Dagmar Boedicker

Symposium „Trusted Computing Group (TCG)“
am 2. und 3. Juli 2003 in Berlin im BMWA

Bei der Trusted Computing Group (TCG) handelt es sich um ein Gremium, in dem sich 30 Firmen, unter anderem AMD, HP, IBM, Intel und Microsoft, zusammengeschlossen haben, um offene Standards für Trusted Computing *zu spezifizieren. Vorläufer der TCG in anderer Zusammensetzung war die* Trusted Computing Platform Association (TCPA) *mit etwa 200 Mitgliedern. Ein vorläufiges Ergebnis entfachte unter dem Namen* Palladium *heiße Diskussionen. Microsofts Weiterentwicklung heißt* Next Generation Secure Computing Base (NGSCB).

Das Bundesministerium für Wirtschaft und Arbeit (BMWA) *hatte zu einem zweitägigen Symposium geladen, um die wettbewerbs- und datenschutzrechtlichen Aspekte zu diskutieren und die „bislang höchst kontrovers geführte[n] Diskussion über die tatsächlichen Inhalte und Auswirkungen“ (Ankündigungstext des Bundesministeriums für Wirtschaft und Arbeit) zu versachlichen.* Nach eigener Aussage ist das BMWA am Thema IT-Sicherheit sehr interessiert, vermisst aber zur Zeit volkswirtschaftliche Impulse aus dem IKT-Bereich. Zeitweise schlugen die Wellen hoch, woran der Chaos Computer Club (CCC) natürlich nicht ganz unschuldig war. Sicher hätte auch das FIfF dazu etwas zu sagen gehabt, es war aber nicht geladen, um nicht zu sagen: Es wurde ausgeladen. Dazu aber mehr im Fazit. Zunächst ein möglichst knapper Bericht über die wesentlichen Aspekte des Symposiums, eingeleitet von einer Darstellung des Sicherheitskonzepts der Trusted Computing Group. Wer sich darin schon auskennt, kann das überspringen und gleich weiter lesen, was die Kritiker dazu sagen.

Das Sicherheitskonzept

Trusted Computing wie von der TCG spezifiziert ist ein integriertes Hardware-Software-Konzept. Ein vom Hersteller zertifizierter Chip[2], ein veränderter Chipkarten-Controller, wird fest mit der Platine des PCs, PDAs oder Mobiltelefons[3] verbunden. Dieses *Trusted Platform Module (TPM)*

- erzeugt asymmetrische Schlüssel und Zufallszahlen für die Verschlüsselung,
- speichert Hash-Werte über die Konfiguration in *Platform Control Registers (PCR),* die vor dem und beim Booten eine *Chain of Trust* erzeugen,
- erzeugt einen Genehmigungsschlüssel *(Endorsement Key, EK),* mit dem die Nutzer ihre Schlüssel als vom Trusted Platform Module generiert bestätigen. Auf der Basis des Endorsement Key können *Attestation Identity Keys (AIKs)* von einer externen Zertifizierungsstelle zertifiziert werden. Mit diesen AIKs lassen sich die Schlüssel des Nutzers anonym signieren.
- initialisiert und verwaltet weitere Funktionen wie das Ein- oder Ausschalten des Trusted-Computing-Modus durch den *Eigentümer* (der nicht mit dem *Nutzer* identisch sein muss).

Die Schnittstelle zu den Funktionen des Trusted Platform Module bildet der *TCG-Software-Stack (TSS),* beispielsweise für die Entwicklung standardisierter Verschlüsselungs-APIs[4], Schlüssel-Backup und -Migration, Authentifizierung der Plattform usw.

Beim Start des BIOS und beim Booten prüft das Trusted Computing Module schrittweise den Zustand des PCs und speichert *integrity metrics,* Plattform-abhängige Informationen zum Zustand der Software. Stück für Stück werden die Komponenten des Betriebssystems, die Hardware und die Software geladen und geprüft. Entsprechen die Hash-Werte dem Soll, kann es weitergehen. Wenn sich die Konfiguration deutlich geändert hat, ist eine neue Zertifizierung nötig. Eine Aussage lautet, dass der Benutzer sie selbst durchführen kann, Kritiker behaupten, dass die Änderungen online *abgesegnet* werden müssen und der PC eine neue Zertifizierung braucht.[5] Wenn Inhalte abgerufen werden, haben Anbieter die Möglichkeit, ihre verschlüsselten Inhalte nur in Abhängigkeit von ihren Sicherheitsrichtlinien abzugeben und können dazu verlangen, dass der Rechner sich als vertrauenswürdig gemäß TCG-Attestierung ausweist. Weil wahrscheinlich nur bestimmte Software als vertrauenswürdig anerkannt sein wird, können die Inhalte-Anbieter und Inhaber der digitalen Rechte natürlich Auflagen für die Software machen, beispielsweise einen bestimmten Abrechnungsmodus, Kopierschutz usw.

Das TPM kann nicht vor Hardware-Angriffen schützen, auch nicht vor Spam oder Viren-Attacken. Mit dem TPM wird ein Gerät authentifiziert, nicht die Person, die es nutzt.

Spezifikationen der TCG

Die TCG spezifiziert die Komponenten des Sicherheitskonzepts und außerdem Zertifizierungsanforderungen für spezifische Implementierungen. Als Spezifikationsinstrument werden *Protection Profiles* gemäß der *Common Criteria (IS 15408)* genutzt.
M. Waidner, vom *IBM Privacy Research Institut*, beschrieb auch, was die Trusted Computing Group *nicht* tut:

- Sie zertifiziert weder Anwendungen noch andere Software oder Schlüssel,
- sie nimmt keinen Einfluss auf die Auswahl der Software, die Benutzer auf der Trusted Platform einsetzen,
- und sie implementiert weder Dienste noch Server von Dritten.
- Sie unterhält keine Datenbanken
- und fungiert nicht als *Trusted Third Party,* die die Vertrauenswürdigkeit kommunizierender Geräte attestiert.

Die Kritik

Der wohl polemischste Kritiker war Ross Anderson, Universität Cambridge, UK. Mit handgeschriebenen Folien statt geschniegelter Powerpoint-Präsentationen feuerte er gezielte Salven auf die Versuche der Konzerne, die Selbstbestimmung der IT-Beschäftigten und -Nutzer mit technischen Kniffen einzuschränken. Aber auch Christian Koenig vom Zentrum für Europäische Integrationsforschung nahm kein Blatt vor den Mund. Wo Anderson und verschiedene CCC-Mitglieder Kritik aus technischer Sicht vorbrachten, hatte Koenig eher das Kartellrecht im Blick. Er äußerte den Verdacht, die TCG wolle misstrauischen Juristen möglichst wenig Einblick in die Technik geben: *Security by obscurity.* Gerade dann aber, wenn Juristen etwas obskur erscheine, kontrollierten sie besonders genau – vor allem im Wettbewerbsrecht.

Koenig verwies auf Artikel 81 EG-Vertrag, das Kartellverbot: Es bezieht sich auf abgestimmte Verhaltensweisen, die eine Verfälschung des Wettbewerbs bewirken. Ein Wille der Beteiligten ist dazu nicht nötig, der Effekt kann beispielsweise durch Standards entstehen, die Kompatibilität, Austauschbarkeit, und Interoperabilität regeln. Koenig warnte davor, Wettbewerbskommissar Monti zu unterschätzen: Im Gegensatz zu US-Wettbewerbsschützern, die gern abwarten und erst bei Fehlverhalten zuschlagen, beobachteten die Hüter des EU-Wettbewerbsrechts sehr viel genauer und ließen sich vorab, oft vertraulich, informieren. Microsoft und Intel seien wenig proaktiv in diesen Kontakten, sie schienen Angst wegen vergangener Vorfälle zu haben. Koenig gab die Empfehlung, die Kommission auf dem Laufenden zu halten, meinte aber, das könne im Fall TCG auch schon vertraulich passiert sein.

Informationsfreiheit und informationelle Selbstbestimmung

Ein Schwerpunkt der Kontroverse war das Zusammenspiel zwischen TPM und dem *Digital Rights Management (DRM):* DRM soll die grundgesetzlich verankerten zustimmungsfreien, pauschal vergüteten Nutzungsmöglichkeiten, die das Urheberrecht vorsieht, ersetzen durch individuell lizensierte Nutzungen, es würde damit die Sozialbindung des geistigen Eigentums abschaffen (V. Grassmuck, HU Berlin). Was im real gestorbenen Sozialismus beliebtes Zensurmittel war, die Kontrolle über Vervielfältigungsgeräte aller Art, findet im übrig gebliebenen Kapitalismus einen würdigen Nachfolger. Eine Technik wie TPM ist eine mögliche Basis dafür.

Das Trusted-Computing-Konzept bietet sich natürlich nicht nur für Unternehmen an, auch staatliche Einrichtungen sind sehr interessiert: Anwendungen können Dokumente für einen bestimmten Adressatenkreis ausschließlich verschlüsselt und mit eingeschränkter Nutzung erstellen. Eine solche erzwungene Zugangskontrolle schaltet den Menschen als wichtigsten Unsicherheitsfaktor weitgehend aus, unerwünschte Lecks beispielsweise in Richtung Medien können kaum noch vorkommen. Sollte die organisierte Kriminalität diese Funktionen nutzen wollen (und das wird sie sicherlich), lässt sich vorbeugen: Die *Hintertür* für die Sicherheitsbehörden kann gesetzlich erzwungen werden, auch wenn Firmenvertreter von Microsoft derartige Absichten eindeutig verneinten.

Die informationelle Selbstbestimmung als das Recht, selbst zu entscheiden, wer was über uns weiß, sahen mehrere Teilnehmer bedroht. Sie könnte auch laut BITKOM-Erläuterungen gefährdet sein:

> *„... besteht die Befürchtung, es könnten Konfigurationsdaten des Computers, die beim Zugriff auf Web-Angebote auf einem externen Server abgeglichen werden, von Dritten eingesehen und missbraucht werden."*

Für BITKOM aber kaum Grund zur Beunruhigung:

> *„Die Weitergabe von Konfigurationsdaten an externe Server ist jedoch vom TCPA-Konzept nicht vorgesehen. Ohnehin würden Gefahren, die sich für die informationelle Selbstbestimmung des Nutzers ergeben könnten, durch die bestehenden datenschutzrechtlichen Regeln abgefangen."*[6]

So optimistisch waren die Kritiker nicht. – Ein Diskussionsbeitrag sah die Freiheit der Nutzer durch die kommende Infrastruktur eingeschränkt: Zwar können die Nutzer das Trusted Platform Module abschalten, wenn sie aber bestimmte Webdienste in Anspruch nehmen möchten, entscheidet deren Anbieter über die Verwendung des TPM. In diesem Fall können die Nutzer also lediglich zwischen verschiedenen Anbietern auswählen und das nur solange der Wettbewerb funktioniert. Datenschützer[7] betrachten eine zwangsweise online-Registrierung als rechtswidrig und die Kontrolle von Nutzungsverhalten im privaten Bereich als illegal. Einen Anforderungskatalog haben sie der TCG bereits übergeben. Koenig stellte die berechtigte Frage, welchen Einfluss die Forderungen der Datenschutz-Beauftragten auf die Spezifikationen der TCG haben und erwartet *protokollfeste Ergebnisse.*

Datensicherheit

Eine Gruppe von Studierenden an der TU Berlin, Institut für Informatik und Gesellschaft, sieht folgende Schwierigkeiten:

> *„Das Hauptproblem ‚Break-once-run-everywhere' […] ist noch nicht beseitigt. Um zu verhindern, dass Datenübertragungen [...] abgefangen werden, bevor sie plattformabhängig verschlüsselt werden und so nur noch auf einem bestimmten Computer oder Handy laufen, müsste [...] viel mehr getan werden als das TPM leisten kann."*[8]

Und zum Thema Datensicherung:

> *„Sicherungskopien von unternehmenskritischen Daten, die an die TPMs der entsprechenden Datenserver gebunden sind, könnten im Falle eines Hardwaredefekts unwiederbringlich verloren sein."*[9]

Zu diesem Argument, das auch der CCC anführt, wandte Dirk Kuhlmann, HP, ein, dass die *Sealed Storage* (sicherer Speicherbereich) als geschützter Ort für sensible Daten wie Schlüssel sich auf einem Firmenserver kontrolliert duplizieren lässt. Ein Backup der Schlüssel sei nur für Einzelplatz-Rechner ausgeschlossen. – Die Gruppe von der TU Berlin fordert kundenfreundliche, durchsetzbare Datenschutzbestimmungen und empfindliche Strafen für Datenmissbrauch, damit Kunden dem TCPA-Ansatz vertrauen könnten.

Der CCC brachte weitere Probleme ins Gespräch: *verborgene Kanäle,* über die geheime Schlüssel der Nutzer übertragen werden könnten und die damit den Zugriff auf alle damit verschlüsselten Informationen möglich machen, und die bisher unvollständige Kontrolle der Nutzer über alle auf ihrem Rechner verwendeten Schlüssel.

Wettbewerbsrechtliche Einwände

Zwei Einschränkungen der Nutzer-Autonomie beanstandete Anderson besonders: *Locking-in* und *Product-Tying*. Locking-in bezieht sich auf die Bemühungen der Quasi-Monopolisten, ihre Kunden mit proprietären Formaten, De-facto-Standards und Software-Architekturen am Herstellerwechsel zu hindern. Product-Tying bezieht sich auf Zubehör, das einen wesentlichen Beitrag dazu leistet, bestimmte Produkte wie Drucker oder Handies unter Preis zu verkaufen, weil das Zubehör überteuert angeboten wird und billigere Konkurrenzprodukte ausgesperrt werden. Ein gutes Beispiel sind die Akkus für Handies, die zum Aufladen einen Authentifizierungscode des Herstellers abfragen. Billigere Konkurrenz-Akkus lassen sich mit dem zugehörigen Ladegerät nicht aufladen. Mit der Einführung des Trusted Computing wird nach Andersons Ansicht die Kontrolle der Nutzer nach dem Kauf aber noch einfacher.

Anderson wurde deutlich in Bezug auf Palladium und TCPA. Seine Kritik besagt, dass der Begriff „trusted" mit Vertrauen nichts zu tun hat und lediglich bedeutet, dass ein Programm auf einem PC für Dritte vertrauenswürdig wird, denn sie können dann feststellen, ob es verändert wurde, eine für das *Digital Rights Management* entscheidende Voraussetzung. Nur dann können die Anbieter von Inhalten entscheiden, auf welchen Plattformen und mit welcher Software ihre Waren genutzt werden dürfen. Sie können unlizensierte Software aussperren, über die Art oder Häufigkeit der Nutzung von Inhalten bestimmen und den Preis entsprechend gestalten, über kurz oder lang direkt von ihren Servern aus. Regierungen können mit Hilfe gestaffelter Sicherheitsebenen (*Multi-Level-Security-Levels*, *MLSL)* den Zugang zu ihren Informationen regeln. Auch für den Mail-Verkehr lassen sich Einschränkungen vorab festlegen: Mails sind druckbar oder nicht, Lesbarkeit nur bis zu einem bestimmten Datum, Weiterleitung erlaubt oder nicht, ... Ob solche Einschränkungen sich mit nationalem Recht vereinbaren lassen, ist mehr als fraglich, oft stehen Aufbewahrungsfristen dem entgegen.

Aus wettbewerbsrechtlicher Sicht entscheidend ist aber die Kontrolle der Anbieter über das Nutzungsverhalten nach einem Kauf. Quersubventionierungen von Hardware durch Software-Verkäufe ist das eine Problem, die Bindung der Nutzer an bestimmte Produkte und Plattformen das andere, wenn die Kosten für einen Wechsel zur Konkurrenz *(Switching Costs)* so hoch werden, dass der sich fast automatisch ausschließt. Zur Zeit entstehen bei einem Wechsel Kosten für Schulungen, die Konvertierung der Datenbestände, möglicherweise inkompatible Prozesse. Beim Wechsel von MS-Office zu einer Open-Source-Plattform wie Linux sind diese Kosten etwa vergleichbar mit den geltenden Lizenzgebühren. Sollte Trusted Computing sich als Standard durchsetzen, könnte der Wechsel nicht nur teurer werden sondern womöglich undurchführbar, weil sich beispielsweise die Zugriffsrechte auf verschlüsselte Dokumente durch eine andere Anwendung nur nach Genehmigung durch den Eigentümer (Ersteller) ändern ließen, was nach vielen Jahren der Geschäftsbeziehungen mit unzähligen Kunden ein gewaltiger Aufwand wäre.[10]

Heftige Debatten entspannen sich auch über die Spezifikationen der TCG, über Patente auf einzelne Komponenten und darüber, dass diese Rahmenbedingungen viele kleine und mittlere Software-Anbieter (KMU) und die gesamte Open-Source-Gemeinde ausschließen könnten. So ist die Mitgliedschaft in der TCG teuer, selbst Mitglieder ohne Entscheidungsrecht *(adapters)* zahlen mit 7.500 $US einen hohen Beitrag.

Die Spezifikation ist laut Koenig zwar für ITler, nicht aber für Juristen transparent; das Verfahren ist es überhaupt nicht. In Fällen einer möglichen Marktdominanz durch abgestimmte Verhaltensweisen stellt das Wettbewerbsrecht erhöhte Anforderungen an eine Mitgliedschaft im Standardisierungsprozess. – Die Lizensierung der TCG gilt aber nur gegenüber Mitgliedern, auch die Vereinbarungen für Patente nach *RAND (Reasonable and non-discriminatory licensing)* gelten nur für Mitglieder und der tatsächliche Umgang mit den Patenten bleibt abzuwarten. Nichtmitglieder der TCG haben keinerlei Einfluss und werden in ihrem Wissen über die Entwicklungsvorgaben nachhinken. Eine Ausnahme von kartellrechtlichen Auflagen (Freistellung) kann es übrigens bei angemessener Beteiligung der Verbraucher geben, oder wenn das Gremium den technischen oder wirtschaftlichen Fortschritt besonders fördert. Es darf dann aber keine Beschränkungen durch die beteiligten Unternehmen geben oder Möglichkeiten für sie, für einen wesentlichen Teil der betreffenden Waren den Wettbewerb auszuschalten.

Konstruktive Vorschläge

Eberhard Becker von der Universität Dortmund, Moderator der Arbeitsgruppe „Medienwirtschaft, DRM und Trusted Computing Group" (Section 4) gab einige Hinweise, wohin die TCG sich bewegen sollte: Sie sollte in ihre Reihen auch Non-profit-Organisationen und Vertreter der Open-Source-Gemeinde aufnehmen, wirklich durchsetzbare Sicherheitspolitiken implementieren und die Haftung der Hersteller verbessern, damit könne sie öffentliches Vertrauen erringen.

Von verschiedenen Seiten, besonders den Datenschützern, wurde die Forderung nach überprüfbarem offenem Code ge-

stellt, aber auch weitere konkrete Anforderungen. So müsse der Zugriff auf Daten ohne Protokolle möglich sein. Der Schutz der Urheberrechte lasse sich auch ohne Protokollierung erreichen, dafür sind die Verwertungsgesellschaften einzubeziehen. Die Nutzung müsse auch ohne Internet-Zugang möglich sein, und Updates ohne Einwilligung der Nutzer ausgeschlossen. Es müsse Wahlfreiheit geben: Jede und jeder müssten ihre vertrauenswürdige Instanz selbst aussuchen können, denn wenn dabei ein faktischer Zwang vorhanden sei, könne kein Vertrauen entstehen.

In der Diskussion wurde auch eine *vorlaufende* Regulierung durch EU und nationale Regierungen gefordert. In manchen Bereichen ergibt sich eine Deckung von Wettbewerbs- und Datenschutz-Recht, Vertreter beider Rechtsgebiete sollten also zusammenarbeiten.

Die TCG machte Angebote: Sie will ihre Öffentlichkeitsarbeit verbessern und mit den Kritikern zusammenarbeiten. Auch wenn es bisher bei der TCG keine kostenlose Mitgliedschaft gibt, kündigten ihre Vertreter doch an, zwei beitragsfreie Liason-Mitgliedschaften anzubieten.

Fazit

Ein Problem zog sich durch die gesamte Diskussion auf dem Symposium – die fehlende Trennung zwischen den Nutzer-Gruppen. Anvisierte Nutzer der Trusted Computing Group sind vor allem die Unternehmen *(business user).* Unternehmen, die für eine große Gruppe von Mitarbeiterinnen und Mitarbeitern sichere PCs einsetzen und die Anwendungen oder Dienste kontrollieren möchten, haben ein legitimes Interesse daran, dass diese Mitarbeiter an stabil konfigurierten PCs arbeiten und dort nur die Software einsetzen, die Dienste nutzen und die Inhalte abrufen, die für ihren Aufgabenbereich im Unternehmen erforderlich sind. Privatkopien von urheberrechtlich geschützten Inhalten spielen kaum eine Rolle, der Wunsch der Nutzer, von ihrem PC vielseitig Gebrauch zu machen, ebenso wenig. Informationelle Selbstbestimmung ist zwar ein Grundrecht der Mitarbeiterinnen und Mitarbeiter, wird im betrieblichen Alltag aber leider klein geschrieben.

Privatpersonen dagegen, die ihren PC als Allzweck-Computer schätzen, die eine Film- oder Musiksammlung auf der Festplatte anlegen wollen, ihre Anwendungen beliebig oft ergänzen, umkonfigurieren oder deinstallieren wollen, haben naturgemäß massive Vorbehalte gegenüber einer Sicherheitssoft- und -hardware, die ihre Autonomie einschränkt. Wie betriebliche Nutzer wollen sie selbst entscheiden, was sie im WWW nutzen, herunterladen, weiterleiten, kopieren, usw. – aber sie unterliegen keiner Abwägung von Interessen mit einem Arbeitgeber. Sie haben den Wunsch und legitimen Willen, sich nicht von einer angeblich sicheren Plattform bevormunden zu lassen. Daran könnte das Konsortium sich noch die Zähne ausbeißen, denn Microsofts Ruf ist durch eigene Schuld so beschädigt, dass seine friedlichen Kompromissangebote und Zusagen, Kritik zu berücksichtigen, während des Symposiums regelmäßig auf deutliche Zweifel stießen. Auch Intel hat bereits mit dem Pentium III schlechte Erfahrungen gemacht, und hatte darüber gelogen, auch das wurde ihm zu Recht vorgeworfen. Immer wieder machten die Hersteller zu Datenschutz-relevanten Themen Aussagen des Inhalts, dass sie dieses oder jenes sowieso nicht vorhätten. Hat sich damit der Zweck des Symposiums erfüllt oder handelt es sich um eine Ausrede, weil die Technik noch nicht besteht? Es fragt sich, ob es der TCG gelingen wird, ein eigenes Image aufzubauen, unbeschädigt vom lädierten einiger Mitglieder?

Ein weiteres Problem für die Verständigung unter den Teilnehmern war deren unterschiedliche fachliche Herkunft: Bit-Fiesler und Vertreter von Organisationen der Zivilgesellschaft, Behördenvertreter oder Marketing-Experten, Anwälte und andere Mitglieder der juristischen Fakultät, Informatikerinnen und Informatiker, alle versuchten, aus ebenso verschiedenenartigen Vorträgen Honig zu saugen. Diese (seltene) Art von Experiment ist sicher sehr zu begrüßen, zumal sich der Moderator des ersten Tages, Christian Koenig, zum Anwalt des Publikums machte und Zeit für die Diskussion freizuschaufeln versuchte, wo es nur irgend ging. Ein Diskurs zwischen unterschiedlichen Mitgliedern der Gesellschaft also, der sicher lohnte.

Zu kritisieren ist allerdings der Veranstalter TimeKontor AG, der nicht nur einen besonderen Beleg für IT-Sicherheit lieferte, indem er meine Teilnahmebestätigung zunächst an ein Berliner Unternehmen faxte, bevor er es mir dann mit handschriftlicher Notiz des Erst-Empfängers richtig zustellte. Trotz seiner Aussage, dass die Teilnehmer „nach zeitlichem Eingang der Anmeldungen“ ausgewählt würden, wählte er das FIfF e.V. komplett aus der Teilnahme heraus: zwei seiner Vertreter hatten sich vor mir angemeldet, wurden aber abschlägig beschieden.

Was Ross Anderson feststellt, scheint mir eine gute Zusammenfassung des Symposiums. IT-Sicherheit nähert sich einer ethischen und politischen Krise; sie wird nicht zum Schutz der Privatsphäre genutzt, sondern um Investitionen, Businesspläne u.a. zu schützen. Die Krise allerdings ist nicht wirklich neu, der Dualismus zwischen wirtschaftlichen und grundrechtlichen Interessen auch nicht. Regierungen haben dafür zu sorgen, dass es weiterhin Wettbewerb zwischen den Hard- und Software-Anbietern gibt. Das kann keine rein rechtliche, sondern muss auch eine ökonomische Diskussion sein.

1 *www.trustedcomputinggroup.com*
2 *auch Fritz-Chip genannt, zu Ehren des US-Senators Fritz Hollings, der TCPA als zwingenden Bestandteil sämtlicher Konsumelektronik propagiert (http://moon.hipjoint.de/TCPA-paladium-faq-de.html, Stand 18.5.2003)*
3 *weitere Geräte der Konsumelektronik könnten folgen*
4 *Application Programming Interface*
5 *So eine auf dem Symposium ausliegende FAQ von R. Anderson in Übersetzung von Moon vom 18.5.2003, http://moon.hipjoint.de/tcpa-palladium-faq-de.html. Diese Aussage ließ sich aber nicht bestätigen.*
6 *Bundesverband Informtaionswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM): Erläuterungen – Trusted Computing Platform Alliance (TCPA); vorgelegt beim Symposium*
7 *Alexander Dix, Landesbeauftragter für Datenschutz in Brandenburg*
8 *Luther, Katja et al: TCPA = DRM? Beitrag zum Symposium „Trusted Computing Group“ im BMWA, 2. und 3. Juli 2003*
9 *a.a.O.*
10 *Upgrade IV, 6/2003, S. 38*