.

Dem gegenüber stehen die frustrierten PC-Besitzer (aber auch Firmen), die endlich auf mehr Sicherheit hoffen. Der Liebes- oder Geschäftsbrief soll nur vom bestimmten Empfänger gelesen werden können. Nie wieder soll ein Virus alle Daten löschen und nie wieder soll ein Trojaner die sorgsam erdachten Passwörter ausspähen und den eigenen E-Mail-Account zerstören.

Es sind also Hoffnungen und Angst mit der Entwicklung von „Trusted Computing“ verbunden. Was möglich und was nicht möglich sein sollte, und wie das alles funktionieren könnte, soll der folgende Text klären. Eine Abwägung von Chancen und Risiken aus Sicht der Nutzer und der Industrie soll einen Einstieg in die Thematik erleichtern.

An dieser Stelle sei darauf hingewiesen, dass sich die hier genannten Angaben grundsätzlich auf den derzeitigen Stand der Spezifikationen beziehen, die Fakten aber gleichwohl einem ständigen Wandel durch Veränderungen/Neuerungen unterworfen sind.

## 2.1 Was ist TCPA?

Die TCPA (Trusted Computing Platform Alliance) stellt einen Zusammenschluss von ca. 200 Industrieunternehmen dar, die es sich zur Aufgabe gemacht haben, in einem basisdemokratischen Prozess eine (Hardware-) Plattform (oder besser einer Spezifikation für eine mögliche Umsetzung) zu entwickeln, auf deren Basis es möglich sein soll, Programme in einer gesicherten Umgebung ablaufen zu lassen. Die TCPA wurde im Oktober 1999 gegründet.

Im Kern der Bemühungen der TCPA steht dabei die Verabschiedung einer Spezifikation, nach der Hardwarekomponenten entwickelt werden können, mit denen sich ein „sicherer“ Computer betreiben lässt. Alle Mitglieder der TCPA können sich an der Entwicklung beteiligen. Jedes Unternehmen ist prinzipiell mit einem Veto-Recht ausgestattet, da alle Entscheidungen einstimmig gefällt werden müssen. Faktisch jedoch wurden Entscheidungen zur Standardisierung bei der TCPA hauptsächlich von einigen wenigen marktdominierenden Unternehmen gefällt[1]. Da sich offenbar eine Entmachtung der eigentlichen Entscheidungsträger mit zunehmender Mitgliederzahl der TCPA nicht mehr durchsetzen ließ, wurde im April 2003 die Nachfolgeorganisation „TCG“ (Trusted Computing Group) gegründet, die die Arbeit der TCPA fortsetzte. (Dennoch besteht die TCPA generell weiter, Spezifikationen wurden in jüngster Zeit jedoch von der TCG verabschiedet.)

Die TCG besteht zu einem grossen Teil aus den alten Mitgliedern der TCPA, jedoch vornehmlich aus denen mit ausreichend finanziellem Polster, da die eingeführten Mitgliedsbeiträge nicht unerheblich sind. In der neuen TCG werden die Mitglieder in verschiedene Stufen unterschieden: Promoter, Contributor und Adopter. Die Abstufung ist zwar mit fallenden Mitgliedsbeiträgen verbunden, beinhaltet aber auch den zunehmenden Verlust von Mitbestimmungsrechten beim Standardisierungsprozess.

Nach der neuen Mitgliedsordnung sind nur noch Promoter und Contributoren stimmberechtigt. Diese Mitgliedskategorien weisen hohe Mitgliedsgebühren auf. Fortan sind nur noch Mehrheitsbeschlüsse zu fällen.

Mitglieder der TCG können später die Lizenz zur Umsetzung der TCG-Spezifikationen erwerben. Auch Nicht-Mitgliedern wird diese Möglichkeit eingeräumt, faktisch ist die Möglichkeit aber deutlich erschwert, da die Bedingungen, zu denen Nicht-Mitglieder die Lizenzen erwerben können, von der TCG bestimmt werden können. Es ist also nicht auszuschließen, dass die entstehenden Bestimmungen einen Marktzugang der Konkurrenz zum Bereich Trusted Computing gemäß der TCG-Spezifikationen verhindern. (siehe auch Abschnitt 3.2)

## 2.2 Mitglieder der TCG

Die Mitgliedsliste[2] der TCG weist derzeit Branchengrößen wie AMD, HP, IBM, Intel, Microsoft, Sony, Sun, Nokia, Infineon, TI und viele andere auf. Beachtenswert ist, dass die Mitgliedsliste

[1] siehe [CC03]

[2] die volle Liste findet sich unter [TCGd]

nicht immer offen verfügbar war. Angesichts zahlreicher Protestaktionen gegen die Mitglieder der TCG, hatte man zum Schutz vor weiteren Protesten die Liste vom Webserver genommen.

Als Mitglieder finden sich also auch der Monopolist Microsoft, der Branchenprimus Intel, Unterhaltungsgigant Sony und Handymarktführer Nokia wieder. Als Promoter hat Microsoft großen gestaltenden Einfluss auf die Spezifikationen. Immerhin will Microsoft seinen Bekundungen zufolge TCG 1.2 als Basis für NGSCB (siehe hierzu Abschnitt 4.3.2) verwenden.

# 3 Ziele der TCG

Wie bereits im Abschnitt 2.1 angedeutet wurde, möchte die TCG eine Spezifikation für eine Computerarchitektur entwerfen, die es Angreifern und Viren unmöglich macht, geschützte Dokumente und Daten einzusehen und zu stehlen. Der PC soll sich selbst gegenüber anderen Stellen authentifizieren können. Dabei kann er selbst seine eigene Integrität beweisen und verifizieren. Als PC-Benutzer kann man also feststellen, ob eine Manipulation vorgenommen wurde. Beginnend mit dem Bootvorgang des Computers kann sichergestellt werden, dass nur vertrauenswürdige („sichere“) Programme ablaufen können.

Um das Aushebeln von Sicherheitsmechanismen zu verhindern, muss das zu entwerfende System zahlreichen Anforderungen genügen. Von Bedeutung ist, dass sich die TCG vornehmlich um den Hardwareteil eines sicheren Systems kümmert. Ohne ein „sicheres“ Betriebssystem kann der Schutz von Daten jedoch nicht garantiert werden. Microsoft nennt seine Bemühungen zur Schaffung eines sicheren Betriebssystems (derzeit) NGSCB (siehe hierzu Abschnitt 4.3.2).

In die Entwicklung der TCG inbegriffen ist die TCB (Trusted Computing Base), die aus allen sicherheitsrelevanten Systemkomponenten besteht. Darin befindet sich auch das TPM (Trusted Platform Module, auch „Fritz Chip“), dass im Verhalten einer SmartCard ähnelt und später als Hüter der Schlüssel (dazu später mehr im Abschnitt 4.2) *eines* Systems dient.

Neben der Überprüfung der Integrität der Hardware „für sich selbst“ ist für einen Benutzer wichtig, dass sich auch das System ihm gegenüber authentifiziert, um die Möglichkeit des kompletten Austauschs von Hardware vorzubeugen.

## 3.1 Sicht der Industrie

In der Industrie lassen sich zwei Grundinteressen an Trusted Computing (TC) ausmachen. Zum Einen das der Hardwarehersteller, die durch den Verkauf von TPMs auf Umsatz, sowie bei Mainboards auf ein Differenzierungsmerkmal zur Konkurrenz hoffen. Auf der anderen Seite

finden sich die Rechteinhaber. Diese sehen in TC eine Möglichkeit der wirksamen „Verdongelung“ von Software mit einem konkreten Hardwaresystem oder die Möglichkeit DRM (Digital Rights Management) konsequent durchzusetzen. Allein durch das TPM wird dabei die Einhaltung von Rechten nicht möglich sein. Für DRM wird auch ein sicheres Betriebssystem nötig sein, wobei sich das Interesse von Microsoft zeigt, seine marktbeherrschende Stellung auch bei „sicheren“ Betriebssystemen fortzusetzen.

Microsoft setzt mittlerweile offiziell auf die TCG-Spezifikation 1.2 mit seinem NGSCB auf. Dabei lag das Interesse von Microsoft tatsächlich in den Anfängen des „sicheren“ Betriebssystems auf der Ermöglichung von unumgehbaren Sicherheitsbeschränkungen (siehe hierzu [Mic02]) für DRM. Von vielen Benutzern wurden diese jedoch als Restriktionen wahrgenommen, die sich von Microsoft jedoch schlechter verkaufen ließen, als der umfassende Schutz des PCs, den Microsoft derzeit proklamiert.

Zwar sind keine direkten Rechteinhaber von Material, das DRM ausnützen könnte, in den Reihen der TCG (etwa Disney oder Warner), dennoch stehen mit diesen Filmkonzernen und Musikverlagen potentielle Kunden auf dem Parkett von Microsoft und Co., die mit dem TPM in der Lage sein werden, ruhigen Gewissens ihre Filme und Musik in verschlüsselten Containern anzubieten. Wenn es nach den Plänen von Microsoft geht, dann werden die Nutzungsbedingungen genauestens eingehalten - so garantiert es die Architektur.

## 3.2 Nutzersicht - kritische Stimmen

Die Ankündigungen zu Trusted Computing nach den Plänen der TCG hat in der Vergangenheit zu großen Wellen von Protesten geführt. Viele (private) Nutzer befürchten einen Verlust der Kontrolle über den eigenen Rechner. Daher wurden diverse Seiten (z. B. www.notcpa.org und www.againsttcpa.com) ins Internet gestellt, die sich aktiv gegen die Bemühungen der TCG wenden. Auch bestehende Organisationen wie der Chaos Computer Club (CCC, www.ccc.de) richten sich mit ihrer Kritik gegen die gegenwärtigen Pläne zur Umsetzung des TPM. (Wohlgleich bereits Chips nach der Spezifikation 1.1b z. B. von Infineon produziert werden und in Boards von Intel und IBM stecken; siehe hierzu [ciw].)

### 3.2.1 Forderungen des CCC

Der CCC hat 4 Hauptforderungen[3] aufgestellt, die von der TCG erfüllt werden sollen (Erläuterungen zu den technischen Hintergründen folgen im weiteren Verlauf des Textes, siehe auch Abschnitt 4.2).

- Der Anwender soll die Möglichkeit bekommen, jederzeit volle Kontrolle über alle im TPM gespeicherten Schlüssel (darunter auch der zentrale Schlüssel, Endorsement Key genannt) zu erlangen. Das heißt, dass der Anwender genau festlegen können soll, welcher Schlüssel für welchen Zweck benutzt wird. Damit soll unter anderem verhindert werden, dass sich die Interessen der Industrie einseitig durchsetzen lassen.

- Die Sicherheit, dass die geheimen, im TPM liegenden Schlüssel nicht durch verborgene Kanäle nach außen gelangen dürfen, soll entsprechend der Forderung des CCC, gewährleistet sein. Die geheimen Schlüssel dienen als Zugang zu allen verschlüsselten Dokumenten eines Benutzers. Sollten diese Schlüssel unbemerkt durch irgendwelche Hintertüren den Rechner verlassen können, weil Implementierungsfehler oder Absicht dies ermöglichen, so könnten beliebige Dokumente eines Nutzers von Unbefugten entschlüsselt werden.

- Da das TPM fest auf Mainboards oder anderer Hardware verlötet werden kann, entginge dem Anwender die Möglichkeit seine Schlüssel von einem zum anderen Rechner mitzunehmen (zumal die gespeicherten Schlüssel nicht auslesbar wären). In der Folge wären Szenarien denkbar, in denen ein Nutzer eine Software für einen speziellen Rechner freischaltet. Möchte dieser Nutzer jetzt aber (z. B. auf Grund eines Defekts) seine Hardware wechseln, wären erneute Lizenzgebühren denkbar. Daher fordert der CCC Übertragungswege der Schlüssel von einem auf einen anderen Chip.

- Die 4. Forderung des CCC richtet sich auf die Behandlung von Softwarezertifikaten. Um in einer gesicherten Umgebung ablaufen zu können, soll entsprechende Software mit einem Zertifikat ausgestattet sein. Es soll transparent geregelt sein, zu welchen Bedingungen (also z. B. auch der Preis) welche Instanz Softwarezertifikate ausstellt. Ansonsten entstünde ein großes Mißbrauchspotential, mit dem beliebiger Software die Zertifizierung verweigert können würde.

[3] siehe [Pyl]

### 3.2.2 Bevorteilung von TCG-Mitgliedern?

Wie bereits in Abschnitt 2.1 angedeutet wurde, ist die Politik der TCG in der Öffentlichkeit nicht unbedingt sehr beliebt. Zwar hatte sich die Ursprungsorganisation TCPA tatsächlich sehr basisdemokratisch formiert, die Nachfolgeorganisation TCG hingegen läßt nur zahlenden Mitgliedern Stimmrechte zukommen. Dadurch in es den in Abschnitt 2.2 erwähnten Mitgliedern (vor allem denen der Kategorie „Promoter“ [4]) möglich, ihre Politik zum Design der Spezifikationen durchzusetzen. Wie in [CC03] angedeutet wird, droht sich ein Kartell zu entwickeln, dass die Standards für Trusted Computing bestimmen könnte.

Die TCG schützt sich mit vergleichsweise hohen Mitgliedsgebühren für die stimmberechtigten Kategorien vor unerwünschten Konkurrenten, die möglicherweise aus dem Open-Source-Bereich stammenden. Statt, gemessen am Jahresumsatz, den Mitgliedsbeitrag festzulegen, geschieht die Festlegung pauschal. Damit sind aber finanzschwache Unternehmen, die sich die Beträge von rund 7500 US-Dollar pro Jahr und die zusätzlich anfallenden Lizenzgebühren nicht leisten können, von vornherein aussen vor.

Unternehmen hingegen, die in der TCG Mitglied sind, haben folgende Vorteile:

- Sie können die Spezifikation nach ihren Wünschen inhaltlich beeinflussen.
- Wissen über technische Details erreicht sie deutlich früher.
- Die Spezifikationen stehen zur Umsetzung in Produkten früher bereit.
- Als Mitglied können sie zu günstigeren Konditionen (sowohl Preis als auch Bedingungen) die notwendigen Lizenzen erwerben.

Daraus ergeben sich klare Wettbewerbsvorteile.

Allerdings muss man der TCG zugute halten, dass sie im Punkt der fehlenden Mitbestimmung bei der Lizenzierungs- und Spezifikationspolitik mittlerweile auch eine kostenlose Mitsprache eingeräumt hat. Dennoch ergeben sich hieraus noch keine Stimmrechte, so dass es faktisch immer noch nach „dem Willen der Großen“ gehen kann.

### 3.2.3 Microsofts Rolle

Weitaus problematischer (aus kartellrechtlicher Sicht) ist die Lage im Bereich der „sicheren“ Betriebssysteme. Da Microsoft durch seine marktbeherrschende Stellung eine festgelegte API[5]

[4] die vollständige Liste der Mitglieder findet sich unter: [TCGd]
[5] Application Programming Interface, API

vorgeben kann, die dann für den gesamten Markt verbindlich sein dürfte, sofern externe Software irgendwelcher Entwickler im sicheren Teil des Betriebssystems laufen soll, ist diese technische Spezifikation in Form der Softwareschnittstelle ein Instrument, die Marktchancen der Konkurrenz massiv zu beschneiden.

Neben der API hat Microsoft noch weitere Möglichkeiten seine Stellung am Markt weiter auszubauen[6]:

- Durch die API kann Microsoft sich selbst Zugang zu Betriebssystemmitteln für Anwendungen aus dem eigenen Hause sicherstellen, die für andere Mitbewerber verschlossen oder nur beschränkt verfügbar sind. Da Microsoft vom Betriebssystem bis zur darauf aufsetzenden Anwendung Software herstellt, kann für alle Schritte internes Wissen verwendet werden.

- Die Mitgliedschaft in der TCG in Kombination mit der marktbeherschenden Stellung ermöglicht es Microsoft Rahmenbedingungen auf Märkten (z. B. Chipmärkte) durchzusetzen, die ohne die Mitwirkung in der TCG nicht möglich wären.

  Weiterhin kann Microsoft Bedingungen an die Hersteller künftiger Hardware (auch Nicht-Mitglieder der TCG) stellen, denn das geplante NGSCB wird auf der 1.2-Spezifikation der TCG und erweiterten Anforderungen an Ein- und Ausgabemedien (siehe Abschnitt 4.3.2) basieren. Möchten Anbieter microsoftkonforme Rechner mit „sicheren“ Betriebssystemen ausliefern, werden sie die Forderungen von Microsoft erfüllen müssen. Im Umkehrschluss sind sogar Anpassungen seitens der TCG an die Microsoftforderungen denkbar, womit der Standardisierungsprozess von Microsoft kontrolliert würde.

- Letztlich ist auch die mögliche Bindung von Inhalten an das Microsoftbetriebsystem denkbar. Im Zeichen von DRM kann Microsoft seine eigenen Formate für Medien etablieren und Inhalteanbieter an das neue Betriebssystem binden, wenn die Inhalte einen Schutz durch NGSCB erfahren sollen.

Es bleibt festzuhalten, dass die Gefahr besteht, dass sich die Marktbeherrschung von Microsoft, auch in anderen Märkten, weiter ausdehnt. Es bestehen Möglichkeiten DRM durchzusetzen und den Computer der Kontrolle durch den Anwender mehr und mehr zu entziehen.

[6] vgl. [CC03]

Der schleichende – bereits bestehende – Einzug von TPMs in die Rechner, wird möglicherweise nachträglich gegen den Willen der Nutzer, sofern diese sich nicht bestimmten multimedialen Inhalten verschließen wollen, genutzt, um umfassende Beschränkungen der Nutzerrechte zu Gunsten der Rechteinhaber und bestehenden Monopolisten durchzusetzen.

# 4 Architektur

## 4.1 Spezifikation der TCG

### 4.1.1 Funktionsumfang des Trusted Platform Module (TPM)

Das TPM stellt den eigentlichen Kern der hardwareseitigen Umsetzung der TCG-Spezifikationen dar. In Hardware gegossen, sollen fünf Erweiterungen der PC-Architektur den PC sicherer machen[7] (auch Mircosofts NGSCB sieht die gleichen Erweiterungen als Hardwarebasis vor):

- Sealing: Um die „Versiegelung“ des System sicherzustellen, müssen über das TPM zunächst alle TCB-Gefährdenden (Trusted Computing Base, TCB) Komponenten überprüft werden. Dazu gehören das BIOS, der Bootsektor und auch eventuelle Bootloader. Weiterhin müssen alle Komponenten, die als Module eines Kernels oder im Sicherheitskontext des Administrator laufen, überprüft werden.

  Die Überprüfung wird vom CRTM (Core Root of Trusted Module[8]) durchgeführt. Direkt nach dem Start des PCs bestimmt das CRTM anhand einer Hash-Funktion nach dem SHA-1-Standard die BIOS-Konfiguration und die BIOS-Parameter. Erst nach Abschluss dieser Überprüfung kommt das TPM ins Spiel, das den ermittelten Hash-Wert über ein besonders abgeschirmtes Register entgegen nimmt.

  Im nächsten Schritt erhält das BIOS vom TPM die Kontrolle über den Rechner und überprüft die oben genannten Komponenten wiederum anhand einer Hashfunktion. Nur als sicher erkannte Komponenten werden anschließend geladen.

- Schutz kryptographischer Schlüssel: Alle Schlüssel des Systems befinden sich im TPM. Der Endorsement Key als zentraler Schlüssel zur Erzeugung weiterer Schlüssel über den sicheren Zufallsgenerator liegt „unabhörbar“ im TPM verborgen.

  Gleichwohl sieht die TPM-Spezifikation 1.2 vor, dass der TPM-Kernschlüssel gelöscht werden kann („revoke trust“), und das Schlüssel über „Transport Protection“ sicher von

[7] vgl. [ARC03]
[8] manipulationssichere Erweiterung des BIOS

einem in den anderen TPM migriert werden können. Um das Löschen und Anlegen eines neuen Endorsement Keys zu ermöglichen, muss nach den Plänen der TCG zwingendermaßen eine dritte Instanz die Generierung, Überprüfung und Signierung übernehmen[9].

- Authentifizierung: Damit der Benutzer sicherstellen kann, dass er ein nicht kompromitertes System vor sich stehen hat, sind z. B. ein Bild oder ein Text denkbar, das/der verschlüsselt im TPM abgelegt sind und nur erscheinen können, wenn alle Hashfunktionen die korrekten Werte zurückliefern.

  Anders herum erfordert die TCG-Spezifikation eine Authentifizierung des Benutzers gegenüber dem System. Diese Erkennung geht so weit, dass ein Schalter die physische Präsenz des Benutzers am PC überprüfen soll. In der Spezifikation wird gefordert, dass die Implementierung durch Hardware geschieht, der Schalter jedoch nicht bei Einschalten des Rechners automatisch ausgelöst wird. (Ziel dieser Funktion ist das Unterbinden der Remote-Übernahme eines PCs.)

  Im Sinne von „Attestation“[10] ist es auch für andere IT-Systeme wichtig, die Integrität eines entfernten Rechners überprüfen zu können. Dazu gehören ebenfalls Mechanismen, einen Rechner z. B. über WAN-Verbindungen[11] hinweg authentifizieren zu können. In diesem Zusammenhang ist es wichtig, dass für eine, durch TCG-Mechanismen gesicherte Verbindung, beide Teilnehmer die TCG-Spezifikation erfüllen müssen, also mit Trusted Computing Hardware ausgestattet sein müssen.

- sicherer Timer

- sicherer Zufallsgenerator: In existierenden Rechnern werden Zufallszahlen zur Erzeugung von kryptografischen Schlüsseln nicht durch einen in Hardware gegossenen Zufallsgenerator erzeugt, vielmehr beruhen die erzeugten Schlüssel auf Softwareimplementierungen, die durch das zufällige Zeitverhalten zwischen RTC (Real Time Clock) und Eingabegeräten einen Wert erzeugen. Die Zufallswerte des TPM-internen Generators sollen nicht mehr von äußeren Faktoren abhängen.

Zu beachten ist, dass das TPM als passiver Chip auf dem Board keinen direkten Eingriff in das System vornehmen kann. Außerdem steht und fällt die Sicherheit mit der korrekten Im-

[9] siehe hierzu auch [ghi03]
[10] vgl. [KC]
[11] Wide Area Network, WAN

plementierung der TCB. Sollten versehentliche Programmfehler oder beabsichtigte Backdoors in einer der Sicherheitskomponenten auftreten, steht das Vertrauen der Verbraucher auf dem Spiel. So betont Mike Ferron-Jones von Intel auch „Wir werden in den TPM definitiv keine Hintertüren einbauen“[12]. Je kleiner der TCG-Kern ist, desto wahrscheinlicher lassen sich Fehler vermeiden.

Falsch ist die Annahme, dass man einen „sicheren“ Computer im Sinne der Vorstellung der TCG lediglich durch Software schaffen könnte. Sofern die Möglichkeit besteht, dass ein Computer physisch verändert wird, ließen sich Software-Angriffe nicht mehr sicher abwehren. Angesicht zunehmender Verbreitung von PDAs, Notebook und Handys ist die Wahrscheinlichkeit eines physischen Zugriffs auf die Hardware deutlich wahrscheinlicher geworden.

Ein Zugriff oder eine Manipulation auf Speicherzellen des RAM beispielsweise ist bei gängigen PCs denkbar. Dadurch ließen sich in der Folge entweder direkt kritische Daten auslesen oder aber Softwarekomponenten zum Schutz der Daten derart verändern, dass der Schutz anschließend nicht mehr gegeben ist.

### 4.1.2 Entwicklung der Spezifikation

Als erstes wichtiges Werk der damaligen TCPA wurde im Juli 2001 die TCPA-Spezifikation 1.1 verabschiedet. Seit dieser Version bis zur TCG-TPM-Spezifikation 1.2, die im November 2003 offiziell verabschiedet wurde, wurden vor allem vier Punkte erweitert[13]:

- Direct Anonymous Attestation: Im Sinne von „Direct Proof“ oder „Zero Knowledge Attestation“ kann der TPM-Chip seine Indentität ohne Rückgriff auf eine Drittinstanz beweisen[14].

- Locality: Das TPM soll externe Software-Prozesse (wie z. B. eine „sicheres“ Betriebssystem) autorisieren und dann sichere und unsichere externe Prozesse mit unterschiedlichen Privilegien ausführen können.

- Delegation: Nach der bisherigen Spezifikation durften „sichere“ Anwendungen / Betriebssysteme nur komplett oder überhaupt nicht auf die im TPM gespeicherten Daten zugreifen. Durch die Neuerungen in der Spezifikation sind zukünftig Abstufungen in der

[12] siehe [Ste03a]
[13] vgl. [ghi]
[14] Durch den Austausch von Informationen, können sich zwei Gegenstellen beweisen, dass sie das gleiche Geheimnis kennen.

Autorisierung (und entsprechend dem Zugriff auf das TPM) möglich, um die Verwaltung von sicheren Anwendungen und verschiedenen Komponenten zu erleichtern.

- Not-Volatile Storage: Mit der neuen Spezifikation werden dem Besitzer des TPM nichtflüchtige Bereiche im Speicher des Chips von mindestens 20 Byte eingeräumt. In diesem Data Integrity Register können beliebige Daten, wie z. B. zusätzliche Zertifikate und Schlüssel des Nutzers liegen.

Neben diesen Änderungen sind ein monotoner Zähler und ein Tick Counter vorgesehen, um Replay-Attacken verhindern zu können, und ein Schutz (Transport Protection) der TPM-Schlüssel, damit diese sicher von einem zum anderen Chip migriert werden können.

Entgegen der Ankündigungen von HP und Intel auf dem Intel Developer Forum im Herbst 2003, fehlt der Hinweis auf den löschbaren Endorsement Key. Dieses Feature nennt sich neuerdings „revoke trust“.

Die Spezifikation hatte eine lange Zeit mit der Abstimmungsordnung der damaligen TCPA zu kämpfen, da sich hier keine Mehrheiten finde ließen. Erst mit der Gründung der TCG war eine Ordnung geschaffen worden, in der die Spezifikation 1.2 mehrheitsfähig war.

## 4.2 Hardware

### 4.2.1 Funktionsprinzip

Die grundlegende Kombination von Hardwarekomponenten und ihrer Orientierung in der Gesamtarchitektur, nach den Plänen der TCG, wird in Abbildung 1 dargestellt. Außerdem lassen sich hier grundlegende Funktionsweisen des TPM erkennen.

### 4.2.2 Intels Hardware–Implementierung

Intels zukünftige Hardwareplattform für „Secure Computing“, wie es bei Intel heißt, wird LaGrande genannt, und geht über die Anforderungen der TCG hinaus. Bei der Entwicklung, die sich im übrigen noch etwa zwei Jahre von der Marktreife entfernt befindet, geht es Intel auch um Datenschutz und Nutzerrechte. Jeff Austin[15] betonte, dass ein sicherer Computer aber weit mehr als einen einzelnen Chip braucht, um zu funktionieren.

In der TCG-Spezifikation verankert sind z. B. so genannte „Attestation Identity Keys“ (AIKs), die zum Schutz der Privatsphäre auf Basis eines zentralen Schlüssels eine beliebige

[15] im Interview mit der c’t, vgl. [Ste03b]

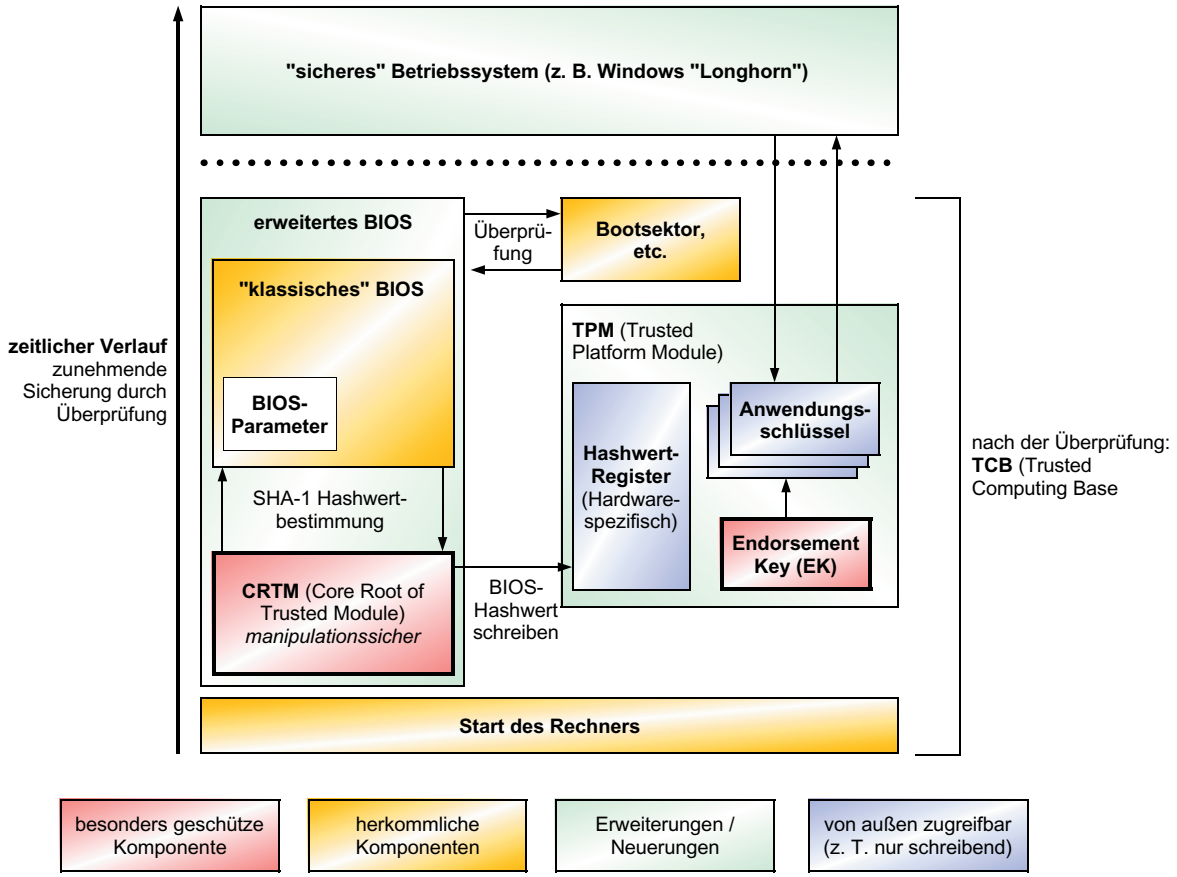


Abbildung 1: Hardware Architektur: Ebenen und Komponenten

Anzahl von Alias-Keys für einzelne Transaktionen erzeugen. Eine dritte Instanz überprüft in diesem Fall, ob ein spezielles System als vertrauenswürdig gilt.

LaGrande soll betriebssystemunabhängig sein, auch wenn Microsofts NGSCB als eine gute Kombinationsmöglichkeit angesehen wird. Dabei ist LaGrande lediglich „Benutzer“ des TPM und greift auf den sicheren Schlüsselspeicher, den Zufallsgenerator und den RSA / asymmetrischen Verschlüsselungsalgorithmus zurück. Zukünftige Prozessoren sollen problemlos bezüglich der Taktraten mit den TPMs zusammenarbeiten können.

Als Erweiterungen der TCG-Spezifikation ist unter anderem „Protected Execution Environment“ vorgesehen. In bisheriger Hardware laufen alle Programme in grundsätzlich nicht durch Hardware voneinander getrennten Speicherbereichen ab. Dadurch haben Programme, wie z. B. Treiber, die auf einer niederen Systemebene laufen, prinzipiell Zugriff auf alle Aktionen anderer Anwendungen. Durch LaGrande sollen geschützte Umgebungen eingeführt werden, die (mit gewissen ähnlichkeiten zu Microsofts NGSCB) parallel zu der bisherigen Rechnerarchitektur

laufen. Ebenso wie bei Microsoft[16], sind Verschlüsselungen aller Ein- und Ausgabekanäle, aber auch aller dazwischenliegenden Busse etc. erforderlich.

## 4.3 Software

### 4.3.1 Voraussetzungen

Wie bereits in den vorangegangenen Kapiteln erwähnt wurde, kann eine sichere Software grundsätzlich nur auf Basis einer sicheren Hardwareplattform (TCB) funktionieren. Dabei sind aber auch andere Plattformen, als die von der TCG vorgeschlagenen, denkbar. Insbesondere die in Abschnitt 3.2 genannten Forderungen wären einfacher mit einer frei beweglichen SmartCard-Lösung (zur Speicherung der Schlüssel) realisierbar. Daher ist es nicht verwunderlich, dass Microsoft sich für sein sicheres Betriebssystem zunächst nicht auf den Entwurf der TCG festlegen wollte.

### 4.3.2 Microsoft: Next Generation Secure Computing Base (NGSCB)

Zunächst nannte Microsoft (MS) in der Vergangenheit seine Bemühungen ein sicheres Betriebssystem zu entwickeln Palladium[17]. Nachdem der Begriff aber eine deutlich negative Bedeutung in der Öffentlichkeit erlangt hatte, änderte MS den Namen in Next Generation Secure Computing Base, kurz NGSCB um.

Die Entwicklungen zum kommenden Windows mit Codenamen „Longhorn“, in den NGSCB integriert werden soll, stehen derzeit im Bezug auf die sicherheitskritischen Komponenten noch in den Anfängen. Ein Release der neuen Version ist erst für das Jahr 2005 geplant.

Dabei gesteht selbst Microsoft sich mittlerweile ein[18], dass es um die Computersicherheit, insbesondere derer mit dem Windows-Betriebssystemen, nicht gerade rosig bestellt ist. Aktuelle Computer / Nutzer sind nicht vor Softwareschädlingen wie Viren, Key-Loggern oder Programmen, die die Ausgabe des Bildschirm umleiten, geschützt. In einer ersten Vorstellung hielt es Microsoft für möglich, gegen all diese Krankheiten des PCs ein Mittel zu finden, musste jedoch mittlerweile eingestehen[19], dass ein Virus sich z. B. in Bereichen eines Startskripts einsetzen könnte, dessen Bereich nicht von dem TPM-Modulen oder NGSCB überprüft wird. Damit könnte der Bootvorgang verändert werden, ohne dass der sichere Teil des Betriebssystem hierüber

[16] siehe Abschnitt 4.3.2
[17] zwischenzeitlich auch „Vaulted Computing“ genannt, vgl. [Him03]
[18] vgl. [Ger03e]
[19] siehe hierzu auch [ARC03]

informiert würde[20]. Eine Sicherheit lässt sich wohl nur für den „sicheren“ Teil („Nexus“) des Betriebssystems und der darin laufenden Anwendungen realisieren.

Dennoch lässt sich die Bedeutung eines „sicheren“ Betriebssystem nicht leugnen: die von der TCG entworfene Hardwareplattform allein kann keinen „sicheren“ Computer erzeugen. Allein durch die Tatsache, dass es sich beim TPM um einen passiven Chip handelt, dürfte verdeutlichen, dass eine vollständige Absicherung über TPM unmöglich ist[21]. Bisherige verbreitete Betriebssysteme wie Windows und Linux sind allerdings nicht auf Sicherheit getrimmt und erfüllen nicht die hohen Anforderungen an ein manipulationssicheres Betriebssystem. Ob Microsofts Longhorn allerdings diesen hohen Anforderungen genügen wird, ist indes nicht sicher[22].

Man darf also gespannt sein, in wie weit eine mögliche (und angesichts der Größe eines aktuellen Betriebssystems wahrscheinliche) Fehlimplementierung zu weit aus mehr Sicherheitsproblemen führt als bisher. Klar sein dürfte, dass das Sicherheitsbewußtsein von Otto-Normal-Nutzern angesichts der vollmundigen Versprechen Microsofts nicht gerade steigen dürfte.

### 4.3.3 Nexus und Longhorn: Microsofts Sicherheitsarchitektur

Die Grundidee der neuen, in Windows Codename „Longhorn[23]“ integrierten, Architektur ist der parallele Betrieb zweier Kernel. Longhorn[24] wird auf der Hardware der TCG-Spezifikation 1.2[25] aufbauen. Entsprechend Abbildung 2 stehen sich zwei Bereiche der Architektur gegenüber:

- Standard-Modus: Dieser Modus wird auch Left Hand Side (LHS) genannt, und umfasst ein komplettes „klassisches“ Betriebssystem, in dem auch künftig noch herkömmliche, nicht für Longhorn geschriebene, Anwendungen laufen können. Da der riesige Umfang des Windows-Codes eine Absicherung des Systems nahezu unmöglich macht (wenn auch noch alte Anwendungen wie bisher laufen können sollen), ist die LHS zur Abdeckung des abwärtskompatiblen Teils des Betriebssystems da, während die rechte Seite (Right Hand Side, RHS), den sicheren Teil darstellt.

  Aus der Erhaltung des „alten“ Windows folgt dann aber auch, dass im linken Teil wie bisher Schadprogramme wie Viren und Trojaner laufen können. Um dennoch ein „Über-

[20] zu den Einzelheiten der Struktur des MS-Betriebssystems: siehe unten
[21] siehe „Anforderungen“ in [ARC03]
[22] Als Beispiele für Microsofts Fehler in der Vergangenheit seien exemplarisch die bestehenden Probleme mit dem Internet Explorer und der Versuch der Verschlüsselung von Office-Dokumenten genannt
[23] siehe hierzu auch [GHPM03]
[24] Schema zur Architektur siehe Abbildung 2
[25] ergänzt um weitere sichere Komponente, siehe dazu Abschnitt 4.3.4

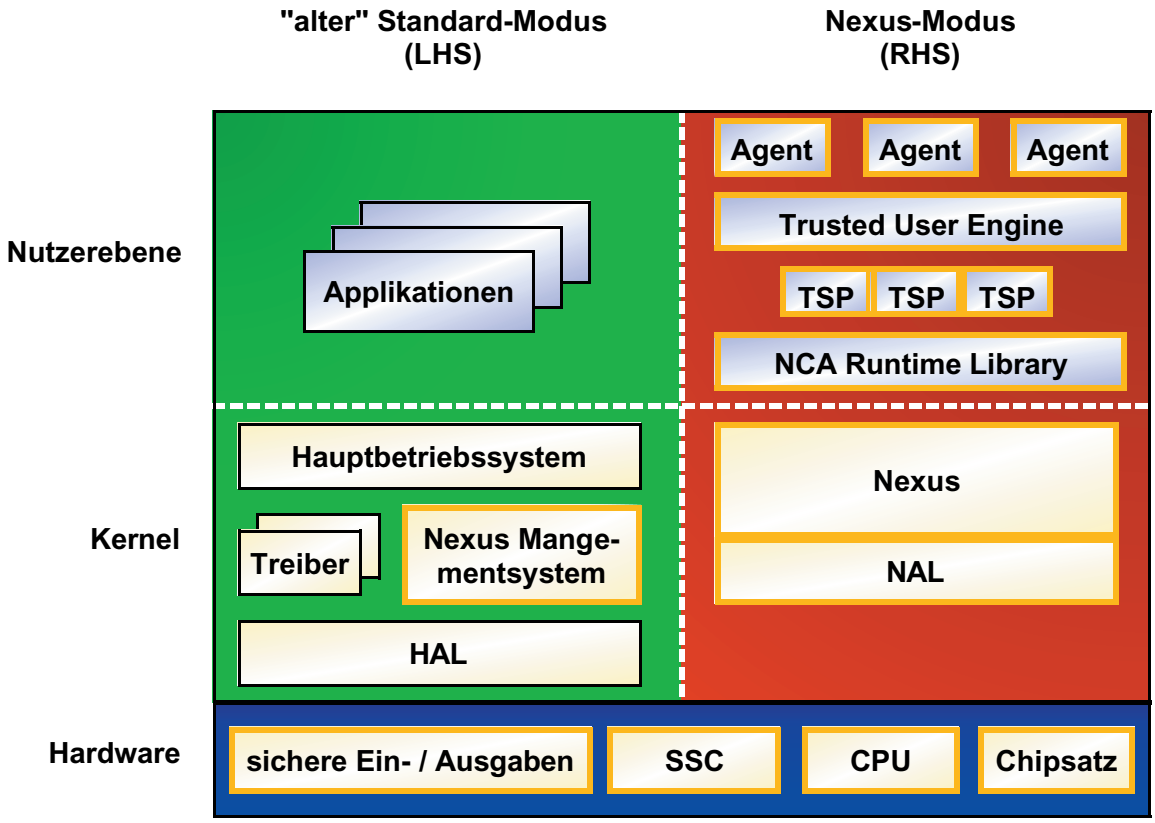


Abbildung 2: NGSCB-Architektur, nach „NGSB Quadrants“ in [Him03]

greifen“ auf die rechte Seite zu verhindern, gelten gegenüber dem bisherigen Windows folgende Einschränkungen, die, über entsprechende Hardware[26] abgesichert, realisiert werden müssen:

  - Windows-Anwendungen dürfen nicht mehr den kompletten Speicherinhalt von einem (beliebigen) Ort an einen anderen bewegen.
  - Der Prozessor kann von Anwendungen nicht mehr in den Real Mode versetzt werden.

- Nexus-Modus: Dies ist die rechte Seite[27] des Systems mit dem neuen Sicherheitskernel „Nexus“. Wie in Abbildung 2 zu sehen ist, basiert dieser Modus auf dem NAL[28], einem Pendant zur HAL[29] der LHS. Sichere Anwendungen heißen bei Nexus nicht einfach „sichere Anwendungen“, sondern Nexus Computing Agents (NCA, kurz Agents) und fußen

[26] vgl. Abschnitt 4.3.4
[27] im folgenden auch RHS genannt
[28] Nexus Abstraction Layer, NAL
[29] Hardware Abstraction Layer, HAL

auf der „Trusted User Engine“ (TUE). Damit Anwendungen auf der rechten Seite auf den Scheduler und die Thread-Verwaltung zurückgreifen können, existiert für jeden „Agenten“ ein Schattenprozess auf der linken Seite[30].

Der Nexuskern läuft in einem komplett isolierten Speicherbereich ab, und führt nur gesicherte Anwendungen aus[31], die wiederum jeweils in ihrem eigenen gesicherten Speicherbereich arbeiten. Da die rechte Seite der linken Seite grundsätzlich nicht vertrauen darf, funktioniert die Kommunikation mit der linken Seite nur gekapselt über die NAL und den Nexus Manager, der als Treiber auf der linken Seite arbeitet und Daten entgegennimmt. Alle Daten werden zunächst validiert[32], kommt es hier zu Fehlern bei der Übereinstimmung von erwartetem und ankommenden Datenstrom, werden die Datenpakete komplett verworfen[33].

Da sich der NGSCB-Teil von Longhorn derzeit noch in der Entwicklung befindet, sind noch nicht alle Details bekannt, noch ist es sicher, ob nicht einige Konzepte geändert / angepasst werden müssen. Für den Release von Longhorn ist es dann auch geplant, dass der Nexuskernel (beispielsweise durch einen Open-Source-Kernel) ausgetauscht werden kann. Außerdem sollen das klassische Windows und NGSCB (sprich die rechte Seite) weitgehend unabhängig voneinander laufen, so dass sich der Nexuskern sogar nachträglich laden lassen soll. Nicht möglich sein soll allerdings der parallele Betrieb zweier Nexus-Varianten.

Die NGSCB-Pläne Microsofts haben zwei grundlegende Vorteile gegenüber den Vorstellungen der TCG: das klassische Windows[34] läuft parellel zum sicheren Teil (Nexus), ohne das der Anwender möglicherweise hin- und herschalten muss und zum Zweiten können die Agenten auch dann sicher laufen, wenn auch nur die TCB und der eigentliche NGSCB-Teil auf Sicherheit überprüft wurden[35].

[30] siehe hierzu auch [Him03]
[31] vgl. hierzu [GHPM03]
[32] in diesem Zusammenhang spricht Microsoft von einer „Vorhalle“ (porch), in die die Daten zunächst gelangen
[33] Als Beispiel (vgl. [GHPM03]) sei eine NGSCB-kompatible Word-Version genannt, die eine Datei verschlüsseln oder mit einer Signatur versehen lassen möchte. Dazu wird die Datei an einen Agenten (NCA) übergeben, der anschließend das Ergebnis wieder zurückschickt. An dieser Stelle sei bemerkt, dass Anwendungen der rechten Seite keinen direkten Zugriff auf die Hardware (wegen der NAL) haben, und der Schreibzugriff in diesem Fall von der Word-Anwendung der linken Seite ausgeführt würde.
[34] für die Abwärtskompatiblität
[35] vgl. [ARC03]

Nicht zu vergessen sind aber auch die Nachteile des „wir-wollen-so-wenig-wie-möglich-an-Windows-neu-entwickeln“-Konzepts: es wird einige neue zusätzliche Hardware erforderlich sein, damit „Longhorn“ wie geplant laufen kann (siehe Abschnitt 4.3.4).

### 4.3.4 Extra-Wurst: Microsofts (Hardware-) Sonderwünsche

Damit NGSCB funktionieren kann[36], benötigt es die TCB[37], also einer Hardwareumgebung, die den Sicherheitanforderungen für den Betrieb eines „sicheren“ Betriebssystems genügt.

Dazu gehört als Grundstein für die Speicherung der Schlüssel das TPM[38] der TCG[39]. Zudem müssen sich der Prozessor und Speicher in einen sicheren Zustand versetzen lassen. Zur Ein- und Ausgabe werden herkömmliche Komponenten nicht mehr ausreichen. Damit Tastatur- und Mauseingaben nicht mehr abgehört werden können[40], muss die Übertragung der Signale verschlüsselt erfolgen. Dies betrifft natürlich auch die Grafikkarten für die Ausgabe. Analoge Ausgabeformate a la RGB dürften dann entgültig passe sein, da diese nicht (so ohne weiteres) verschlüsselt werden können. Ebenso ist die Nutzung von seriellen Schnittstellen oder PS/2 nicht vertrauenswürdig. Selbst der aktuelle USB-Standard reicht wahrscheinlich nicht aus, um die Anforderungen zu erfüllen. „In internen Microsoftpapieren ist von einer USB-Spezifikation 2.3 die Rede“[41].

Wie die Arbeit an der Hardware aussieht, verrät unter anderem der Abschnitt 4.2.2. Um wirklichen Schutz zu garantieren, müssen auch alle Übertragungskanäle auf den Mainboards, die kritische Daten transportieren, über eine Verschlüsselung verfügen.

# 5 Fazit - Ausblick auf die Entwicklung

Vertrauen scheint ein wichtiger Punkt für den Erfolg von Trusted Computing zu sein, das hat mittlerweile auch Microsoft erkannt: “Wir sind uns im Klaren darüber, dass zur Glaubwürdigkeit der Software eine unabhängige Überprüfung durch Dritte nötig sein wird.“[42]. Es bleibt abzuwarten, ob Microsoft seine Firmenpolitik derart ändern wird, dass zukünftig Externe Einblicke in den Code erhalten werden.

[36] siehe hierzu [Him03], „Unterbau“
[37] Trusted Computing Base, TCB
[38] Trusted Platform Module, TPM
[39] Trusted Computing Group, TCG
[40] etwa um Passwörter auszuspähen
[41] siehe [Him03]
[42] siehe Manferdelli in [Ger03e]

Je offener die TCG mit ihren Informationen und dem Prozess der Standardisierung und Kritik an diesem umgeht, desto besser sehen die Chancen für Trusted Computing aus.

Immer noch sind einige Probleme ungeklärt[43]:

- Wie kann ein sicherer Ein- und Ausgabepfade für die Fernwartung von NGSCB aussehen? Wie kann erwirkt werden, dass eine Sprachausgabe abgesichert wird?
- Um NGSCB in einem großen Rahmen zu nutzen, werden Trust Center für die Zertifizierung vonnöten sein, Microsoft plant eigenen Bekundungen zufolge jedoch ein eigene Zertifizierungsstelle, zeigt aber auch noch keine Alternativen auf.

Nicht zu vergessen ist eine entstehende Abhängigkeit von der absolut korrekten Implementierung - sowohl auf Software- als auch auf Hardware-Seite. Sicherheitslücken würden nicht nur das Vertrauen in Trusted Computing nachhaltig schädigen, sondern unter Umständen auch eine gigantische Menge (eine entsprechende Verbreitung von Trusted Computing vorausgesetzt) an Daten schlagartig unsicher machen.

Letztlich werden die Anwender klären müssen, ob sie Trusted Computing-Komponenten wollen - und ob sie damit auch Trusted Computing zu einen Siegeszug verhelfen.

[43] Auszug; siehe [Him03]

# 6 Anhang

**Mitgliedsliste der TCG**

Promoters: AMD, Hewlett-Packard, IBM, Intel Corporation, Microsoft, Sony Corporation, Sun Microsystems Inc.

Contributors: Agere Systems, ARM, ATI Technologies Inc., Atmel, Broadcom Corporation, Comodo, Fujitsu Limited, Fujitsu Siemens Computers, Gemplus, Infineon, Legend Limited Group, National Semiconductor, Nokia, NTRU Cryptosystems, Inc., NVIDIA, Philips, Phoenix, Rainbow Technologies, Inc., RSA Security, Inc., SCM Microsystems, Inc., Seagate Technology, Shang Hai Wellhope Information, Silicon Storage Technology, Inc., Standard Microsystems Corporation, STMicroelectronics, Texas Instruments, Utimaco Safeware AG, VeriSign, Inc., Wave Systems

Adopters: Ali Corporation, American Megatrends, Inc., AuthenTec, Inc., Gateway, M-Systems Flash Disk Pioneers, Silicon Integrated Systems Corp., Softex, Inc., Toshiba Corporation, Winbond Electronics Corporation

# 7 Literaturverzeichnis

Der Text wurde unter Verwendung der folgenden Literatur erstellt.

## Literatur

[ARC03] Sadeghi Ahmad-Reza and Stüble Christian. Vertrauen ist gut. *c't, Magazin für Computer Technik*, (13), 2003.

[CC03] Koenig Christian and Neumann Christian. ... und raus bist du. *ix*, (11), 2003.

[ciw] ciw. *Pentium-4-Mainboard mit Trusted Platform Module.* heise online, http://www.heise.de/bin/nt.print/newsticker/data/ciw-03.12.03-000. Retrieved 2003-12-03.

[ciw03] ciw. Hotline. *c't, Magazin für Computer Technik*, (8), 2003.

[Ger03a] Himmelein Gerald. Trusted computing. *c't, Magazin für Computer Technik*, (15), 2003.

[Ger03b] Himmelein Gerald. Trusted computing. *c't, Magazin für Computer Technik*, (6), 2003.

[Ger03c] Himmelein Gerald. Trusted computing. *c't, Magazin für Computer Technik*, (8), 2003.

[Ger03d] Himmelein Gerald. Trusted computing. *c't, Magazin für Computer Technik*, (9), 2003.

[Ger03e] Himmelein Gerald. Trusted computing: Ngscb wird ein großer erfolg. *c't, Magazin für Computer Technik*, (12), 2003.

[ghi] ghi. *Veröffentlichung der neuen Spezifikation für Trusted Computing.* heise online, http://www.heise.de/newsticker/data/ghi-11.11.03-000/. Retrieved 2003-11-18.

[ghi03] ghi. Trusted computing: Tpm-spezifikation 1.2 offiziell. *c't, Magazin für Computer Technik*, (24), 2003.

[GHPM03] Himmelein Gerald, Schulz Hajo, Siering Peter, and Withof Matthias. Longhorns tragende teile. *c't, Magazin für Computer Technik*, (24), 2003.

[Him03] Gerald Himmelein. Blick ins schloss. *c't, Magazin für Computer Technik*, (12), 2003.

[Him04] Gerald Himmelein. Vertrauenswürdig für wen? *c't, Magazin für Computer Technik*, (01), 2004.

[Joh] Lettice John. *Bad publicity, clashes trigger MS Palladium name change.* The Register, http://www.theregister.co.uk-content-4-29039.html. Retrieved 2003-11-18.

[KC] Kursawe Klaus and Stüble Christian. *Improving End-user Security and Trustworthiness of TCG-Platforms.* Saarland University, Germany, sa. Retrieved 2003-11-25.

[Mic02] Plura Michael. Digital rights management. *c't, Magazin für Computer Technik*, (24), 2002.

[Pyl] Pylon. *TCPA - Whom do we have to trust today?* Chaos Computer Club, http://www.ccc.de/digital-rights/forderungen. Retrieved 2004-01-17.

[Ros] Anderson Ross. *'Trusted Computing' Frequently Asked Questions.* http://www.cl.cam.ac.uk/rja14/tcpa-faq.html. Retrieved 2003-11-18.

[Ste] Krempl Stefan. *IDF: Mehr Schlüsselfreiheiten bei neuer Trusted-Computing-Spezifikation.* heise online, http://www.heise.de/newsticker/data/wst-17.09.03-001/. Retrieved 2003-11-18.

[Ste03a] Krempl Stefan. Schlüsselfreiheiten. *c't, Magazin für Computer Technik*, (23), 2003.

[Ste03b] Krempl Stefan. Trusted computing: Hardware lügt nicht. *c't, Magazin für Computer Technik*, (11), 2003.

[TCGa] Incorporated Trusted Computing Group. *TPM Main, Part 1 Design Principles.* Trusted Computing Group, https://www.trustedcomputinggroup.org/downloads/tpmwg–mainrev62_Part1_Design_Principles.pdf. Retrieved 2003-11-18.

[TCGb] Incorporated Trusted Computing Group. *TPM Main, Part 2 TPM Structures*. Trusted Computing Group, https://www.trustedcomputinggroup.org/downloads/tpmwg–mainrev62_Part2_TPM_Structures.pdf. Retrieved 2003-11-18.

[TCGc] Incorporated Trusted Computing Group. *TPM Main, Part 3 Commands*. Trusted Computing Group, https://www.trustedcomputinggroup.org/downloads/tpmwg–mainrev62_Part3_Commands.pdf. Retrieved 2003-11-18.

[TCGd] Incorporated Trusted Computing Group. *Trusted Computing Group: Current Members*. Trusted Computing Group, https://www.trustedcomputinggroup.org/about/members. Retrieved 2003-11-18.

[TCGe] Incorporated Trusted Computing Group. *Trusted Computing Group (TCG) Main Specification*. Trusted Computing Group, https://www.trustedcomputinggroup.org/press/news/TPM_release_110503.pdf. Retrieved 2003-11-18.