Eine Bewertung von TCPA unter technischen und ökonomischen Aspekten

Diplomarbeit

eingereicht bei
Prof. Dr. Kai Rannenberg
Lehrstuhl für Betriebswirtschaftslehre,
insb. Wirtschaftsinformatik, Mehrseitige Sicherheit und M-Commerce
Fachbereich Wirtschaftswissenschaften
Johann Wolfgang Goethe-Universität
Frankfurt am Main

Betreuer:
Heiko Roßnagel

von
cand. rer. pol. Patrick Sauerwein

http://p3ppi3.bei.t-online.de

Studienrichtung: BWL

Inhaltsverzeichnis

Abbildungsverzeichnis V
Tabellenverzeichnis VII
Abkürzungsverzeichnis VIII
Symbolverzeichnis X

1 Problemstellung 1

2 Von der TCPA zur TCG 4

2.1 Beweggründe 4

2.2 Historie der „Trusted Computing Platform Alliance“ 6

2.3 Die Trusted Computing Group 8

3 Die Informations-Ökonomie 11

3.1 Technologie 12
3.1.1 Komplementäre, Kompatibilität und Standards 13
3.1.2 Infrastrukturelle und geschäftsrelevante Technologien 13

3.2 Information 14
3.2.1 Informationsgüter als Erfahrungsgüter 14
3.2.2 Informationsgüter als öffentliche Güter 15

3.3 Erlösmodelle 15
3.3.1 Erlösquellen 16
3.3.2 Erlösformen 17

3.4 Differenzierung von Produkten und Preisen 18
3.4.1 Preisdiskriminierung ersten Grades 18
3.4.2 Preisdiskriminierung zweiten Grades 19
3.4.3 Preisdiskriminierung dritten Grades 20

3.5 Lock-in und Wechselkosten 20
3.5.1 Klassifizierung von Lock-in Effekten 21
3.5.2 Der Lock-in Zyklus 24

3.6 Angebotsseitige Größenvorteile 26
3.6.1 Skaleneffekte 26
3.6.2 Verbunderträge 26

3.7 Nachfragerseitige Größenvorteile 27

4 Standardisierung 29

4.1 Definition 29
4.1.1 Gründe für Standards 30
4.1.2 Formen von Standards 30

4.2 Klassifizierung von Standards 31
4.2.1 Leistung versus Kompatibilität 32
4.2.1.1 Evolution 32
4.2.1.2 Revolution 33

4.2.2 Offenheit versus Kontrolle....34
4.2.2.1 Offenheit....35
4.2.2.2 Kontrolle....36
4.2.3 Allgemeine Netzwerk-Strategien....36
4.2.4 Coopetition....37
4.3 Standardisierungsallianzen....39
4.3.1 Wettbewerb zwischen und innerhalb von Standards....39
4.3.2 Allianzgestaltung zur Standardisierung....39
4.4 Kooperative Standardisierung....41
4.4.1 Die Leistungen von Kompatibilität und Standards....41
4.4.2 Die Kosten von Kompatibilität und Standards....42
4.5 Schlüsselressourcen....43
4.6 Geistiges Eigentum....44
4.6.1 Querlizenzierung und Patent-Pools....46
4.6.2 RAND-Lizenzierung....47
4.7 Funktionen in der Standardisierungsallianz....48
4.7.1 Die Mitglieder der TCG....49
4.7.1.1 Promoters....49
4.7.1.2 Contributors....49
4.7.1.3 Adaptors....50
4.7.2 Business Webs....50
5 Trusted Computing....52
5.1 Abgrenzung und Überblick....52
5.2 Grundkonzept von vertrauenswürdigen Plattformen....53
5.2.1 Root of Trust for Measurement (RTM)....55
5.2.2 Trusted Computing Group Software Stack (TSS)....55
5.3 Das Trusted Platform Module (TPM)....57
5.3.1 Root of Trust for Reporting (RTR)....58
5.3.2 Root of Trust for Storing (RTS)....60
5.3.3 TPM Architektur....62
5.3.4 TPM Funktionalitäten....66
5.3.4.1 Integrität….67
5.3.4.2 Geschützter Speicher....68
5.3.4.3 Identität….71
5.3.4.4 Sicheres Booten und authentisierte Bootprozesse....72
5.4 Implementierung im PC....73
6 Anwendungen und Szenarien....76
6.1 Verfügbare Umsetzungen....76
6.1.1 Herstellung der Komponente TPM....76
6.1.2 Einsatz der TPM Komponente im System....77
6.2 Intel LaGrande....78
6.3 Next-Generation Secure Computing Base (NGSCB)....80
6.3.1 Architektur....80
6.3.2 Arbeitsablauf....82

6.3.3 Kernelemente der geschützten Betriebsumgebung 84
6.3.3.1 Strenge Prozess Isolation 85
6.3.3.2 Versiegelter Speicher 85
6.3.3.3 Attestierung 86
6.3.3.4 Sichere Wege zum Nutzer 86
6.3.4 Beispielanwendung „Rights Management Services“ (RMS) 87

6.4 Anwendungen unter dem Betriebssystem Linux 88
6.4.1 IBM's Global Security Analysis Lab (GSAL) 88
6.4.2 Open Source Linux Projekt „Enforcer“ 89

7 Bewertung 92

7.1 Bewertung der kooperativer Standardisierung 92

7.2 Hardwarekompatibilität und Netzwerkexternalitäten 93
7.2.1 Szenario 93
7.2.2 Gleichgewicht bei Einweg-Kompatibilität 94

7.3 Technologischer Vorteil und Standardisierung 96
7.3.1 Statischer Ansatz der Adoption einer neuen Technologie 96
7.3.2 Dynamischer Ansatz der Adoption einer neuen Technologie 98
7.3.2.1 Annahmen 99
7.3.2.2 Technologische Adoption bei perfekten Substituten 100

7.4 Schwächen und Risiken 101

8 Zusammenfassung 104

Literaturverzeichnis 107

Abbildungsverzeichnis

Abbildung 1: Typen der Attacken oder entdeckter Missbrauch im Jahresvergleich 1

Abbildung 2: Geschätzte Summen der Verluste für das Jahr 2003 2

Abbildung 3: Anzahl der berichteten Vorfälle an CERT 5

Abbildung 4: Berichtete Schwachstellen an CERT 5

Abbildung 5: TCPA Organisationsstruktur 7

Abbildung 6: Überblick der bisher verfassten Dokumente 10

Abbildung 7: Technology Push und Market Pull im Zusammenspiel 11

Abbildung 8: Erlösquellen im Internet 16

Abbildung 9: Der Lock-in Zyklus 25

Abbildung 10: Ergebnis von positivem Feedback 28

Abbildung 11: Adoptionsdynamiken 28

Abbildung 12: Trade-off zwischen Leistung und Kompatibilität 32

Abbildung 13: Trade-off zwischen Offenheit und Kontrolle 35

Abbildung 14: Das Value Net 38

Abbildung 15: Skala zur Einordnung der Strategien von Eigentumsrechten 45

Abbildung 16: Generelles Modell vertrauenswürdiger Plattformen 54

Abbildung 17: TSS Architektur 57

Abbildung 18: Transitive Bindung des EK an die Plattform über das TPM 59

Abbildung 19: Benutzergruppen 61

Abbildung 20: Komponenten der TPM Architektur 63

Abbildung 21: Die acht Betriebsmodi des TPM 64

Abbildung 22: Beispiel für eine Hierarchie der Speicherung 69

Abbildung 23: Migrierbarkeit und Nicht-Migrierbarkeit von Daten 70

Abbildung 24: Beweis der Echtheit einer vertrauenswürdigen Plattform sowie deren Identitäten 71

Abbildung 25: Architektur der vertrauenswürdigen Komponenten im PC 74

Abbildung 26: Integritätsmessungen und Berichten in einem PC 75

Abbildung 27: Erweiterungen der Intel LaGrande Hardware 78

Abbildung 28: NGSCB System Überblick 81

Abbildung 29: Interaktion zwischen Anwendungen, OS und Hardware 83

Abbildung 30: Ver- und Entsiegelung von Geheimnissen 85

Abbildung 31: Ablauf von „Rights Management Services“ 88

Abbildung 32: Entwurf der „Bear Plattform“ als Web-Server 91

Abbildung 33: Indifferenzkurven bei perfekten Substituten 101

Tabellenverzeichnis

Tabelle 1: Meilensteine der TCPA 8

Tabelle 2: Level und Beiträge der TCG-Mitgliedschaft 9

Tabelle 3: Erlössystematik 17

Tabelle 4: Typen von Lock-in und den zugehörigen Wechselkosten 22

Tabelle 5: Allgemeine Netzwerkstrategien 37

Tabelle 6: Ausschnitt der US-Top 20 Patente 2003 nach Markenname 44

Tabelle 7: Platform Configuration Register im PC 75

Tabelle 8: Statisches Adoptionsspiel bei neuer Technologie 97

Abkürzungsverzeichnis

3DES:	Triple Data Encryption Standard
API:	Application Programming Interface
AIK:	Attestation Identity Key
BBB:	BIOS Boot Block
BIOS:	Basic Input Output System
CA:	Certification Authority
CRTM:	Core Root of Trust for Measurement
DAA:	Direct Anonymous Attestation
EAL:	Evaluation Assurance Level
EC:	Endorsement Certificate
EFF:	Electronic Frontier Foundation
EK:	Endorsement Key
FBI:	Federal Bureau of Investigation
HMAC:	Hash-based Message Authentication Code
ISO:	International Standard Organisation
LILO:	Linux Loader
LPC:	Low Pin Count
LSM:	Linux Security Module
MSCAPI:	Microsoft Cryptography Application Programming Interface
OIAP:	Object Independent Authorization Protocol
OSAP:	Object Specific Authorization Protocol
OS:	Operating System
PCR:	Platform Configuration Register
PDA:	Personal Digital Assistant
PKCS:	Public Key Cryptography Standards
PKI:	Public Key Infrastructure
PP:	Protection Profile
RAND:	Reasonable and non-discriminatory
RMS:	Rights Management Services
RTM:	Root of Trust for Measurement
RTR:	Root of Trust for Reporting
RTS:	Root of Trust for Storage

S-MIME:	Security Multi-parts for Multi-purpose Internet Mail Extensions
SSC:	Security Support Component
SSL:	Secure Socket Layer
SRK:	Storage Root Key
TBB:	Trusted Building Block
TC:	Trusted Computing
TCB:	Trusted Computing Base
TCG:	Trusted Computing Group
TCPA:	Trusted Computing Platform Alliance
TP:	Trusted Platform
TPM:	Trusted Platform Module
TPS:	Trusted Platform Subsystem
TSS:	Trusted Platform Support Service
UPE:	Undercut-Proof Equilibrium
W3C:	World Wide Web Consortium
YACA:	Yet Another Certification Authority
ZKP:	Zero Knowledge Proof

Symbolverzeichnis

n:	Anzahl an Teilnehmern
λ:	Anzahl der Unternehmen in einer Industrie
η:	Eine gegebene Grundgesamtheit
α:	Intensität der Netzwerkexternalitäten
τ:	Eine bestimmte Zeitperiode
δ:	Differenzierung, Transport- und Wechselkosten
t:	Zeit
U:	Nutzen eines Konsumenten
π_i:	Gewinn eines Unternehmens i
p_i:	Preis des Unternehmens i
W:	Soziale Wohlfahrt

1 Problemstellung

Die Konvergenz von Medien, Telekommunikation sowie Informationstechnologie führt zu einer gesteigerten Interaktion zwischen den Computergeräten dieser drei Wirtschaftssektoren. Zugleich steigt die Anzahl mutierender Würmer, Viren und Trojanische Pferde, wie z.B. Varianten der Bagle- und Sober-Würmer oder der Netsky- und MyDoom-Viren, im Tagesrhythmus und bedrohen die Sicherheit von Computerplattformen. Die Daten der Systeme sind daher potenziellen Risiken ausgesetzt. Um dieser steigenden Bedrohung zu entgegnen, entwickelt die industrielle Initiative „*Trusted Computing Group*“ (TCG), ehemals „*Trusted Computing Platform Alliance*“ (TCPA), einen Standard, welcher die Sicherheit der verschiedenen Gerätetypen verbessern soll. *Abbildung 1* dokumentiert dabei die Sicherheitsmängel, welche durch die verschiedenen Typen der Attacken oder den entdeckten Missbrauch veranschaulicht werden.

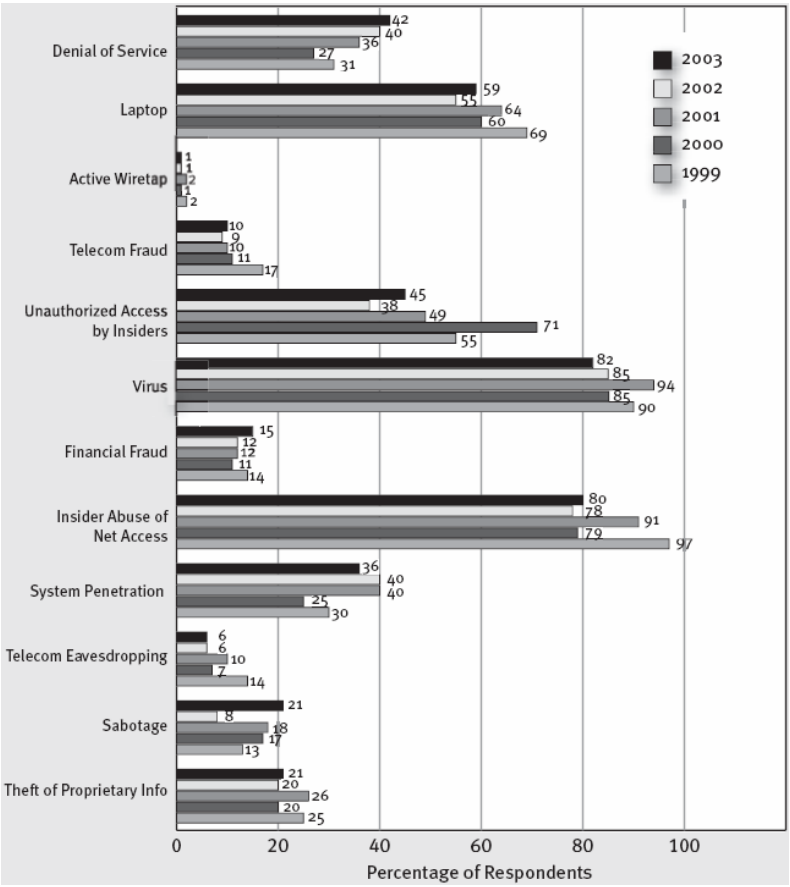

Abbildung 1: Typen der Attacken oder entdeckter Missbrauch im Jahresvergleich[1]

[1] Vgl. CERT (2004)

Speziell Viren und der Missbrauch der Netzwerkzugänge innerhalb des Unternehmens können aus der *Abbildung 1* als häufigste Ursache entnommen werden. Verlust des Laptops, nicht autorisierte Zugriffe durch Insider und Denial of Service Angriffe folgen auf den weiteren Plätzen. Die Gesamtkosten der Computerkriminalität sind zwar unter das Niveau vom Jahre 2000 gefallen, speziell von 2002 auf 2003 haben sich diese mehr als halbiert, obwohl seit 1999 besonders die Urheberrechtsverletzungen proprietärer Informationen stetig angestiegen sind. Der Verlust proprietärer Informationen steht mit 21 Prozent nicht direkt im Vordergrund der obigen Abbildung. Allerdings schlägt der Diebstahl von proprietären Informationen mit 35 Prozent der Gesamtkosten der Computerkriminalität zu buche und führt damit die geschätzten Verluste aus *Abbildung 2* an.[2]

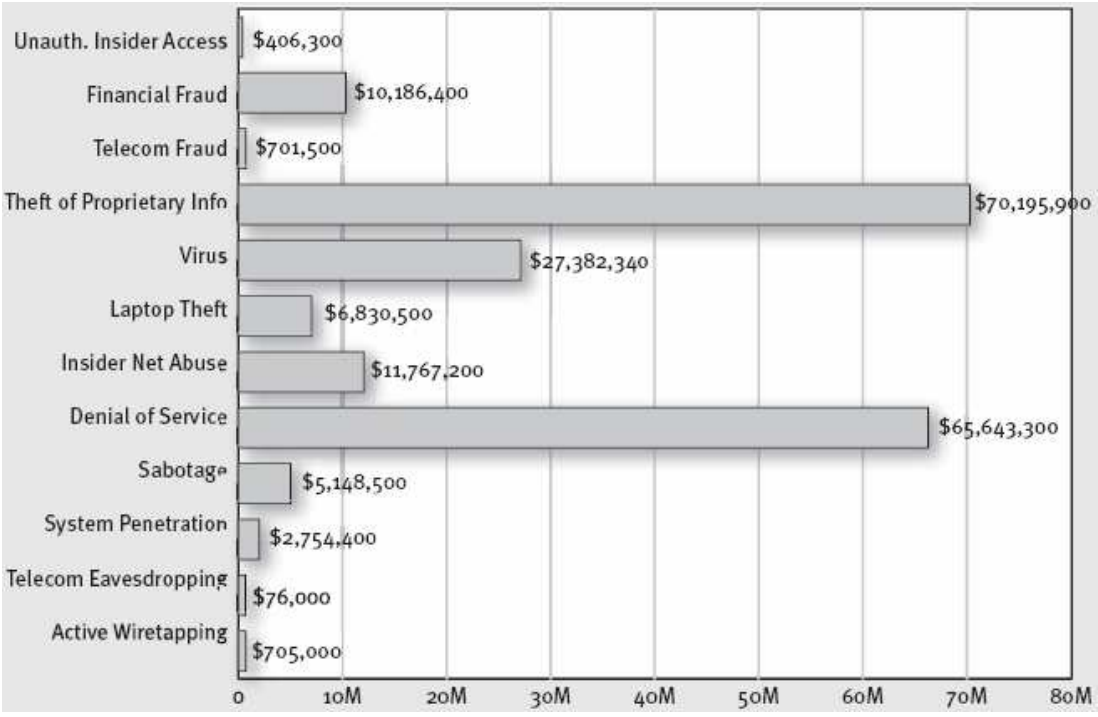

Abbildung 2: Geschätzte Summen der Verluste für das Jahr 2003[3]

Auf Platz zwei folgen Denial of Service Angriffe, die Kosten von ca. 65,6 Millionen Dollar verursachen. Viren, Missbrauch des Netzes durch Insider sowie finanzieller Betrug folgen auf weiteren Plätzen.[4] In der Studie vom Computer Security Institute werden die Bestrebungen der TCG, vertrauenswürdige Plattformen herzustellen, als

---

[2] Vgl. Computer Security Institute (2003), S. 20

[3] Vgl. Computer Security Institute (2003)

[4] Vgl. Computer Security Institute (2003)

mögliche Lösung des Problems des Diebstahls von proprietären Informationen betrachtet. Deren Effekte werden sich voraussichtlich in fünf bis zehn Jahren auf die Computersicherheit bemerkbar machen.[5] Auch das „Federal Bureau of Investigation" (FBI) hat mittlerweile eine Initiative zusammen mit der Entertainment- und Softwareindustrie gegen den Diebstahl von urheberrechtlich geschütztem Material abgeschlossen, da die Verluste in der Summe mehrere Billionen Dollar verursachen.[6]

Die beiden ersten Abbildungen in Verbindung mit dem dazugehörigen Zahlenmaterial belegen die Diskrepanz der TCG. Dazu stützt sich die TCG auf die steigende Anzahl an Attacken und Missbräuche, ohne die geschätzten Verluste der einzelnen Attacken zu berücksichtigen. Gerade die enorme wirtschaftliche Bedeutung von Information und deren Missbrauch offenbart allerdings einen möglichen Antrieb, die Sicherheit bestehender Rechnersysteme zu verbessern. Diese Erkenntnis ist jedoch nicht übereinstimmend mit der Triebkraft der TCG, die ihre Initiative auf die steigende Anzahl an Schwachstellen stützt, um vermutlich ihre eigentlichen Beweggründe zu verschleiern.

Ziel dieser Arbeit ist zum einen den technischen Standard der TCG sowie mögliche Umsetzungen vorzustellen und zum anderen die Standardisierung unter ökonomischen Ansichten zu untersuchen, um sie anschließend zu bewerten. Dazu wird im zweiten Kapitel ein erster Einblick über das Standardisierungsgremium, deren Beweggründe sowie den historischen Kontext zwischen TCPA und TCG gegeben. Das dritte Kapitel dient als Grundlage und Einführung in die Informationsökonomie, um die Komplexität und Zusammenhänge hinsichtlich der Standardisierung und abschließenden Bewertung in den folgenden Kapiteln besser zu erfassen. Neben der Technologie und Information spielt die Auswahl der Erlöse in Verbindung mit der Preisdiskriminierung eine wichtige Rolle. Bezüglich der Standardisierung und Bewertung haben Lock-in sowie Wechselkosten erhebliche Auswirkungen auf die Konsumenten. Das gilt ebenfalls für die Größenvorteile, vor allem auf die Netzwerkexternalitäten.

---

[5] Vgl. Computer Security Institute (2003)

[6] Vgl. FBI National Press Office (2004)

Die Standardisierung der TCG wird im vierten Kapitel ausführlicher behandelt, wobei Standards definiert, abgegrenzt und klassifiziert werden. Zudem wird die kooperative Standardisierung in Form einer Allianz sowie die daraus folgende Problematik des Umgangs mit geistigem Eigentum eingegangen. Das fünfte Kapitel geht direkt auf die technischen Spezifikationen der TCG ein, erklärt das Grundkonzept vertrauenswürdiger Plattformen und behandelt als Schwerpunkt die Komponente des „Trusted Platform Modules“ (TPM) sowie dessen Implementierung in einen Computer. Im Anschluss daran werden im sechsten Abschnitt technischen Umsetzungen auf praktische Anwendungen und Szenarien vorgestellt. Dazu werden als Erstes verfügbare Umsetzungen sowie die Hardwarearchitektur am Beispiel von Intel LaGrande dargestellt, worauf die anschließenden Softwareanwendungen unter den beiden Betriebssystemen Windows und Linux aufbauen. Das siebte Kapitel behandelt die Bewertung der kooperativen Standardisierung und zeigt die Zusammenhänge zwischen Hardwarekompatibilität und Netzwerkexternalitäten auf. Darüber hinaus wird die Adoption dieser neuen Technologie unter statischen und dynamischen Ansätzen berechnet und abschließend die Schwächen und Risiken dieser neuen Technologie erläutert.

2 Von der TCPA zur TCG

2.1 Beweggründe

In Veröffentlichungen der TCG wird als Grund zur Rechtfertigung vertrauenswürdiger Plattformen das Problem der Softwareattacken angeführt. *Abbildung 3* zeigt die ansteigende Bedrohung durch die Anzahl der berichteten Vorfälle an CERT von automatisierten Softwareattacken aufgrund der fortgeschrittenen und automatisierten Angriffswerkzeuge, der schnell zunehmenden Anzahl entdeckter Schwachstellen und die ansteigende Mobilität der Nutzer.[7]

[7] Vgl. CERT (2004)

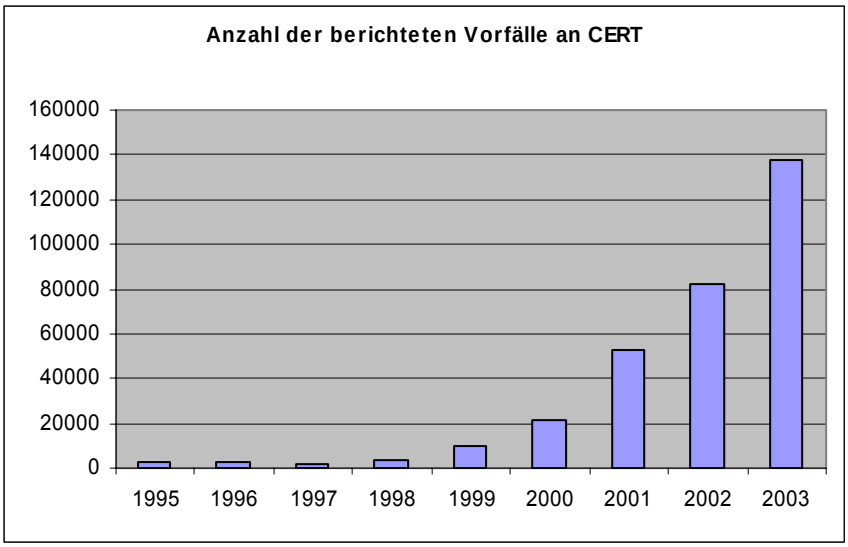

Abbildung 3: Anzahl der berichteten Vorfälle an CERT[8]

Die schnell steigende Anzahl der Schwachstellen schafft eine vorteilhafte Situation für Angreifer, da die Probleme verbunden mit der Aktualisierung von Korrekturen in Form von Patches mehr als eine Schwachstelle aufweisen.[9] Auch wenn in *Abbildung 4* ein leichter Rückgang im Jahr 2003 von 4129 auf 3784 der berichteten Schwachstellen ersichtlich ist, so sind diese keineswegs zu vernachlässigen.[10]

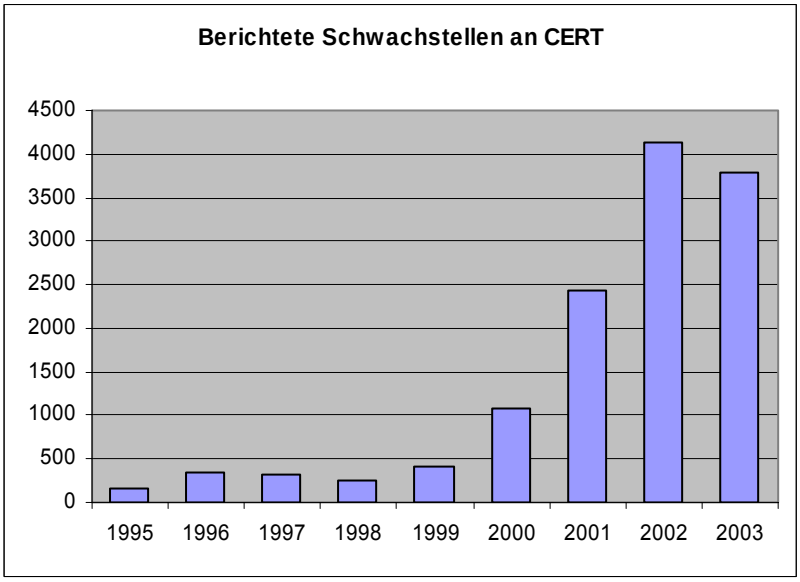

Abbildung 4: Berichtete Schwachstellen an CERT[11]

---

[8] Vgl. CERT (2004)

[9] Vgl. TCG Backgrounder (2003), S. 3

[10] Vgl. CERT (2004)

[11] Vgl. CERT (2004)

Besonders Client-Systeme sind gefährdet, da diese typischerweise keinen Sicherheitsadministrator haben, der sich um Korrekturen durch Patches kümmert. Hinzu haben Angreifer steigendes Interesse an Client-Systemen, aufgrund der wertvollen gespeicherten Informationen von mobilen Systemen. Es besteht also das Risiko von elektronischem Diebstahl wertvoller persönlicher oder unternehmensbezogener Daten sowie von Informationen über die Authentisierung und Identifizierung mit denen Eindringlinge großen Schaden verursachen können. Jedoch reichen softwarebasierte Sicherheitsmechanismen nicht mehr aus, um ausreichend Schutz für wertvolle Informationen zu geben. Dieses Risiko wird durch die Mobilität der Benutzer noch weiter verstärkt, wie z.B. durch den möglichen physischen Diebstahl oder Verlust der Endgeräte. Die TCG verfolgt daher einen hardwarebasierten Ansatz, um die Sicherheit von Informationen über möglichst viele Rechnergeräte, bei gleichzeitiger Entwicklung von Anwendungen und Kompatibilität, zu gewährleisten.[12]

2.2 Historie der „Trusted Computing Platform Alliance“

Die „Trusted Computing Platform Alliance“ verstand sich als eine industrielle Arbeitsgruppe, welche im Januar 1999 von Compaq, Hewlett-Packard (HP), International Business Machines (IBM), Intel und Microsoft gegründet wurde. Ziel dieser Allianz war es einen Standard zu spezifizieren, der erweiterte Hardware- und OS-basierte vertrauenswürdige Computer-Plattformen liefert. Der Ansatz dazu war eine Spezifikation zu entwerfen, die es erlaubt ein Hardwaremodul als Massenprodukt in möglichst viele Plattformen zu implementieren. Des Weiteren sollten Softwarehersteller dazu ermuntert werden, Programme für die neue Hardware zu schreiben. Der Anwendungsbereich der Spezifikation ist die Hardware-, OS- und BIOS-Ebene. Dabei sollten existierende Technologien ergänzt werden, wie X.509, IPSEC, IKE, VPN, PKI, Smart Cards, Biometriken, S-MIME und TLS, anstatt diese neu zu definieren. Ein erster Entwurf der Spezifikation wurde am 11.10.1999 bekannt gegeben und gleichzeitig wurden andere Unternehmen unter Geheimhaltungsvereinbarung eingeladen an diesen offenen Industriestandard mitzuarbeiten. Diesem Aufruf folgten bis zum 31. Juli 2003 genau 201 Unternehmen.[13]

---

[12] Vgl. TCG Backgrounder (2003), S. 3 f.

[13] Vgl. TCPA Membership (2003)

Die TCPA gliedert sich, wie nachfolgend in *Abbildung 5* ersichtlich, in drei Unterkommission und fünf Arbeitsgruppen auf:

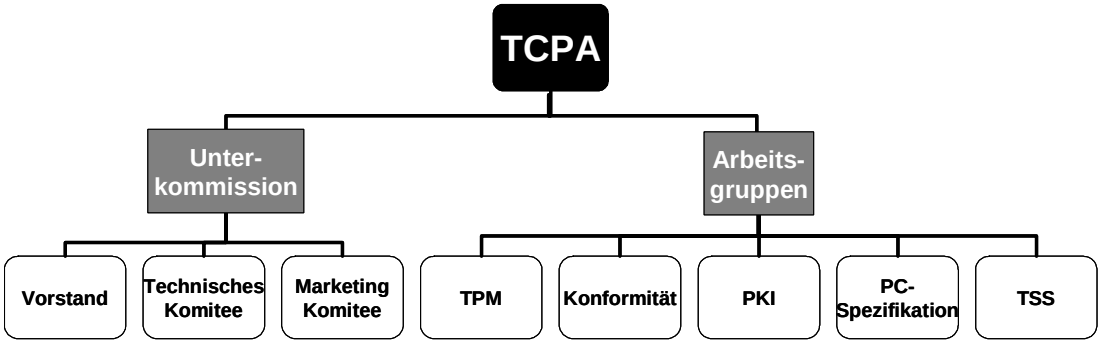

Abbildung 5: TCPA Organisationsstruktur[14]

Die Unterkommission der TCPA wurde durch Vorstand, Technisches- und Marketing-Komitee repräsentiert. Der Vorstand bestand aus den fünf Gründungsmitgliedern, welche die TCPA durch organisatorische Entwicklungen und Entscheidungsprozesse führte. Die technische Verantwortung für die Spezifikationen und die Ausrichtung der technischen Arbeitsgruppen hatte das technische Komitee, welches ebenfalls aus den fünf Gründungsmitgliedern bestand. Das Marketing-Komitee bestand aus allen Mitgliedern und entwickelte Marketing- und Promotion-Pläne. Dagegen war die TPM-Arbeitsgruppe für die Hauptspezifikationen zuständig, die im Hinblick auf Implementierung und Kompatibilität zu untersuchen und weiter zu entwickeln waren. Die gemeinsamen Kriterien der Schutzprofile, welche zur Zertifizierung der Stufe EAL3 von TCPA Produkten notwendig waren, wurden von der Arbeitsgruppe für Konformität definiert. Diese beinhaltet das TPM Protection Profile und das Connection Profile. Die PKI-Arbeitsgruppe konstruierte das Protokoll, um Identitätsbeglaubigungen zu erlangen sowie die Definitionen für das X.509 Zertifikat. Die spezifische PC-Arbeitsgruppe entwarf die Kompatibilitätsspezifikation bezüglich des TCPA Boot-Prozesses auf einer Intel kompatiblen PC Plattform.[15]

---

[14] Eigene Darstellung

[15] Vgl. Vgl. Pearson, S. et. al. (2002), S. 277 ff.

Die Meilensteine der TCPA im zeitlichen Kontext:

Datum	Meilensteine
Januar 99	Gründung der TCPA
Oktober 99	Erster Entwurf der Hauptspezifikationen
September 01	Hauptspezifikationen v1.0 und PC-Spezifikationen v1.0
August 01	Hauptspezifikationen v1.1
November 01	Errata Hauptspezifikationen v1.1a
Januar 02	Errata Hauptspezifikationen v1.1b
Juli 02	TPM Protection Profile v1.9.7
April 03	Bekanntgabe der TCG und Einstellung der TCPA

Tabelle 1: Meilensteine der TCPA[16]

2.3 Die Trusted Computing Group

Die „Trusted Computing Group“ wurde am 08. April 2003 als gemeinnütziges und wohltätiges Unternehmen gegründet und hat ihren Firmensitz in Oregon, USA. Ziel der TCG ist „development, definition and promotion of hardware-enabled trusted computing and security technology, including related hardware and related software components, across multiple platforms, peripherals and devices.”[17] Ergebnisse der TCG sind Hardware- und Software-Spezifikationen, Whitepapers, ein Logo-Programm sowie Schutzprofile, Marketing Programme und Verfechtung der ordentlichen Nutzung der Spezifikationen auf Plattformen sowie Anwendungen. Die TCG hat ein in der Satzung festgelegtes Organisations- und Steuerungs-Modell, welches den industriellen Standardisierungsgremien ähnlich ist:[18]

- Offene Mitgliedschaft auf verschiedenen Ebenen (Promoters, Contributors, Adopters).
- Der Vorstand besteht aus den Unternehmensgründern (Promoters) und gewählten Mitwirkenden (Contributors).
- Mehrere Arbeitsgruppen die für Promoter- und Contributer-Mitglieder offen sind sowie deren aktive Teilnahme.

---

[16] Eigene Darstellung

[17] TCG-Backgrounder (2003), S. 4

[18] Vgl. TCG-Backgrounder (2003), S. 4

- Faire Lizenzierung zwischen den Mitgliedern nach dem RAND-Prinzip (**R**easonable **A**nd **N**on-**D**iscriminatory), d.h. jedem Mitglied wird zu angemessenen und gleichen Bedingungen die Möglichkeit gegeben, das Patent zu nutzen.

- ¾-Mehrheitsstimmrecht auf Vorstands- und Arbeitsgruppen-Ebene, um den Ablauf zu erleichtern.

Die drei Typen der Mitgliedschaft unterscheiden sich nicht nur im jährlichen Mitgliedsbeitrag wie in *Tabelle 2*, sondern auch im Grad der Verantwortung sowie dem Vorzug auf gewisse Rechte. Bei einer aktuellen Anzahl von 48 Mitgliedern hätte die TCG ceteris paribus somit eine jährliche Einnahmequelle von $ 890.000,00.[19] Auf die verschieden Typen der Mitgliedschaft wird in Abschnitt 4.7.1 näher eingegangen.

Level	Jährlicher Beitrag	Anzahl der Mitglieder	Jährliche Einnahmen
Promoter	$50.000,00	7	$350.000,00
Contributer	$15.000,00	31	$465.000,00
Adaptor	$7.500,00	10	$75.000,00
Summe	**$72.500,00**	**48**	**$890.000,00**

Tabelle 2: Level und Beiträge der TCG-Mitgliedschaft[20]

Einen Überblick über die bereits verfassten Dokumente der TCG ist in *Abbildung 6* dargestellt. Davon sind allerdings nur die Hauptspezifikationen in den Versionen 1.1b und 1.2 in den Teilen eins bis drei, die TCG Software Stack in Version 1.1 und die PC-Spezifikationen in Version 1.1 öffentlich zugänglich. Die Hauptspezifikation in der Version 1.1b gibt zusätzlich noch einen Ausblick über die Architektur und entspricht im wesentlichen der TCPA Spezifikation Version 1.1b. Alle restlichen Dokumente sind nur für Mitglieder bestimmt. Die Abbildung zeigt darüber hinaus eine zukünftige Ausrichtung der TCG durch die hellblau hinterlegten Felder.

[19] Vgl. TCG-Current Members (2004)

[20] Eigene Darstellung

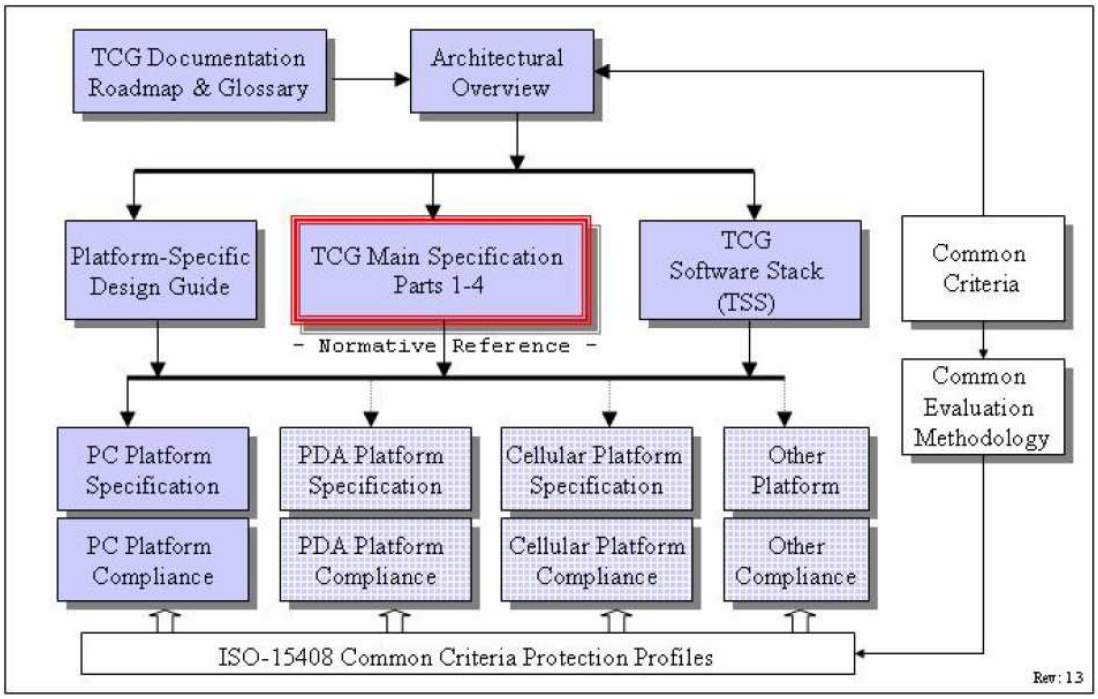

Abbildung 6: Überblick der bisher verfassten Dokumente[21]

Die kommenden Spezifikationen betreffen somit Plattformen für Mobiltelefone und Personal Digital Assistants (PDAs). Allerdings besteht auch noch die Option, für weitere Plattformen Spezifikationen zu veröffentlichen. Alle Spezifikationen sind dabei zu den Common Criteria ISO 15408 konform. Die Common Criteria entsprechen Richtlinien zur Bewertung und Prüfung der Sicherheit von Informationstechnik. Dadurch wird die Vertrauenswürdigkeit von IT-Produkten in die IT-Sicherheitsfunktionalität angezeigt und durch ein Zertifikat nachgewiesen. Über das Konzept der Schutzprofile, auch Protection Profiles genannt, wird ein Sicherheitsstandard gesucht, der die Bedürfnisse aus Sicht des Anwenders zur IT-Sicherheit berücksichtigt. Die Prüfung und Bewertung geschieht dabei unabhängig von bereits existierenden Produkten.[22]

[21] Vgl. TCG TPM Specification Version 1.2 (2003a), S. V

[22] Vgl. BSI (2003b)

3 Die Informations-Ökonomie

Technologie- und Informationsgüter nehmen eine zunehmend zentrale Rolle in der heutigen Gesellschaft ein.[23] Die steigende Bedeutung von Information und deren Digitalisierung, sowie die Konvergenz der drei Industrien Medien, Telekommunikation und Informationstechnologie, belegen den Übergang von der Industrie- zur Informationsgesellschaft. Diese wird im Wesentlichen durch das Zusammenspiel von Marktentwicklung und technologischer Innovation angetrieben, was in *Abbildung 7* dargestellt wird.

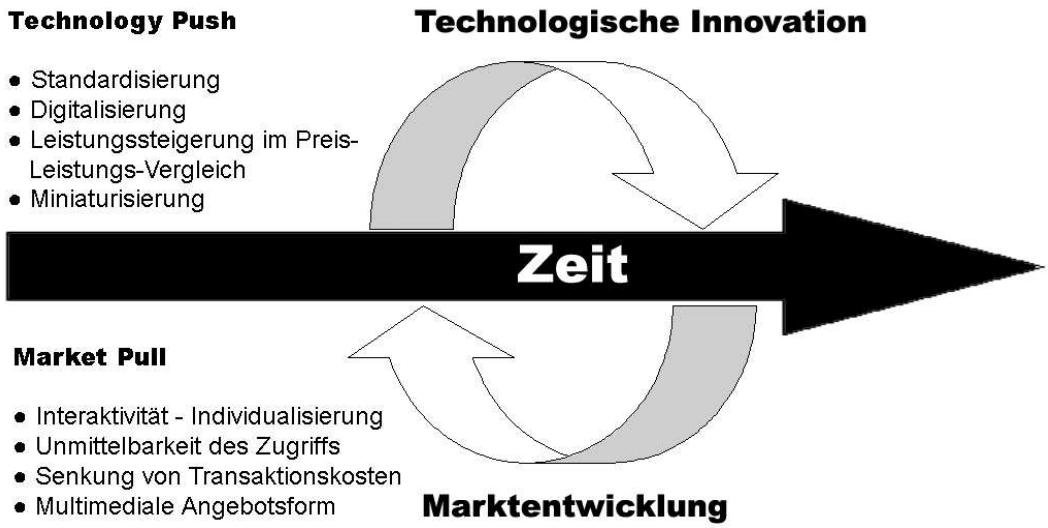

Abbildung 7: Technology Push und Market Pull im Zusammenspiel[24]

Als Erstes wäre an dieser Stelle der „Market Pull“ zu nennen, welcher durch vier Triebkräfte gekennzeichnet ist und dem Kunden einen hohen Zusatznutzen bietet:[25]

- Die Individualisierung von Inhalten durch Modularisierung seitens der Anbieter sowie die Interaktivität des Nutzers.
- Unmittelbarkeit des Zugriffs auf Informationen in Echtzeit, unabhängig von Zeit und Raum.
- Senkung von Transaktionskosten durch Such- und Filterfunktionen.

---

[23] Vgl. Eimeren, B.; Gerhard, H.; Frees, B. (2002), S. 354 f.

[24] Vgl. Zerdick, A. (2001), S. 156

[25] Vgl. Zerdick, A. (2001), S. 154 f.

- Multimediale Angebotsformen in Form von Audio, Video, Text, Bild und Grafik.

Im Kontext dieser Ausarbeitung ist der „Technology Push“ der weitaus relevantere Faktor, dessen Leistungssteigerungen der Kommunikations- und Informationstechnologien aus vier Merkmalen besteht:[26]

- Digitalisierung von Informationen in digitale Einheiten wie Bits und Bytes.
- Leistungssteigerungen bei simultanem Preisverfall der Techniken, wie z.B. Moore’s Gesetz.
- Miniaturisierung der Komponenten, wie z.B. die zunehmende Integrationsdichte von Mikroprozessoren.
- Standardisierung als Voraussetzung zur Verwirklichung der oben beschriebenen Potenziale.

In den folgenden Unterkapiteln werden grundlegende Erkenntnisse der Internet-Ökonomie dargestellt, welche zum grundlegenden Verständnis beitragen sollen.

3.1 Technologie

Die Informationsökonomie besteht im Wesentlichen aus den beiden Komponenten Information und der zugehörigen Technologie. Das Wort Technologie stammt aus dem Griechischen und bedeutet die Lehre von der Technik und deren Anwendung.[27] In Zusammenhang mit Information ist Technologie die Infrastruktur, um Informationen zu speichern, suchen, kopieren, filtern, manipulieren, sehen, übertragen und zu erhalten. Die Technologie bildet gewissermaßen die Umhüllung zur Lieferung der Informationen an den Endkonsumenten.[28]

---

[26] Vgl. Zerdick, A. (2001), S. 150 f.

[27] Vgl. Akademie.de (2004)

[28] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 8

3.1.1 Komplementäre, Kompatibilität und Standards

Computer sind ohne einen Monitor oder installierter Software nicht brauchbar, d.h. ein Gut muss mit anderen Gütern zusammen konsumiert werden, was in den Wirtschaftswissenschaften als komplementär bezeichnet wird. Insbesondere kaufen Konsumenten in komplementären Märkten Systeme, anstelle einzelner Komponenten. Diese Aussage trifft auch auf den Fall der TCG zu, wo neue Sicherheitskomponenten im Hardwaredesign einer Plattform spezifiziert werden, die Teile des Systems sind. Dabei spielen komplementäre Produkte eine große Rolle, welche eine Komponente eines Systems beschreiben. Um allerdings komplementäre Produkte zu produzieren, müssen diese kompatibel sein, d.h. sie müssen auf einem gleichen Standard agieren. Unternehmen sollten ihren Fokus also nicht nur auf den Wettbewerb im Markt richten, sondern auch auf komplementäre Anbieter und andere Mitarbeiter, um mit ihnen zu kooperieren. Dies birgt wiederum eine gewisse Koordinationsproblematik in sich, wie Unternehmen sich auf einen Standard einigen und den damit verbundenen monopolfeindlichen Streitfragen. Komplementäre Produkte sind somit ausschlaggebende Faktoren in Märkten für Informationsgüter.[29]

3.1.2 Infrastrukturelle und geschäftsrelevante Technologien

Für jede Unternehmung sind Technologien mit Bezug zu ihrem Kerngeschäft von großem Interesse, speziell wenn ein quantifizierbarer „Return on Investment“ dabei in Aussicht steht. Darüber hinaus lassen sich zwei Kategorien von Technologien differenzieren, nämlich infrastrukturelle und geschäftsrelevante Technologien.

Die Spezifizierung der TCG betrifft in erster Linie das Hardwaredesign von Plattformen, was für die Mehrzahl der Endnutzer eine infrastrukturelle Technologie darstellt. Infrastrukturelle Technologien sind meist gar nicht oder nur sehr wenig in Geschäftsprozesse integriert, weswegen Nutzer generell mehr in geschäftsrelevante Technologien investieren.[30]

Geschäftsrelevante Technologien sind hingegen abhängig von den wirtschaftlichen Interessen der Unternehmen, weshalb je nach Unternehmung einerseits ein System als geschäftsrelevant, anderseits allerdings auch als infrastrukturell angesehen wer-

---

[29] Vgl. Shy, O. (2001), S. 2 f.

[30] Vgl. Jakobs, K.; Procter, R.; Williams, R. (2001), S. 3 ff.

den kann. Beispielsweise sind E-Mails für Microsoft im Bezug auf das Produkt „Outlook“ geschäftsrelevant, wohingegen E-Mails für Banken von infrastruktureller Natur sind.[31]

3.2 Information

Im Zusammenhang der Ausarbeitung wird der Begriff Information weit gefasst, und zwar als *"... anything that can be digitized - a book, a movie, a record, a telephone conversation"*[32]. Dabei sind die aufgezählten Objekte Beispiele für Informationsprodukte und werden im weiteren Verlauf Informationsgüter genannt. Insbesondere sei auf den dualen Charakter von Medienprodukten hingewiesen, welcher aus Information und Medium besteht. Information selbst ist ein immaterielles Gut, weshalb zur Verbreitung, Verarbeitung oder Speicherung ein physisches Medium benötigt wird.[33]

Informationsgüter besitzen drei wesentliche Eigenschaften, die sie von physischen Gütern unterscheiden, weswegen Transaktionen auf Märkten für Informationsgüter massiv beeinflusst werden:[34]

- Informationsgüter als Erfahrungsgüter.
- Informationsgüter als öffentliche Güter.
- Anbieterseitige und nachfragerseitige Größenvorteile (s. Kapitel 3.6 und 3.7).

3.2.1 Informationsgüter als Erfahrungsgüter

Informationsgüter offenbaren ihren Wert erst mit ihrer Nutzung, weshalb ex-ante Unsicherheit bei der Informationsnutzung vorliegt. Ferner basiert eine Einschätzung der Bewertung von Informationsgütern auf subjektiven Erwartungen, was den Handel mit Informationen erschwert. Folge des Erfahrungsgutcharakters ist das Informationsparadoxon von Arrow, welches als notwendige Eigenschaft die Unsicherheit von Informationsgütern zu Grunde legt. Zusätzliche Bedingung des Informationsparadoxon ist die Nicht-Rivalität im Konsum, d.h. es besteht die Möglichkeit Informationen zu behalten und gleichzeitig weiterzugeben. Als weitere Voraussetzung darf

---

[31] Vgl. Jakobs, K.; Procter, R.; Williams, R. (2001), S. 3 ff.

[32] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 3

[33] Vgl. Stähler, P. (2002), S. 191

[34] Vgl. Varian, H. R. (1998), S. 3

nach einmaliger Musterung der Information ein erneuter Konsum keinerlei Nutzen stiften. Die Gültigkeit des Paradoxons hängt also von der wiederholten Nutzung der Information ab.[35] Abhilfe schaffen Vorschauen auf Teile des Guts, wie z.B. Demoversionen von Programmen mit eingeschränkter Nutzung. Eine weitere Kompensation wird durch Rezensionen, Besprechungen und Kritiken durch Experten geschaffen. Das Vertrauen in die Reputation des Produzenten in Form von Markenbildung ist eine weitere Möglichkeit. Marken stellen dabei Metainformationen dar, die das Risiko des Abnehmers beim Wiederholungskauf reduzieren.[36]

3.2.2 Informationsgüter als öffentliche Güter

Hinsichtlich der Rechte der Veränderung, Übertragung und Nutzung von Information besteht keine Rivalität, da dieselbe Information an Dritte weitergegeben werden kann und gleichzeitig beliebig viele Menschen die Information besitzen oder verarbeiten können. Allerdings herrscht eine Rivalität bezüglich des Rechtes entstehende Gewinne durch die Vermarktung von Information zu vereinnahmen.[37] Dadurch entsteht die Problematik der Produktpiraterie, welche durch zwei Möglichkeiten gelöst werden kann:[38]

- Materielle Verhinderung der Informationsweitergabe durch Koppelung der Information an physische Trägermedien oder
- Juristische Durchsetzung der Eigentumsansprüche mit entsprechenden Rechtsmitteln, welche z.B. das Urheberrecht oder Patente sanktionieren.

3.3 Erlösmodelle

Die Entscheidung über Erlösmodelle und deren Preispolitik bestimmen, wie und in welcher Höhe Erlöse zur Finanzierung der Unternehmung erzielt werden. Dabei geht dem Entscheidungsbereich der Preispolitik die Entscheidung über die Anwendung von Erlösmodellen logisch voraus, was als zweistufiger Entscheidungsprozess bezeichnet wird. Die Wahl des Erlösmodells wird in preispolitischen Beiträgen meist

---

[35] Vgl. Hass, B.H. (2002), S. 54 f.

[36] Vgl. Varian, H. R. (1998), S. 4 f.

[37] Vgl. Varian, H. R. (1998), S. 6 ff.

[38] Vgl. Hass, B.W. (2002), S. 40 ff.

als gelöst betrachtet, weswegen in diesem Kapitel erst die verschiedenen Erlösmodelle vorgestellt werden.[39] Im Anschluss daran wird eine Zusammenstellung über die Preisdifferenzierung dargestellt. Erlösmodelle lassen sich in zwei Dimensionen unterteilen: Zum einen werden die Absatzobjekte vorgestellt, welche Erlöse generieren, nämlich die sog. Erlösquellen. Zum anderen wird analysiert, welche Eigenschaften die Erlösquellen aufzeigen, wonach anschließend die Erlösformen gegliedert werden.[40]

3.3.1 Erlösquellen

Die unterschiedlichen Erlösquellen im Internet sind in *Abbildung 8* aufgezeigt und lassen sich in Produkte, Kontakte und Informationen einteilen.

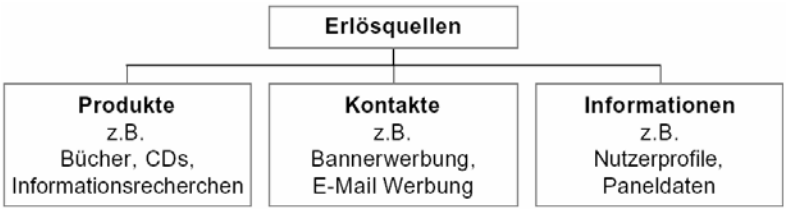

Abbildung 8: Erlösquellen im Internet[41]

Bei Erlösen aus dem Absatz von Produkten wird das eigentliche Produkt verkauft, wobei die Ware selbst ein materielles oder immaterielles Gut sein kann. Die Erlösquelle Kontakte kann neben der Erlösquelle Produkte stehen oder diese ersetzen. Hier wird der Kontakt zu den Kunden des eigenen Produktes verkauft, um beispielsweise Erlöse durch Werbung oder Sponsoring zu generieren. Dabei können Interdependenzen zwischen den Erlösquellen auftreten. Die Erlösquelle Information aggregiert Informationen über Konsumenten und verkauft diese dann an Dritte. In vielen Fällen werden die drei genannten Erlösquellen kombiniert genutzt. Ebenso kann diese Zusammensetzung der Erlösquellen parallel stattfinden oder zeitlich gestaffelt sein. Dies fällt unter den Begriff „Windowing“.[42]

---

[39] Vgl. Zerdick, A. (2001), S. 24 f.

[40] Vgl. Hass, B. H. (2002), S. 120 ff.

[41] Vgl. Skiera, B.; Lambrecht, A. (2000), S. 817

[42] Vgl. Skiera, B.; Lambrecht, A. (2000), S. 815 ff.

3.3.2 Erlösformen

Die Erlössystematik der Internet-Ökonomie ist in *Tabelle 3* mit entsprechenden Beispielen dargestellt. Direkte Erlöse werden auch direkt vom Kunden bezogen, wohingegen indirekte Erlöse von Dritten erhalten werden. Transaktionsabhängige Erlöse stammen von einer Interaktion zwischen Kunde und Unternehmung oder eine einzelne, vermarktungsfähige Transaktion im weitesten Sinne.

Erlössystematik		
	Direkte Erlösgenerierung	Indirekte Erlösgenerierung
Transaktionsabhängig	● Transaktionserlöse i.e.S. ● Verbindungsgebühren ● Nutzungsgebühren	● Provisionen
Transaktionsunabhängig	● Einrichtungsgebühren ● Grundgebühren	● Bannerwerbung ● Data-Mining-Erlöse ● Sponsorship

Tabelle 3: Erlössystematik[43]

Direkte transaktionsabhängige Erlösformen bestehen aus Transaktionserlösen im engeren Sinne, Verbindungsgebühren und Nutzungsgebühren. Bei Transaktionserlösen im engeren Sinne erfolgt eine Zahlung aufgrund quantitativer Kriterien durch den Kunden an das Unternehmen, der im Gegenzug ein Produkt oder eine Dienstleistung erhält. Verbindungs- und Nutzungsgebühren entstehen für die Nutzung, bzw. den Zugang einer Dienstleistung. Indirekte transaktionsabhängige Erlöse entstehen durch Provisionen, d.h. über die Vermittlung von Transaktionen an Dritte, wie z.B. bei „Affiliate"-Programmen. Direkte transaktionsunabhängige Erlösformen treten bei Einrichtungs- und Grundgebühren auf, welche die ständige Nutzung für Produkte und Dienstleistungen bereitstellen. Indirekte transaktionsunabhängige Erlösformen kommen in Form von Bannerwerbung, Data-Mining und Sponsorship vor. Bei Bannerwerbung wird Werbefläche der eigenen Webseite an Dritte zur Verfügung gestellt. Data-Mining-Erlöse werden durch die Aggregation von Kundeninformationen an Dritte generiert. Erlöse per Sponsorship werden über zeitlich begrenzte, exklusive Vermietung von Werberaum an Dritte geschaffen. Staatliche Erlöse sind für Unternehmungen bisher vernachlässigbar.[44] Selbstverständlich können die Erlösformen im Internet beliebig kombiniert werden, wobei zwei Zieldimensionen bei der Entscheidung über den geeigneten Erlösmix zu berücksichtigen sind. Zum einen sind dies die

---

[43] Vgl. Wirtz, B. W. (2001), S. 410

[44] Vgl. Wirtz, B. W. (2001), S. 410

anfallende Kostenstruktur bei der Anordnung der Erlösformen aus Unternehmenssicht und zum anderen das Nutzungsverhalten und die Nutzenwahrnehmung beim Konsumenten.[45]

3.4 Differenzierung von Produkten und Preisen

Preis- und Produktdifferenzierung spielen aufgrund der hohen Fixkosten und den marginalen variablen Kosten in der High-Tech-Industrie eine große Rolle. In Anlehnung an den Ökonomen A. C. Pigou existieren drei Typen von Preisdifferenzierung:[46]

- **Preisdiskriminierung ersten Grades**: Verkauf an jeden Nutzer zu einem differenzierten Preis.
- **Preisdiskriminierung zweiten Grades**: Anbieten einer Produktlinie aus der sich die Nutzer die Version heraussuchen können, welche ihnen am besten entspricht.
- **Preisdiskriminierung dritten Grades**: Differenzierte Preise für unterschiedliche Gruppen an Konsumenten.

3.4.1 Preisdiskriminierung ersten Grades

In diesem Extremfall werden dem Konsument hochgradig personalisierte Produkte zu hoch personalisierten Preisen verkauft. Das Phänomen ist bekannt als „Mass Customization“ und „Personalisierung“. Eine kundenspezifische Anpassung ist für Informationsgüter sowie physische Güter möglich. Darüber hinaus lässt der Konsument sich nach Ort, Demographie oder seinem letzten Kaufverhalten unterscheiden, was eine relativ günstige und signifikante Marktforschung per Internet ermöglicht. Im Monopolfall stellen die Unternehmen jedem Konsument den für ihn am höchsten zu zahlenden Preis in Rechnung und schöpfen somit die vollständige Konsumentenrente ab. Bei vollkommener Konkurrenz und unter Annahme der Informationstransparenz gestattet die Personalisierung der Preise für Unternehmen eine Annäherung an den Reservationspreis für jeden Konsumenten. Zusätzlich wird jeder Konsument selbst zu einem Marktplatz, welcher ausgefochten werden muss. Allerdings häufen

---

[45] Vgl. Zerdick, A. (2001), S. 29

[46] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 39 ff.

sich mit der Personalisierung ebenfalls die datenschutzrechtlichen Probleme. Vertrauen ist hier das Problem, denn der Kunde will kontrollieren, wie und welche Informationen über ihn genutzt werden. Die Unternehmen können zwar die Bedürfnisse der Konsumenten besser befriedigen, allerdings werden verbesserte Leistungen auch in Rechnung gestellt. Vorgegebene Verträge steuern diese Märkte in Abhängigkeit von Transaktionskosten, die mit verschiedenen Vereinbarungen verbunden sind. Beispielsweise können bilaterale Verträge mit personellen Informationen zur Steigerung der Effizienz genutzt werden, wenn die Transaktionskosten niedrig sind. Daneben ist Werbung ein weiteres Thema im Zusammenhang mit Personalisierung, da viele Services starke Einnahmen daraus schöpfen.[47]

3.4.2 Preisdiskriminierung zweiten Grades

Bei der Preisdiskriminierung zweiten Grades wird eine Produktlinie angeboten, aus der sich der Konsument die Version heraussuchen kann, welche ihm am besten entspricht. Jedem Interessenten wird das gleiche Preismenü für eine Produktreihe vorgestellt, was als „Produktlinien Preissetzung“, „Marktsegmentierung“ oder „Versioning“ bezeichnet wird. Die Informations-Technologie unterstützt neben der Erhebung von Informationen über den Konsumenten, auch die Gestaltung von Produktlinien, um verschiedene Versionen des Produktes selbst zu produzieren.[48] Der Konsument wählt aus den angebotenen Versionen die mit dem für ihn am höchsten Nutzen aus, was als Selbstselektion bezeichnet wird. Um die Selbstselektion zu begünstigen, können folgende Produktdimensionen behilflich sein: Verzögerung, Benutzeroberfläche, Komfort, Bildauflösung, Schnelligkeit der Operation, Leistungsfähigkeit, Funktionen, Umfang, Beeinträchtigungen oder Support.[49] Diese Produktdimensionen dienen der Produktgestaltung und sollten zusätzlich mit Markt- und Produktanalysen unterstützt werden. Nach Vollendung des Hochpreisproduktes wird die Qualität über die angesprochenen Produktdimensionen herabsetzt, um weitere Versionen zu schaffen. Die Anzahl der Versionen ergibt sich aus der Produkt- und Marktanalyse oder nach der Faustregel „Standard“, „Professionell“ und „Gold“, wobei der wirtschaftliche Fokus des Produktes auf der professionellen Version liegt. Die Faustregel basiert

---

[47] Vgl. Varian, H. R. (2003), S. 13 ff.

[48] Vgl. Varian, H. R. (2003), S. 16 f.

[49] Vgl. Varian, H. R. (1997), S. 2 und Shapiro, C.; Varian, H. R. (1998), S. 60

auf dem psychologischen Phänomen der „übertriebenen Aversion“, weshalb der Konsument aus den angebotenen Alternativen vermehrt die mittlere Stufe wählt. Problematisch ist jedoch die Kannibalisierung der eigenen Produkte bei der Gestaltung von Produktlinien. Dabei werden insbesondere Konsumenten mit hoher Zahlungsbereitschaft von Niedrigpreisprodukten angezogen. Abhilfe schaffen Preisreduzierungen des Hochpreisproduktes oder Qualitätsminderungen des Niedrigpreisproduktes.[50]

3.4.3 Preisdiskriminierung dritten Grades

Preisdiskriminierung dritten Grades bedeutet Verkauf zu verschiedenen Preisen an verschiedene Gruppen. Unter Wettbewerbsbedingungen besteht für Unternehmen der Anreiz den Konsumentennutzen zu maximieren. Generell schneiden Konsumenten hier besser ab, aufgrund der fixen Kosten der Serviceabwicklung und den beim Konsumenten zu beobachteten Menge an Charakteristiken. Die Preisdiskriminierung gibt den Unternehmen zusätzliche Flexibilität im Umgang mit den Fixkosten. Existieren keine Fixkosten fällt der Konsumentennutzen, obwohl der gesamtwirtschaftliche Ertrag steigt. Bei heterogenen Konsumenten fällt die Konsumentenrente grundsätzlich und die Gewinne steigen im Wettbewerb, die Wohlfahrt hingegen fällt unter Umständen leicht.[51]

3.5 Lock-in und Wechselkosten

Wechselkosten und Lock-in Effekte sind einzigartig im Zusammenhang mit Informations-Systemen. Dabei werden die mit dem Wechsel von einem Produkt zu einem anderen Produkt verbundenen Kosten als Wechselkosten bezeichnet. Daneben führen z.B. dauerhafte Investitionen in komplementäre Anlagegüter einer bestimmten Marke zu hohen Wechselkosten, wenn neue inkompatible Systeme aufgrund von Produktlebenszyklen am Markt entstehen. Ein einfacher Systemwechsel ist damit abhängig von den Wechselkosten, d.h. sind die Wechselkosten der Technologie einer Marke zu einer anderen substantiell, ist der Nutzer eingeschlossen, was als Lock-in Effekt bezeichnet wird. Lock-in Effekte treten dabei beim Konsument, Anbieter und

---

[50] Vgl. Varian, H. R. (2003), S. 17

[51] Vgl. Varian, H. R. (2003), S. 17 f.

Zulieferer auf. Die totalen Wechselkosten ergeben sich aus der Addition aus Konsumenten- und Anbieterkosten:[52]

Totale Wechselkosten = Kosten des Konsumenten + Kosten des Anbieters

Die Kosten des Anbieters sind deswegen für eine Analyse relevant, um die Akquisitionskosten eines Kunden zu berechnen. Entsprechen die Qualität und die Kosten denen der Konkurrenz, dann stimmt der Kundenkapitalwert exakt mit den totalen Wechselkosten überein:[53]

Gewinne vom aktuellen Kunden = Totale Wechselkosten + Qualitäts- / Kostenvorteil

Somit lässt sich der Wert einer installierten Basis an Kunden antizipieren und wie viel Kapital investiert werden müsste, um diese aufzubauen. Wechselkosten beeinflussen auch den Preiswettbewerb in zwei entgegengesetzte Richtungen. Zum einen führen Preissteigerungen nur dann zu einem Wechsel eines gebundenen Konsumenten, wenn die Preisdifferenz die Wechselkosten der Konkurrenz überschreiten. Andererseits steigert es auch den Wettbewerb im Markt, um ungebundene Konsumenten für eine Technologie zu gewinnen.[54]

3.5.1 Klassifizierung von Lock-in Effekten

Es existieren verschiedene Typen von Wechselkosten, die den Grad der Lock-in Effekte beeinflussen. Eine Klassifizierung der verschiedenen Lock-in Effekte erfolgt in *Tabelle 4*.

---

[52] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 112

[53] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 114

[54] Vgl. Shy, O. (2001), S. 5

Typen von Lock-in	Wechselkosten
Vertragliche Bindung	Schadensersatz oder vereinbarte Vertragsstrafen
Permanenter Erwerb	Austausch des Equipments; neigt mit den Jahren zu sinken
Markenspezifisches Training	Erlernen eines neuen Systems betrifft direkte Kosten und verlorene Produktivität
Information und Datenbanken	Konvertierung von Daten in ein neues Format
Spezialisierte Lieferanten	Aufbringung von neuen Lieferanten
Suchkosten	Kombinierte Käufer- und Verkäuferkosten
Treueprogramme	Jeden verlorenen Gewinn von bestehenden Anbietern, inklusive möglichen Bedarf den gesamten Nutzen wiederaufzubauen

Tabelle 4: Typen von Lock-in und den zugehörigen Wechselkosten[55]

Vertragliche Bindungen können je nach Vertrag zu Schadensersatzforderungen oder Vertragsstrafen führen. Eine Form ist die vertragliche Bindung an Bedürfnisse, d.h. der Käufer bezieht seinen kompletten Bedarf exklusiv von einem bestimmten Abnehmer über einen gewissen Zeitraum. Darüber hinaus gibt es auch vertragliche Bindungen bezüglich der Abnahmemenge. Dies bedeutet der Käufer verpflichtet sich zu einer Mindestbestellmenge mit der Option den Zulieferer zu Wechseln, wenn der Lieferant die Bedürfnisse nicht ausreichend befriedigt. Die Konditionen, die Qualität der Leistungserfüllung, die Dauer sowie die automatische Verlängerung solcher Verträge spielen zudem eine große Rolle. Sind die Vertragsstrafen oder Schadensersatzforderungen hoch genug, existiert ein Lock-in-Effekt.[56]

Beim *permanenten Erwerb* wird ein Initialkauf getätigt und der Konsument muss danach weitere Komplementärgüter kaufen, die mit dem Produkt arbeiten. Gewinne werden hier meist über den Sekundärmarkt generiert, wobei durch schnelle technologische Vorteile ein schneller Verfall des ökonomischen Wertes der Komplementärgüter zu geringen Lock-in Effekten führt. Ebenso führt der Handel mit gebrauchten Komplementärgütern, sowie Miete oder Leasing zu einer Senkung des Lock-in Effektes. Dabei sind zwei Typen, nämlich der Technologie- und Lieferanten-Lock-in, zu erkennen. Lieferanten genießen überdies noch beim Verkauf der Komplemen-

[55] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 117

[56] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 116 ff.

tärgüter den Besitz von Patenten oder Urheberschutz. Das typische Beispiel für diesen Fall ist Hardware.[57]

Markenspezifisches Training steht eng in Verbindung mit dem permanenten Erwerb von Produkten und ist charakteristisch für Computer-Software. Der Konsument wird darauf trainiert ein Produkt zu nutzen, welches auf einem speziellen Standard betrieben wird. Die Wechselkosten steigen mit der Zeit und beinhalten das Erlernen und Trainieren der Konsumenten sowie die verlorene Produktivität, welche aus der Adoption des neuen Systems resultiert.[58]

Informationen und Datenbanken stellen ebenfalls eine Klasse für sich dar, da Hard- und Software dazu genutzt werden, Informationen und Datenbanken zu speichern bzw. zu managen. Jede Software generiert Dateien, die ein spezielles digitales Format benutzen. Die Einführung einer neuen Software führt zusätzlich zu Konvertierungen, um alten Datensätze nicht zu verlieren. Eine Ansammlung der Daten kann im Laufe der Zeit genauso steigen, wie die Wechselkosten. Rohdaten sind für eine Umwandlung von einem ins andere Format einfacher zu portieren, allerdings nutzen Lieferanten den Unterschied zwischen proprietären und standardisierten Formaten aus, um die Wechselkosten der Konsumenten zu steuern.[59]

Spezialisierte Lieferanten können Konsumenten auch stark abhängig machen, sobald ein einziger Anbieter im Laufe der Zeit die Ausrüstung stellt. Die Wechselkosten sind somit abhängig von alternativen Anbietern, welche vergleichbare Ausrüstungen verkaufen. Je höher allerdings der Spezialisierungsgrad ist, desto schwieriger ist es Anbieter in Zukunft zu finden. Die Auswahl der Bedingungen und Optionen können das Abhängigkeitsverhältnis mindern, sowie die duale Beschaffung, indem eine alternative Lieferantenquelle am Leben erhalten wird.[60]

Suchkosten sind speziell für Massenmärkte von Bedeutung. Diese fallen an, wenn Käufer und Verkäufer sich gegenseitig versuchen zu finden, um eine Geschäftsbeziehung aufzubauen. Zudem werden die Suchkosten zweiseitig getragen und zwar

---

[57] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 118 ff.

[58] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 121 f.

[59] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 122 f.

[60] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 123 ff.

von den Konsumenten sowie den möglichen Anbietern. Die Suchkosten des Konsumenten entstehen durch den Wechsel der Marke, psychologische Kosten des Wechsels tief eingewurzelter Angewohnheiten, die Zeit und den Aufwand neue Anbieter zu finden und das Risiko einen unbekannten Anbieter auszuwählen. Dagegen entstehen Suchkosten möglicher Anbieter, durch das Erreichen und Akquirieren neuer Kunden inklusive Werbungskosten. Darüber hinaus entstehen dem Anbieter weitere Suchkosten in Form von: Kosten ein Geschäft abzuschließen, Kosten einen neuen Kunden einzurichten, Risiko mit unbekannten Kunden zu handeln und das Kreditrisiko. Zwar sind durch die Informations-Ökonomie verschiedene Suchkosten reduziert worden, allerdings wird immer ein gewisser Grad an Beharrungsvermögen und Loyalität des Konsumenten gegenüber bestehenden Anbietern bestehen bleiben.[61]

Treueprogramme gelten als künstlicher Lock-in, da diese ein Konstrukt von Firmenstrategien sind. Kunden werden für wiederholte Käufe belohnt, wobei explizit Anreize geschaffen werden, um überwiegend bei einem Anbieter zu kaufen. Konsumenten büßen hier bestimmte Kredite ein, wenn sie nicht regelmäßig bei einem Anbieter kaufen. Ferner entstehen Vorteile basierend auf dem Gesamtverbrauch, welche Teil der totalen Wechselkosten werden, die entweder der Konsument verliert oder der neue Anbieter bei einem Wechsel trägt. Begünstigungen für den Kunden werden somit hinsichtlich ihrer historischen Käufe genutzt, um Wechselkosten zu erzeugen. Eine Auszahlung an den Kunden oder gewisse Begünstigungen können auch an bestimmte Meilensteine des Gesamtverbrauchs gekoppelt werden.[62]

3.5.2 Der Lock-in Zyklus

Der Lock-in ist ein dynamisches Konzept, welcher sich in einem Zyklus aus Brand Selection, Sampling, Entrenchment und Lock-in wie in *Abbildung 9* darstellen lässt.

---

[61] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 126 f.

[62] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 127 ff.

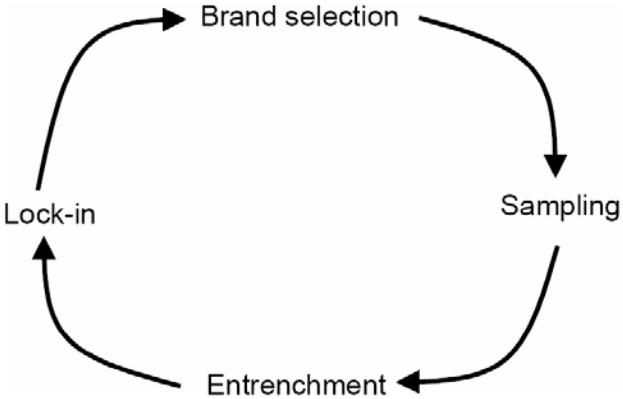

Abbildung 9: Der Lock-in Zyklus[63]

In einem ersten Schritt wählt der Konsument die Marke aus. Dies wird in der Abbildung als „*Brand selection*“ bezeichnet. Bei der ersten Wahl hat der Konsument keine Präferenz für eine Marke, d.h. der Konsument ist in keinen Lock-in „geboren“, sondern er wird erst durch die getroffene Auswahl eingeschlossen. In der „*Sampling*“-Phase probiert der Konsument die neue Marke und deren Vorteile. Aufgrund der marginalen Kosten von Information werden kostenlose Proben des Herstellers, wie z.B. bei Demoversionen von Software, verteilt, um neue Konsumenten zu akquirieren. Allerdings kann der Konsument die kostenlose Probe niemals in eine lohnende Einnahme umwandeln, da der Anbieter langfristig durch seine Marktmacht die Konsumentenrente abschöpfen kann. Die „*Entrenchment*“-Phase erreicht der Konsument, wenn er die neue Marke benutzt und Präferenzen gegenüber anderen Marken entwickelt. Investiert der Konsument dabei schon in Komplementärgüter, tritt der Lock-in hier schon ein. Normalerweise versucht der Anbieter diese Phase zu überstehen, indem er aktive Überlegungen über andere Marken verzögert, damit die Wechselkosten des Konsumenten steigen. Dies endet in der *„Lock-in“*-Phase, in der die Wechselkosten unerschwinglich teuer sind. Bei Wiedereintritt in die Phase der Auswahl der Marke sind die Wechselkosten schon höher als in der ersten Runde. Der Konsument wechselt die Marke oder wägt die bestehende gegen Alternativen ab, ohne diese auszuwählen. Steigen die Wechselkosten mit der Zeit, ist es aufgrund des Zyklus sinnvoll den Wert der installierten Basis zu betrachten, um den zukünftigen Kundenwert abzuschätzen und nachfolgend die Investments zu entscheiden.[64]

---

[63] Vgl. Shapiro, C.; Varian, H.R. (1998), S. 132

[64] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 131 ff.

3.6 Angebotsseitige Größenvorteile

Angebotsseitige Größenvorteile lassen sich durch *Skalen-* und *Verbundvorteile* auf Anbieterseite realisieren. Dabei treten die beide Größenvorteile in den Märkten der Informationsökonomie zusammen auf.

3.6.1 Skaleneffekte

Skaleneffekte resultieren bei zunehmender Ausbringungsmenge durch das Sinken der daraus resultierenden Stückkosten, was auch als Fixkostendegression bezeichnet wird.[65] Die einmalig anfallenden Fixkosten werden selbst als „First-Copy-Costs" oder „Sunk-Costs" bezeichnet und fallen meist vor dem Produktionsprozess an. Bei der Reproduktion und dem Vertrieb von digitalisierten Informationsgütern betragen die Grenzkosten nahezu Null. Information ist also kostspielig in der Produktion, aber günstig in der Reproduktion, d.h. die Produktion von Informationsgütern birgt hohe Fixkosten bei äußerst marginalen variablen Kosten. Zentrales Ziel in Märkten mit sog. „economies of scale" ist das Erreichen einer hohen Produktionsmenge. Dabei ist eine günstige Startposition auf der Erfahrungskurve durch Übernahmen bekannter Technologien sowie niedrige Preise zu Beginn vorteilhaft. Zudem fördern hohe Investitionen in den Bekanntheitsgrad und Referenzkunden das Erreichen einer hohen

Produktionsmenge. Trotzdem sollte eine hohe Verfügbarkeit gesichert werden. Allgemein liegen die Gründe für angebotsseitige Skaleneffekte in der effizienten Produktion aufgrund größerer Anlagen, im Einsatz verbesserter Fertigungsverfahren sowie besserer Einkaufskonditionen und der Fixkostendegression. Des Weiteren lassen sich Erfahrungskurveneffekte bezüglich der kumulierten Produktionsmenge über mehrere Perioden realisieren.[66]

3.6.2 Verbunderträge

Verbundvorteile entstehen durch die gemeinsame Herstellung verschiedener Produkte im Verbund, welche kostengünstiger sind, als die Herstellung jedes einzelnen Produktes. Genauer gesagt, fallen bei den sog. „economies of scope" die Gesamtkosten der Herstellung eines Produktprogramms niedriger aus, als die Summe der Herstellungskosten der einzelnen Produkte bei getrennter Herstellung. Im ökonomischen

---

[65] Vgl. Nieschlag, R.; Dichtl, E.; Hörschgen, H. (1997), S. 136

[66] Vgl. Varian, H. R. (2003), S. 24 ff.

Sinn werden also Inputfaktoren von mehreren Produkten gemeinsam genutzt.[67] Zudem sollen Kostensynergieeffekte bei einer breiten Produktpalette genutzt werden. Auch durch gegenseitigen Kompetenztransfer können Verbundeffekte verwirklicht werden. Diese sind besonders bei Informationen im Rahmen von „Content Syndication" von Bedeutung, wo eine Mehrfachverwertung von Inhalten durch den Vertrieb an Dritte stattfindet.[68]

3.7 Nachfragerseitige Größenvorteile

Nachfragerseitige Größenvorteile werden als Netzeffekte oder Netzwerkexternalitäten bezeichnet und treten vor allem bei Gütern mit derivatem Nutzen für den Konsumenten auf.[69] Netzwerke in Verbindung mit Informationssystemen können als „virtuell" charakterisiert werden, deren Verbindungen zwischen den Knoten nicht sichtbar sind. Dagegen sind die Verbindungen von „realen" Netzwerken zwischen den Knoten physikalische Verknüpfungen. Externalitäten entstehen, wenn ein Marktteilnehmer andere beeinflusst, ohne dass eine Ausgleichszahlung erfolgt.[70] Netzwerk-Externalitäten sind in der Regel positiv, d.h. ein Netzwerk wird größer und wertvoller, wenn ein neuer Teilnehmer hinzukommt. Abgeleitet davon ist der Wert eines Netzwerkes abhängig von der Anzahl an Teilnehmern n, die bereits miteinander verbunden sind. Diese Feststellung lässt sich über Metcalfe's Gesetz folglich darstellen:[71]

$$(1) \qquad n(n-1) = n^2 - n$$

Der Wert eines Netzwerkes steigt quadratisch mit der Anzahl ihrer Nutzer.[72] Direkte Netzwerk-Externalitäten beziehen sich somit auf die Anzahl der Teilnehmer, wohingegen indirekte Netzwerk-Externalitäten sich auf das Angebot an Komplementärgüter bezieht.[73] Positive Netzwerk-Externalitäten führen zu „positivem Feedback".

---

[67] Vgl. Panzar, J.C.; Willig, R.D. (1981), S. 71

[68] Vgl. Hass, B.H. (2002), S. 47 f.

[69] Vgl. Shapiro, C.; Katz, M. (1985) S. 424

[70] Vgl. Varian, H. R. (2003), S. 31. ff.

[71] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 183 f.

[72] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 183 f.

[73] Vgl. Katz, M.; Shapiro, C. (1985), S. 424 f.

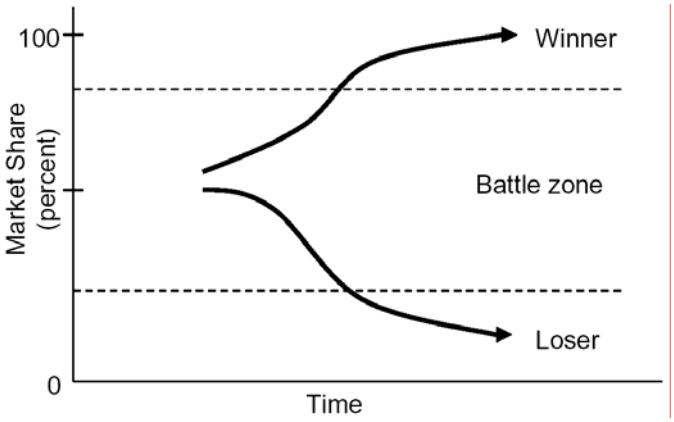

Abbildung 10: Ergebnis von positivem Feedback[74]

Positives Feedback führt zu extremen Marktergebnissen wie in der obigen Abbildung ersichtlich. Der Starke wird immer stärker während der Schwache beständig schwächer wird. Im Extremfall führen positive Feedbacks zu einer Marktdominanz, indem sich ein einziges Unternehmen oder eine Technologie durchsetzt.[75]

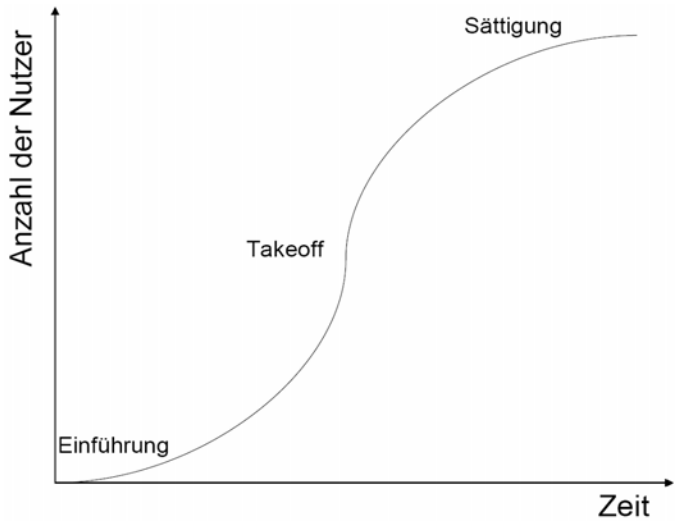

Abbildung 11: Adoptionsdynamiken[76]

Die Adoption einer neuen Technologie, wie in *Abbildung 11* erkennbar, folgt dem Verlauf einer S-Kurve in drei Phasen: [77]

1.) Flach während der Einführung,

---

[74] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 177

[75] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 175 ff.

[76] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 178

[77] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 178 f.

2.) steiler Anstieg während des Takeoffs, wenn positives Feedback zum tragen kommt, gefolgt von

3.) einer Niveauanpassung im zeitlichen Kontext, sofern die Sättigung erreicht ist.

Ist die kritische Masse einmal erreicht und das Produkt erlangt die Takeoff-Phase, hat der Verkäufer eine installierte Basis von Konsumenten hervorgerufen. Dies entspricht der Anzahl an Konsumenten, welche in die Technologie des Verkäufers eingeschlossen sind.[78]

4 Standardisierung

4.1 Definition

Standards spielen eine wesentliche Rolle bei der Konvergenz von Medien-, Informations- und Kommunikationstechnologie sowie bei Unternehmen, die Standards als Unternehmensstrategie einsetzen. In diesen Märkten bildet sich aufgrund des Kompatibilitätsdrucks der Hersteller, Distributoren und Erfahrungen der Konsumenten eine oder eine kleine Anzahl an Technologien als Standard heraus. Standards sind zwangsläufig Nebenerscheinungen von Systemen, bei denen komplementäre Produkte zusammenarbeiten, um die Bedürfnisse der Nutzer zu befriedigen.[79] Im weitesten Sinn kann ein Standard als eine Richtlinie oder Konvention verstanden werden, mit dem Ziel, bestimmte Mindesteigenschaften sicherzustellen.[80]

Bestehende Standards werden von Business Webs verwendet, um diese in neue Netzwerke einzubetten und zu revolutionieren, was „Interfection“ genannt wird.[81] Die Standardisierung selbst soll den Lernaufwand straffen, Planungssicherheit für weitere Investitionen geben sowie für alle Teilnehmer die Kompatibilität von Teil-

---

[78] Vgl. Shy, O. (2001), S. 5

[79] Vgl. Shapiro, C. (2001a), S. 1

[80] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 228

[81] Vgl. Brandenburger, A.M., Nalebuff, B.J. (1995)

systemen sicherstellen.[82] Der eigene Wert aufgrund eines Standards lässt sich wie folgt berechnen:[83]

Eigener Wert = Eigener Anteil x gesamter Industriewert

Aus Sicht der gewinnmaximierenden Perspektive macht es daher Sinn unter bestimmten Umständen einen Standard zu übernehmen. Der gesamte Industriewert ist dabei stark von der Größe des Markts abhängig, welche den Standard einführt und deren Akzeptanz.[84]

4.1.1 Gründe für Standards

Standards entstehen oft in Märkten mit zunehmenden Skalenerträgen, wo die Anzahl und Größe von Unternehmen, welche die gleichen Kernprodukte und Konstruktionsmerkmale einsetzen, wesentlich sind. Daneben sind Netzwerkexternalitäten und Lock-in Effekte vorhanden, sobald Konsumenten komplementäre Produkte nutzen oder in markenspezifisches Training investieren. Standards verringern die Kosten der Erweiterung, des Wachstums und des Nutzens von verwandten Produkten und fallen proportional zu den relevanten Märkten an, die den Standard akzeptieren. Konsumenten haben zudem generell ein größeres Interesse an standardisierten als an equivalenten nicht- standardisierten Produkten.[85]

4.1.2 Formen von Standards

Nach Buxmann lassen sich drei Formen der Entstehung von Standards unterscheiden:[86]

- *Marktliche Standardisierung*: Das System oder die Komponenten eines Systems von Unternehmen setzen sich am Markt durch und es entsteht ein De-facto-Standard, wie es im Fall der TCG geschehen soll.

---

[82] Vgl. Zerdick, A. (2001), S. 151 und 209

[83] Vgl. Varian, H. R. (2003), S. 35

[84] Vgl. Varian, H. R. (2003), S. 35 f.

[85] Vgl. Axelrod, R. et. al. (1995), S. 1495

[86] Vgl. Buxmann, P. (2001), S. 546

- *Standardisierung durch Komitees*: Zwischen unterschiedlichen Interessensgruppen wird im Rahmen eines Verhandlungsprozesses ein Standard entwickelt.

- *De-jure-Standardisierung*: Durch eine vorgesetzte staatliche Behörde wird ein Standard definiert.

Die marktliche Standardisierung und die Standardisierung durch Komitees können auch in gemischtem Verhältnis als Hybridform auftreten. Schließlich werden die Standardisierung durch Komitees und die De-jure-Standardisierung zugleich als Normierung bezeichnet.[87] Allgemeines Ziel standardisierender Unternehmen ist die Erstellung von offenen technischen Spezifikationen und deren Durchsetzung am Markt. Auffällig ist dabei die hohe Bedeutung, welche dem Internet beigemessen wird. Vorteile marktlicher Standardisierungsgremien gegenüber offiziellen Gremien sind die Schnelligkeit und ein gemeinsames Ziel. Durch den geringen Verwaltungsaufwand der Standardisierungskomissionen können die Gremien effektiver Arbeiten. Dies führt zwangsläufig zu einer Beschleunigung der Brauchbarkeit von Spezifikationen. Ferner haben die Unternehmen ein gemeinsames Ziel, was zum Erreichen der jeweiligen Geschäftsinteressen von Bedeutung ist und wiederum der Geschwindigkeit gegenüber offiziellen Gremien zu Gute kommt. Diese Aussage ist bei Beachtung der globalen Kommunikationsinfrastruktur allerdings nur bedingt richtig, da hier erforderliche Leistungsmerkmale und Anforderungen wichtiger als Geschwindigkeit sind. Des Weiteren ist die aktive Teilnahme an solchen Standardisierungsgremien wie im Fall der TCG unter Umständen kostenintensiv. Dies führt tendenziell zum Ausschluss der Mitarbeit kleinerer Unternehmen.[88]

4.2 Klassifizierung von Standards

Bei der Spezifisierung eines Standards existieren zwei grundlegende Trade-offs, welche die Netzwerkstrategie einer Standardisierung maßgeblich beeinflussen:

- Leistung versus Kompatibilität,

- Offenheit versus Kontrolle.

---

[87] Vgl. Farrell, J.; Saloner, G. (1988), S. 235 ff.

[88] Vgl. Jakobs, K. (2002), S. 84

4.2.1 Leistung versus Kompatibilität

Abbildung 12 illustriert zwei Ansätze, wie das Beharrungsvermögen von Konsumenten überwunden werden kann. Dabei handelt es sich um einen Trade-off zwischen der Evolutionsstrategie der Kompatibilität und zum anderen der Revolutionsstrategie der Leistung. Allerdings können die beiden Ansätze auch kombiniert werden. Die Strategien wägen die Stärken von Innovationen gegenüber Netzwerkexternalitäten ab. Eine Verbesserung der Leistung ist zudem auf Kosten von steigenden Wechselkosten der Konsumenten möglich, *vice versa*. Der Evolutionsansatz geht mit einer limitierten Leistung und hoher Kompatibilität einher, wohingegen eine hohe Leistung mit geringer Kompatibilität den Revolutionsansatz abbildet.[89]

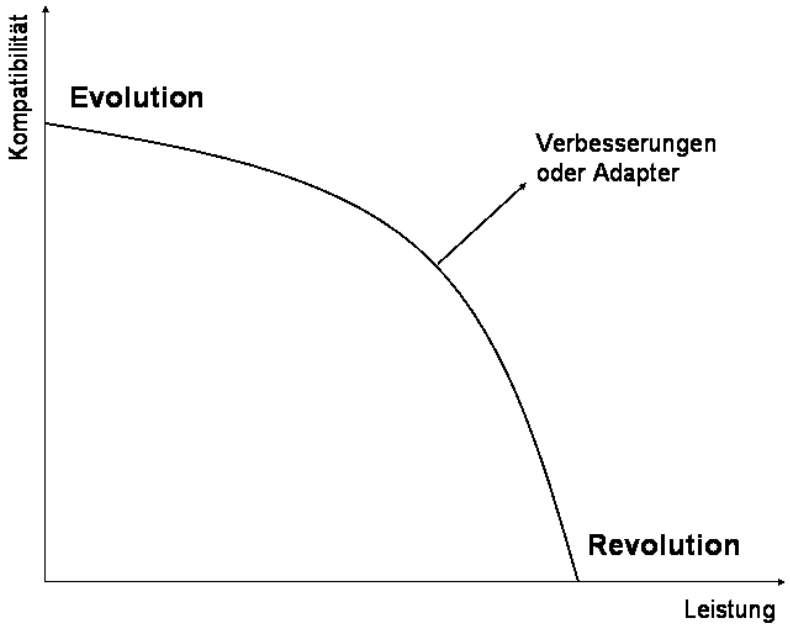

Abbildung 12: Trade-off zwischen Leistung und Kompatibilität[90]

4.2.1.1 Evolution

Die Evolutionsstrategie offeriert dem Konsument einen einfachen Migrationspfad mit dem Fokus die Wechselkosten soweit zu reduzieren, damit ein Großteil der Nutzer die neue Technologie ausprobieren kann. Bei virtuellen Netzwerken wird eine Möglichkeit benötigt, Kompatibilität zu bestehenden Produkten zu schaffen. Schnittstellen sind dabei kritisch, da zu Beginn versucht wird das neue Netzwerk mit der

---

[89] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 190

[90] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 191

alten installierten Basis aufzubauen. Die Einschränkung der Leistung um Rückwärtskompatibilität zu schaffen, führt zu Eintrittsmöglichkeiten für Wettbewerber, welche möglicherweise einer Revolutionsstrategie nachkommen. Des Weiteren treten technische und gesetzliche Hindernisse auf:[91]

Technische Hindernisse treten beim Trade-off zwischen Kompatibilität und Leistung auf, da eine Technologie entwickelt werden soll, die zu existierenden Produkten kompatibel ist. Eine dynamische Möglichkeit ist die Einweg-Kompatibilität, wie das Beispiel Microsoft Office zeigt, bei der die neueren Datei-Formate in älteren Office-Versionen nicht lesbar sind, jedoch umgekehrt. Das Motiv eines Upgrades basiert entweder aufgrund neuer Möglichkeiten oder der Kompatibilität mit anderen Produkten. Weiterhin löst gutes Engineering und Produktdesign das Trade-off-Problem, allerdings interessiert den Benutzer nicht nur eine Komponente, sondern das komplette System.[92]

Darüber hinaus können *gesetzliche und vertragliche Hindernisse* beim Aufbau eines Migrationspfades entstehen, da bereits bestehende Rechte am geistigen Eigentum und Patente den Pfad blockieren können oder der Hersteller Lizenzgebühren für die Nutzung verlangen kann.[93]

4.2.1.2 Revolution

Die Revolutionsstrategie bietet zwingend Leistung des neuen Produktes, um sog. Pioniere sowie beeinflussbare Nutzer zu gewinnen. Diese Strategie wird meist in schnell wachsenden Märkten angewendet. Die neuen Konsumenten können dabei die kritische Masse bilden und den Bandwagon-Effekt einleiten. Erst nach Erreichen einer kritischen Masse an Nutzer entwickelt sich das Netzwerk von alleine, was als Bandwagon-Effekt bezeichnet wird. Neben schnell wachsenden Märkten oder Konsumenten mit einem geringen Lock-in bildet sich die Leistung relativ zur Rückwärtskompatibilität stärker heraus. Erfolgreiche Technologien folgen dabei dem typischen S-Kurvenverlauf wie in *Abbildung 11*.[94]

---

[91] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 191 ff.

[92] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 193 ff.

[93] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 195

[94] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 195 f.

4.2.2 Offenheit versus Kontrolle

Der zweite fundamentale Trade-off, welcher bei der Standardisierung getroffen werden muss, ist die Entscheidung eines offenen oder eines proprietären Standards. Lock-in-Effekte und Wechselkosten spielen hierbei eine große Rolle. Dazu sind eine proprietäre Kontrolle und eine installierte Basis für einen Anbieter wertvoller, als wenn Wettbewerber den eingeschlossenen Konsumenten Produkte anbieten. Das Netzwerk ist somit wertvoller, sobald die Möglichkeit der Kontrolle über den Eintritt des Netzwerkes besteht. Eine Öffnung der Technologie mindert hingegen Lock-in Effekte seitens der Konsumenten, ebenso wie Wettbewerber mit vergleichbaren Leistungen. Des Weiteren sind der Erfolg und die Stärke des Trade-offs von der aktuellen Marktposition, den technischen Ressourcen und der Kontrolle über geistiges Eigentum abhängig. Generelles Ziel eines Unternehmens ist nicht nur die Kontrolle über die eigene Technologie, sondern auch die Maximierung des Wertes der eigenen Technologie:[95]

Der Industrie hinzugefügte Gesamtwert
x eigener Anteil am Industriewert
= Eigene Vergütung

Der zur Industrie hinzugefügte Gesamtwert hängt in erster Linie von dem innewohnenden Wert der Technologie ab. Allerdings ist der hinzugefügte Gesamtwert von der Netzwerkgröße abhängig und wie weit die Technologie im Zeitverlauf bereits adoptiert wurde. Dagegen hängt der Eigenanteil am Industriewert vom eigenen Marktanteil, der Gewinnspanne, jeglichen Lizenzzahlungen und den Effekten der neuen Technologie auf die Verkäufe anderer Produkte ab. Die Offenheit einer Technologie bestimmt sich durch den hinzugefügten Gesamtwert der Industrie, wohingegen der Eigenanteil am Industriewert die Kontrolle über eine Technologie beschreibt. Zur Maximierung des Wertes der eigenen Technologie in Netzwerkmärkten muss allerdings der Wert mit Wettbewerbern geteilt werden, da die Informationstechnologie aus Systemen besteht und eine Steigerung des Wertes einer Komponente sich zwangsläufig auf weitere überträgt. Der Zusammenhang zwischen Offenheit und Kontrolle einer Technologie wird in Abbildung 13 dargestellt.[96]

---

[95] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 198

[96] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 198 f.

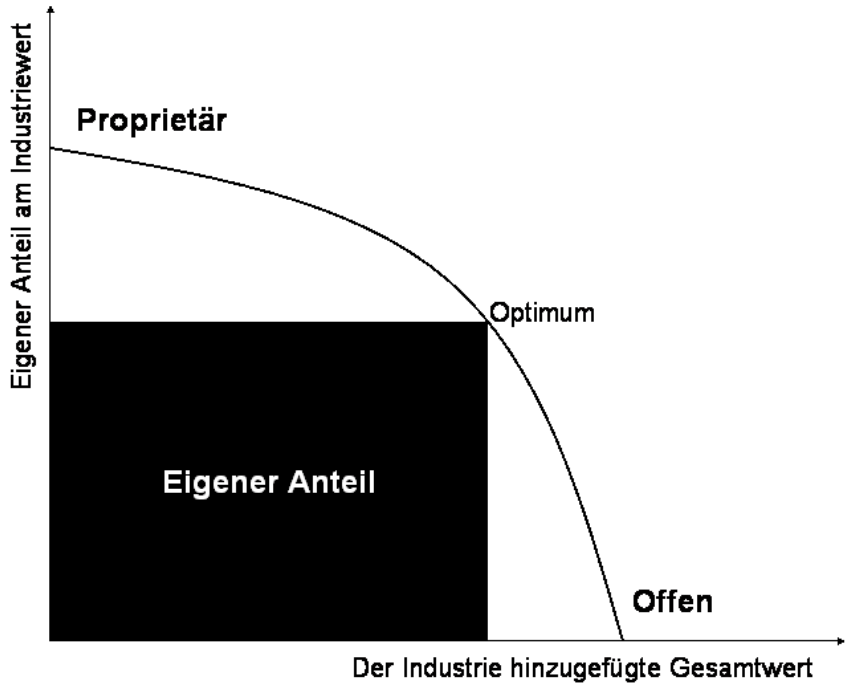

Abbildung 13: Trade-off zwischen Offenheit und Kontrolle[97]

4.2.2.1 Offenheit

Offenheit entsteht sobald verschiedene Produkte miteinander arbeiten sollen, was eine Koordination im Produktdesign notwendig macht. Das Ganze ist dabei größer als die Summe der einzelnen Teile. Der Begriff der Offenheit steht zudem im Auge des Betrachters.[98] Die TCG versteht unter Offenheit zum einen die Mitgliedschaft und Teilnahme an der Organisation und zum anderen die Offenheit des Industriestandards an sich, mit der Umsetzung der Hard- und Software-Spezifikationen.[99] Allerdings beinhaltet Offenheit mehr als Spezifikationen, da die Wahl des richtigen Zeitpunkts zusätzlich einfließt. Des Weiteren lassen sich zwei Kategorien unterscheiden:[100]

- *Vollständige Offenheit* erlaubt Produkte dem Standard entsprechend anzufertigen ohne etwas zu der Entwicklung beigesteuert zu haben.

---

[97] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 198

[98] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 199 ff.

[99] Vgl. TCG-Backgrounder (2003)

[100] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 200

- Beim *Allianz* Ansatz steuert jedes Mitglied etwas zum Standard bei und im Gegenzug darf jedes Mitglied, Produkte entsprechend des Standards herstellen. Allianzmitglieder haben in der Regel einen garantierten freien Zugang zum geschaffenen Netzwerk, wohingegen Außenstehende blockiert werden oder spezielle Entgelte für den Zugang entrichten müssen. Dieser Ansatz entspricht dem der TCG.

Unter Allianzen wird im Zusammenhang dieser Ausarbeitung eine Gruppe von Unternehmen verstanden, die ein gewisses Ziel formulieren, indem eine spezielle Technologie oder einen Standard vorangetrieben wird, wie es bei der TCG der Fall ist. Insbesondere Neufirmengründungen unterstützen Offenheit, da Markteintrittsbarrieren wie eine installierte Basis neutralisiert und Allianzen aufgebaut werden können. Offene Standards verlagern jedoch den Wettbewerb von der Technologie zu Marketing, Markennamen und Distribution. Dazu spielen die Kontrolle über eine installierte Basis, technische Überlegenheit und geistige Eigentumsrechte Schlüsselrollen.[101]

4.2.2.2 Kontrolle

Unternehmen in besonders starken Positionen, wie beispielsweise Marktführer, können starke Kontrolle über neu eingeführte Technologien ausrichten. Diese Unternehmen sind mächtig genug, um Produktstandards und Schnittstellen zu kontrollieren. In seltenen Fällen resultiert ihre Stärke aus technischer Überlegenheit gegenüber anderen Technologien. Trotz der Vormachtsstellung haben diese Unternehmen viel zu verlieren, wenn sie einen unausgereiften Standard fördern.[102]

4.2.3 Allgemeine Netzwerk-Strategien

Je nachdem welcher Trade-off zwischen Kompatibilität und Leistung, bzw. zwischen Proprietär und Offenheit getroffen werden, ergeben sich nach Shapiro und Varian vier Strategien, die in *Tabelle 5* zusammengefasst sind:

	Kontrolle	**Offenheit**
Kompatibilität	Kontrollierte Migration	Offene Migration
Leistung	Leistungsspiel	Diskontinuität

[101] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 200 f.

[102] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 203

Tabelle 5: Allgemeine Netzwerkstrategien[103]

Das *Leistungsspiel* bedingt die Einführung einer neuen inkompatiblen Technologie über die der Hersteller eine starke proprietäre Kontrolle behält. Diese Strategie ist besonders interessant für Neueinsteiger, die keine installierte Basis besitzen und somit Kompatibilitäten nicht berücksichtigen müssen.[104]

Eine *offene Migration* ist besonders konsumentenfreundlich, da neue Produkte von vielen Herstellern angeboten werden und somit geringe Wechselkosten bestehen. Dieser Ansatz macht am meisten Sinn, wenn besondere Produktionsressourcen bestehen und sich somit angebotsseitige Skalenerträge realisieren lassen.[105]

Die Strategie der *Diskontinuität* bezieht sich auf eine neue Technologie, die von verschiedenen Herstellern erhältlich ist, welche allerdings inkompatibel zur existierenden Technologie ist. Eine effiziente Herstellung, Softwareerweiterungen oder Mehrwert-Services eignen sich besonders für diese Taktik.[106]

Die *kontrollierte Migration* offeriert dem Konsument eine neue, verbesserte, proprietäre Technologie, die kompatibel zur existierenden Technologie ist. Bei Marktdominanz kann die Einführung der neuen Technologie als Premium-Version der alten Technologie eingeführt werden, um hohe Zahlungsbereitschaften der Konsumenten für Verbesserungen abzuschöpfen. Kontrollierte Migration entspricht oft einer dynamischen Form der Preisdiskriminierung zweiten Grades und erhöht zusätzlich die Barrieren für Markteintrittswillige.[107] Diese Strategie verfolgt auch die TCG, indem die proprietäre Technologie, bei gleichzeitiger Bewahrung der Kompatibilität zur bestehenden Technologie, erweitert und verbessert wird.

4.2.4 Coopetition

Standards sind von einer Vielzahl an Gremien spezifiziert, die zum einen konkurrieren und zum anderen miteinander kooperieren. Allerdings haben die Teilnehmer an solchen Gremien den gemeinsamen Nenner eine Win-Win-Situation zu schaffen,

---

[103] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 204

[104] Vgl. Shapiro, C.; Varian, H. R. (1998), S. 204 f.

[105] Vgl. Shapiro, C.; Varian, H. R. (1998), S.206

[106] Vgl. Shapiro, C.; Varian, H. R. (1998), S.206

[107] Vgl. Shapiro, C.; Varian, H. R. (1998), S.205

indem miteinander ein größerer Wert geschaffen wird, um später wegen den Anteilen zu konkurrieren. Die Wege der Kooperation und des Wettbewerbs sind im Begriff Coopetition zusammengefasst.[108] Um die Win-Win-Situation besser klassifizieren zu können, dient das Value Net aus *Abbildung 14*.

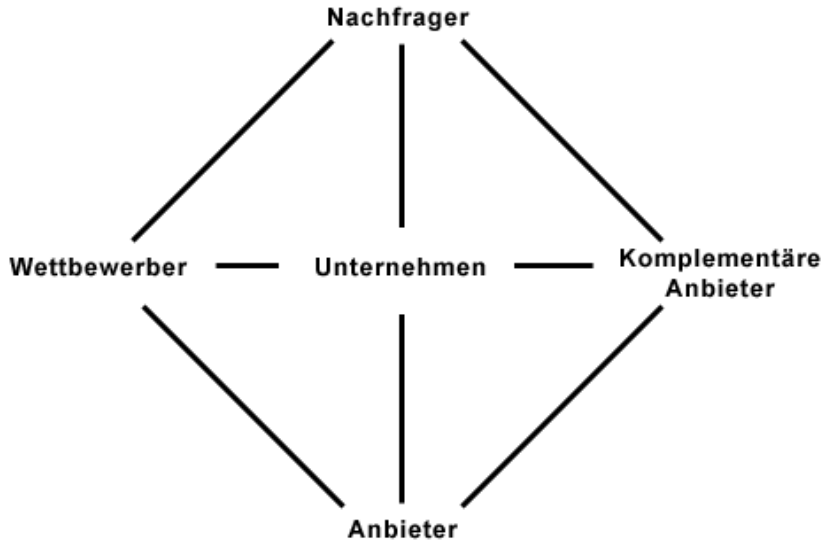

Abbildung 14: Das Value Net[109]

Hier wird aus Sicht der eigenen Unternehmung eine Strategie aufgebaut und durch einen spieltheoretischen Ansatz fünf Elemente abgeleitet, wie Spieler, Wertschöpfung, Regeln, Taktiken und Abgrenzungsbereich. Dabei findet eine horizontale Kooperation zwischen Unternehmen auf der gleichen Stufe der Wertschöpfungskette statt und betrifft aus Unternehmenssicht den Wettbewerb und die komplementären Anbieter. Dagegen erfolgt die vertikale Kooperation auf unterschiedlichen Stufen der Wertschöpfungskette und zwar vom Anbieter über die eigene Unternehmung bis zum Nachfrager. Zudem ist dieses Konzept dynamisch, da keine Rolle fest fixiert ist, sondern die Spieler immer wieder wechseln, das eigene Unternehmen eingeschlossen.[110] Im Fall der TCG erfolgt eine horizontale sowie vertikale Kooperation der Unternehmen über die unterschiedlichen Stufen der Wertschöpfungskette.

---

[108] Vgl. Brandenburger, A. M.; Nalebuff, B. J. (1995), S. 59

[109] Vgl. Brandenburger, A. M.; Nalebuff, B. J. (1995), S. 60

[110] Vgl. Brandenburger, A. M.; Nalebuff, B. J. (1995), S. 60 ff.

4.3 Standardisierungsallianzen

Unter Standardisierungsallianzen werden ein oder mehrere Unternehmen verstanden, die sich zusammenschließen, um eine Standard-Technologie zu entwickeln oder die Adoption eines Standards zu fördern. Unternehmen fördern dabei De-facto-Standards, indem die eigenen proprietären Methoden als Standard vorangetrieben werden oder durch Beitritt einer Allianz, welche Standards entwickelt und intensiviert.[111]

4.3.1 Wettbewerb zwischen und innerhalb von Standards

Unternehmen haben generell die Auswahl aus Wettbewerb zwischen und innerhalb von Standards. Standardisierung beinhaltet dabei Strategien zwischen vertikal verwandten Unternehmen und Strategien zwischen horizontalen Wettbewerbern. Vertikale verwandte Unternehmen zielen dabei mehr auf komplementäre Anbieter ab, wohingegen horizontale Wettbewerber über die Kompatibilität gegenüber Wettbewerbern entscheiden, welche Strategie gewählt wird.[112]

Standardisierungsallianzen kombinieren hingegen Elemente aus Wettbewerb zwischen Standards und Wettbewerb innerhalb von Standards. Dabei wird die Standardisierung durch Allianzen auf zwei logischen Ebenen durchgeführt. Auf der ersten Ebene wird Wettbewerb zwischen Standards unter Netzwerken und Gruppen oder Firmen vollzogen, die eine spezielle technologische Grundform unterstützen. Danach verlagert sich die Rivalität innerhalb der Gruppen oder Firmen, was als Wettbewerb innerhalb des Standards bezeichnet wird.[113]

4.3.2 Allianzgestaltung zur Standardisierung

Eine besondere Herausforderung im Rahmen des Wettbewerbs von Systemgütern umfasst die Gestaltung der Gruppe, die den Standard fördert und gestaltet. Dabei ist die potentielle Größe der Allianz ein Wert für die Wahrscheinlichkeit der erfolgreichen Umsetzung einer Standardisierung und beeinflusst Unternehmen positiv der Allianz beizutreten. Generell haben Standardisierungsallianzen einerseits das Problem einen Standard technologisch zu spezifizieren und andererseits diesen am Markt

---

[111] Vgl. Axelrod, R. et. al. (1995), S. 1493

[112] Vgl. Besen, S. M.; Farrell, J. (1994), S. 117 ff.

[113] Vgl. Keil, T. (2002), S. 210

zu etablieren. Beim Spezifizieren eines Standards handelt es sich um Schaffung von Wissen, dagegen ist die Adoption am Markt eine Verbreitung von Wissen.[114]

Während der Spezifizierung des Standards sollte die Organisation die notwendigen Ressourcen gewährleisten, jedoch sollten eine schnelle Entscheidungsfindung und Kompromisse möglich sein. Deshalb benötigt eine effektive Spezifizierung im Kern eine kleine Anzahl an Mitgliedern, die komplementäre Ressourcen besitzen. Allerdings führt eine größere Anzahl an Sponsoren durch die unterschiedlichen Interessen zu einer Verlangsamung der Entscheidungsfindung und Kompromissen.[115] Im Fall der TCPA haben anfangs nur fünf wesentliche Gründer und Förderer fungiert, die im Zuge der TCG auf sieben Vorstandsmitglieder erweitert wurden. Künftig wird wohl auf der nächsten Mitgliederversammlung eine weitere Aufstockung des Vorstandes der TCG von sieben auf neun Sitze vorgenommen, um die beiden Contributoren Seagate und VeriSign zu integrieren.[116]

Um den Standard schnell und erfolgreich am Markt zu etablieren, ist es notwendig unverzüglich eine installierte Basis aufzubauen. Im Fall der TCG besitzen die zentralen Mitglieder der Allianz jeweils einen großen Marktanteil in ihrem Kerngeschäft. Dies sollte zur Erreichung der kritischen Masse reichen, um den Standard erfolgreich am Markt zu platzieren. Darüber hinaus haben Unternehmen die Möglichkeit zu relativ geringen Kosten über den Status des Adopters am Standard frühzeitig teilzunehmen. Zusätzlich erlangen diese Unternehmen über die RAND-Lizenzierung Zugang zu den Patenten und Urheberrechten des Standards, was die Wahrscheinlichkeit der erfolgreichen Umsetzung weiter stärkt.[117]

Die Allianzstruktur der TCG lässt sich am besten als halboffen beschreiben, da der Zugang zu den Promotoren limitiert und geschlossen ist, wohingegen die Contributoren und Adaptoren Gruppen offen sind. Die Gestaltung der TCG kombiniert die Vorteile der Kontrolle von geschlossenen Allianzen mit den Vorteilen der Marktdurchdringung von offenen Allianzen. Dabei spielt die Wahl der Partner innerhalb der geschlossenen Gruppe eine kritische Rolle. Ebenso sind die Marktanteile und die

---

[114] Vgl. Keil, T. (2002), S. 210 f.

[115] Vgl. Keil, T. (2002), S. 210 f.

[116] Vgl. Ward, J. (2004), S. 76

[117] Vgl. Keil, T. (2002), S. 211

Reputation der geschlossenen Allianz als kritisch zu beurteilen, da die Gestaltung der Erwartungen von zukünftigen Adaptoren berührt werden und folglich enormen Einfluss auf die erfolgreiche Etablierung am Markt haben.

4.4 Kooperative Standardisierung

In der Betriebswirtschaft wird unter dem Begriff Kooperationen die „freiwillige Zusammenarbeit von Unternehmen, die rechtlich selbstständig bleiben“[118] verstanden. Dies erfolgt zur Steigerung der gemeinsamen Wettbewerbsfähigkeit unter teilweiser Abgabe gewisser Souveränitäten. Eine kooperative Standardisierung einigt sich mit anderen Unternehmen verschiedener hierarchischer Stufen über Kompromisse auf einen Standard. Ein Industriestandard kann allerdings durch die Kooperation Auswirkungen auf die Effizienz und die Wohlfahrt einer Ökonomie haben, was wiederum das Kartellamt zu überprüfen hat. Shapiro nennt hierfür folgende Gründe:[119]

1. Die Kooperation beeinflusst verschiedene Produkteigenschaften anders, als sie vielleicht unter dem Einfluss des Wettbewerbs entstanden wären.
2. Kooperationen eliminieren den vorzeitigen Wettbewerb zwischen Standards.
3. Kooperationen ermöglichen mehreren Unternehmen einen Industriestandard anzubieten, wohingegen der Wettbewerb zwischen Standards zu einem einzigen proprietären Produkt führt.

4.4.1 Die Leistungen von Kompatibilität und Standards

Zunächst ist eine größere Realisierung von Netzwerkeffekten durch Kompatibilität möglich, wonach der Konsument durch eine Maximierung des Netzwerkes profitiert. Im Fall von Hard- und Software-Netzwerken profitieren Konsumenten durch die angebotenen Komponenten über den Zugang zu großen Märkten für ihre Software. Dies führt schließlich zu steigenden Beitritten eines Standards und zu steigender Vielfalt der Produkte. Ebenso erhöht sich der Innovations- und Preiswettbewerb im Angebot von Softwarekomponenten. Kompatibilität führt folglich zu erweitertem Wettbewerb zwischen den Herstellern komplementärer Produkte sowie Gebrauchtmärkten. Darüber hinaus werden die Konsumenten vom Risiko geschützt, auf einem

---

[118] Vgl. Wikipedia (2004)

[119] Vgl. Shapiro, C. (2001a), S. 7

Produkt sitzen zu bleiben, indem die Produkte kompatibel sind.[120] Ferner wird durch einen Standard ein erfolgreicher Start eines Netzwerkes eingeleitet, sowie der Wettbewerb innerhalb eines offenen Standards ermöglicht.[121]

4.4.2 Die Kosten von Kompatibilität und Standards

Standardisierung führt auch zu Kosten, wie die Einschränkung von Unternehmen in der Produktgestaltung. Statische Verluste entstehen durch Reduzierung in der Vielfalt. Dynamische Verluste machen sich durch Ausschluss von Unternehmen bemerkbar, bei denen durch Forschung und Entwicklung innovative Produkte entstehen, die nicht dem Standard entsprechen. Beide Einschränkungen verursachen Kosten zur Zeit der neuen Produkterstellung, wobei später die Möglichkeit besteht, auf Kosten der Kompatibilität eine neue Generation mit verbesserten Leistungen einzuführen. Zusätzlich bestehen Auswirkungen auf den Wettbewerb, indem aufgrund der Bedeutsamkeit von Kompatibilität eine Fokussierung auf ein bestimmtes Netzwerk erfolgt. Die steigende Adoption eines Herstellerprogramms führt somit nicht zu einem Wettbewerbsvorteil, da auch die Konkurrenz mit zunehmender Netzwerkgröße profitiert. Mit anderen Worten führt somit eine zunehmende Adoption eines bestimmten Produktes zu einem Wettbewerbsvorteil durch die Steigerung des Wertes der Software relativ zu den Programmen, die nicht Teil dieses Netzwerkes sind. Als Konsequenz der Kompatibilität konkurrieren die Unternehmen somit innerhalb eines Standards um Anteile anstatt für einen Markt. Dies geschieht anhand der vier Dimensionen *Preis, Produkteigenschaften, Reputation einer Marke* und *Servicedienstleistungen*. Kooperative Standardisierung dämpft folglich den ex-ante Wettbewerb zwischen Standards, währenddem der Wettbewerb im Produktlebenszyklus steigt.[122] Ebenfalls steigen die Kosten für Konsumenten durch die proprietäre Kontrolle über einen geschlossenen Standard.[123]

---

[120] Vgl. Shapiro, C. (2001a), S. 8

[121] Vgl. Shapiro, C. (2001b), S. 21

[122] Vgl. Shapiro, C. (2001a), S. 7 ff.

[123] Vgl. Shapiro, C. (2001b), S. 21

4.5 Schlüsselressourcen

Um einen Standard erfolgreich im Markt zu platzieren, ist der Besitz von sieben Schlüsselressourcen ausschlaggebend. Nach Shapiro und Varian sind dies:[124]

1. *Kontrolle über eine installierte Basis an Kunden:* Eine große Basis an loyalen oder eingeschlossenen Kunden ermöglicht eine Evolutionsstrategie mit Rückwärtskompatibilität.

2. *Recht am geistigem Eigentum:* Unternehmen die wertvolle Technologien oder Schnittstellen mit Patenten und Urheberrechten kontrollieren, sind in einer sehr starken Position.

3. *Möglichkeit Neuerungen einzuführen:* Die Möglichkeit proprietäre Erweiterungen in Zukunft zu entwickeln, führt zu einer starken Verhandlungsposition.

4. *First-Mover Vorteile:* Je weiter die Produktentwicklung vorangeschritten ist, desto größer ist der Vorteil durch Lerneffekte gegenüber der Konkurrenz und desto stärker wiederum die eigene Position.

5. *Produktionsmöglichkeiten:* Preiswerte Hersteller sind ebenfalls in einer starken Position, wenn sie einerseits Skaleneffekte in Form von Kostenvorteilen und andererseits Herstellungskompetenzen durch Know-how umsetzen können.

6. *Stärke von Komplementären:* Bei der Produktion von Komplementärgütern besteht eine besonders starke Motivation die kritische Masse zu erreichen und zunehmende Skalenerträge zu realisieren. Dies führt dazu eine Führungsposition einzunehmen, welche die Akzeptanz der neuen Technologie steigert, damit die Verkäufe der anderen Produkte die eigenen fördert.

7. *Reputation und Markenname:* Reputation und Markenname sind besonders entscheidend in Netzwerkmärkten, in denen Konsumentenerwartungen eine große Rolle spielen.

---

[124] Vgl. Shapiro, C.; Varian, H. R. (1999), S. 16 ff.

Grundsätzlich können die Ressourcen von Konsumenten sowie von den Technologieanbietern kontrolliert werden, z.B. kann ein Großabnehmer automatisch die installierte Basis aufweisen. Die Kontrolle über eine einzige Ressource ist jedoch nicht ausschlaggebend, um erfolgreich zu sein.[125]

4.6 Geistiges Eigentum

Geistiges Eigentum im Zusammenhang mit Information und Technologie ist ein kritisches Thema, vor allem da Informationsgüter die Eigenschaft öffentlicher Güter besitzen. Zudem ermöglicht der Einsatz einer Technologie die Manipulation von Informationen. Grundlegend wird geistiges Eigentum vom Gesetzgeber durch das Urheberrechtsgesetz und das Patentgesetz geschützt. Das Urheberrechtsgesetz definiert dabei die Eigentumsrechte am verkauften Produkt. Indessen definieren Patentgesetze die Bedingungen für Anreize und Zwänge auf Innovationen von physischen Geräten sowie Software- und Geschäftsprozesse.[126] Der Schutz von geistigem Eigentum ist somit eine zentrale Streitfrage bei einer Standardisierung, welche diese sogar unmöglich machen kann, wenn der Umgang mit geistigen Eigentumsrechten im Vorfeld nicht vereinbart wird. Diese Problematik betrifft auch die TCG, was durch die jüngste Entwicklung der US-Top 20 der Patentanmeldungen untermauert wird:

Platz	Brand US-Patente 2003	Anzahl	TCG Mitgliedsstatus
1	International Business Machines (IBM)	3399 (3399)	Promoter
7	Hewlett-Packard	1699 (1697) +65 Compaq	Promoter
9	Intel	1595 (1595) +10 Level One	Promoter
10	Samsung	1574 (1303)	Contributor
11	Sony	1536 (1360)	Promoter
12	Philips	1495 (1335)	Contributor
13	Fujitsu	1466 (1330)	Contributor
14	Toshiba	1395 (1208)	Adaptor
17	Advanced Micro Devices (AMD)	907 (907)	Promoter

Tabelle 6: Ausschnitt der US-Top 20 Patente 2003 nach Markenname[127]

Die Tabelle zeigt dabei einen Ausschnitt der Patente laut US-Patentserver gemäß der Markennamen inklusive aller Tochterfirmen, die den Namensbestandteil führen und der Mutterfirma in Klammern. Dieser Ausschnitt zeigt die involvierten Mitglieder

---

[125] Vgl. Shapiro, C.; Varian, H. R. (1999), S. 16 ff.

[126] Vgl. Varian, H. R. (2003), S. 6 f.

[127] Vgl. Stiller, A. (2003), S. 20

der TCG sowie deren Status im Standardisierungsgremium. Dabei sind fünf der sieben Promoter unter den US-Top 20 der Patentanmeldungen 2003. Hewlett-Packard geht darüber hinaus weitere Wege und hat zu ihrer strategischen Verwaltung und Vermarktung der Technologien eigens die Firma „Intellectual Property Licensing Group“ gegründet.[128]

Allianzen treten in diesem Zusammenhang in unterschiedlichen Formen auf, abhängig davon, welche Kontrolle sie über Vermögensgegenstände haben, die zum Erfolg eines Standards führen sollen. Querlizenzierung von kritischen Patenten ist in diesem Kontext weit verbreitet, d.h. es werden vertrauliche Informationen unter einer Geheimhaltungsvereinbarung geteilt. Einige Firmen erhoffen sich dadurch Lizenzeinnahmen und verhandeln Lizenzvereinbarungen, um entscheidende Verbündete anzuwerben. Andere Unternehmen erhoffen sich mit Hilfe von Produktionsvorteilen oder Time-to-Market Fähigkeiten Vorsprünge, so lange sie nicht durch Patente oder überzogene Lizenzgebühren blockiert werden. Allianzen umfassen dabei die komplette Distanz zwischen vollständiger Offenheit und Kontrolle wie *Abbildung 15* aufzeigt.[129]

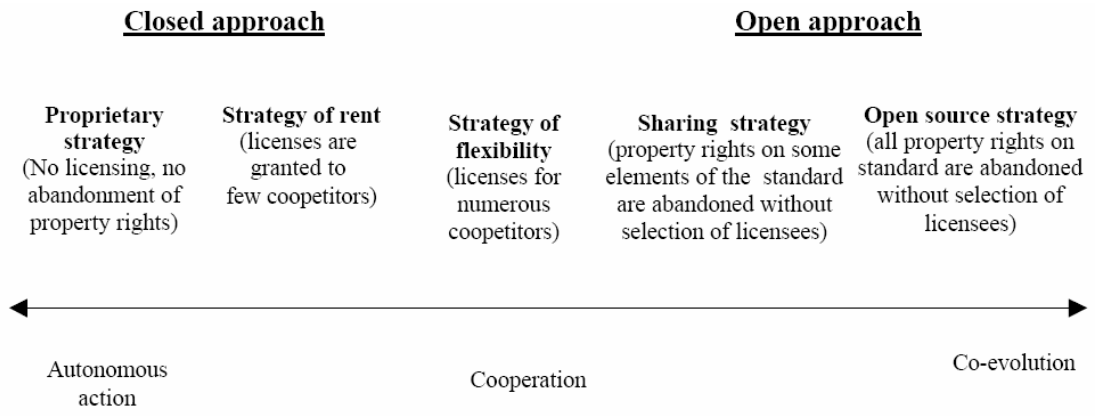

Abbildung 15: Skala zur Einordnung der Strategien von Eigentumsrechten[130]

Am rechten Ende des Spektrums befindet sich der offene Ansatz der „Co-evolution“, der die Diffusion von Standards dank Netzwerkexternalitäten unterstützt und den Bandwagon-Effekt beschleunigt. Dabei führt ein offener Ansatz nicht automatisch zum ökonomischen Erfolg, noch ist die Technologie für Außenstehende frei verfüg-

---

[128] Vgl Hewlett Packard (2004b)

[129] Vgl. Lecocq, X.; Demil, B. (2002), S. 6 ff.

[130] Vgl. Lecocq, X.; Demil, B. (2002), S. 7

bar. Hingegen gestattet der geschlossene Ansatz „Autonomous action“ am linken Ende des Spektrums eine strenge Kontrolle über eine Technologie oder Schlüsselkomponente, deren Entwicklung und ökonomische Gewinne. Darüber hinaus besteht die Möglichkeit die Ansätze zu vermischen, um beispielsweise einen offenen Ansatz über seine Verbesserungen und Erweiterungen zu kontrollieren, wie es z.B. die Firmen Sun mit Java oder Apple mit Macintosh machen. Das Ausnutzen eines proprietären Standards ist eine autonome Strategie und führt den Konsument zu einer abgeschlossenen Gemeinschaft in Abhängigkeit der Technologie des Anbieters. Andererseits schafft die Strategie des offenen Ansatzes ein Netzwerk von verbundenen Wettbewerbern, in der mehrere Anbieter die gleiche Technologie nutzen.[131]

4.6.1 Querlizenzierung und Patent-Pools

Während des Standardisierungsprozesses kontrollieren verschiedene Firmen Eigentumsrechte, die zusammen kombiniert werden müssen, um Produkte am Markt zu platzieren. Dazu müssen die Teilnehmer bedeutungsvolle Patente zur Erreichung des Standards querlizenzieren, was unter gerechten Bedingungen geschehen sollte. Werden die Patente dabei einzeln kontrolliert, entstehen höhere Preise als unter einer gemeinsamer Kontrolle.[132] Traditionell werden *Querlizenzierungen* zwischen Wettbewerbern mit laufenden Lizenzgebühren vom Kartellamt nicht gerne gesehen, da diese zu Preissteigerungen führen und Kartelle bewirken.[133] Dies trifft allerdings nicht auf gering laufende Lizenzgebühren zu, sondern eher auf im Voraus festgesetzte Zahlungen. Ein weiteres Thema betrifft Lizenzgewährungen von zukünftigen Patenten, welche die Anreize von Unternehmen reduzieren Forschung und Entwicklung zu betreiben, da der Wettbewerb die Verbesserungen imitieren kann. Trotzdem ist dieses Argument so in der Praxis nicht zu beobachten, wie die Halbleiterbranche belegt. Jedoch bleiben Zweifel bezüglich Querlizenzierungen, ob diese die Effektivität steigern, besser Produkte am Markt platzieren und schnellere Phasen im Produktdesign bewirken.[134]

---

[131] Vgl. Lecocq, X.; Demil, B. (2002), S. 7 f.

[132] Vgl. Shapiro, C. (2001a), S. 15 f.

[133] Vgl. Katz, M.; Shapiro, C. (1985b)

[134] Vgl. Shapiro, C. (2001b), S. 12 f.

Ein weiterer Weg standardkonforme Produkte herzustellen, ist die Verfügung eines *Patent-Pools*, indem alle blockierenden Patente von einer Einheit lizenziert und koordiniert werden. Ein Schlüsselproblem spielen dabei Unternehmen, die konkurrierende oder blockierende Patente halten, bzw. was der Standard als blockierende Patente definiert.[135] Aus diesem Grund ist es wichtig komplementäre, d.h. blockierende und essentielle Patente in einen Pool mit einzubeziehen. Überdies wird der Wettbewerb gefördert, was bei substituierenden oder rivalisierenden Patenten nicht der Fall ist.[136]

4.6.2 RAND-Lizenzierung

Im Umgang mit patentierter Technologie im Rahmen von Standardisierungsverfahren gibt es verschiedene Taktiken. Die TCG hat die Problematik des Umgangs mit geistigen Eigentumsrechten im Standardisierungsgremium durch die RAND-Lizenzierung gelöst, auf die im Folgenden näher eingegangen wird. RAND steht als Abkürzung für „**R**easonable **A**nd **N**on-**D**iscriminatory“ und fordert eine faire Lizenzierung, d.h. jedem Mitglied wird zu angemessenen und gleichen Bedingungen die Möglichkeit gegeben, das Patent zu nutzen. In einem Entwurf des „World Wide Web Consortium“ (W3C) ist eine kurze Definition für die RAND Lizenzierung veröffentlicht, welches unter anderem von beiden Promotoren Microsoft und Hewlett Packard mitverfasst wurde. Eine RAND Lizenz ist eine Lizenz, die[137]

- für jeden weltweit verfügbar sein soll, der implementieren will.
- sich über alle wesentliche Ansprüche, wie z.B. Patente, des besitzenden und kontrollierenden Lizenznehmers erstreckt.
- eventuell limitiert ist in der vorgeschlagenen Implementierung und was wirklich vom Vorschlag benötigt wird.
- abhängig von einer Unterstützung von wechselseitigen RAND Lizenzierungen sein darf und sich über alle wesentliche Ansprüche des besitzenden und kontrollierenden Lizenznehmers erstreckt.

---

[135] Vgl. Shapiro, C. (2001a), S. 15 f.

[136] Vgl. Shapiro, C. (2001b), S. 17 ff.

[137] Vgl. Weitzner, D. J. et. al. (2001)

- abhängig von angemessenen und fairen Lizenzgebühren sein kann.
- keine weiteren Abhängigkeiten und Restriktionen beim Gebrauch jeglicher Technologie, Eigentumsrechte, oder andere Restriktionen im Verhalten des Lizenznehmers auferlegen darf. Allerdings sind angemessene, übliche Bedingungen verwandt mit dem Betrieb und der Erhaltung der Lizenzbeziehung wie folgt zu berücksichtigen: Abschlussprüfung, Auswahl des Gesetzes und Beilegungen von Rechtsstreitigkeiten.

Die eigentlichen Lizenzbedingungen werden jedoch unter den Mitgliedern verhandelt. Diese Patentierungspolitik deckt sich weitgehend mit Standardisierungsgremien großer Technologieunternehmen und bietet dem Lizenzinhaber ein Entgelt für seine Entwicklungsarbeit. Zusätzlich ist ein Vehikel geschaffen, um patentierte Technologie in einen Standard einfließen zu lassen und darüber hinaus De-facto Standards nachträglich zu standardisieren. Allerdings können sich Open-Source Entwickler in der Regel kaum Lizenzgebühren leisten, was zwangsläufig die Interoperabilität bedroht und Zwei-Klassen-Software fördert. Ein weiteres Problem birgt die Definition des Begriffs „angemessen“, die bislang noch nicht eindeutig bestimmt ist.[138]

4.7 Funktionen in der Standardisierungsallianz

Um einen Standard erfolgreich zu entwickeln, lassen sich drei Funktionen einer Standardisierungsallianz aufzeigen. Als erstes wäre die Funktion der Technologie innerhalb des Standardisierungsgremiums zu nennen, welche die schnelle Entwicklung eines Standards garantieren soll. Des Weiteren sollten ein oder mehrere Unternehmen in der Allianz die wichtigsten Anwender des Standards repräsentieren, damit dementsprechende Marktbedürfnisse im Standard berücksichtigt werden. Zuletzt werden ein oder mehrere Mitglieder aus der Allianz benötigt, welche die Funktion des Architekten und Anwender repräsentieren. Dessen Aufgaben sind die Erhaltung und der reibungslose Ablauf der Prozesse als Knotenpunkt im Netzwerk.[139]

---

[138] Vgl. Coursey, D. (2002)

[139] Vgl. Keit, T. (2002), S. 212

Nachfolgend wird ein Überblick von der Mitgliederstruktur und deren Rolle in der TCG gegeben. Die Business Webs spiegeln einen möglichen Ausblick der Rollenverteilung nach einer Standardisierung wieder.

4.7.1 Die Mitglieder der TCG

Bei der Gründung der TCG wurde versucht, die Organisation und Struktur entsprechend industrieller Standardisierungsgremien anzupassen. Direkt beim Eintritt in die TCG wird entschieden, welchen Status das Mitglied einnimmt.

4.7.1.1 Promoters

In der jetzigen Konstellation sind sieben gelistete Firmen auf dieser obersten Rangstufe und zwar AMD, Hewlett-Packard, IBM, Intel, Microsoft, Sony und Sun Microsystems.[140] Einzig diese sieben Firmen sind einflussreich in der TCG.[141] Diese Mitglieder haben permanent Anspruch auf einen Sitz im Vorstand der TCG und zahlen je Unternehmen einen Jahresbeitrag von $ 50.000,00. Eine Erweiterung dieser Rangstufe sowie Satzungsänderungen sind nur mit einer ¾-Mehrheit der aktuellen Mitglieder dieser Ebene möglich. Dagegen werden die meisten Entscheidungen in der TCG mit einer $\frac{2}{3}$-Mehrheit getroffen. Somit wird das Blockieren verschiedener Bewegungsrichtungen während des Standardisierungsprozesses vermieden.[142] Es besteht das Recht neue Promotoren vorzuschlagen sowie das Recht die Organisation zweckgerichtet zu verändern. Des Weiteren haben Promotoren vollen Website-Zugriff, einschließlich der Diskussionsgruppen und Mailinglisten, sowie Zugriff auf vertrauenswürdige Informationen, wie Vorveröffentlichungen von Spezifikationsentwürfen und interne Arbeitsdokumente. Ferner besteht ein Anrecht der Teilnahme und Aktivität an Arbeitsgruppen oder speziellen Gremien.[143]

4.7.1.2 Contributors

Auf der mittleren Rangstufe der TCG befinden sich aktuell 31 gelistete Mitglieder, von denen jedes Unternehmen einen jährlichen Beitrag von $ 15.000,00 zahlen muss.

---

[140] Vgl. TCG-Current Members (2004)

[141] Vgl. BSI (2003)

[142] Vgl. Ward, J. (2004), S. 76

[143] Vgl. TCG-Bylaws (2003)

Die Kriterien der Zulassung dieser Ebene bestimmt der Vorstand, insbesondere die Promotoren. Generelle Voraussetzung sind ein ökonomisches Interesse oder eine besondere Bedeutung des Erfolges für die TCG. Es besteht das Recht einen Vertreter zur Wahl in den Vorstand zu nominieren, der dann die gleichen Rechte wie ein Promoter besitzt. Die Contributors Seagate und VeriSign sollen dabei künftig für ein Jahr in den Vorstand gewählt werden.[144] Darüber hinaus haben Contributors vollen Website-Zugriff sowie Zugriff auf vertrauenswürdige Informationen. Ebenfalls besteht ein Anrecht der Teilnahme und Aktivität an Arbeitsgruppen oder speziellen Gremien.

4.7.1.3 Adaptors

Auf der offiziellen TCG Webseite befinden sich zurzeit nur zehn gelistete Adaptors, wovon jedes Mitglied einen Beitrag von $ 7.500,00 bezahlen muss. Sie haben Zugang zu veröffentlichten Entwürfen der Spezifikationen im Mitgliederbereich. Allerdings haben Adaptoren nur selektierten Zugriff auf die Webseite sowie limitierten Zugang zu Diskussionsgruppen und Mailing-Listen. Zudem haben Adaptoren kein Stimmrecht in der TCG. Jedoch entscheidet jedes Unternehmen selbst, ob es als Contributor oder Adaptor der TCG beitritt.[145]

4.7.2 Business Webs

Business Webs bestehen aus einer Anzahl von Firmen, die eine gemeinsame Architektur benutzen, um unabhängig voneinander wertschöpfende Teilleistungen zu erstellen, welche sich gegenseitig ergänzen.[146] Ein Standard und überdurchschnittliche Renditen sind dafür vorausgesetzte Bedingungen. Die Systemarchitektur eines Business Webs wird durch ein Element vereinigt, welches entweder auf Markt, Kunden oder Technologie basiert. Aufgrund der technologischen Ausrichtung der TCG, ist für die vorliegende Ausarbeitung nur „*Technology Webs*“ relevant. Diese basieren auf einen De-facto-Standard, der im Mittelpunkt des Systems steht, worauf die Komponenten ausgerichtet werden. Kompatibilität der Schnittstellen ist dabei von hoher Wichtigkeit, um das Zusammenwirken der Komplementärgüter mit der Kern-

---

[144] Vgl. TCG Press Room (2003)

[145] Vgl. TCG-Bylaws (2003)

[146] Vgl. Zerdick, A. (2001), S. 182

technologie zu gewährleisten. Der Wert der Kerntechnologie und deren Komponenten hängen von der Größe und dem Wachstum des Technology Webs ab. Mit der steigenden Anzahl an Teilnehmern im Business-Web, steigen die indirekten Netzeffekte für den Kunden sowie positive Externalitäten stellen sich ein. Ist die Kerntechnologie zusätzlich proprietär, steigen die Wechselkosten und es entstehen Lock-in Effekte. Innerhalb des Technology Webs konkurrieren die Firmen untereinander um Anteile, allerdings schaffen sie auch Werte für spezielle Gruppen von Unternehmen, die eine allgemeine Technologie Plattform eingeführt haben. Teilnehmende Firmen des Technology Webs können zwei hierarchische Positionen einnehmen. Der „*Shaper*“ kontrolliert die Kerntechnologie des Business Webs, wohingegen der „*Adapter*“ diese anerkennt und seine Komplementärleistungen danach ausrichtet.[147]

Der Erfolg des Shapers lässt sich dabei an vier Faktoren festsetzen:[148]

- *Eigentumsrechte an einer Schlüssel-Plattform-Technologie*, welche weitere Architekturen gestaltet und die Basis für Lock-in Effekte bildet.
- *Entbündelung des Geschäfts*, um weitere Möglichkeiten für weitere Teilnehmer zu schaffen.
- *Vertrauen in ökonomische Anreize* anstatt Allianzstrukturen oder vertragliche Beziehungen, um weitere Teilnehmer zu mobilisieren.
- *Aktives Management der dynamischen und überdurchschnittlichen Renditen*, um Webwachstum zu beschleunigen sowie Kunden- und Teilnehmer-Lock-in Effekte.

Shaper streben nach Beschleunigung der dynamischen und überdurchschnittlichen Renditen des kompletten Technology Webs, d.h. nicht auf Firmenebene wird versucht die Einführung einer Technologie zu forcieren, sondern auf Technology Web Ebene. Indessen lassen sich beim Adapter drei Erfolgsfaktoren aufzeigen:[149]

- *Frühe Teilnahme in gewinnenden Technology Webs*.

---

[147] Vgl. Hagel, J. (1996), S. 6 ff.

[148] Vgl. Hagel, J. (1996), S. 10 f.

[149] Vgl. Hagel, J. (1996), S. 11

- *Aggressiver Wettbewerb für Anteile im Technology Web*.
- *Verbindende und breit gefächerte Positionen*, um zum einen die eigene Strategie an der des Shapers auszurichten und zum anderen zum Schutz vor unerwartenden Wendungen des Shapers.

5 Trusted Computing

Die Trusted Computing Group schlägt eine Lösung vor, um die Sicherheit von Plattformen zu verbessern. Dazu wird das Hardware Design um eine Sicherheitskomponente erweitert. Im Folgenden wird dies näher erläutert.

5.1 Abgrenzung und Überblick

Eine „Trusted Platform“ bedeutet übersetzt eine „vertrauenswürdige Plattform“ und setzt sich somit aus den zwei Begriffen Vertrauen und Plattform zusammen. Die TCG versteht unter einer *Plattform* im weitesten Sinne eine rechnende Einheit, die üblicherweise mit anderen Einheiten kommuniziert. Vertrauen hingegen ist ein relativ komplexer Begriff und beinhaltet verschiedene Ansätze, die sich auf Verhaltens- und Sozialkomponenten zurückführen lassen. Einerseits sammelt und unterstützt eine Trusted Platform die Beweise des Verhaltens dynamisch, um über die Vertrauenswürdigkeit einer Plattform Auskunft zu geben. Andererseits tragen Trusted Platforms dazu bei, die soziale Komponente von Vertrauen zu steigern, indem die Vertrauenswürdigkeit über die korrekte Implementierung und Operation von vertrauenswürdigen Plattformen versichert wird.[150] Die TCG definiert *Vertrauen* in Anlehnung an den dritten Teil der Common Criteria als etwas, „if it always behave in the expected manner fort he intended purpose“.[151] Eine Trusted Platform ist folglich eine Plattform mit einer vertrauenswürdigen Komponente in Form einer eingebauten Hardware, die diese als Grundlage für Vertrauen von Softwareprozessen nutzt.[152] Überdies ermöglichen vertrauenswürdige Plattformen einer Entität die aktuelle Softwareumgebung

[150] Vgl. Pearson, S. et. al. (2002), S. 9 ff.

[151] Vgl. Pearson, S. et. al. (2002), S. 10

[152] Vgl. Pearson, S. et. al. (2002), S. 5

einer Plattform festzustellen und Daten an eine bestimmte Softwareumgebung in der Plattform zu versiegeln.[153]

Damit eine Entität entscheiden kann, ob sie einer Plattform vertrauen kann, spezifiziert die TCG Messmethoden und Wege für Messmethoden, um ihre Vertrauenswürdigkeit zu zeigen. Dabei existieren zwei Wurzeln der Vertrauenswürdigkeit, nämlich das „Roots of Trust for Measurement“ (RTM) und das „Roots of Trust for Reporting“ (RTR).

Das RTM startet die Messprozesse über den Weg, wie die Plattform arbeitet. Zudem kann es je nach Plattformtyp variieren, entspricht aber der gesamten Plattform selbst. Dabei ist es notwendig ein Kernelement zu haben, dem absolut vertraut werden kann, was im Falle der PC-Implementierung dem „Core Root of Trust for Measurement“ (CRTM) entspricht. Es besteht aus kritischem und essentiellem Code, z.B. innerhalb des BIOS selbst, und startet einige Messungen über die Komponenten der Recheneinheit.

Das RTR entspricht dem „Trusted Platform Module“ (TPM) und speichert die Ergebnisse der Messprozesse. Dabei berichtet das TPM verschlüsselt die momentanen Messwerte und verhindert die Freigabe von Geheimnissen, wenn die neuen Messwerte nicht mit den gespeicherten übereinstimmen. In der Regel ist das TPM ein völlig passiver manipulationssicherer Chip, der Messwerte zur Verfügung stellt.[154]

5.2 Grundkonzept von vertrauenswürdigen Plattformen

Einen generellen Ausblick über das Grundkonzept vertrauenswürdiger Plattformen verschafft *Abbildung 16*.

---

[153] Vgl. TCG Main Specification Version 1.1b, S. 2

[154] Vgl. Pearson, S. et. al. (2002), S. 10 f.

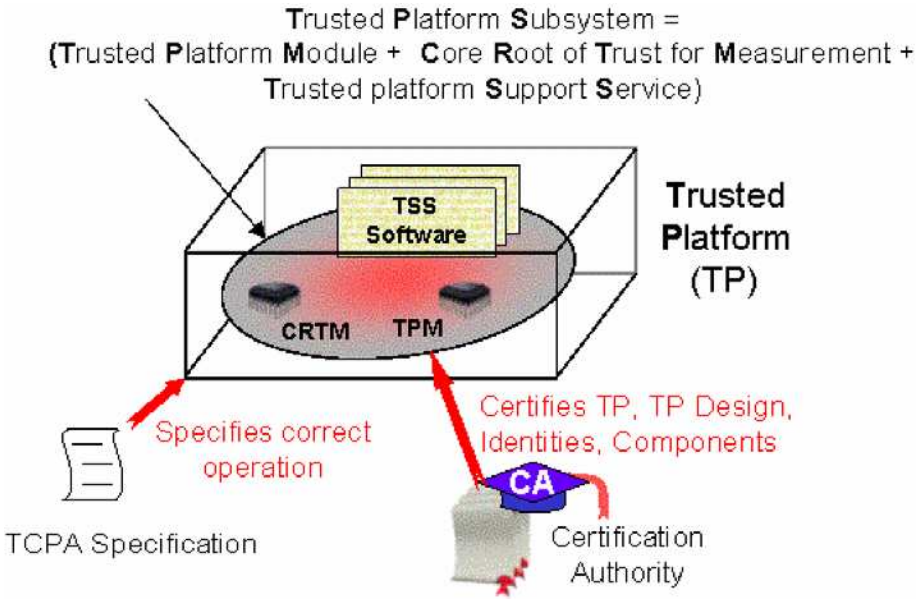

Abbildung 16: Generelles Modell vertrauenswürdiger Plattformen[155]

Vertrauenswürdige Plattformen bestehen demzufolge aus drei Komponenten, die durch die Spezifikationen der TCG definiert werden. Der eigentlich Hardwareteil ist das „Trusted Platform Module“ (TPM) und bildet die Hauptkomponente in den Spezifikationen. Das „Core Root of Trust for Measurement“ (CRTM) ist die erste Software, die während des Bootprozesses startet und physikalisch im TPM fixiert werden kann, was allerdings nicht zwingend vorgeschrieben ist. Die „Trusted Computing Group Software Stack“ (TSS) unterstützt verschiedene Funktionen, die zur Kommunikation mit der Plattform und anderen notwendig sind. Die beiden Komponenten CRTM und TSS unterstützen folglich nur das TPM, weshalb das TPM als Kernelement in dieser Arbeit im Mittelpunkt steht. Zusätzlich zum Trusted Subsystem werden „Certification Authorities“ (CA) bei der Verwendung von Trusted Platforms eingebunden, um für deren Echtheit zu bürgen.[156] Darüber hinaus bürgen diese Zertifizierungsinstanzen für das TP Design, das TPM, Identitäten und Komponenten der vertrauenswürdigen Plattform.[157]

---

[155] Vgl. Pearson, S. (2002), S. 6

[156] Vgl. Pearson, S. et. al. (2002), S. 7 f.

[157] Vgl. Pearson, S. et. al. (2002), S. 59 ff.

5.2.1 Root of Trust for Measurement (RTM)

Vom „Roots of Trust for Measurement“ (RTM) wird überhaupt erst Vertrauen in die Messprozesse bestätigt. Um diese Ebene des Vertrauens zu bieten, beinhaltet das RTM viele Komponenten. Dabei beinhaltet das RTM eine Kernkomponente, auf deren Integrität das Vertrauen in alle Messungen basiert. Dieses Kernelement ist das „Core Root of Trust for Measurement“ (CRTM) von der die Plattform ihren zuverlässigen Zustand ausführt.[158] Das RTM Programm ist grundsätzlich das erste Programm, welches auf der Plattform ausgeführt wird, um die Ausführung bedenklicher Software zu verhindern. Überdies sollte ein RTM folgende Fähigkeiten aufweisen:[159]

- Ausdrückliche Ausführung nur von den Programmen, für welche die Entität sich für das RTM verbürgt.
- Standhaltung von Softwareattacken und Formen physischer Angriffe, die durch das Schutzprofil der Plattform inbegriffen sind.
- Exaktes Messen von mindestens einer metrischen Integrität, welche die Softwareumgebung der Plattform abbildet.
- Exakte Erfassung gemessener Integritätsmetriken zu einem TPM.
- Aufnahme von Details des Messprozesses und aller Integritätsmetriken zum Messspeicher der Trusted Platform.

5.2.2 Trusted Computing Group Software Stack (TSS)

Das „Trusted Computing Group Software Stack“ bietet eine standardisierte Softwareschnittstelle, um die sicherheitsrelevanten Funktionen des TPM und die Entwicklung von Anwendungen sowie die Kompatibilität über unterschiedliche Plattformtypen ansteuern zu können. Darüber hinaus stellt die TSS Programmierschnittstellen für Anwendungen wie PKCS#11 und MSCAPI basierende Anwendungen

---

[158] Vgl. TCG Main Specification Version 1.1b, S. 3

[159] Vgl. Pearson, S. et. al. (2002), S. 62 f.

sowie Bibliotheken für Gerätetreiber zur Verfügung. Die Konzeptionsziele der TSS sind primär:[160]

- Anbieten eines Eingangspunktes für Anwendungen, um die Funktionen des TPM anzusprechen.
- Bereitstellung eines synchronisierten Zugangs zum TPM.
- Verbergen bildender Befehlsströme mit zugehöriger Byteanordnung und Ausrichtung an den Anwendungen.
- Steuerung der TPM Ressourcen.
- Veröffentlichung von TPM Ressourcen, wenn notwendig.

Eine Zusammenfassung über die Architektur der TSS folgt in *Abbildung 17* dargestellt. Der TPM-Gerätetreiber wird typischerweise vom TPM-Hersteller zur Verfügung gestellt und arbeitet im Kernelbetrieb, wo er auch geladen wird. Dabei sind die TPM-Gerätetreiber vom TPM-Hersteller und Betriebssystem bestimmt und haben zusätzliche Funktionen wie die Stromverwaltung der jeweiligen Plattform. Ausführungen des Nutzerbetriebes haben keine direkten Rechte auf Ausführungen im Kernbetrieb. Der Nutzerbetrieb setzt sich wiederum aus System- und Nutzerprozessen zusammen. Teil des Systemprozesses ist die TCG-Gerätetreiber-Bibliothek, welche den Übergang vom Kernel- zum Nutzerbetrieb bildet und vom Hersteller hinterlegt wird. Die TSS hat überdies exklusiv die Rechte an den Gerätetreibern, d.h. keine andere Anwendung hat zusätzliche Verbindungen zum TPM außer der TSS. Die TSS-Kerndienste kommunizieren mit dem TPM über eine Schnittstelle, welche von der TCG-Gerätetreiber-Bibliothek bereitgestellt wird. Diese Kerndienste besitzen einfache und erweiterte Module für die Schlüsselverwaltung und effiziente Regelungen der begrenzten Ressourcen des TPM. Dabei ist die Schnittstelle der TSS-Kerndienste elementar gestaltet, damit einfache Techniken zur Kontrolle und Anfragedienste das TPM prägen. Den Übergang zu den TSS-Dienstanbietern bildet die Schnittstelle der TSS-Kerndienste, welche dem Wechsel vom System- zum Nutzerprozess darstellen. Die-TSS Dienstanbieter sind Module auf höchster Ebene, die durch objekt-orientierte Schnittstellen für Anwendungen die Ressourcen einer Platt-

---

[160] Vgl. TCG Software Stack Specification Version 1.1, S. 11

form beanspruchen. Ferner haben TSS-Dienstanbieter die Möglichkeit auf TSS-Kerndienste, wie z.B. Schlüsselmanagement, zurückzugreifen. Ein spezielles Modul ist der RPC-Server, der die Funktionen und Daten der TSS-Kerndienste von einer Plattform zur anderen fördert.[161]

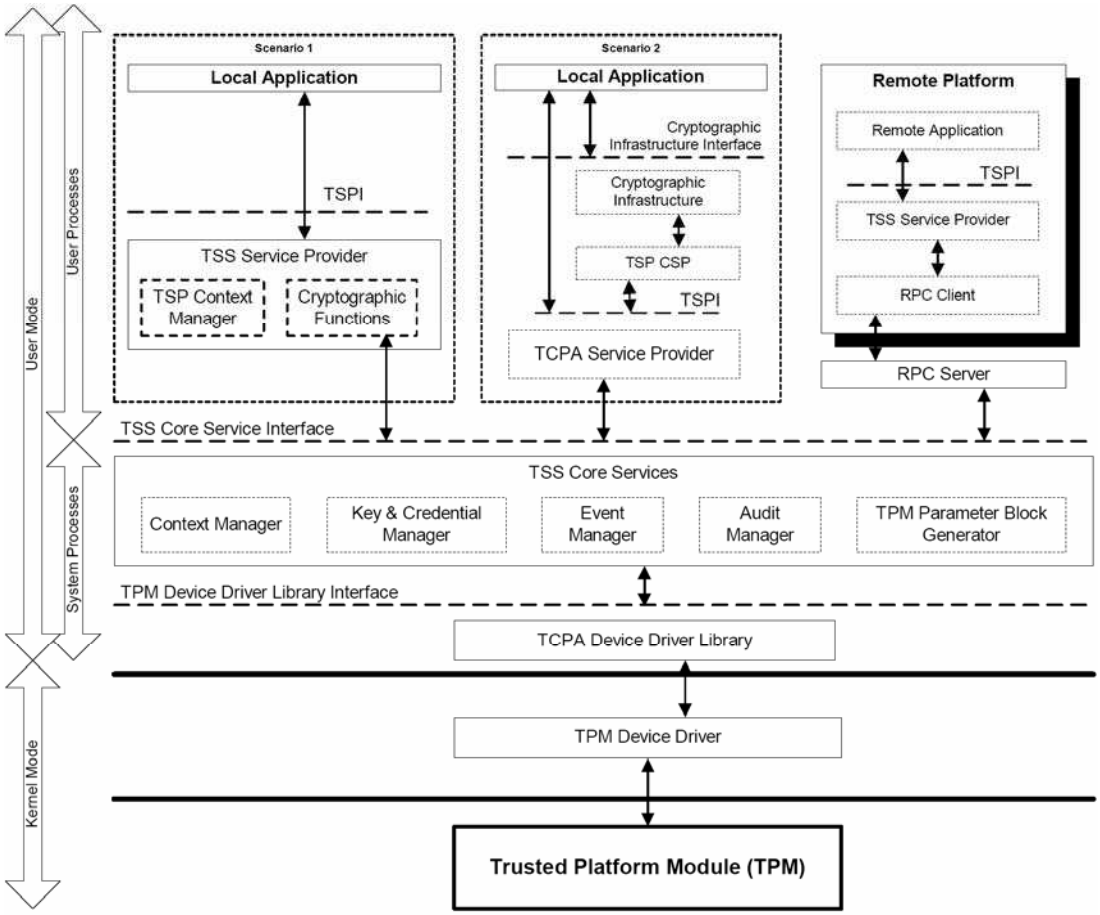

Abbildung 17: TSS Architektur[162]

5.3 Das Trusted Platform Module (TPM)

Das „Trusted Platform Module“ (TPM) kann auf den ersten Blick als eine erweiterte Smart Card angesehen werden, die als spezieller Hardwarechip innerhalb einer vertrauenswürdigen Plattform implementiert ist.[163] Die Kosten des TPM sollen in der Herstellung relativ gering sein, was auch den minimalistisch gehaltenen Funktionsumfang erklärt. Um dennoch einen Kompromiss zwischen Kosten und Nutzen zu

---

[161] Vgl. TCG Software Stack Specification Version 1.1, S. 16

[162] Vgl. TCG Software Stack Specification Version 1.1, S. 17

[163] Vgl. Pearson, S. et. al. (2002), S. 58

schaffen, spezifiziert die TCG eine Mindestforderung der Vertrauenswürdigkeitsstufe 3 nach der Common Criteria.[164] Die Vertrauenswürdigkeitsstufe 3 (EAL 3) ist methodisch getestet sowie überprüft und schafft Vertrauenswürdigkeit durch eine Analyse des Entwurfs des TOE auf hoher Ebene, um das Sicherheitsverhalten zu erfassen.[165] Um den physischen Schutz zu gewährleisten, verlangt die Spezifikation die Anlehnung an die FIPS 140-2, welche auf der zweiten Ebene eine Platzierung von Siegeln oder Schichten als Beweis zur Manipulation verlangt.[166] Somit gewährleistet die FIPS 140-2 das ordnungsgemäße Arbeiten der kryptographischen Einheit.[167]

Überdies bildet das TPM die Wurzel des Vertrauens für das Berichten der Messungen, das „Root of Trust for Reporting“ (RTR), und die Wurzel des Vertrauens für geschützte Speicherung, das „Root of Trust for Storing“ (RTS). Das TPM sollte nach Pearson folgende Ansprüche erfüllen:[168]

- Standhalten jeglicher Form von Softwareangriffen und physischen Angriffen, die durch das Schutzprofil der Plattform inbegriffen sind.
- Empfang und Speicherung der gemessenen Integritätsmetriken.
- Bereitstellung von Auszügen aller Sequenzen von den gebildeten Integritätsmetriken.

5.3.1 Root of Trust for Reporting (RTR)

Das „Root of Trust for Reporting“ (RTR) ist verantwortlich für die Herstellung von Plattform Identitäten, das Berichten der Plattformkonfiguration, den Schutz berichteter Werte und die Herstellung des Bezugs der Attestierung von berichteten Werten. Dabei teilt das RTR die Verantwortung von geschützten Messauszügen in Interaktion mit dem RTS. Diese Interaktion ist als kritisch zu sehen, da sie einem Angreifer die Möglichkeit gibt, extern den Datenfluss zu beobachten. Aus diesem Grund emp-

---

[164] Vgl. Pearson, S. et. al. (2002), S. 229

[165] Vgl. Gemeinsame Kriterien Version 2.1 (1999), S. 62

[166] Vgl. Pearson, S. et. al. (2002), S. 229 f.

[167] Vgl. TCG TPM Specification Version 1.2 (2003a), S. 63

[168] Vgl. Pearson, S. et. al. (2002), S. 63

fiehlt die TCG die beiden Komponenten in eine Einheit zu implementieren, ohne externe Busse.[169]

Das RTR hat als eindeutige kryptographische Identität den „Endorsement Key“ (EK) an sich gebunden, der als Kennzeichnung dient und die Echtheit eines individuellen TPM beweist. Die Erstellung des EK in das TPM kann in der Praxis sowohl extern als auch intern geschehen. Die externe Implementierung erfolgt in einer sicheren Umgebung, in der vorher der EK erzeugt und während der Produktion eingefügt wird. Entsprechend resultiert die interne Erstellung des EK nach einem Kommando im TPM selbst.[170] Der EK dient nur zur Einführung des TPM Eigentümers und zur Herstellung der „Attestation Idendity Keys“ (AIK) und deren Verifikation eingesetzt. Zudem ist der EK transitiv über das TPM an die Plattform gebunden, was in *Abbildung 18* dargestellt wird.[171]

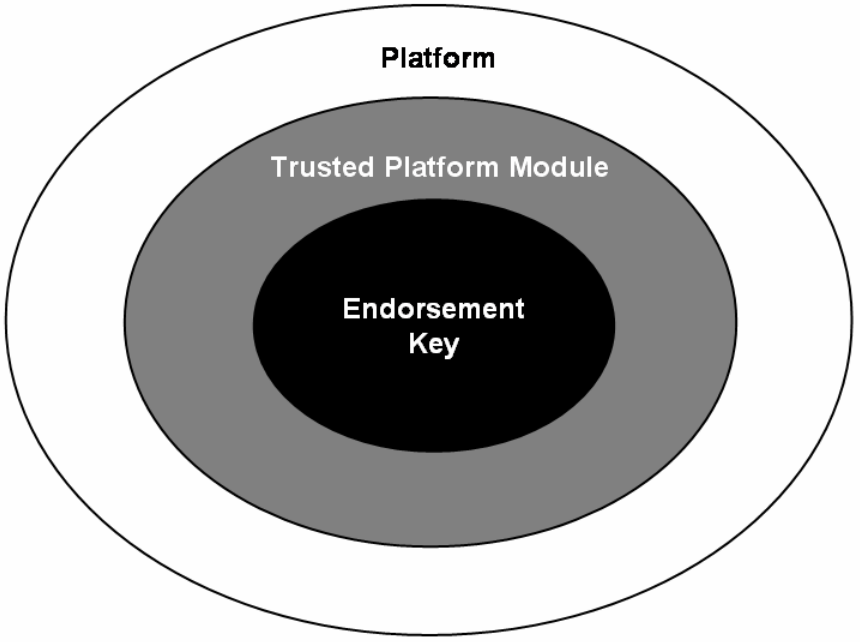

Abbildung 18: Transitive Bindung des EK an die Plattform über das TPM[172]

Der EK ist an ein einziges TPM gebunden, wobei der private Schlüssel das TPM nie verlässt. Ein TPM ist überdies immer an eine Plattform gebunden. Aus diesem Zu-

---

[169] Vgl. TCG TPM Specification Version 1.2 (2003a), S. 44

[170] Vgl. Pearson, S. et. al. (2002), S. 69

[171] Vgl. TCG TPM Specification Version 1.2 (2003a), S. 44 f.

[172] Eigene Darstellung

sammenhang lässt sich aufgrund von Transitivität schließen, dass der EK auch immer an eine Plattform gebunden ist:[173]

$$EK \rightarrow TPM \ , \ TPM \rightarrow Plattform \Rightarrow EK \rightarrow Plattform$$

Über den eindeutigen EK und den daraus entstandenen AIK-Identitäten ist es allerdings auch möglich Ansammlungen von Aktivitäten aufzuzeichnen, was wiederum datenschutzrechtliche Bedenken aufwirft. Um dies zu verhindern, unterstützt die Spezifikation das Benutzen von domänenspezifischen AIKs, die vom Plattformeigentümer kontrolliert werden und unterbindet die Nutzung des EK. Ein AIK ist ein asymmetrisches Schlüsselpaar, welches von einem 2048 Bit RSA-Schlüssel erstellt wird. Der AIK ist im Grunde nichts anderes als ein Pseudonym für den plattformspezifischen EK, von dem durch das TPM beliebig viele AIKs erstellt werden können. Allerdings zwingt das TPM den AIK nur zur Signatur von Daten, die auch vom TPM generiert worden sind, d.h. der AIK bietet keine Verschlüsselung. TPM generierte Daten stammen beispielsweise aus dem „Platform Configuration Register“ (PCR).[174] Das PCR ist Teil des flüchtigen Speichers des RTS mit mindestens 16 abgeschirmten Speicherstellen, welche jeweils über 160 Bit innerhalb des TPM verfügen.[175] Um einen AIK zu erzeugen und den Berechtigungsnachweis zu aktivieren wird die Autorisierung des TPM Eigentümer benötigt. Allerdings müssen AIKs nicht innerhalb des TPM gespeichert werden, sondern es genügt die Speicherung außerhalb, solange diese verschlüsselt sind und die Integrität geschützt ist. Die AIKs sind hingegen nur durch das TPM nutzbar.[176]

5.3.2 Root of Trust for Storing (RTS)

Das „Root of Trust for Storage“ (RTS) bildet die zweite Wurzel des Vertrauens eines TPMs und stellt den Schutz der benutzten Daten des TPM bereit, die außerhalb in externen Speichergeräten gehalten werden. Die Anspruchnahme des Eigentums eines TPMs ist der Prozess ein gemeinsam benutztes Geheimnis in eine TPM abgeschirmte

---

[173] Vgl. TCG TPM Specification Version 1.2 (2003a), S. 45

[174] Vgl. TCG TPM Specification Version 1.2 (2003a), S. 45 f.

[175] Vgl. TCG TPM Specification Version 1.2 (2003a), S. 21 f.

[176] Vgl. TCG TPM Specification Version 1.2 (2003a), S. 45 f.

Speicherstelle einzufügen.[177] Allgemein unterscheidet Pearson zwischen abgeschirmten Speicherstellen und geschützten Prozessen. Ein geschützter Prozess ist eine einwandfreie Operation, bei der es notwendig ist, dass der Plattform vertraut werden kann. Geschützte Prozesse haben bevorzugten Zugang zu abgeschirmten Speicherstellen. Hingegen sind abgeschirmte Speicherstellen Bereiche, in denen Daten gegen Störungen und Beobachten geschützt sind.[178] Grundsätzlich können verschiedene Personen lokal sowie per Fernzugriff auf eine Plattform zugreifen, welche sich bezüglich ihrer Zugriffsrechte unterscheiden, wie *Abbildung 19* illustriert.

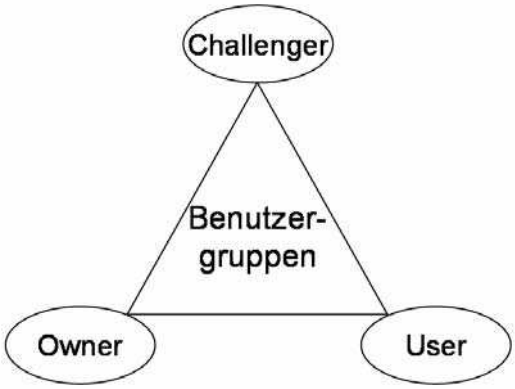

Abbildung 19: Benutzergruppen[179]

Die elementarste Person einer vertrauenswürdigen Plattform ist der TPM Eigentümer, auch „Owner" genannt, da alle Operationen durch ihn oder seine Autorisierung ausgeführt werden können. Der Eigentümer besitzt exklusive Rechte das TPM zu aktivieren, wobei die Autorisierung das TPM zu nutzen durch physische Präsenz bei der Plattform oder durch ein geteiltes Geheimnis, zuzüglich kryptographischer Techniken sichergestellt wird.[180] Die Entität, welche die Plattform nutzt, ist der „User", wobei der Benutzer einer Plattform durchaus User und Owner in einer Person sein kann. Im System der TCG ist der „Challenger" die Entität, welche Auskunft über den Zustand der Plattform wünscht, um ihr vertrauen zu können. Ein Challenger kann erneut auch User oder Owner sein.

---

[177] Vgl. TCG TPM Specification Version 1.2 (2003a), S. 47

[178] Vgl. Pearson, S. et. al. (2002), S. 66

[179] Eigene Darstellung

[180] Vgl. Pearson, S. et. al. (2002), S. 95 ff.

Jede Entität ist TPM Eigentümer, welche das gemeinsam genutzte Geheimnis kennt. Gleichzeitig wird mit der in Anspruchnahme des Eigentums eines TPMs ein neuer „Storage Root Key“ (SRK) für die geschützte Speicherung von Daten und ein neuer Prüfwert für das TPM eingeführt. Der Beweis des Eigentümers erfolgt über die Aufforderung, ein gemeinsam bekanntes Geheimnis zu überprüfen.[181] Somit bietet das RTS Vertraulichkeit und Integrität für externe „Blobs“. Blobs sind geschützte Objekte des TPM und bestehen aus „Klumpen“ von Daten oder Schlüsseln. Eine Freigabe der Informationen findet dabei nur in einer genannten Umgebung statt, dessen Werte vom PCR spezifiziert werden. Geschützte Daten des RTS können darüber in ein anderes TPM migriert werden. Die Anzahl und Größe der Werte, die vom RTS gehalten werden, sind nur von der verfügbaren Speichergröße der Plattform abhängig.[182]

5.3.3 TPM Architektur

Das TPM unterstützt als Mindestanforderung die Algorithmen RSA, SHA-1 und HMAC, wobei auch DSA oder Elliptic-Curve unterstützt werden können. Alle verfügbaren Algorithmen und Protokolle müssen allerdings im TPM und im Berechtigungsnachweis der Plattform einbezogen sein. Gründe für die Spezifizierung der Algorithmen sind einerseits die Definition einer Basis an Algorithmen für die Kompatibilität und andererseits die Identifizierung passender Schlüsselgrößen und deren sicherer Gebrauch in Protokollen. *Abbildung 20* zeigt die wichtigen Komponenten eines TPM.[183]

---

[181] Vgl. TCG TPM Specification Version 1.2 (2003a), S. 27

[182] Vgl. TCG TPM Specification Version 1.2 (2003a), S. 47

[183] Vgl. TCG TPM Specification Version 1.2 (2003a), S. 11

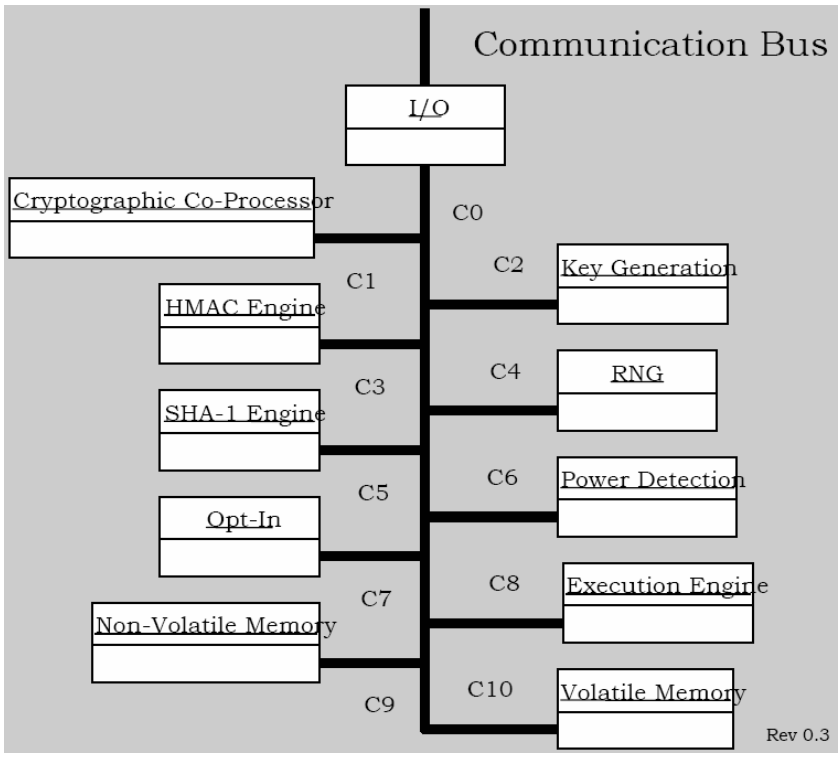

Abbildung 20: Komponenten der TPM Architektur[184]

C0 in der obigen Abbildung zeigt die *Input/Output-Komponente*, welche den Informationsfluss über den Kommunikationsbus regelt. Dabei werden Protokolle passend für die Kommunikation über externe und interne Busse ver- und entschlüsselt. Darüber hinaus steuert die I/O-Komponente die Meldungen an die entsprechenden Komponenten. C1 zeigt den *kryptographischen Koprozessor* der Operationen wie asymmetrische Schlüsselgeneration, asymmetrische und symmetrische Ver- bzw. Entschlüsselung, Hashing sowie Generierung von Zufallszahlen ausführt. Diese Ressourcen des TPMs unterstützen die Generierung von Zufallsdaten, Signatur und die Vertraulichkeit in gespeicherte Daten. Alle Speicherschlüssel und „Attestation Identity Keys“ (AIK) müssen dabei eine Mindeststärke von 2048 Bit RSA oder größer aufweisen. C2 weist die *Schlüsselgenerierung* im TPM auf, in dem RSA Schlüsselpaare sowie symmetrische Schlüssel generiert werden. Die Schlüsselgenerierung ist generell eine geschützte Funktion, wobei der private Schlüssel in einer abgeschirmten Stelle gespeichert wird. Die *HMAC-Engine* wird durch C3 in der Abbildung dargestellt und beweist die Kenntnis und Echtheit ankommender Abfragen der Autorisierungsdaten. Bei der Berechnung der HMAC-Parameter wird eine Schlüssellänge von 20 Byte und eine Blockgröße von 64 Byte verlangt. Die Komponente *„Random*

[184] Vgl. TCG TPM Specification Version 1.2 (2003a), S. 11

Number Generator" (RNG) wird durch C4 abgebildet und ist ausschliesslich für die Generierung von Zufallszahlen verantwortlich. Das TPM nutzt diese Zufallszahlen für Nonces, Schlüsselgenerierung und Zufälligkeit bei Signaturen.[185] Ein Nonce ist ein Zufallswert mit der Länge von 20 Byte zum Schutz von Wiederholungen und anderen Angriffen.[186] Die *SHA-1 Engine*, dargestellt durch C5, ist die Ressource für den Hash-Algorithmus im TPM, welche unter anderem die Messungen während des Bootprozesses unterstützt. Zudem ist das Ergebnis eines SHA-1 Algorithmus 160 Bit lang. C6 zeigt die Komponente der „*Power detection*", welche den Leistungszustand des TPM in Verbindung mit der Plattform festlegt. Die C7 Komponente *Opt-In* stellt Mechanismen und Absicherungen bereit, um ein TPM ein-/auszuschalten, de-/aktivieren oder freizugeben/sperren. Dabei kann das TPM acht verschiedene Betriebsmodi annehmen, wie *Abbildung 21* zeigt, welche dementsprechend die mögliche Auswahl an Anwendungsszenarien darstellt.

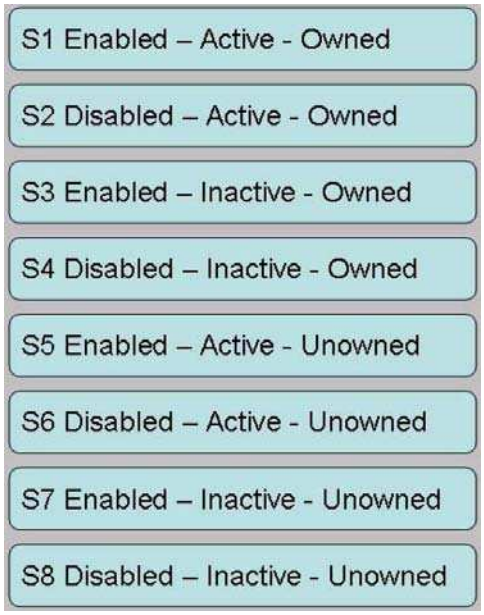

Abbildung 21: Die acht Betriebsmodi des TPM[187]

S1 bildet dabei den vollen Umfang aller TPM Funktionen ab, wohingegen bei S8 alle Funktionen des TPM ausgeschaltet sind, bis auf die Funktion den Zustand zu ändern.[188] Außerdem berichtet das TPM immer über seine Ressourcen und führt Selbst-

---

[185] Vgl. TCG TPM Specification Version 1.2 (2003a), S. 11 ff.

[186] Vgl. TCG TPM Specification Version 1.2 (2003b), S. 22

[187] Vgl. TCG TPM Specification Version 1.2 (2003a), S. 11

[188] Vgl. TCG TPM Specification Version 1.2 (2003a), S. 35 f.

tests durch.[189] Des Weiteren hält die Opt-In Komponente den Zustand von persistenten sowie flüchtigen Bitschaltern. Das Setzen der Schalter erfordert die Autorisierung des TPM Eigentümers oder die physische Präsenz bei der Plattform. Der Hersteller bestimmt dabei die Methoden, welche bei der physischen Präsenz angewendet werden müssen, um diesen Status zu erreichen. Hintergrund der physischen Präsenz ist die Verhinderung von Fernzugriffen auf das TPM, welche z.B. beim Einschalten einer Plattform notwendig ist.[190] Die physische Präsenz ist ein Signal von der Plattform an das TPM, welche direkte Interaktion einer Person mit der Plattform impliziert, bevor ein Kommando ausgeführt wird. Spezielle Sonderrechte, wie z.B. Löschen des jetzigen Eigentümers eines TPM, temporäres Deaktivieren oder Sperren eines TPM, benötigen physische Präsenz.[191] Dieses Signal kann durch die Betätigung eines Schalters, durch Drücken einer Taste auf der Tastatur oder durch das Setzen eines Jumpers geschehen. Die Umsetzung wird allerdings nicht zwingend von der TCG vorgeschrieben.[192] C8 bildet die Komponente *„Execution Engine“* ab, welche den Programmcode startet, um TPM Kommandos auszuführen, die von der Input-/Output Komponente empfangen wurden. Dabei stellt die Komponente die Isolation der Operationen sowie die Abschirmung und den Schutz der Speicherstellen sicher. C9 der *Abbildung 20* zeigt die abgeschirmte Komponente *„Non-Volatile Memory“*, die zur Speicherung persistenter Identitäten und Zustände des TPM benutzt wird. Der permanente Speicher beinhaltet Daten wie z.B. den „Endorsement Key“ (EK), ist für die Zuordnung zuständig und wird von Entitäten benutzt, die vom TPM Eigentümer autorisiert worden sind. Zusätzlich befindet sich im abgeschirmten permanenten Speicher des TPM das „Data Integrity Register“ (DIR), dessen Kommandos im Versionswechsel der Spezifikationen von Version 1.1b auf 1.2 stillgelegt worden sind. Trotzdem muss Platz für mindestens ein DIR geschaffen werden, welches Werte von 160 Bit halten muss.[193] C10 in *Abbildung 20* illustriert die *„Volatile Memory“* Komponente im TPM und besteht aus mindestens 16 PCRs mit jeweils 160 Bit. Die PCRs bewahren dabei die Anordnung der Messungen bei, deren Identifizierung über

---

[189] Vgl. Pearson, S. et. al. (2002), S. 99

[190] Vgl. TCG TPM Specification Version 1.2 (2003a), S. 17 ff.

[191] Vgl. TCG TPM Specification Version 1.2 (2003a), S. 42 f.

[192] Vgl. TCG TPM Specification Version 1.2 (2003a), S. 121

[193] Vgl. TCG TPM Specification Version 1.2 (2003a), S. 19

einen Index stattfindet. Dabei ist es möglich eine unbegrenzte Anzahl an Messungen in einem PCR über kumulierte Hashwerte zu speichern.[194] Zudem ist es möglich in diesem Abschnitt zehn Spalten mit RSA Schlüsselpaaren temporär zu speichern. Da die Möglichkeit bestehtbeliebig viele chiffrierte Schlüssel extern zu speichern, können diese bei erneutem Gebrauch in den Speicher geladen werden. Daneben werden „key handles“ im volatilen Speicher abgelegt, welche geladenen Schlüsseln temporäre Namen geben, damit nachfolgende Kommandos am richtigen Schlüssel ausgeführt werden, wenn mehrere Schlüssel geladen sind. Ebenso werden „authorization session handles“ volatil gespeichert, um den Autorisierungszustand der Daten über mehrere Plattformen zu identifizieren. Die Sitzungen der Autorisierung werden durch die beiden Protokolle„Object Independent Authorization Protocol“ (OIAP) und „Object Specific Authorization Protocol“ (OSAP) erstellt.[195] Das OIAP erlaubt den Austausch eines Nonce, der 160 Bit zufällig erstellter Daten entspricht, mit einem speziellen TPM. Sobald die Sitzung aufgebaut ist, kann der Nonce zur Autorisierung der Nutzung jeder Entität angewendet werden, welche vom TPM gesteuert wird. Die Sitzung kann unbegrenzt leben, bis eine Seite die Sitzung beendet.[196] Indessen baut ein OSAP mit Hilfe eines Nonce die Sitzung nur zu einer Entität auf. Überdies ist die OSAP Sitzung an ein bestimmtes TPM Objekt gebunden. Dazu benutzt die Sitzung ein kurzlebiges Geheimnis aus HMAC in Verbindung mit den Autorisierungsdaten des Zielobjektes im Austausch mit dem Nonce am Anfang der Sitzung. Die Sitzung wird entweder von einer Seite beendet oder vom TPM nach Benutzung des kurzlebigen Geheimnisses erzwungen, wenn neue Autorisierungsdaten eingesetzt wurden.[197]

5.3.4 TPM Funktionalitäten

Die Funktionalitäten des TPM sind in vier Kategorien einteilbar, die folgend näher erläutert werden:

- Integrität,
- Geschützter Speicher,

---

[194] Vgl. TCG TPM Specification Version 1.2 (2003a), S. 21 f.

[195] Vgl. Safford, D. (2003)

[196] Vgl. TCG TPM Specification Version 1.2 (2003a), S. 49 f.

[197] Vgl. Pearson, S. et. al. (2002), S. 107 f.

- Identität sowie
- Sicheres Booten und authentifizierte Bootprozesse.

5.3.4.1 Integrität

Ein vertrauensvoller Weg Informationen über ein System zu sammeln und zu speichern, lässt sich mittels Speicherung und Auszügen aus Messinformationen realisieren, was als Integritätsmetriken benannt wird. Integritätsmessungen stützen somit Beweise über das Verhalten einer Plattform. Zusätzlich wird das Vertrauen durch soziale Mechanismen, insbesondere Berechtigungsnachweise in Form von Zertifikaten, weiter gesteigert.[198] Diese Integritätsmetriken werden dann in den PCRs von den Messagenten des RTM abgelegt, welche Informationen der ganzen Plattform messen. In die PCRs werden dann die Summen aller Messergebnisse in Form von Integritätsmetriken in der Länge eines SHA-1 Auszuges geschrieben, wobei auch die Reihenfolge festgelegt ist. Dies birgt den Vorteil eine unendliche Anzahl an Ergebnissen in ein einziges Register zu speichern, wobei kein Messergebnis abgelegt werden muss, um Platz für neue Messergebnisse zu machen.[199] Gleichzeitig protokollieren das RTM und die zugehörigen Messagenten die Messungen in einen ungeschützten Speicher. Das Protokoll beinhaltet eine Beschreibung der gemessenen Entität und einer entsprechender Integritätsmetrik, welche im TPM aufgezeichnet wurde. Zudem kann das Protokoll den Wert jeder Sequenz der Integritätsmetriken reproduzieren. Die Messauszüge sind dabei mit den existierenden Inhalten der PCR über die resultierenden Daten der Hash-Prozesse verknüpft. Das PCR befindet sich überdies in einer abgeschirmten Speicherstelle und wird folgend genutzt:[200]

- Beweisen des Zustandes der Rechnerumgebung durch Integritätssignatur der Daten zu einer bestimmten Zeit. Das TPM verknüpft Auszugsdaten, die aus beliebigen Daten und einen Nonce von einem Dritten bestehen können, mit den PCR-Werten und signiert diese dann, was als Integritätsherausforderung bezeichnet wird.

---

[198] Vgl. Pearson, S. et. al. (2002), S. 137

[199] Vgl. Pearson, S. et. al. (2002), S. 138 ff.

[200] Vgl. Pearson, S. et. al. (2002), S. 138 f.

- Prüfung der Werte, bevor Geheimnisse des geschützten Speichers angezeigt werden.
- Prüfung der Werte, ob der Bootprozess auch wie geplant abläuft.

Damit demnach zuverlässig die aktuelle Hard- und Softwarekonfiguration an lokale und ferne Herausforderer berichtet werden kann, wurde eine Integritätsherausforderung und Integritätsantwort entwickelt, was nichts anderes als ein Challenge-Response Verfahren ist und der Attestierung entspricht. Dieses Verfahren wird auch als dynamische gegenseitige Authentifizierung bezeichnet. Der Herausforderer sendet einen erzeugten Nonce (Challenge) an die Zielplattform und die Antwort (Response) wird nach der Authentisierung des Herausforderers berichtet, sofern dieser zugangsberechtigt ist, die TPM Identität zu nutzen. Daraufhin koordiniert der „Trusted Platform Agent“ (TPA), welcher Teil des OS ist, das Angebot der Integritätsmetriken an den Herausforderer. Das TPM signiert den Nonce und die aktuellen PCR Werte mit einer TPM Identität. Danach nimmt der TPA die Protokolle der gemessenen Software vom Speicher des TPM sowie die Zertifikate der relevanten Speicher und bündelt diese Informationen, um sie zum Herausforderer zu senden. Dieser Vorgang entspricht dann der Integritätsantwort. Demzufolge kann der Herausforderer nach der Antwort entscheiden, ob er der Zielplattform vertraut und mit ihr interagieren will. Dabei trifft der Herausforderer die Entscheidung, da nur er den Zustand der Plattform kennt, welcher genügend Vertrauen für den beabsichtigten Verwendungszweck hat. Zur weiteren Absicherung besteht ein Zeitintervall zwischen dem Beginn und dem Ende einer vertrauenswürdigen Transaktion, das eine entsprechende Anforderung der Integritätsmetriken davor und danach erfordert.[201]

5.3.4.2 Geschützter Speicher

Das TPM ist in der Lage eine unbegrenzte Anzahl an privaten Schlüsseln und anderen Daten sicher außerhalb des TPMs auf einem beliebigen Speichermedium zu speichern. An der Spitze der Schlüsselhierarchie der geschützten Speicherung von Daten steht der „Storage Root Key“ (SRK), ein asymmetrisches 2048 Bit RSA Schlüsselpaar, dessen Privatschlüssel niemals das TPM verlässt, wie *Abbildung 22* zeigt. Al-

[201] Vgl. Pearson, S. et. al. (2002), S. 76 f.

lerdings besteht die Möglichkeit den SRK durch den Systemeigentümer zu löschen.[202]

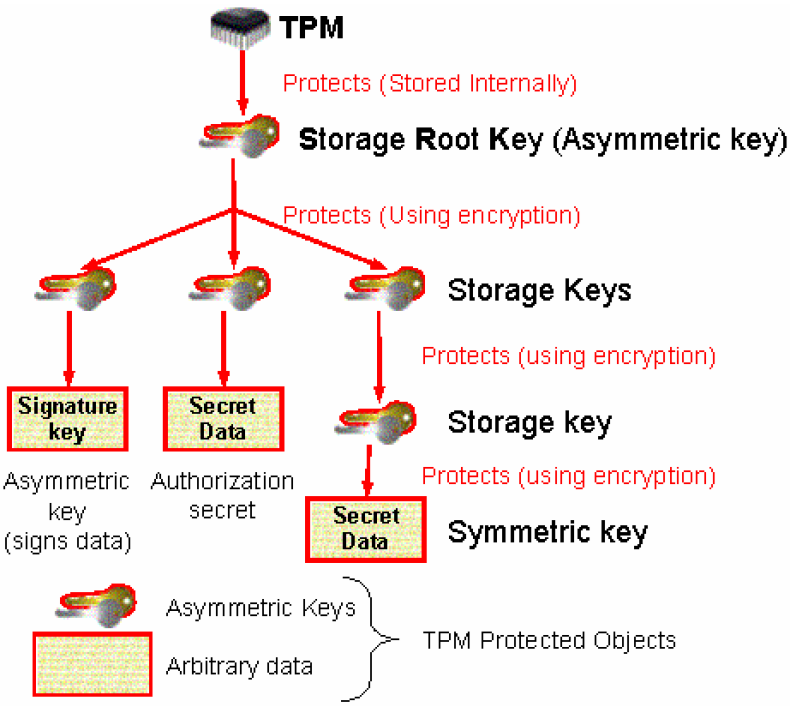

Abbildung 22: Beispiel für eine Hierarchie der Speicherung[203]

Die Speicherung der Daten außerhalb des TPMs ermöglicht eine einfachere Migration von vertraulichen Daten auf eine andere Plattform und die Wiederherstellung nach einer Fehlfunktion der Plattform. Das TPM erzeugt einen „Klumpen“ (Blob) an geheimen Daten, was einer verschlüsselten Datei mit entsprechender Header-Information und Daten in Form eines Schlüssels entspricht. Die Header-Informationen entsprechen dem derselben Größe eines SHA-1 Auszuges von 20 Byte und dienen zur Autorisierung der Daten. Als Geheimnisse kommen beliebige Daten oder ein Schlüssel in Frage, wobei die beliebigen Daten vom TPM exportiert werden können, wohingegen Schlüssel, die innerhalb des TPMs zum Einsatz kommen, nie exportiert werden. Diese können generell zur Chiffrierung oder zur Signatur benutzt werden. Allerdings werden Chiffrierungsschlüssel nicht zur Signatur benutzt, vice versa. Indessen werden nur Schlüssel zur Signatur beliebiger Daten verwendet, die von einer Entität beantragt und autorisiert sind, diese zu nutzen. Dies betrifft auch die AIK zur Signatur einer TPM Identität. Zusätzlich können beliebige Daten im

---

[202] Vgl. TCG Main Specification Version 1.1b, S. 145 ff.

[203] Vgl. Pearson, S. (2002), S. 10

geschützten Speicher explizit als migrierbar oder nicht-migrierbar identifiziert werden, wie *Abbildung 23* darstellt.

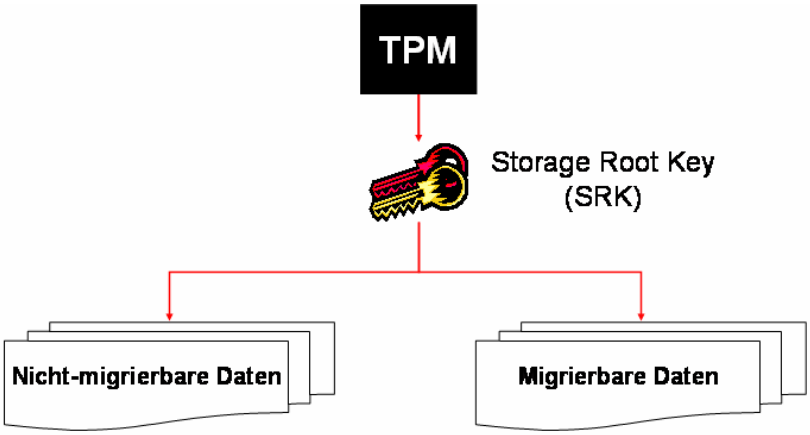

Abbildung 23: Migrierbarkeit und Nicht-Migrierbarkeit von Daten[204]

Jedes TPM enthält einen SRK, der vom TPM auf Anforderung des Eigentümers generiert wurde. Darüber hinaus wird bei der Übernahme des TPMs durch den Eigentümer das Autorisierungsgeheimnis für den Eigentümer sowie für den SRK erstellt und optional noch der öffentliche Teil des SRK an den Eigentümer ausgegeben.[205] Unter dem SRK erstrecken sich nun migrierbare und nicht-migrierbare Schlüssel. Der Migrationsschlüssel (Migration Root Key) befindet sich direkt unterhalb des SRK.[206] Migrierbare Schlüssel haben keine Garantie über ihren Ursprung. Dagegen sind nicht-migrierbare Schlüssel vom TPM erstellt, wo sich auch noch der private Schlüssel befindet.[207] Nicht-migrierbare Daten werden innerhalb des TPMs erstellt und verlassen dieses auch niemals. Jeder migrierbare Schlüssel kann durch den Besitzer jedes migrierten Vorläufers extrahiert werden. Um allerdings Missbrauch migrierter Schlüssel vorzubeugen, ist es möglich den migrierbaren Schlüssel mit einem nicht-migrierbaren Schlüssel zu chiffrieren.[208] Obendrein ist es möglich Daten und Schlüssel an bestimmte PCR Werte zu koppeln oder an ein bestimmtes OS, was

---

[204] Eigene Darstellung

[205] Vgl. Safford, D. (2003)

[206] Vgl. TCG Main Specification Version 1.1b, S. 145 ff.

[207] Vgl. Pearson, S. et. al. (2002), S. 86 f.

[208] Vgl. TCG Main Specification Version 1.1b, S. 145 ff.

über die „Versiegelung“ geschieht. Die Plattform wird also durch das TPM an einen zulässigen Softwarezustand gebunden.[209]

5.3.4.3 Identität

Vertrauensvolle Plattformen unterstützen mehrere Plattform-Identitäten, welche die Nutzung einer Trusted Platform garantieren. Dabei wird die eigentliche Identität des TPMs durch den Endorsement-Key repräsentiert. Allerdings wird der EK zur Erzeugung neuer Pseudonyme, den AIK, benutzt, um den nötigen Datenschutz zu gewährleisten. Dazu wird aber eine vertrauenswürdige Verifizierungsstelle benötigt, welche die Generierung einer Identität durch ein TPM bestätigt. Die Zertifikate dienen der Überprüfung der Echtheit einer vertrauenswürdigen Plattform sowie als Beweis der beglaubigten Identitäten, dessen Durchführung in *Abbildung 24* dargestellt wird.

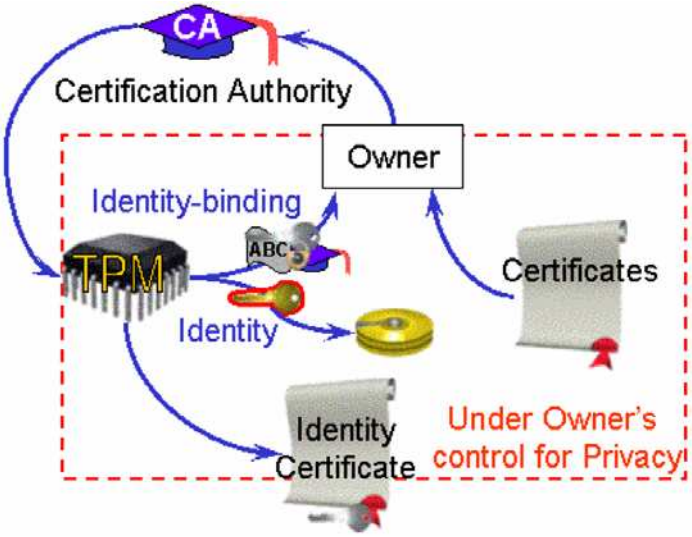

Abbildung 24: Beweis der Echtheit einer vertrauenswürdigen Plattform sowie deren Identitäten [210]

Jede Identität wird durch ein individuelles TPM generiert und durch eine PKI Zertifizierungsinstanz (CA) beglaubigt. Dabei wird jede Identität durch einen asymmetrischen 2048 Bit RSA Schlüssel und eine beliebige textliche Zeichenkette des Eigentümers, welche zur Identifizierung des Pseudonyms dient, zufällig generiert. Schließlich signiert der Eigentümer mit dem EK des TPM die Informationen und sendet diese an die Zertifizierungsinstanz. Diese beweist die Echtheit der vertrauenswürdigen

---

[209] Vgl. Pearson, S. et. al. (2002), S. 159 ff.

[210] Vgl. Pearson, S. (2002), S. 9

Plattform, um die erstellten Identitäten von der Zertifizierungsinstanz beglaubigt zu bekommen.[211]

Die genannten TPM Identitäten sind demnach Plattformidentitäten, in dessen Namen das TPM Daten signieren kann. TPM Identitäten müssen vom Eigentümer durch das TPM generiert und zugänglich gemacht werden. Ein TPM kann dabei mehrere Identitäten besitzen, wobei sich genau eine Zertifizierungsinstanz für Datenschutz für jede dieser Identitäten verbürgt. Überdies können unterschiedliche TPM Identitäten von gleichen oder unterschiedlichen Nutzern gebraucht werden. Die Identitäten werden für Integritätssignaturen, Integritätsherausforderungen und zur Zertifizierung von Beschreibungen anderer Schlüssel in der Plattform verwendet.[212]

In der Spezifikation Version 1.2 wurde zusätzlich die „Direct Anonymous Attestation" (DAA) entwickelt, welche eine direkte Attestierung der Eigenschaften einer Plattform erlaubt ohne die Notwendigkeit eine Zertifizierungsstelle zwischenzuschalten. Die benutzte Technik hierfür ist bekannt als „Zero Knowledge Proof" (ZKP).[213] Das Zero Knowledge Verfahren kann als spezielle Challenge-Response-Technik betrachtet werden.[214] Dabei besteht die Möglichkeit einen Challenger von der Gültigkeit des TPMs überzeugen, ohne den öffentlichen Schlüssel des EK oder einen anderen einzigartigen Bezeichner zu offenbaren. Dazu werden aber DAA-Zertifikate benötigt, welche während der Interaktion mit dem Prüfer über das DAA-Protokoll benutzt werden.[215]

5.3.4.4 Sicheres Booten und authentisierte Bootprozesse

Die TCG Literatur trägt kaum Informationen über sicheres Booten und authentisierte Bootprozesse bei, allerdings werden diese von Hewlett Packard und dem Open-Source Projekt Enforcer namentlich als Funktion erwähnt, weshalb diese hier vorgestellt werden. Inwieweit sicheres Booten und authentifizierte Bootprozesse tatsächlich eingesetzt werden sollen, bleibt infolgedessen abzuwarten. Die Kommandos für

---

[211] Vgl. Pearson, S. (2002), S. 7 f.

[212] Vgl. Pearson, S. et. al. (2002), S. 78 ff. und 121 ff.

[213] Vgl. TCG TPM v1.2 Specifications Changes (2003), S. 4 f.

[214] Vgl. Eckert, C. (2003), S. 384

[215] Vgl. TCG TPM v1.2 Specifications Changes (2003), S. 4 f.

die DIR wurden in den Spezifikationen von Version 1.1b auf 1.2 eingestellt, trotzdem schreibt Version 1.2 zwingend die Implementierung eines DIR vor.[216] Beim authentisierten Booten überprüft das System die aktuelle gebootete Software, indem das RTM zusammen mit dem TPM bei der Aufnahme des Bootprozesses in die PCRs und Messprotokolle kooperiert. Die Plattform kann dazu in jedem beliebigen Zustand kommen, jedoch wird dieser aufgezeichnet und berichtet. Das TPM kann sogar das Booten der Plattform unterbinden, was als sicheres Booten bezeichnet wird, sofern die Software Sequenzen nicht mit speziellen Hashwerten übereinstimmen. Dazu werden die DIR innerhalb des TPM benötigt, die jeder lesen kann, aber Autorisierung des Eigentümers benötigen, um beschrieben zu werden.[217] Während der Bootsequenz vergleicht das RTM die Hashwerte des PCRs mit den erwarteten Hashwerten des DIRs. Stimmen die Werte des PCRs nicht denen des DIRs überein, wird der Bootprozess angehalten und eine Fehlermeldung ausgegeben.[218]

5.4 Implementierung im PC

Die TPM Spezifikation ist grundsätzlich plattform-unabhängig, allerdings hat die TCG Spezifikationen in der Version 1.1 für die gezielte Implementierung in einen PC veröffentlicht, auf die im Folgenden eingegangen wird. Sie dient als Referenzdokument zur Implementierung einer 32 Bit PC Architektur. Das Dokument basiert auf den Hauptspezifikationen in der Version 1.1b und definiert insbesondere:[219]

- Die Nutzung der PCR im Übergang vom Pre-Boot zum Post-Boot Zustand,
- Die Funktionen des CRTM,
- Die TSS und deren Zugang zum TPM,
- Das Leistungsverhalten und Initialisierungszustände,
- Und Richtlinien für die Option ROMs.

---

[216] Vgl. TCG TPM Specification Version 1.2 (2003a), S. 19

[217] Vgl. MacDonald, R.; Smith, S.; Marchesini, J.; Wild, O. (2003a), S. 6

[218] Vgl. Pearson, S. (2002), S. 90 f.

[219] Vgl. TCG PC Specific Implementation Specification Version 1.1, S. 6

Einen kurzen Entwurf über die PC Architektur einer vertrauenswürdigen Plattform gibt *Abbildung 25*. Das CRTM und das TPM sind dabei die einzigen vertrauenswürdigen Komponenten des Motherboards, welche zusammen mit der vertrauenswürdigen Verbindung den „Trusted Building Block“ (TBB) bilden.[220]

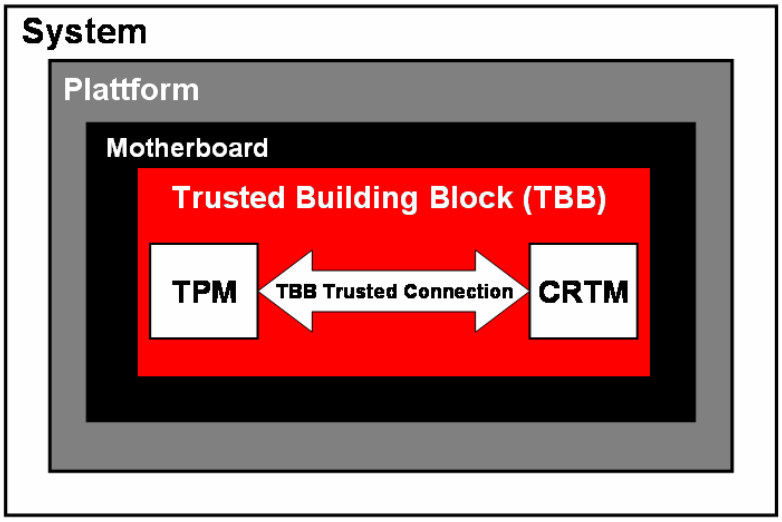

Abbildung 25: Architektur der vertrauenswürdigen Komponenten im PC[221]

Die Verbindung zwischen CRTM und TPM wird durch transitives Vertrauen der beiden Komponenten gewährleistet, wobei das CRTM die Wurzel des Vertrauens bildet. Dazu bildet die Integrität dieser Komponente Basis für das Vertrauen in alle Messungen, wobei das CRTM ein unveränderlicher Teil des Initialisierungscodes der Plattform sein muss, welcher nach der Rücksetzung der Plattform ausgeführt wird. Im Fall der PC-Implementierung kann das CRTM auf zwei Arten eingebaut werden. Einerseits kann das CRTM als „BIOS Boot Block“ (BBB) auftreten, d.h. das BIOS besteht aus einem BBB und einem Post-BIOS, die beide von einander unabhängig sind. Andererseits kann das CRTM aus dem kompletten BIOS bestehen. Um die Kette des Vertrauens zu schließen, wird das TPM zum einen über eine Smart Card oder über einen physisch verlöteten Chip an eine Plattform gebunden. In der Praxis wird der physisch verlötete Chip auf einer Steckkarte über den LPC-Bus realisiert. *Tabelle 7* zeigt ferner die Reihenfolge der PCRs, in welche die Integritätsmetriken während des Bootvorgangs protokolliert werden müssen. Dabei ist festgelegt, welche Werte

---

[220] Vgl. TCG PC Specific Implementation Specification Version 1.1, S. 12

[221] Eigene Darstellung

oder Komponenten in das Register protokolliert werden.[222] Auffällig ist auch die Reservierung der acht von mindestens 16 geforderten PCRs in der Spezifikation. Jedoch soll sich die Anzahl der PCR in der kommenden PC-Spezifikation von 16 auf 24 PCR erhöhen.[223]

Index	PCR Usage
0	CRTM, BIOS and Platform Extensions.
1	Platform Configuration.
2	Option ROM Code.
3	Option ROM Configuration and Data.
4	IPL Code (usually the MBR).
5	IPL Code Configuration and Data (for use by the IPL code).
6	State Transition and Wake Events.
7	Reserved for future usage.

Tabelle 7: Platform Configuration Register im PC[224]

Abbildung 26 zeigt die Prozesse der Messungen von Integritätsmetriken in einem PC, wobei in diesem Beispiel das CRTM als BBB realisiert wurde. Die Durchführungen während des Bootprozesses wurden in der Grafik jedoch nicht berücksichtigt.

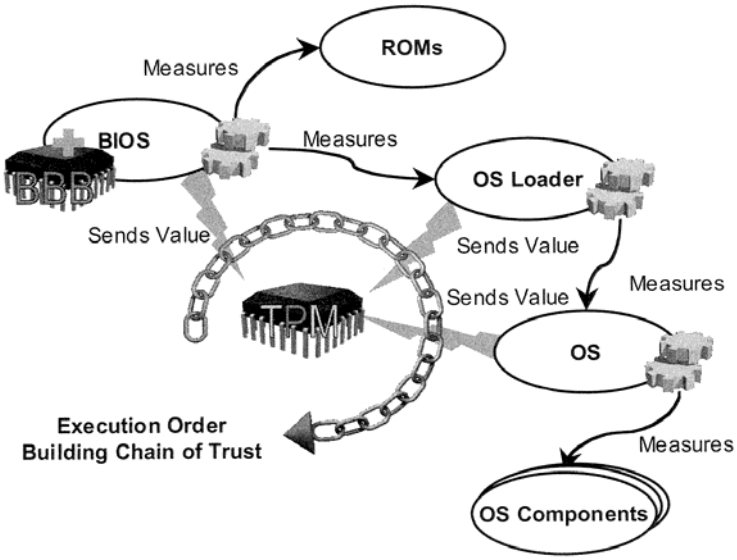

Abbildung 26: Integritätsmessungen und Berichten in einem PC[225]

Im Beispiel startet das BBB den Bootprozess und misst über einen Selbsttest die eigenen Werte sowie die des kompletten BIOS. Diese Integritätsmetriken werden pro-

---

[222] Vgl. TCG PC Specific Implementation Specification Version 1.1, S. 12 ff.

[223] Vgl. TCG TPM v1.2 Specifications Changes (2003), S. 13

[224] Vgl. TCG PC Specific Implementation Specification Version 1.1, S. 14

[225] Vgl. Pearson, S. (2002), S. 75

tokolliert und im PCR-0 abgelegt, welches sich innerhalb des volatilen Speichers des TPMs befindet. Danach finden weitere Messungen von Komponenten der Plattform statt, deren Werte protokolliert und in die jeweiligen PCR abgelegt werden.[226]

6 Anwendungen und Szenarien

6.1 Verfügbare Umsetzungen

In der Praxis sind unlängst verfügbare Umsetzungen der Spezifikation erhältlich, welche sich allerdings auf ältere Spezifikationsversionen beziehen. Die vorgestellten Beispiele in diesem Abschnitt sollen lediglich deutlich machen, wie viele TPM Komponenten bereits heute in Systemen zum Einsatz kommen, auch wenn diese noch nicht nahtlos in die Betriebssysteme integriert wurden.

6.1.1 Herstellung der Komponente TPM

Jeweils ein TPM wird bereits von den drei Herstellern Atmel, Infineon oder National Semiconductor produziert, welche alle über den LPC-Bus auf dem Motherboard implementiert werden.

Atmel ist der Weltmarktführer in der Produktion von TPM Sicherheitschips mit einem Marktanteil von 95 % und über 5 Millionen verkaufter TPM Chips seit 1998.[227] Das Atmel TPM AT97SC3201 ist eine schlüsselfertige Lösung auf einem Chip mit der entsprechenden Konformität zu den Spezifikationen 1.1b, das alle Funktionen unterstützt.[228] Der Nachfolger ist für April 2004 angekündigt und trägt die Bezeichnung AT97SC3202. Dieses TPM ist mit den Spezifikationen in Version 1.2 konform und unterstützt alle Erweiterungen wie Transport-Sitzungen, Echtzeit-Uhr, Lokalität, Speichern und Wiederherstellen von Zusammenhängen, direkte anonyme Attestation, permanenten Speicher und Delagation. Eine weitere wichtige Neuerung ist die Erhöhung der PCRs von 16 auf 32 Register. Bei einer Bestellmenge von 10.000 Stück sollen die Kosten für ein Atmel AT97SC3202 4$ pro Stück betragen.[229]

---

[226] Vgl. Pearson, S. (2002), S. 75 f.

[227] Vgl. Atmel (2004a)

[228] Vgl. Atmel (2004b)

[229] Vgl. Atmel (2004b)

Infineon nennt sein TPM SLD9630TT1.1 / M2009 und ist am Anfang diesen Jahres mit EAL3 zertifiziert worden.[230] Die Komponenten des SLD9630TT1.1 bestehen aus einem sicheren Controller, 64 kb ROM, 8 kb RAM und einem 16 kb EEPROM. Daneben ist das TPM von Infineon deckungsgleich zur Hauptspezifikation in Version 1.1b.[231]

Das National Semiconductor TPM trägt den Namen PC21100 (SafeKeeper) und ist konform zu den TCPA-Spezifikation in Version 1.1. Dabei wird das TPM als LPC-basierender Sicherheits-Controller verstanden, mit voller TSS Implementierung, TPM Firmware und PKCS#11 und CSP Unterstützung.[232]

6.1.2 Einsatz der TPM Komponente im System

Definitiv werden schon heute TPM-Chips der oben genannten Hersteller in Systeme bzw. Endprodukte eingebaut und verkauft. Das Intel Mainboard D865GRH ist für Desktop-Rechner bestimmt, welches mit dem TPM SLD9630TT1.1 von Infineon bestückt ist. Daneben ist das D865GRH ein Micro-ATX-Board und unterstützt die aktuellen Pentium 4 Prozessoren von Intel mit Hyperthreading. Den Hardware-Eigenschaften nach zu urteilen, ist dieses Board für den Einsatz in größeren Unternehmen gedacht, insbesondere auf den Markt für Office-Desktop-Rechner. Dazu bündelt Intel das Softwareprodukt „Embassy Trusted Suite“ von der Firma Wave Systems.[233] Über die Embassy Trusted Suite lässt sich das TPM zur Verschlüsselung und Signierung von Daten auf dem PC anwenden. Die Embassy Trusted Suite unterstützt zudem die bereits vorgestellten TPMs sowie das HP ProtectTools Embedded Security[234] und das IBM Embedded Security Subsystem (ESS).[235] Hewlett Packard vertreibt seine Software „ProtectTools Embedded Security” mit den Notebooks NC6000 und NC8000, die mit dem TPM SLD9630TT1.1 von Infineon bestückt sind.[236] Das IBM ESS ist bisher für ausgewählte ThinkPad Notebooks und Think-

---

[230] Vgl. Bödecker, P. (2004)

[231] Vgl. Infineon (2003), S. 2

[232] Vgl. National Semiconductor (2002)

[233] Vgl. Intel (2003a)

[234] Vgl. Hewlett Packard (2004a)

[235] Vgl. Wave Systems (2004)

[236] Vgl. Hewlett Packard (2004a)

Centre[237] sowie Netvista Desktop Systeme erhältlich, welche das integrierte Sicherheitssubsytem 2.0 von IBM unterstützen.[238] Das Sicherheitssubsytem besteht aus dem TPM AT97SC3201 von Atmel und der IBM Client Security Software.[239]

6.2 Intel LaGrande

Auch Intel hat einen eigenen Ansatz zum Trusted Computing entwickelt, dessen Initiative als „Safer Computing“ bezeichnet wird. Safer Computing setzt sich zum Ziel „to advance platform security and provide a hardware hardened framework for continued innovation in protection of sensitive information.”[240] Das Schlüsselelement zur Umsetzung der Vision ist die Technologie LaGrande, welche den PC vor Software-Attacken schützen soll, währenddem die Leistung, Einsatzflexibilität, Handhabung und die Rückwärtskompatibilität instand gehalten werden. Bei der LaGrande Technologie handelt es sich um eine Reihe von erweiterten Hardwarekomponenten. Wie in *Abbildung 27* ersichtlich sind dies der Prozessor, Chipsatz, Maus und Tastatur, Grafik und das TPM.[241]

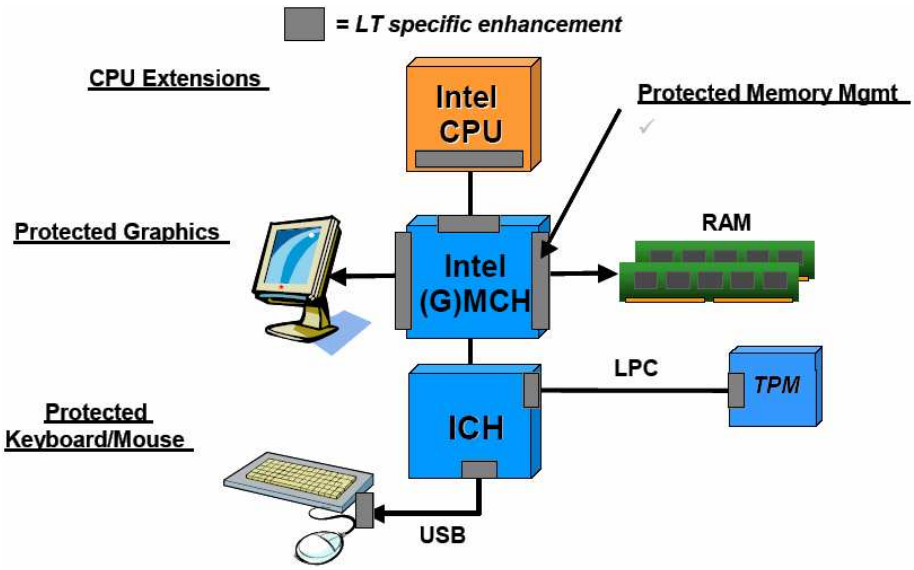

Abbildung 27: Erweiterungen der Intel LaGrande Hardware[242]

---

[237] Vgl. IBM (2003)

[238] Vgl. IBM (2004)

[239] Vgl. BSI (2003)

[240] Intel (2003c), S. 2

[241] Vgl. Intel (2003c), S. 2

[242] Vgl. Intel (2003c), S. 4

Der existierende IA-32 *Prozessor* muss um die Möglichkeit mehrere Umgebungen oder Partitionen zu bearbeiten, erweitert werden. Diese Erweiterung erlaubt die Existenz einer Standardpartition und einer geschützten Partition. Anwendungen in der geschützten Partition laufen isoliert und können nicht von anderen Anwendungen der Plattform beobachtet werden. Des Weiteren wird der Zugang zu den Hardwareressourcen durch Erweiterungen des Prozessors und des Chipsatzes erschwert. Weitläufigere Verbesserungen des Prozessors betreffen den Betrieb bei Ereignissen, Richtlinien für das Steuern von Ausführungen in der geschützten Betriebsumgebung und Anleitungen, um einen sicheren Software Stack zu implementieren.

Der *Chipsatz* muss gleichfalls um weitere Elemente für die geschützte Betriebsumgebung ergänzt werden. Diese Ergänzungen beinhalten:

- Die Möglichkeit Methoden zum Speicherschutz zu erzwingen,
- Erweiterungen zum Schutz des Datenzugangs des Speichers,
- geschützte Kanäle für die Grafik sowie die Ein- und Ausgabe und
- eine Schnittstelle zum TPM.

Daneben führen Erweiterungen der *Maus und Tastatur* zur sicheren Kommunikation zwischen diesen Eingabegeräten und den geschützten Anwendungen.

Verbesserungen am *Grafik*-System ermöglichen geschützten Anwendungen Ausgabeinformationen an den Bildspeicher zu senden, ohne das dieser beobachtet oder manipuliert wird.

Das *TPM* muss an den PC über den LPC-Bus angeschlossen werden, um hardwarebasierte Mechanismen zur Speicherung oder Verschlüsselung von Daten zu unterstützen.[243]

Die Verfügbarkeit der LaGrande Technik sieht Intel in den nächsten zwei bis drei Jahren, wobei diese dann vorerst für Desktop-PCs und mobile Plattformen erhältlich sein wird.[244] Zielgruppen sind in erster Linie Unternehmen mit kritischen und hochwertigen Anwendungen, wie z.B. Banken, Versicherungen, Gesundheitswesen und

---

[243] Vgl. Intel (2003c), S. 3

[244] Vgl. Intel (2003b)

staatliche Einrichtungen. Sie werden als frühe Adaptoren angesehen, welche einen Mehrwert in der Sicherheit sehen, größere Erfahrungen mit Sicherheit sowie deren Infrastruktur haben und früher dazu geneigt sind, in solche Techniken zu investieren.[245]

6.3 Next-Generation Secure Computing Base (NGSCB)

Microsoft hat einen eigenen Ansatz vertrauenswürdiger Technologien entwickelt, den sie „Trustworthy Computing" nennen. Unter diesem Begriff versteht Microsoft "*helping to ensure a safe and reliable computing experience that is both expected and taken for granted*"[246]. Laut Microsoft ist dieser Ansatz ein unternehmensweites Vorgehen, um dem Vertrauensanspruch und die Verantwortung gegenüber der Computerindustrie gerecht zu werden. Die vier Ziele *Sicherheit, Datenschutz, Verlässlichkeit und Integrität des Geschäftsgebarens* sollten dabei realisiert werden.[247] Momentan entwickelt Microsoft die erste Version eines sicheren Betriebssystems unter dem Projektnamen „Longhorn", der angekündigte Nachfolger für das Betriebssystem Windows XP. Die Sicherheitskomponenten von Longhorn wurden zunächst unter dem Begriff „Palladium"[248] erfasst, welcher aufgrund mangelnder Transparenz und schlechten Image eingestellt wurde. Somit wurde aus der Sicherheitsinitiative „Palladium" die „Next-Generation Secure Computing Base" (NGSCB).

Next-Generation Secure Computing Base (NGSCB) ist die notwendige Innovation zur Umsetzung von Microsofts Vision des Trustworthy Computing, wobei die NGSCB Technologie als Mittel zum Zweck angesehen werden kann. Die NGSCB Technologie benutzt Hardware- und Softwarekomponenten, um den Nutzern Sicherheit, Datenschutz und Systemintegrität zu gewährleisten.[249]

6.3.1 Architektur

Abbildung 28 zeigt einen Einblick in das System und deren Umgebung der NCGSB sowie deren isolierte Komponenten, dargestellt durch die vertikale rote Linie. Dabei

---

[245] Vgl. Intel (2003d), S. 12

[246] Microsoft (2004)

[247] Vgl. Microsoft (2004)

[248] Vgl. Carroll, A.; Juarez, M.; Polk, J.; Leininger, T. (2002)

[249] Vgl. Microsoft (2003d), S. 1 f.

unterscheidet das System der NGSCB zwischen Benutzer und Kernel Mode, wobei PC sowie Tastatur und Maus die sichere Ein- und Ausgabe darstellen.[250]

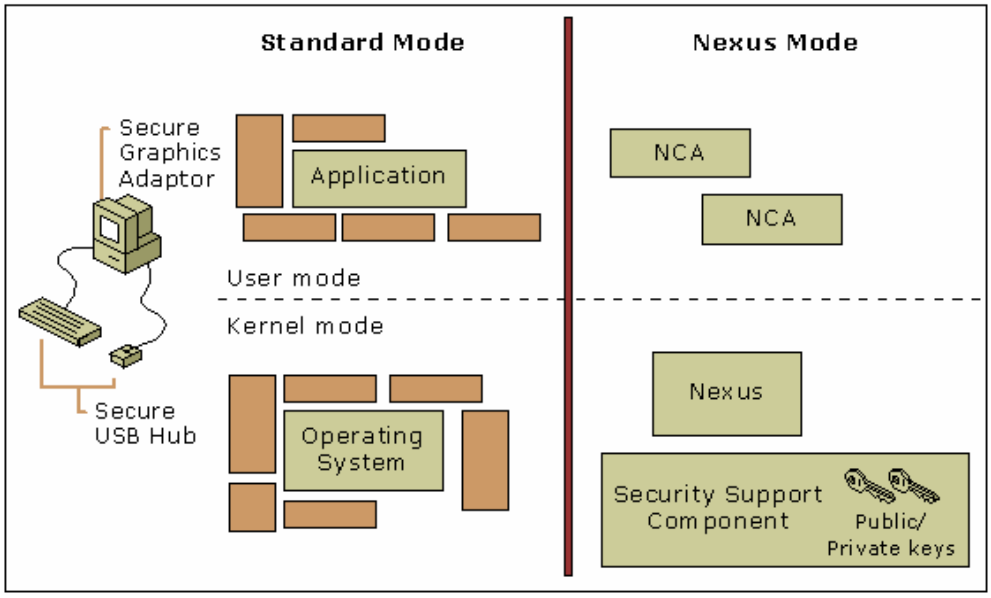

Abbildung 28: NGSCB System Überblick[251]

Die linke Seite bildet den Standard Mode ab, welcher im Wesentlichen dem klassischen Betriebssystem von heute entspricht. Im rechten Teil der Abbildung befindet sich der Nexus Mode, der Zugriff auf die Hardware „Security Support Component" (SSC) hat. Das SCC entspricht dem TPM-Chip der TCG.[252] Beide Systeme existieren nebeneinander auf einem einzigen Computer, wobei ein Referenzmonitor beide Systeme voneinander isoliert, damit sich diese nicht wechselseitig stören. Die beidseitige Existenz der Systeme lässt sich konzeptuell über eine Partitionierung des Computers realisieren, bei der beide Betriebsumgebungen nebeneinander auf der gleichen Hardware laufen.[253] Der Nexus Mode ist die geschützte Betriebsumgebung des abgeschlossenen Speichers und teilt sich in zwei Teile auf:[254]

- **Nexus:** Der Nexus ist ein Sicherheitskernel, welcher eine geschützte Betriebsumgebung durch die Isolierung bestimmter Speicherbereiche erzielt. Dabei werden Verschlüsselungstechnologien zum Authentifizieren und

---

[250] Vgl. Microsoft (2003f)

[251] Vgl. England, P.;Lampson, B.; Manferdelli, J.; Peinado, M.; Willman, B. (2003), S. 59

[252] Vgl. Microsoft (2003c)

[253] Vgl. England, P.;Lampson, B.; Manferdelli, J.; Peinado, M.; Willman, B. (2003), S. 58 f.

[254] Vgl. Microsoft (2003f), S. 8 f.

Schutz von Daten zur Ein- und Ausgabe sowie Speicherung unterstützt.[255] Der Nexus wird während des Startvorgangs authentifiziert und erzeugt danach die geschützte Betriebsumgebung innerhalb von Windows. Erst nach erfolgreicher Authentifizierung hat der Nexus erst Zugang zum TPM und den dort abgelegten Geheimnissen. Dazu unterstützt der Nexus Funktionen des TPM, wie Speicherung von kryptographischen Schlüsseln und Verschlüsselungsmechanismen. Des Weiteren identifiziert sowie authentifiziert der Nexus die NCAs und kontrolliert deren Zugang über einen Referenzmonitor, der Teil des Nexus Sicherheitskernels ist.[256]

- **Nexus Computing Agent (NCA):** Eine NCA ist eine vertrauenswürdige Software Komponente, bzw. eine Anwendung, Teil einer Anwendung oder ein Service, welcher vom Nexus in der geschützten Betriebsumgebung betrieben wird.[257] Jede NCA läuft dabei in der geschützten Betriebsumgebung, isoliert von jeder Anwendung, die nicht explizit mit ihr in Verbindung steht. Alle NCAs kontrollieren ihre eigene Vertrauenswürdigkeit und müssen sich nicht gegenseitig vertrauen. Zudem stellt eine NCA Anfragen an die Funktionen des Nexus, der über Hashwerte die Einzigartigkeit einer NCA ermittelt. Diese Hashwerte dienen wie schon oben angeführt der Vertrauenswürdigkeit gegenüber Entitäten, wie z.B. einem Benutzer, einer IT-Abteilung, einem Hersteller oder einem Verkäufer.[258]

6.3.2 Arbeitsablauf

Die Plattform mit NGSCB Technik hat als primäres Ziel Sicherheit und Systemintegrität zu gewährleisten. *Abbildung 29* gibt eine Einsicht über die Interaktion zwischen Hardware, OS und Anwendungen im System, zur Erlangung der genannten Ziele.

---

[255] Vgl. Microsoft (2003f), S. 8 f.

[256] Vgl. Microsoft (2003e), S. 6 f.

[257] Vgl. Microsoft (2003f), S. 8 f.

[258] Vgl. Microsoft (2003e), S. 7

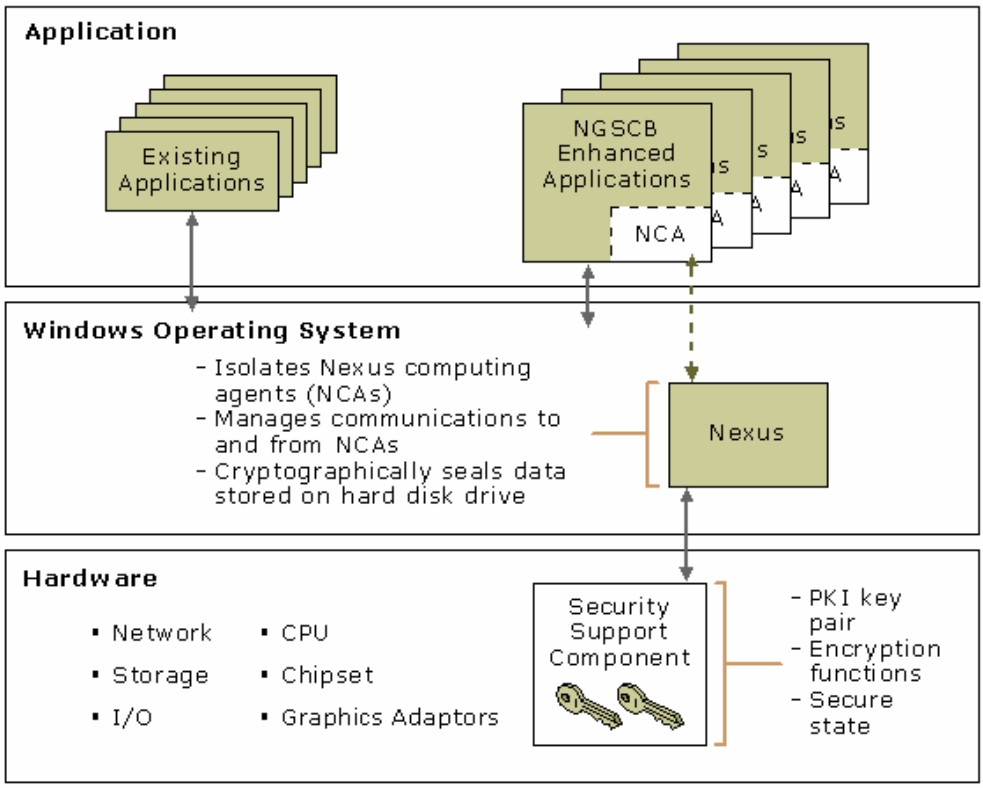

Abbildung 29: Interaktion zwischen Anwendungen, OS und Hardware [259]

Auf der Anwendungsebene benutzt das NGSCB System die gleichen Prozesse und virtuellen Speichermodelle wie das klassische OS. Allerdings unterscheiden sich diese hinsichtlich ihrer Authentifizierung und Zugriffskontrollen auf die Services des Nexus. Das klassische Betriebssystem hat keinen Zugriff auf den Nexus, der erst nach erfolgreicher Authentifizierung Zugriff auf die Services der Hardware hat, speziell auf das TPM alias SSC. Benutzt ein Anwender eine vertrauenswürdige Anwendung im abgeschlossenen Speicher, erscheinen alle Prozesse in einem eigens dafür erstellten vertrauenswürdigen Fenster mit einem Logo und einem nicht editierbaren Banner. Der Anwender erwirbt durch das System:[260]

- **Erweiterte Benutzerkontrolle:** Der Benutzer entscheidet, ob er die NGSCB Erweiterungen nutzen will, welche nicht zwingend vorgeschrieben und in der Standardeinstellung ausgeschaltet sind.
- **Authentifizierter Betrieb:** Über Hashwerte wird die Vertraulichkeit der Identität und Authentifizierung von Anwendungen sichergestellt. Der Benut-

[259] Vgl. Microsoft (2003f), S. 9

[260] Vgl. Microsoft (2003e), S. 10 ff.

zer kann daraufhin Methoden definieren, die den Zugang zu versiegelten Geheimnissen, basierend auf dem Hashwert, beschränken.

- **Zugangskontrolle zu geschützten Ressourcen:** Der Sicherheits-Referenzmonitor ist Teil des Nexus Kernels, welcher benutzerdefinierte Methoden zum Zugang auf vertrauenswürdige Anwendungen garantiert.
- **Plattformintegrität:** Das System ermöglicht den Fernzugriff auf Unternehmensnetzwerke, indem verschiedene separate Identitäten für diese Bedürfnisse erstellt werden.
- **Schutz gegen Diebstahl von Identitäten, autorisierter Zugang und andere Attacken:** Der Nutzer kontrolliert durch eindeutige Kennungen, Methoden und Kategorien von Daten, unter welchen Bedingungen Geheimnisse offenbart werden.
- **Kompatibilität zu existierenden Anwendungen und Services:** Das NGSCB System ist eine Erweiterung der Ressourcen, ohne störend auf die aktuellen Programme einzuwirken. Die bisherigen Anwendungen sind also auf einem System mit NGSCB Software weiter lauffähig, benötigen allerdings Erweiterungen, um auf die Ressourcen des Nexus Modes zugreifen zu können.
- **Vertraulichkeit der Daten und Integrität der Software:** Jede vertrauenswürdige Anwendung hat die Möglichkeit durch den Einsatz der neuen Technik, Attacken auf die geschützten Daten mittels andere Anwendungen zu verhindern.

6.3.3 Kernelemente der geschützten Betriebsumgebung

Generell sind alle Services des NGSCB Systems nicht zwingend vorgeschrieben und stehen unter der Kontrolle des Nutzers.[261] Dazu können Entwickler auf die vier folgenden Ressourcen des NGSCB Systems zurückgreifen:

---

[261] Vgl. England, P.;Lampson, B.; Manferdelli, J.; Peinado, M.; Willman, B. (2003), S. 59

6.3.3.1 Strenge Prozess Isolation

Daten werden durch höhere Sicherheitsanforderungen geschützt, indem ein Teil des Speichers von der geschützten Betriebsumgebung isoliert wird.[262] Strenge Prozess Isolation erreicht die NGSCB Technik durch Isolation eines bestimmten Adressraums innerhalb des „Random Acces Memory“ (RAM), um einen „abgeschlossenen Speicher“ zu erzeugen. Zusätzlich haben die „Direct Memory Acces“ (DMA) Schnittstellen keinen Lese- und Schreibzugriff auf den abgeschlossenen Speicher des RAMs, was über den DMA Ausschlussvektor gewährleistet wird. Dieser Vektor bestimmt über eine Hardware Speicherkarte die abgeschlossenen Speicherbereiche und deren Zugriff von DMA Schnittstellen. Eine Isolation des RAM Speichers blockiert somit jeden Zugriff von Programmen des Arbeitsspeichers auf den abgeschlossenen Speicher. Diese geschützte Betriebsumgebung besteht aus dem Nexus und den Nexus Computing Agents (NCA).[263]

6.3.3.2 Versiegelter Speicher

Der versiegelte Speicher ist ein kryptographischer Zugangskontrollmechanismus, bei dem der Benutzer eines Geheimnisses festlegt, welche Anwendung dieses auch wieder öffnen kann. Vertraulichkeit und Integrität persistent gespeicherter Daten wird durch deren Verschlüsselung auf der Festplatte gewährleistet.[264] Die Daten werden durch den Nexus geschützt, der sie mit Schlüsseln des TPMs bzw. SSCs chiffriert.[265] *Abbildung 30* zeigt ein einfaches Beispiel zur Verdeutlichung der Versiegelung.

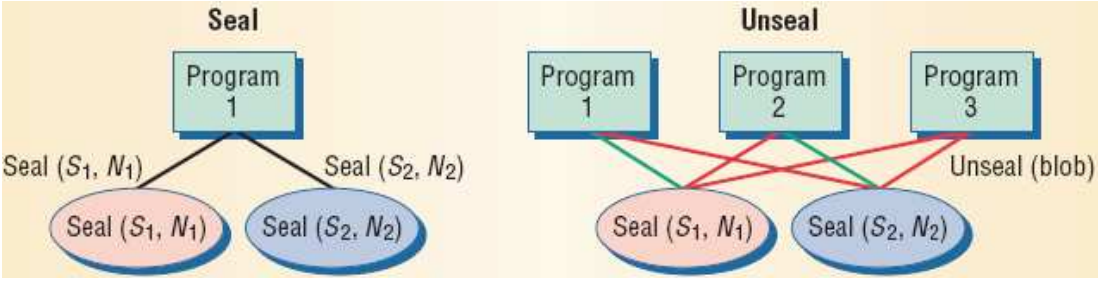

Abbildung 30: Ver- und Entsiegelung von Geheimnissen[266]

---

[262] Vgl. Microsoft (2003b)

[263] Vgl. Microsoft (2003e), S. 4 f.

[264] Vgl. Microsoft (2003b)

[265] Vgl. Microsoft (2003e), S. 8

[266] Vgl. England, P.;Lampson, B.; Manferdelli, J.; Peinado, M.; Willman, B. (2003), S. 57

Die Versieglung benötigt eine geheime Zeichenkette, den Hashwert des Programms, das die versiegelten Daten öffnen darf, und den Hashwert der Anwendung, der die Versieglung aufruft, damit die Datenquelle beim Öffnen wieder identifiziert werden kann. Eine authentifizierte Stammfunktion wird zur Verschlüsselung der Datenstruktur und zu deren Integrität benutzt. Das Öffnen eines versiegelten Speichers setzt eine Versieglung logisch voraus. Dabei verifiziert die Eingabe die Integrität und entschlüsselt diese dann intern.[267]

6.3.3.3 Attestierung

Die Attestierung ist eine Variante der asymmetrischen Verschlüsselung, welche Anwendungen über deren Hashwerte an Dritte authentifiziert. Als Voraussetzung muss eine Plattform ein zertifiziertes asymmetrisches Schlüsselpaar (AIK) besitzen.[268] Der Mechanismus der Attestierung in Verbindung mit einer Infrastruktur von Lizenzen und Zertifikaten erlaubt dem Benutzer bestimmte Eigenschaften der Betriebsumgebung an einen Herausforderer und an Ferndienstanbieter zu offenbaren. Dazu überprüft der Ferndienstanbieter die empfangenen Daten und attestiert den rechtmäßigen Zustand der Hard- und Software.[269] Zudem wird eine Bestätigung eines Nonces an einen Empfänger durch Hinzufügen von Datenauszügen und über die digitale Signatur des Nonces attestiert.[270]

6.3.3.4 Sichere Wege zum Nutzer

Durch Verschlüsselung von Ein- und Ausgabe stellt das System einen sicheren Weg über die vertrauenswürdigen Anwendungen von der Tastatur und Maus zum Bildschirm sicher.[271] Dieser Mechanismus schützt den Benutzer vor Anwendungen, welche die Tastenanschläge aufzeichnen oder vor Fernzugriffen durch Trojanische Pferde, die einem Angreifer die Möglichkeit geben, wie ein berechtigter lokaler Anwender zu agieren. Sichere Eingabe wird über die Erweiterung von Tastaturen und Universal Serial Bus (USB) Schnittstellen erreicht. Ebenso werden Erweiterungen der

---

[267] Vgl. England, P.;Lampson, B.; Manferdelli, J.; Peinado, M.; Willman, B. (2003), S. 56 f.

[268] Vgl. England, P.;Lampson, B.; Manferdelli, J.; Peinado, M.; Willman, B. (2003), S. 57

[269] Vgl. Microsoft (2003e), S. 8 f.

[270] Vgl. Microsoft (2003b)

[271] Vgl. Microsoft (2003b)

Ausgabeschnittstellen erwartet, welche den Schutz des Videospeichers verbessern sollen.[272]

6.3.4 Beispielanwendung „Rights Management Services“ (RMS)

Das NGSCB System bietet eine erweiterte Sicherheitsgrundlage, die neue Anwendungen ermöglicht. Dazu gehören unter anderem die Anwendungen von Smart Cards, Netzwerk Anmeldungen, autorisierte Transaktionen, das Signieren von Dokumenten sowie das Rechtemanagement von Daten, worauf in diesem Abschnitt näher eingegangen wird.

Mit der Veröffentlichung von Windows Server 2003 wurde die technische Anwendung des Rights Management Services (RMS) eingeführt, welches auch von Microsoft Office 2003 Professional unterstützt wird. Das RMS von Microsoft ist eine „*information protection technology that works with RMS-enabled applications to help safeguard digital information from unauthorized use*.“[273] Zur Realisierung von RMS werden vertrauenswürdige Entitäten, Nutzungsrechte sowie Konditionen und Verschlüsselungen permanent notwendig.[274] Hier zeigt sich eine mögliche Anwendung des Rechtemanagements von Daten, dessen Wirkung durch das TPM und den Einsatz von NGSCB noch wesentlich verstärkt werden kann.

Bisherige Beispiele von RMS Einsatzszenarios sind der Schutz vertraulicher E-Mails, Erzwingen von Rechten am Dokument und der Schutz sensibler Inhalte eines Intranets. Der Schutz vertraulicher Daten und deren Befugnissen daran werden durch eine Definition des Autors über die Nutzung von Informationen erreicht. Somit hat der Empfänger der Information nur noch eingeschränkte Rechte, wie z.B. ein einziges Mal Leserechte am Dokument. Das RMS schützt Informationen im on- und offline Zustand, innerhalb und außerhalb einer Firewall.[275] *Abbildung 31* zeigt den Ablauf von RMS bzw. deren Architektur.

---

[272] Vgl. Microsoft (2003e), S. 9

[273] Microsoft (2003h), S. 6

[274] Vgl. Microsoft (2003h), S. 6

[275] Vgl. Microsoft (2003g), S. 2

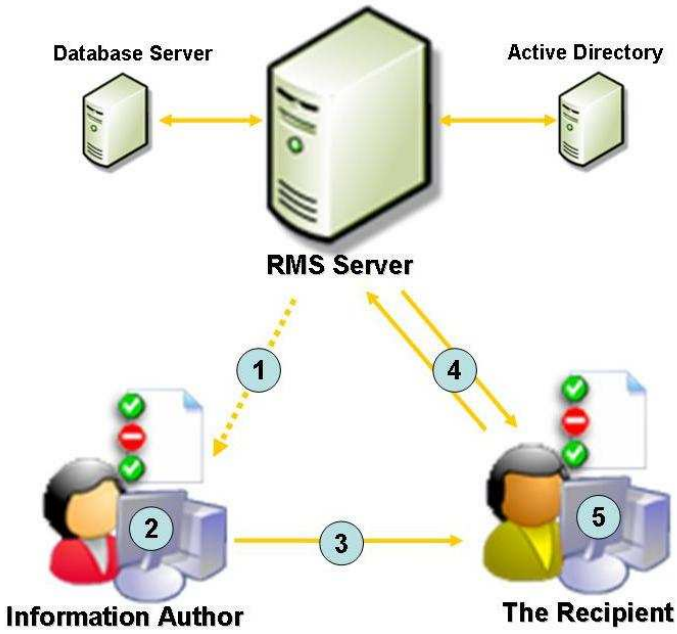

Abbildung 31: Ablauf von „Rights Management Services“[276]

Im ersten Schritt wird ein bestimmter Benutzerkreis und deren Rechte auf dem RMS-Server definiert und hinterlegt. Danach können diese vertrauenswürdigen Entitäten über eine RMS-Anwendung rechtlich geschützte Dateien erstellen, welche z.B. gelesen und ausgedruckt, allerdings nicht vom Empfänger editiert werden können. Nachfolgend verschlüsselt die Anwendung die Datei mit deren Herausgaberechte, welche im dritten Schritt an den Empfänger gesendet werden. Der Empfänger stellt dann nach dem Öffnen der Datei im vierten Schritt eine Anfrage an den RMS-Server, um die Benutzerzertifikate und die Nutzungsrechte zu bestätigen. Eine Nutzungslizenz in Verbindung mit der RMS-Anwendung erzwingt dann im fünften Schritt die Benutzungsrechte des Autors beim Empfänger.[277] Der Grad dieser bereits verfügbaren Sicherheit kann allerdings noch durch die Erweiterung von NGSCB erheblich gesteigert werden.

6.4 Anwendungen unter dem Betriebssystem Linux

6.4.1 IBM's Global Security Analysis Lab (GSAL)

IBM's Global Security Analysis Lab hat umfangreiche Analysen bezüglich der TPM-Implementierung in IBM Notebooks unter dem Betriebssystem Linux getätigt. Um

---

[276] Vgl. Microsoft (2003g), S. 2

[277] Vgl. Microsoft (2003g), S. 2

die Transparenz und die Funktionen des Chips transparenter zu gestalten, hat die IBM GSAL ein Paket für einen TPM-Chip veröffentlicht.[278] Dieses Paket ist keine komplette TSS Implementierung, d.h. es besteht kein Zugang zur Verwaltung von Schlüsseln sowie deren Migration oder Sicherung, kein Ressourcen- oder Prüfungsmanagement und keine Synchronisation für gleichzeitige Anfragen.[279] Das Paket des Quellcodes besteht aus fünf Komponenten, nämlich des kompletten Quellcodes des Linux Gerätetreibers, Beispielprogramme, libtcpa, ein GRUB- und ein Loopback-Patch. Der Quellcode des Gerätetreibers erlaubt das Kompilieren eines ladbaren Moduls für den Kernel. Die Gerätetreiber Bibliothek libtcpa enthält die TPM Kommandos, welche zu Aktionen wie der Umgang mit Schlüsseln, dem Signieren etc. gebraucht werden können. Deren Umgang wird durch die mitgelieferten Beispielprogramme vertieft.[280]

6.4.2 Open Source Linux Projekt „Enforcer“

Das Open Source Projekt „Enforcer” ist ein „Linux Security Module designed to improve integrity of a computer running Linux by ensuring no tampering of the file system”.[281] Ziel des Projektes ist einen gewöhnlichen Linux Desktop in einen virtuell sicheren Koprozessor zu transformieren, indem das TPM und die Spezifikationen dafür genutzt werden. Überdies soll dieses Ziel durch die Benutzung von Open-Source geschehen, was durch die Benutzung eines Apache Web Servers und SSL realisiert wurde.[282] Dazu agiert der Enforcer mit dem TPM, um auf höherer Ebene Sicherheit für Software und sensitive Daten zu schaffen.[283] Der Begriff Enforcer leitet sich von dem englischen Verb „to enforce“ ab, was übersetzt „erzwingen“, „durchsetzen“ oder „durchführen“ heißt.[284] Seit August 2003 ist die aktuelle Alpha Version 0.3 erhältlich und beinhaltet das Linux Enforcer Module, einen aktiven Linux Loader (LILO) und eine Bibliothek auf Benutzebene. Das Linux Enforcer Module ist ein „Linux Security Module“ (LSM), das die Integrität einer Plattform mit

---

[278] Vgl. IBM's Global Security Analysis Lab (2004a)

[279] Vgl. IBM's Global Security Analysis Lab (2004b)

[280] Vgl. Safford, D.; Kravitz, J.; van Doorn, L. (2003)

[281] Wild, O. (2003)

[282] Vgl. MacDonald, R.; Smith, S.; Marchesini, J.; Wild, O. (2003a), S. 15

[283] Vgl. Wild, O. (2003)

[284] Vgl. LEO Dictionary Team (2004)

dem Betriebssystem Linux verbessern soll. Das LSM läuft kontinuierlich, unterstützt sicheres Booten, schützt Geheimnisse sowie andere sensible Daten und bindet diese an eine bestimmte Software. Entdeckt der Enforcer eine modifizierte Datei, können mehrere Zustände einzeln oder kombiniert eintreten:[285]

- Zugriffsverweigerung zu der Datei,
- Vorfall wird im System protokolliert,
- Aufmerksamkeit auf Modifizierung des Systems richten oder
- Verwehrung zur TPM Hardware.

Durch die Benutzung eines Apache Web Servers sowie SSL wird der ganze Ansatz dynamisch, selbst die Server Schlüsselpaare. *Abbildung 32* skizziert, wie Vertrauen im dynamischen Fall von Serverschlüsselpaaren verlaufen kann. Das System ist dabei nach der Häufigkeit der Änderungen von Elementen aufgeteilt:

- *Kurzlebige* operationale Daten,
- *Mittelbeständige* Software und
- *Langlebige* Daten, wie der Kernel.

Der Security Admin kontrolliert dabei die von mittlerer Dauer beständige Softwarekonfiguration über Signaturen und deren öffentliche Schlüssel und das Enforcer Module ist Teil des langlebigen Kerns.

---

[285] Vgl. Wild, O. (2003)

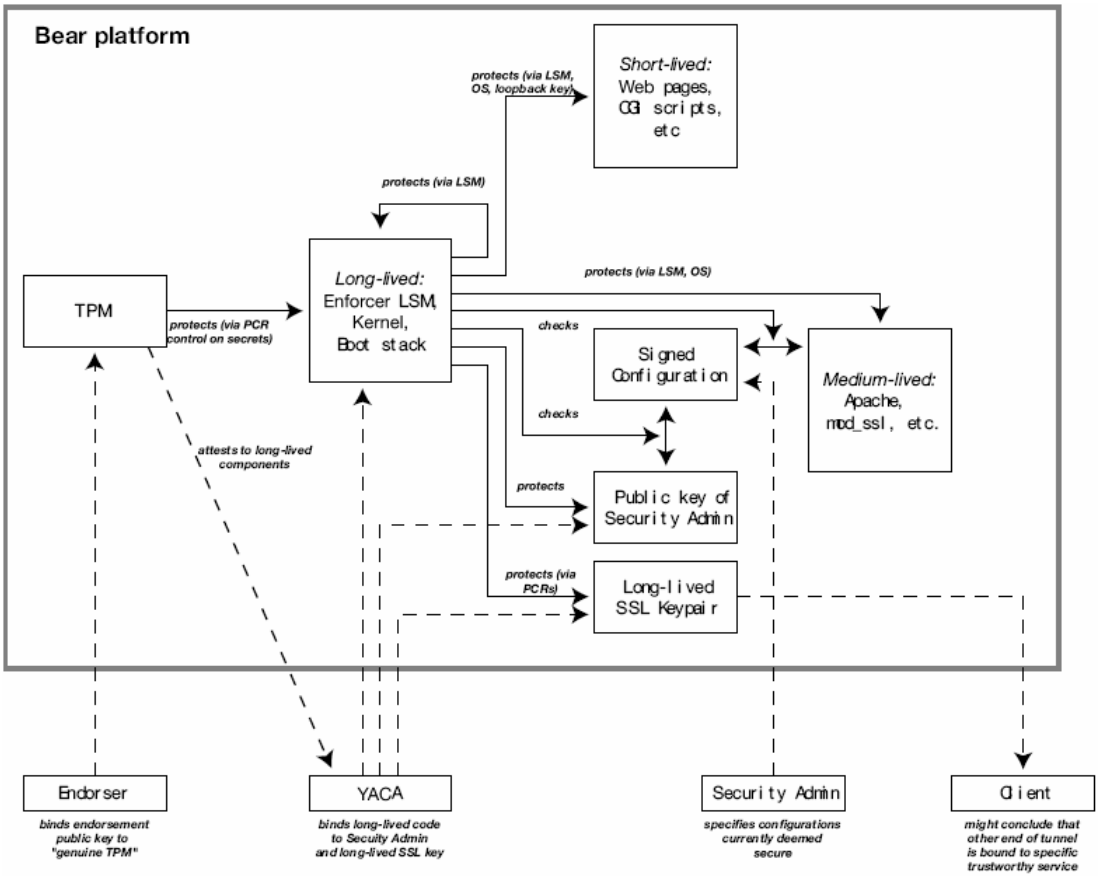

Abbildung 32: Entwurf der „Bear Plattform“ als Web-Server[286]

Zudem signiert der Security Admin eine Beschreibung der mittelbeständigen Software, von der er denkt, dass sie sicher ist. Der sichere Bootprozess gewährleistet die Integrität des langlebigen Kerns und dessen Zugriff auf die Geheimnisse. Danach überprüft der Enforcer die Richtigkeit der Beschreibungen des System Admins und benutzt dann den sicheren Speicher, um kurzlebige operationale Daten zu handhaben. Weiter werden Beschreibungen mit einer Seriennummer in Form eines Wasserzeichens versehen, um die Aktualität der Beschreibungen zu garantieren.[287]

---

[286] Vgl. MacDonald, R.; Smith, S.; Marchesini, J.; Wild, O. (2003b), S. 19

[287] Vgl. MacDonald, R.; Smith, S.; Marchesini, J.; Wild, O. (2003b), S. 9 ff.

7 Bewertung

7.1 Bewertung der kooperativer Standardisierung

Generelle Aussagen bezüglich der Auswirkungen von kooperativer Standardisierung auf Wettbewerb, Effizienz und Konsumenten-Wohlfahrt sind per se schlecht möglich. Standardisierung wird in erster Linie bevorzugt, um kollektiv eine kritischen Masse an Nutzer zu erreichen und den Bandwagon-Effekt auszulösen. Fundamentale Eigentumsrechte in Form von Patenten von zwei oder mehreren Unternehmen können zudem entscheidend zum Erfolg beitragen. So lange wie Netzwerkeffekte stark genug sind und der Standard nicht die Produktvielfalt einschränkt, sind kooperative Standardisierungen sogar wünschenswert, vorausgesetzt die verschiedenen Hersteller bieten konkurrierende Programme an. Das Ergebnis eines Standards kann sehr effizient sein, wenn sich die Produktvielfalt dementsprechend entfalten kann. Folglich wird auch beachtenswerter Wettbewerb bewahrt unter Ausnutzung der Netzwerkeffekte.[288]

Shapiro erachtet aber den Zwang der Teilnehmer eines Standards Lizenzgebühren zu zahlen für problematisch, da dies eine induzierte Form der geheimen Absprache wäre. Taucht beispielsweise je ein Teil der geistigen Eigentumsrechte der Mitglieder in einem Standard auf, wäre das ein Zeichen für eine geheime Absprache. In der Regel kommen Unternehmen jedoch zusammen, um ein Produkt erfolgreich im Markt zu platzieren, ohne geistigen Eigentumsrechte anderer zu verletzen. Des Weiteren tauchen kartellrechtliche Zweifel an einem Standardisierungsprozess auf, wenn Unternehmen einer Industrie einen Standard annehmen und dieser ihre geistigen Eigentumsrechte umfasst. Dies dient zur Monopolisierung des Marktes und wird durch die fairen und angemessenen Konditionen wie die RAND abgeschwächt. Jeder Produzent dieses Standards muss daraufhin Lizenzabgaben an die Förderer des Standards bezahlen.[289]

---

[288] Vgl. Shapiro, C. (2001a), S.10

[289] Vgl. Shapiro, C. (2001a), S.10 f.

7.2 Hardwarekompatibilität und Netzwerkexternalitäten

7.2.1 Szenario

Ein Computersystem ist aus Hard- und Software zusammengesetzt. Die Hardware besteht z.B. aus Platinen, Hauptprozessor, Speicherchips und -geräten, Verbindungsanschlüssen, Tastatur, Drucker, Scanner und Monitor. Software ist im weitesten Sinne Information, welche in Paketen verkauft wird und unterschiedliche Kommandos des Nutzers auf dem Computer ausführt. Ein besonderer Teil dieser Software betrifft das Betriebssystem, welche als Interpreter der Maschinensprache dient.[290]

Genau ein ähnliches Szenario des Computersystems soll hier modelliert werden. Die TCG spezifiziert einen Standard für die Hardwarekomponente TPM. Diese Hardwarekomponente ist Teil der Hardware des Computersystems, welche vom einem entsprechenden Betriebssystem gesteuert wird. Da Microsoft im Jahr 2003 einen weltweiten Marktanteil von 96,3 % hatte[291], wird zur Vereinfachung als Betriebssystem eine Version von Windows als Software im Computersystem angenommen. Zwei Computersysteme sind dabei miteinander kompatibel, wenn diese zusammen arbeiten können. Im vorliegenden Fall ist dies nur eingeschränkt möglich, da die neue Hardware nur über eine Erweiterung des Betriebssystems angesprochen werden kann, wie es im Fall von Microsoft die Komponente NGSCB sein wird. Es handelt sich somit um eine Einweg-Kompatibilität, da eine neue Version des Betriebssystems kompatibel zum alten ist, allerdings nicht umgekehrt. Die Nutzer des neuen Computersystems können folglich aufgrund der Einweg-Kompatibilität bereits auf eine große installierte Basis zurückgreifen und Netzwerkexternalitäten realisieren. Bei den beiden angebotenen Computersystemen, einerseits mit TPM und andererseits ohne, handelt es sich im weiteren Sinne um perfekte Substitute. Zur weiteren Vereinfachung wird ein Markt mit zwei Anbietern untersucht, unter der Annahme heterogener Konsumenten, welche unterschiedliche Präferenzen für unterschiedliche Marken aufweisen. Des Weiteren werden Produktionskosten von Null für jede Firma unterstellt, wobei:

- p_A der Preis für ein Computersystem mit TPM ist und

---

[290] Vgl. Shy, O. (2001), S. 13 f.

[291] Vgl. derStandard.at (2004)

- p_B der Preis für ein System ohne TPM.

Alle potentiellen Konsumenten werden in zwei Typen aufgeteilt: η Konsumenten sind TPM-orientierte Kunden, wohingegen die restlichen η Konsumenten herkömmliche Computersysteme kaufen wollen. Der Nutzen U der beiden Konsumenten lässt sich allgemein nach Shy wie folgt beschreiben:[292]

$$(2) \qquad U_A \overset{def}{=} \begin{cases} \alpha(q_A + q_B) - p_A \\ \alpha q_B - p_B - \delta \end{cases} \mapsto \begin{matrix} kauft\ A; A\ ist\ kompatibel\ zu\ B \\ kauft\ B; B\ ist\ inkompatibel\ zu\ A \end{matrix}$$

$$(3) \qquad U_B \overset{def}{=} \begin{cases} \alpha(q_A + q_B) - p_A - \delta \\ \alpha q_B - p_B \end{cases} \mapsto \begin{matrix} kauft\ A; A\ ist\ kompatibel\ zu\ B \\ kauft\ B; B\ ist\ inkompatibel\ zu\ A \end{matrix}$$

Ein Konsument der TPM orientiert (i) ist, sich allerdings für ein System ohne TPM (j) entscheidet, hat einen negativen Nutzen von δ (mit $i,j = A,B$ und $i \neq j$). Der negative Nutzen ist exogen gegeben und kann als Transport-, Differenz- oder Wechselkosten-Parameter angesehen werden. Ein Computernutzer i erfreut sich an einem Netzwerknutzen von αq_i, wenn der Computer i inkompatibel zu j ist. Allerdings genießt er $\alpha(q_A + q_B)$, vorausgesetzt System i ist kompatibel mit j. Der Parameter $\alpha > 0$ gibt also die Intensität der Netzwerkexternalitäten an, wobei α auch für den Grad der Wichtigkeit von Kompatibilität des Konsumenten steht.

Eine weitere Annahme des Modells stellt die Unterscheidung der Präferenzen der Konsumenten dar, welche einen stärkeren Einfluss auf den Nutzen als die Netzwerkgröße hat. Diese Annahme verhindert ein Gleichgewicht, in dem alle Konsumenten sich für das gleiche Produkt aufgrund der vorherrschenden Netzwerkeffekte entscheiden, obwohl die eigenen Präferenzen unterschiedlich sind.[293] Der zu analysierende Markt hat eine große Anzahl an Konsumenten, weshalb die Nutzer beider Systeme als konstant angenommen werden.[294]

7.2.2 Gleichgewicht bei Einweg-Kompatibilität

Im Fall von Einweg-Kompatibilität besteht eine asymmetrische Situation, in der ein Produzent ein Computersystem mit TPM (A) kompatibel zum bisherigen System (B)

---

[292] Vgl. Shy, O. (2001), S.27

[293] Vgl. Shy, O. (2001), S. 27 f.

[294] Vgl. Shy, O. (2001), S. 28

macht. Auf diese Erweiterung (A) kann das herkömmliche System (B) jedoch nicht zugreifen. Zur Lösung des Problems wird auf das „Undercut-Proof Equilibrium“ (UPE) Modell zurückgegriffen. Im UPE wählt jeder Anbieter den Preis, welcher den eigenen Gewinn maximiert. Allerdings muss der gewählte Preis niedrig genug sein, damit rivalisierende Anbieter es für nicht erstrebenswert erachten günstigere Preise zu setzen, um damit Kunden abzuwerben.[295]

Die Grundgesamtheit der Konsumenten ist auf die zwei Möglichkeiten A und B aufgeteilt, somit kaufen η Konsumenten ein System. Jeder TPM Nutzer erwirbt dabei einen Netzwerknutzen von $\alpha 2\eta$, wobei jeder Nutzer eines herkömmlichen Systems $\alpha\eta$ erhält. Insofern der Hersteller des Computersystems mit TPM (A) also den Produzent ohne (B) unterbietet, steigt die Netzwerkgröße der Nutzer ohne TPM um η. Dies realisiert A durch das Unterbieten des Preises von B wie folgt: $p_A = p_B - \delta + \alpha\eta$. Dagegen führt das Unterbieten eines Systems ohne TPM (B) von (A) nicht zu einer Steigerung der Netzwerkgröße der Benutzer des TPMs, da Computer mit TPM (A) kompatibel zu PC’s ohne TPM (B) sind und dadurch nur eine maximale Netzwerkgröße von 2η erhalten werden kann. Herkömmliche PC-Systeme müssen also zur Unterbietung der TPM-Computersysteme einen Preis von $p_B = p_A - \delta$ setzen.[296] Ein Preispaar $\left(p_A^U, p_B^U\right)$ erzeugt ein UPE unter folgenden Voraussetzungen:

(4a) $\pi_B^U = p_B^U \eta \geq \left(p_A^U - \delta\right)2\eta$,

(4b) $\pi_A^U = p_A^U \eta \geq \left(p_B^U - \delta + \alpha\eta\right)2\eta$.

Dies führt zu folgenden Gleichgewichtspreisen:

(5a) $p_A^U = 2\delta - \frac{2\alpha\eta}{3}$ und (5b) $p_B^U = 2\delta - \frac{4\alpha\eta}{3}$.

---

[295] Vgl. Shy, O.; Morgan, P. B. (2000), S. 1

[296] Vgl. Shy, O. (2001), S.32

Einsetzten der Preise (5a) und (5b) in (4a) und (4b) führt zu nachfolgenden Gewinnen:

(6a) $\pi_A^U = 2\eta\left(\delta - \frac{\alpha\eta}{3}\right)$ und (6b) $\pi_B^U = 2\eta\left(\delta - \frac{2\alpha\eta}{3}\right)$.

Aus den berechneten Gleichgewichtspreisen in (5a/b) und den daraus resultierenden Gewinnen (6a/b) lassen sich nachfolgende Aussagen treffen: Im Szenario der Einweg-Kompatibilität kann der Hersteller des kompatiblen Systems mit TPM einen höheren Preis als der Produzent von bisherigen Computersystemen ansetzen und erwirtschaftet somit auch einen höheren Gewinn, ceteris paribus. Jedoch ist diese Aussage nicht auf alle Typen der Computerindustrie anwendbar und daher nur ein mögliches Ergebnis.[297]

(7a) $U_A = \frac{8\alpha\eta}{3} - 2\delta$ und (7b) $U_B = \frac{7\alpha\eta}{3} - 2\delta$.

Der Konsumentennutzen eines Computersystems mit TPM ist nach dem Einsetzen der Preise in die Nutzenfunktionen der Konsumenten höher als ohne, da $U_A > U_B$, ceteris paribus.

Die soziale Wohlfahrt wäre in diesem Szenario nur die zweitbeste Lösung:[298]

(8) $W_{gesamt} = \eta U_A + \eta U_B + \pi_A + \pi_B = 3\alpha\eta^2$

Allgemein erlangen Unternehmen einen größeren Vorteil, wenn es möglich ist, kompatible Systeme zu angemessenen Kosten zu produzieren. Dabei erwirtschaften Unternehmen einen höheren Mehrwert vom Konsumenten, obwohl sich der Bruttonutzen des Konsumenten durch die Kompatibilität verbessert.[299]

7.3 Technologischer Vorteil und Standardisierung

7.3.1 Statischer Ansatz der Adoption einer neuen Technologie

Technologiewechsel benötigen in der Regel eine komplette Überarbeitung des Produktes, der Eigenschaften und Funktionen. Großes Interesse besteht dann darüber, ob

---

[297] Vgl. Shy, O. (2001), S.32 f.

[298] Vgl. Shy, O. (2001), S.35

[299] Vgl. Shy, O. (2001), S.35

die neue Technologie von einer gegebenen großen installierten Basis an existierenden inferioren Technologien angenommen wird. Dieser Fragestellung sind indirekt auch die Mitglieder der TCG ausgesetzt, da sie eine neue Technologie spezifizieren, um dann später einzeln oder im Verbund einen Teil ihrer Produkte sowie Investitionen darauf auszurichten, damit die neue Technologie sich als Standard im Markt etabliert. Zur Verdeutlichung wird das Spiel aus *Tabelle 8* in Betracht gezogen, in dem zwei Nutzer oder Firmen die Möglichkeit haben, sich jeweils für die neue oder

alte Technologie zu entscheiden. Unter der alten Technologie werden die bisherigen Angebotenen PC-Systeme ohne TPM verstanden. Andererseits wird unter der neuen Technologie PC-Systeme mit TPM begriffen.

		Nutzer B			
		Neue Technologie		**Alte Technologie**	
Nutzer A	**Neu**	***a***	***a***	***c***	***d***
	Alt	***d***	***c***	***b***	***b***

Tabelle 8: Statisches Adoptionsspiel bei neuer Technologie[300]

Sodann wird unterstellt, dass beide Nutzer Netzwerkexternalitäten für beide Technologien aufweisen, was formal als $a > d$ und $b > c$ angenommen wird. Das Benutzen der gleichen Technologie wie der andere Nutzer führt somit zu einem höheren Nutzen oder Gewinn, als eine Technologie alleine einzusetzen. Unter dieser Annahme liegen zwei Nashgleichgewichte für das Spiel vor, nämlich *(Neu,Neu)* und *(Alt,Alt)*.

Hat das gespielte Nashgleichgewicht *(Alt,Alt)* als Ergebnis und Paretodominiert den Ertrag *(Neu,Neu)* wird diese Situation als „excess inertia" bezeichnet. Dies ist der Fall, wenn $b < a$ und *(Alt,Alt)* gespielt wird. Excess inertia tritt also auf, sobald die neue Technologie einen höheren Nutzen für beide Nutzer erbringt, allerdings alle Nutzer im Gleichgewicht auf der alten Technologie verharren. Mit anderen Worten, auf die TCG bezogen, tritt excess inertia ein, sofern das PC-System mit TPM einen höheren Nutzen liefert, die Nutzer aber lieber auf dem alten PC-System festhalten.

Ist *(Neu,Neu)* das gespielte Nashgleichgewicht und *(Alt,Alt)* Paretodominant, wird diese Situation „excess momentum" genannt. Excess momentum tritt auf, wenn eine neue Technologie eine alte ersetzt, aber die alte Technologie einen höheren Nutzen

---

[300] Vgl. Shy, O. (2001), S. 82

bzw. Profit an beide Nutzer erbringt als die neue Technologie. Im Fall des oberen Spiels entsteht die Situation excess momentum, wenn $b > a$ ist und *(Neu,Neu)* gespielt wird.[301] Im Bezug auf das neue PC-System mit TPM tritt excess momentum auf, falls der Nutzen des alten PC-Systems höher ist als der neue mit TPM und die Nutzer trotzdem die neue Technologie annehmen.

7.3.2 Dynamischer Ansatz der Adoption einer neuen Technologie

Netzwerkexternalitäten entstehen hauptsächlich auf der Nachfragerseite und geben eine Erklärung dafür, warum manche Technologien öfter ersetzt werden als andere. Shy analysiert drei wichtige Faktoren, welche die Wahl des richtigen Zeitpunktes und die Häufigkeit der Adoption einer Technologie beeinflussen:[302]

1. Grad der Substitution von Konsumenten zwischen der Netzwerkgröße und Erwerb einer verbesserten Technologie,
2. Wachstumsrate der Technologie und Größe der Grundgesamtheit an Konsumenten,
3. Grad der Kompatibilität einer neuen Technologie und deren Kompatibilität zur alten.

Der Grad der Kompatibilität bezieht sich in erster Linie auf die Rückwärtskompatibilität, d.h. ein neues Modell ist kompatibel mit dem älteren Modell, aber nicht notwendiger Weise umgekehrt.[303] Dies entspricht wiederum dem Fall der TCG, da das TPM eine optionale Komponente des Systems ist und somit nur der neuen Technologie zugänglich ist, wobei jedoch die Kompatibilität zur alten Technologie gewahrt bleibt. Die neue Technologie wird stärker vom Konsument angenommen, wenn dieser die Qualität und Netzwerkgröße als substituierbar betrachtet. Der Grund liegt darin, dass eine Steigerung der Qualität der Technologie eine wesentliche Nutzensteigerung verursacht, selbst wenn sich die Netzwerkgröße nicht verändert. Dagegen ist der Grad der Substitution gering, bis eine Steigerung der Qualität durch die Stei-

---

[301] Vgl. Shy, O. (2001), S. 82 f.

[302] Vgl. Shy, O. (2001), S. 84

[303] Vgl. Shy, O. (2001), S. 16

gerung der Netzwerkgröße kompensiert wird. Dies trifft exakt auf die Computerindustrie zu, wo nicht jede Verbesserung im Markt angenommen wird.[304]

7.3.2.1 Annahmen

Für die weitere Betrachtung wird pro Periode t (für t=1,2,…) zwischen zwei individuellen Gruppen unterschieden:[305]

- η_t = neue Konsumenten,
- η_{t-1} = alte Konsumenten.

Dies entspricht der Situation von überschneidenden Konsumenten in einer Ökonomie, welche auch als „Generation von Konsumenten“ bezeichnet werden.[306]

Die Qualität des potentiellen Standes der Technik wird als T_t (mit $T_t > 0$ und t = 1, 2, 3,…) bezeichnet und ist exogen über die Zeit gegeben. V_t ist der aktuelle Qualitätslevel einer Technologie in Periode t, d.h. eine neue Technologie muss nicht notwendigerweise adoptiert werden, wobei $V_t \leq T_t$ für alle t ist.[307]

$$(9) \qquad V_t = \begin{cases} T_t & \textit{wenn neue Konsumenten in t die neue Technologie adoptieren} \\ V_{t-1} & \textit{sonst.} \end{cases}$$

Gleichung (9) zeigt die aktuelle Technologiequalität, welche von den neuen Konsumenten η_t in Periode t konsumiert werden. Zudem wächst der potentielle Stand der Technik linear um den konstanten Faktor λ:

$$(10) \qquad T_t = \lambda t$$

Ein Konsument nimmt ein Produkt nur an, sofern dieser neu ist, wobei er seinen Nutzenzuwachs nur in der ersten Periode verbraucht. Ferner erwirkt der Nutzen jedes neuen Konsumenten Netzwerkexternalitäten, der sich durch eine Steigerung des

---

[304] Vgl. Shy, O. (2001), S. 84

[305] Vgl. Shy, O. (2001), S. 84

[306] Vgl. Shy, O. (2001), S. 84

[307] Vgl. Shy, O. (2001), S. 85

Nutzens mit zunehmender Anzahl an Konsumenten auswirkt, falls die gleiche Technologie benutzt wird.[308]

Der Nutzen eines neuen Konsumenten der Generation τ lässt sich wie folgt beschreiben:

$$(11) \quad U^{\tau} = \begin{cases} u(T_{\tau}, \eta_{\tau}) & \textit{neue Konsumenten adoptieren aktuelle Techno}\log\textit{ie} \\ u(V_{\tau-1}, \eta_{\tau-1} + \eta_{\tau}) & \textit{neue Konsumenten adoptieren alte Techno}\log\textit{ie} \end{cases}$$

Beide obigen Nutzenfunktionen steigen monoton in beiden Argumenten, wobei:

$$(12) \quad u(T_{\tau}, \eta_{\tau}) \geq u(V_{\tau-1}, \eta_{\tau-1} + \eta_{\tau})$$

Eine neue Technologie, wie z.B. ein Computersystem mit TPM, wird von neuen Konsumenten nur angenommen, wenn der Nutzen des Produkts mit der höheren Qualität verknüpft mit der geringeren Netzwerkgröße den Nutzen des Produktes der alten Technologie übertrifft.[309]

7.3.2.2 Technologische Adoption bei perfekten Substituten

Eine technologische Adaption bei perfekten Substituten setzt lineare Präferenzen voraus:

$$(13) \quad U^{\tau} = \begin{cases} T_{\tau} + \eta_{\tau} & \textit{neue Konsumenten adoptieren aktuelle Techno}\log\textit{ie} \\ V_{\tau-1}, \eta_{\tau-1} + \eta_{\tau} & \textit{neue Konsumenten adoptieren alte Techno}\log\textit{ie} \end{cases}$$

Die nachfolgende Abbildung illustriert die Indifferenzkurven, die aus der Nutzenfunktion (13) abgeleitet werden können.

---

[308] Vgl. Shy, O. (2001), S. 85 f.

[309] Vgl. Shy, O. (2001), S. 87

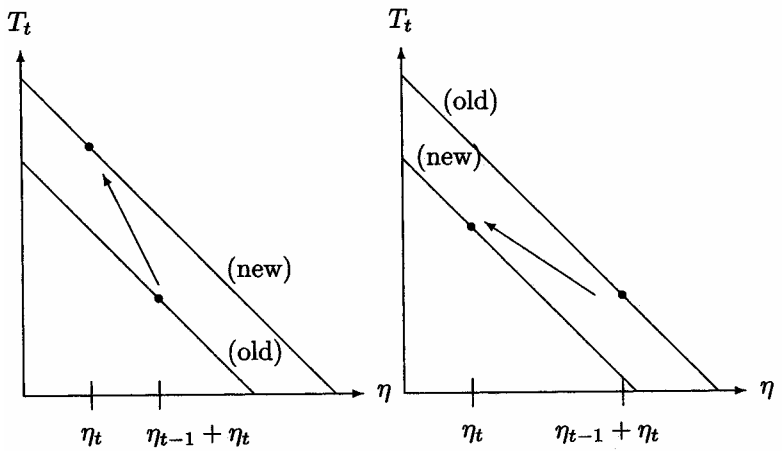

Abbildung 33: Indifferenzkurven bei perfekten Substituten[310]

Auf der linken Seite der Abbildung wird die Adoption einer neuen inkompatiblen Technologie zu einem bestimmten Zeitpunkt abgebildet, dessen Produktvorteil den Nutzenverlust der Netzwerkeffekte der alten Technologie überwiegt. Da im vorhandenen Szenario Einweg-Kompatibilität vorherrscht, ist der Nutzenverlust durch Netzwerkeffekte marginal vorhanden, da die Abwärtskompatibilität den Zugriff auf das bestehende Netzwerk erlaubt. Demgegenüber zeigt der rechte Graph, wie die neue Technologie nicht angenommen wird, da die Verbesserung der Qualität des Produktes nicht ausreichend hoch ist, um den Netzwerkeffekt zu kompensieren.[311] Da vorher der Nutzen eines Computersystems mit TPM als höher eingestuft wurde, dürfte die TPM Technologie demzufolge am Markt adoptiert werden, ceteris paribus.

7.4 Schwächen und Risiken

Die Schwächen und Risiken in Bezug auf „Trusted Computing“ beruhen in der Öffentlichkeit zum Teil auf Annahmen über mögliche Einsatzszenarios. Gründe dafür sind die Inkonsistenz der bereits veröffentlichten Dokumente der TCG und noch immer nicht abgeschlossenen Spezifikationen für das TPM. Dabei wurden technische Details bereits sehr ausgiebig behandelt, jedoch blieben wirtschaftliche Beweggründe und konkrete Anwendungsszenarien bisher im Hintergrund.[312] Ferner sind die Spezifikationen der TCG nur Empfehlungen an einen Hersteller eines TPMs, d.h. er hat die Freiheit nicht alle definierten Funktionen der TPM Spezifikationen in jede

---

[310] Vgl. Shy, O. (2001), S. 89

[311] Vgl. Shy, O. (2001), S. 89

[312] Vgl. BSI (2003)

Komponenten zu implementieren.[313] Auch die US Bürgerrechtsorganisation „Electronic Frontier Foundation“ (EFF) hat ihre Bedenken über Trusted Computing geäußert und sehen ein Problem der existierenden Entwürfe, da diese entscheidend durch die Veröffentlichung beschädigt und neue Risiken für die Wettbewerbsfähigkeit und konsumentenunfreundliches Verhalten dargelegt wurden. Weiter wäre eine falsche Implementierung der Hersteller von Trusted Computern möglich.[314] Auch wird die Attestierung einer Plattform beanstandet, speziell der Druck auf Verlangen eines Challengers eine Attestierung vorzulegen. Als Lösung hierzu schlägt die EFF einen „Owner Override“ vor. Eine Attestierung inklusive Owner Override würde einem Challenger in Kenntnis setzen, wenn die Software des Computers ohne Wissen des Eigentümers verändert worden wäre.[315]

Definitiv ist es möglich mit einem TPM Informationen an eine Plattform zu binden. Dabei sei erneut darauf hingewiesen, dass die Begriffe „Information“ und „Plattform“ weit gefasst sind, um die Dimension dieser Technologie besser zu erfassen. Diese neue Technologie ermöglicht es also Information an ein physisches Medium zu binden, um dessen Verbreitung, Verarbeitung oder Speicherung zu kontrollieren. Dadurch wird die wesentliche Eigenschaft von „Information als öffentliches Gut“ wirksam eingeschränkt und ein Kontrollmechanismus über den Gebrauch von Information ermöglicht. Folglich lassen sich daher auch neue Erlöse mit bestehenden Produkten erschließen, wenn diese um weitere Funktionen und Anwendungen bezüglich des „Trusted Computing“ erweitert werden. Darüber hinaus kann die Preisdiskriminierung für Informationsgüter stärker ausgenutzt werden, was demzufolge die Konsumentenrente reduziert und die Produzentenrente steigert. Das TPM in Verbindung mit NGSCB kann infolgedessen als unterstützende Komponente betrachtet werden, welche die Gewinne von Informationsgütern der Unternehmen maximiert. Mit der neuen Technologie können also höhere Erlöse indirekt oder direkt durch die Anwendungen erzielt werden. Direkte Erlöse beziehen sich auf die Anwendung selbst, demgegenüber beziehen sich die indirekten Erlöse auf die erzeugten Informationen der Anwendung. Die Bindung von Information an eine Plattform steigert dazu das Poten-

---

[313] Vgl. TCG TPM v1.2 Specifications Changes (2003), S. 2

[314] Vgl. Schoen, S. (2003), S. 5

[315] Vgl. Schoen, S. (2003), S. 8 ff.

tial von Lock-in Effekten, indem die Migration der Daten einer vertrauenswürdigen Plattform die Wechselkosten erhöht.[316] Autoren oder Herausgeber von Information könnten die Wechselkosten steigern, indem wichtige Daten des proprietären Systems nur mit der Anwendung des Herausgebers abrufbar sind. Eine Migration der Daten in ein neues Softwaresystem wäre daher sehr schwierig und würde den Benutzer hemmen eine konkurrierende Software zu adoptieren. Zudem ist die Attestierung mitverantwortlich für eine Steigerung der Wechselkosten, da Netzwerkprotokolle in Verbindung mit versiegeltem Speicher die Software-Kompatibilität behindern.[317]

Wesentliche Innovationen im Bereich der Informationstechnik beruhen auf der Vielfältigkeit verfügbarer Lösungen. Allerdings könnten Innovationen und Wachstum durch vertrauenswürdige Plattformen gehemmt werden, behauptet Varian nach einem Ansatz von Eric von Hippel. Als Grund nennt Varian die Kontrolle über das Produkt nach dem Kauf, bzw. die technische Restriktion bestehende Produkte zu modifizieren. Die Benutzer wären dadurch so stark eingegrenzt, dass Konsumenten ihre Ideen unzureichend in die Produkte einbringen könnten. Anwender geben aber eher die Impulse, welche die eigentlichen Innovationen ausmachen, da der Benutzer durch den täglichen Gebrauch viel näher am Produkt ist, wie die Forschungs- und Entwicklungsabteilung eines Herstellers.[318] Trotzdem ist es möglich Anwendungen und Code über die General Public License (GPL) zu vertreiben, welche keine Zertifizierung als Voraussetzung benötigen.[319] Weiterhin kann die Kontrolle über das Produkt nach dem Kauf zu einer weiteren Konzentration der Märkte führen, bzw. zu einem Ausbau der Monopole. Die bereits bestehenden Märkte für Betriebssysteme und der Medienindustrie sind jetzt schon sehr hoch konzentriert, weshalb gerade Standardisierungen in diesem Bereich als kritisch angesehen werden, denn Allianzen könnten mehr etablierten Unternehmen als potentiellen Marktneulingen nützen.[320]

---

[316] Vgl. Anderson, R. (2003a), S. 7 f.

[317] Vgl. Schoen, S. (2003), S.6

[318] Vgl. Varian, H. R. (2002)

[319] Vgl. Safford, D. (2002a), S. 3

[320] Vgl. Varian, H. R. (2002)

8 Zusammenfassung

Die TCG spezifiziert ein vertrauenswürdiges Sicherheitssystem, das eine Komponente eines Systems darstellt. Kompatibilität spielt in diesem Zusammenhang eine wichtige Rolle, wobei die neue Technologie inkompatibel zur alten ist. Allerdings ist das System als Ganzes abwärtskompatibel zu bestehenden Rechnereinheiten und hat somit Zugang zu einem bestehenden Netzwerk. Als Konsequenz der Kompatibilität konkurrieren die Unternehmen innerhalb eines Standards um Anteile anstatt für einen Markt, was anhand der vier Dimensionen *Preis, Produkteigenschaften, Reputation einer Marke* und *Servicedienstleistung* geschieht. Kooperative Standardisierung dämpft folglich den ex-ante Wettbewerb zwischen Standards, währenddem der Wettbewerb im Produktlebenszyklus steigt. Zudem handelt es sich bei dem Standard um eine infrastrukturelle Technologie, in die Konsumenten weniger investieren.

Im Fall der TCG handelt es sich um eine marktliche Standardisierung, aus der ein De-facto-Standard hervorkommt. Die Teilnahme am Standardisierungsgremium ist relativ kostenintensiv, was kleinere Unternehmen tendenziell ausschließt. Dabei verfolgt die Initiative eine kontrollierte Migration als Netzwerkstrategie, d.h. eine neue proprietäre Technologie wird eingeführt, welche die Kompatibilität zur bestehenden Technologie bewahrt. Die Gestaltung der TCG kombiniert die Vorteile der Kontrolle von geschlossenen Allianzen mit den Vorteilen der Marktdurchdringung von offenen Allianzen. Dabei spielt die Wahl der Partner innerhalb der geschlossenen Gruppe eine kritische Rolle. Die geschlossene Gruppe besteht hierarchisch aus den Promoters, den Contributors und den Adaptors. AMD, Hewlett-Packard, IBM, Intel, Microsoft, Sony und Sun Microsystems sind die wirklich einflussreichen Unternehmen der TCG, welche die Promoters als auch den Vorstand zusammenstellen. Ebenso sind die Schlüsselressourcen von Netzwerkeffekten in der Hand der Promotors, die folglich einen enormen Einfluss auf die erfolgreiche Etablierung am Markt haben. Die Problematik des Umgangs mit geistigen Eigentumsrechten hat die TCG über die RAND-Lizenzierung gelöst. Jedoch werden die Eigentlichen Lizenzbedingungen unter den Mitgliedern verhandelt und sind nicht der Öffentlichkeit zugänglich. Daneben können sich Open-Source Entwickler kaum Lizenzgebühren leisten, was zwangsläufig die Entwicklung und Interoperabilität von Software bedroht. Zudem lässt sich die Allianzstruktur als halb offen beschreiben, da der Zugang zu den Promotoren limitiert und geschlossen ist, wohingegen die Contributoren und Adaptoren

Gruppen offen sind. In Bezug auf Coopetition erfolgt eine horizontale sowie vertikale Kooperation der Unternehmen über die unterschiedlichen Stufen der Wertschöpfungskette. Nach der erfolgreichen Standardisierung könnten die Promoters auch die tragende Rolle des Shapers im Technology Web übernehmen, da die Kerntechnologie von ihnen kontrolliert werden würde.

Der TCG Standard besteht aus der Spezifikation des grundlegenden Hardwareteils dem TPM und der Softwareschnittstelle TSS. Das TPM soll sehr kostengünstig in der Produktion sein, aber trotzdem die nötige Sicherheit für die Plattform gewährleisten. Dazu wurde das TPM nach den Common Criteria EAL 3 und FIPS 140-2 zertifiziert, um die Vertraulichkeit sowie den physischen Schutz zu gewährleisten. Der physische Schutz ist jedoch nicht ausreichend gegeben. Weiter bietet das TPM Integrität, geschützten Speicher, Identität sowie sicheres Booten und authentifizierte Bootprozesse als Funktionalität, wobei die Identität die Grundlage für die Attestierung bildet. Durch die Attestierung kann sich ein Challenger über Integrität der Hard- und Software einer Rechnereinheit Sicherheit verschaffen. Allerdings entscheidet der Challenger auch, ob er einem fremden Computer vertraut. Kritisch ist auch die Migrierbarkeit von Daten und Schlüsseln zu betrachten, speziell die der nicht migrierbaren Schlüssel und deren chiffrierte Daten. Nicht migrierbare Schlüssel helfen Informationen an eine Plattform zu binden und dämpfen somit die Eigenschaft von Information als öffentliches Gut. In Verbindung mit dem TPM ermöglichen nicht migrierbare Schlüssel einen Kontrollmechanismus über den Gebrauch von Information. Dadurch werden außerdem die Wechselkosten und gleichzeitig die Lock-in Effekte von Informationen verstärkt.

In der Bewertung der Einweg-Kompatibilität einschließlich dem Szenario der Computersysteme mit und ohne TPM lassen sich zumindest einzelne Aussagen treffen: Ein Computersystem mit TPM stiftet dem Konsumenten einen höheren Nutzen und kann deswegen vom Hersteller im Preis auch höher angesetzt werden. Somit erwirtschaftet der Hersteller eines Computersystems mit TPM auch höhere Gewinne. Diese Aussage scheint plausibel, solange die Wechselkosten von beiden Computersystemen gleich sind. Die soziale Wohlfahrt wäre in Fall von Kompatibilität und Inkompatibilität allerdings nur die zweitbeste Lösung. Bezüglich der statischen Adoption ergeben sich die zwei Nashgleichgewichte (Neu, Neu) und (Alt, Alt). Beharren die Konsumenten trotz eines höheren Nutzens auf der alten Technologie, tritt „excess

inertia“ ein. Wechseln die Konsumenten zur neuen Technologie, obwohl diese einen niedrigeren Nutzen stiftet, tritt „excess momentum“ ein. Die dynamische Adoption substituierbarer Güter liefert aufgrund des höher stiftenden Nutzens der Einweg-Kompatibilität eine Adoption der TPM-Technologie am Markt. Letztlich bleibt abzuwarten, ob sich die neue Technologie tatsächlich als Standard im Markt etablieren kann und wie sie vom Konsument wirklich akzeptiert wird.

Literaturverzeichnis

Akademie.de (2004): „Technologie“, http://www.net-lexikon.de/Technologie.html (Aufruf: 17.02.2004).

Anderson, R. (2003a): „Cryptography and Competition Policy - Issues with Trusted Computing”, in: Proceedings of 2nd Annual Workshop on Economics and Information Security, http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/tcpa.pdf (Aufruf: 20.03.2004).

Anderson, R. (2003b): „’Trusted Computing’ Frequently Asked Questions - TC / TCG / LaGrande / NGSCB / Longhorn / Palladium / TCPA”, http://www.cl.cam.ac.uk/users/rja14/tcpa-faq.html (Aufruf: 20.03.2004).

Atmel (2004a): „Strong Sales Signal Widespread Acceptance of Trusted Computing Standard”, http://www.atmel.com/dyn/corporate/view_detail.asp?ref=&FileName=5Milllion_TPM.html&SEC_NAME=Product (Aufruf: 10.03.2004)

Atmel (2004b): „Atmel Announces Trusted Computing Group 1.2 Security Processor”, http://www.atmel.com/dyn/corporate/view_detail.asp?ref=&FileName=TPM1.2.html&SEC_NAME=Product (Aufruf: 10.03.2004)

Axelrod, R.; Mitchell, W.; Thomas, R. E.; Bennet, D. S.; Bruderer, E. (1995): „Coalition Formation in Standard-setting Alliances”, Management Science Vol. 41, No. 9.

Besen, S. M., Farrell, J. (1994): „Choosing How to Compete: Strategies and Tactics in Standardization”, Journal of Economic Perspectives (8:2), S. 117-131.

Bödecker, P. (2004): Certification Report, https://www.secure.trusted-site.de/certuvit/pdf/9205BE.pdf (Aufruf: 10.03.2004).

Brandenburger, A. M., Nalebuff, B. J. (1995): „The Right Game: Use Theory to Shape Strategy”, in: Harvard Business Review, July-August, S. 57-71.

BSI (2003a): „Sichere Plattformen und die Trusted Computing Group (TCG)“, http://www.bsi.de/tcg/tcgi0312.htm (Aufruf: 10.03.2004).

BSI (2003b): „BSI-Kurzinformationen zu aktuellen Themen der IT-Sicherheit 'Schutzprofile nach Common Criteria'“, http://www.bsi.bund.de/literat/faltbl/ppschutz.pdf (Aufruf: 23.02.2004).

Buxmann, P. (2001): „Standardisierung und Netzeffekte“, in: WISU 04/01, S. 544-558.

Carroll, A.; Juarez, M.; Polk, J.; Leininger, T. (2002): „Microsoft ‘Palladium’: A Business Overview“, http://www.microsoft.com/presspass/features/2002/jul02/0724palladiumwp.asp (Aufruf: 11.03.2004).

CERT (2004): „CERT/CC Statistics 1988-2003“, http://www.cert.org/stats/cert_stats.html (Aufruf: 18.02.2004).

Computer Security Institute (2003): „CSI/FBI Computer Crime and Security Survey", http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf (Aufruf: 18.02.2004).

Coursey, D. (2002): „MS and IBM: A better way to set Web standards", http://reviews-zdnet.com.com/4520-6033_16-4207168.html (Aufruf: 04.02.2004).

derStandard.at (2004): „Windows-Marktanteil 2003 bei 96,4 Prozent nahezu stabil", http://derstandard.at/druck.asp?id=1550293 (Aufruf: 18.03.2004).

Eckert, C. (2003): IT-Sicherheit: Konzepte - Verfahren - Protokolle, 2. Auflage, München.

Eimeren, B.; Gerhard, H.; Frees, B. (2002): „ARD/ZDF-Online-Studie 2002. Entwicklung der Online-Nutzung in Deutschland: Mehr Routine, weniger Entdeckerfreude", Media Perspektiven, o.J., S. 346- 362, http://www.daserste.de/intern/entwicklung2002.pdf (Aufruf: 11.01.2004).

England, P.;Lampson, B.; Manferdelli, J.; Peinado, M.; Willman, B. (2003): „A Trusted Open Platform", in: IEEE Computer Society, Vol. 36, No. 7, S. 55-62.

Farrell, J.; Saloner, G. (1988): „Coordination through Committees and Markets", The RAND Journal of Economics (19:2), S. 235-252.

FBI National Press Office (2004): „FBI, in partnership with Entertainment and Software Industries announce Anti-Piracy Warning Initiative", http://www.fbi.gov/pressrel/pressrel04/piracy021904.htm (Aufruf: 29.02.2004)

Gemeinsame Kriterien Version 2.1 (1999): „Teil 3: Anforderungen an die Vertrauenswürdigkeit", http://www.bsi.de/cc/cct3_21.pdf (Aufruf: 26.02.2004)

Hagel, J. (1996): „Spider versus Spider", in: McKinsey Quarterly Number 1, S. 5-18.

Hass, B. H. (2002): „Management neuer Medienunternehmen: Ökonomische Grundlagen und Innovative Geschäftsmodelle", München.

Hewlett Packard (2004a): „HP Business PC Security Solutions", http://h18004.www1.hp.com/products/security/ (Aufruf: 10.03.2004).

Hewlett Packard (2004b): „Intellectual property licensing", http://www.hp.com/hpinfo/abouthp/iplicensing/ (Aufruf: 17.02.2004).

IBM (2004): „Definition integrierte IBM Sicherheits-Subsystem 2.0", http://www.pc.ibm.com/europe/wireless/de/security.html (Aufruf: 11.03.2004).

IBM (2003): „SolutionsClient Security Software Version 5.2 Installation Guide", ftp://ftp.software.ibm.com/pc/pccbbs/commercial_desktop/ins52mst.pdf (Aufruf: 11.03.2004).

IBM's Global Security Analysis Lab (2004a): „IBM Watson Research - Global Security Analysis Lab: TCPA Resources", http://www.research.ibm.com/gsal/tcpa/ (Aufruf: 11.03.2004).

IBM's Global Security Analysis Lab (2004b): „TCPA Device Driver for Linux", http://www.research.ibm.com/gsal/tcpa/tpm-1.1b.tar.gz (Aufruf: 11.03.2004).

Infineon (2003): „Trusted Platform Module Flyer", http://www.infineon.com/cmc_upload/documents/079/908/TPMFlyer04-2003.pdf (Aufruf: 10.03.2004).

Intel (2003a): „Intel Desktop Board D865GRH", http://developer.intel.com/design/motherbd/rh/index.htm (Aufruf: 10.03.2004).

Intel (2003b): „LaGrande Technology Architectural Overview", ftp://download.intel.com/technology/security/downloads/LT_Arch_Overview.pdf (Aufruf: 15.03.2004).

Intel (2003c): „Intel Hardware Design – Security", http://www.intel.com/technology/security/ (Aufruf: 15.03.2004).

Intel (2003d): „LaGrande Technology and Safer Computing Overview", http://www.intel.com/technology/security/downloads/LT_overview_fall_idf03.htm (Aufruf: 15.03.2004).

Jakobs, K. (2002): „IT Normen und Standards - Grundlage der Informationsgesellschaft", in: Die Innovative Gesellschaft - Nachfrage für die Lead-Märkte von morgen, Berlin, S. 83-88.

Jakobs, K.; Procter, R.; Williams, R. (2001): „Standardisation and Implementation of Information Technology", in: In Slavinski, G. and Hollis, B. (Eds.) Proceedings of IRMA'2001, the Twelfth International Conference of the Information Resources Management Association, Toronto.

Katz, M.; Shapiro, C. (1985a): „Network Externalities, Competition, and Compatibility", in: American Economic Review, Vol. 75 (1985), S. 424 - 440.

Katz, M.; Shapiro C. (1985b): „On the Licensing of Innovations", Rand Journal of Economics, Winter.

Keil, T. (2002): „De-facto standardization through alliances - lessons from Bluetooth", Telecommunications Policy 26, S. 205-213.

Lecocq, X.; Demil, B. (2002): „Open standard: role of externalities and impact on the industry structure", Open Source Community, Massachusetts Institute of Technology, http://opensource.mit.edu/papers/lecocqdemil.pdf (Aufruf: 01.02.2004).

LEO Dictionary Team (2004): „Suchergebnis für das Verb to enforce", http://dict.leo.org/?p=2Ib6..&search=enforce (Aufruf: 11.03.2004).

MacDonald, R.; Smith, S.; Marchesini, J.; Wild, O. (2003a): „Bear: An Open-Source Virtual Secure Coprocessor based on TCPA", http://www.cs.dartmouth.edu/~sws/papers/msmw03.pdf (Aufruf: 07.03.2004).

MacDonald, R.; Smith, S.; Marchesini, J.; Wild, O. (2003b): „Experimenting with TCPA/TCG Hardware, Or: How I Learned to Stop Worrying and Love The Bear", http://www.cs.dartmouth.edu/~sws/papers/mswm03.pdf (Aufruf: 07.03.2004).

Microsoft (2004): „Trustworthy Computing", http://www.microsoft.com/mscorp/twc/default.mspx (Aufruf: 11.03.2004).

Microsoft (2003a): „The Next-Generation Secure Computing Base: An Overview", http://www.microsoft.com/resources/ngscb/NGSCB_overview.mspx (Aufruf: 11.03.2004).

Microsoft (2003b): „The Next-Generation Secure Computing Base: Four Key Features", http://www.microsoft.com/resources/ngscb/four_features.mspx (Aufruf: 11.03.2004).

Microsoft (2003c): „Microsoft Next-Generation Secure Computing Base - Technical FAQ", http://www.microsoft.com/technet/security/news/ngscb.mspx (Aufruf: 12.03.2004).

Microsoft (2003d): „Privacy-Enabling Enhancements in the Next-Generation Secure Computing Base - White Paper", http://download.microsoft.com/download/8/d/5/8d5ec8cf-3e09-49e0-95dd-0a6a3ded510f/NGSCB_Privacy_Enhancements.doc (Aufruf: 12.03.2004).

Microsoft (2003e): „Security Model for the Next-Generation Secure Computing Base", http://www.microsoft.com/resources/ngscb/documents/NGSCB_Security_Model.doc (Aufruf: 12.03.2004).

Microsoft (2003f): „Secure User Authentication for the Next-Generation Secure Computing Base", http://www.microsoft.com/resources/ngscb/documents/ngscb_authentication.doc (Aufruf: 12.03.2004).

Microsoft (2003g): „Windows Rights Management Services Data Sheet", http://download.microsoft.com/download/6/d/0/6d0c8e76-65ef-4a13-9e8c-28a5caea482f/RMSDataSheet.doc (Aufruf: 15.03.2004).

Microsoft (2003h): „Technical Overview of Windows Rights Management Services", http://download.microsoft.com/download/8/d/9/8d9dbf4a-3b0d-4ea1-905b-92c57086910b/RMSTechOverview.doc (Aufruf: 15.03.2004).

National Semiconductor (2002): „PRODUCT BRIEF - PC21100 (SafeKeeper)", http://cache.national.com/ds/PC/PC21100.pdf (Aufruf: 10.03.2004).

Nieschlag, R.; Dichtl, E.; Hörschgen, H. (1997), „Marketing", 18. Auflage, Berlin.

Panzar, J. C.; Willig, R. D. (1981): „Economies of scale", in: American Economic Review 71:2, S. 268-272.

Pearson, S. (2002): „Trusted Computing Platforms, the Next Security Solution", http://www.hpl.hp.com/techreports/2002/HPL-2002-221.pdf (Aufruf: 04.03.2004)

Pearson, S. et. al. (2002): „Trusted Computing Platforms - TCPA in Context", Prentice Hall, Boston.

Richardson, R. (2003): „CSI/FBI Computer Crime and Security Survey", http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf (Aufruf: 18.02.2004).

Safford, D.; Kravitz, J.; van Doorn, L. (2003): „Take Control of TCPA", in: Linux Journal, Volume 2003, Issue 112, Seite 2.

Safford, D. (2002a): „Clarifying Misinformation on TCPA", http://www.research.ibm.com/gsal/tcpa/tcpa_rebuttal.pdf (Aufruf: 06.03.2004).

Safford, D. (2002b): „The Need for TCPA", http://www.research.ibm.com/gsal/tcpa/why_tcpa.pdf (Aufruf: 06.03.2004).

Schoen, S. (2003): „Trusted Computing: Promise and Risk“, http://www.eff.org/Infra/trusted_computing/20031001_tc.pdf (Aufruf: 04.11.2003).

Shapiro, C. (2001a): „Setting Compatibility Standards: Cooperation or Collusion?“, in: Rochelle et. al., Expanding the Boundaries of Intellectual Property, Oxford University Press, S. 81-102.

Shapiro, C. (2001b): „Navigating the Patent Thicket: Cross Licenses, Patent Pools, and Standard-Setting“, in: Innovation Policy and the Economy, Vol. I, Josh, Lerner, Adam B., Jaffe, Scott, Stern et. al., MIT Press.

Shapiro, C.; Katz, M. (1985): „Network Externalities, Competition, and Compatibility“, in: The American Economic Review, Volume 75, Issue 3, S. 424-440.

Shapiro, C.; Varian, H. R. (1998): „Information Rules: A Strategic Guide to the Network Economy“, Boston (Mass.).

Shapiro, C.; Varian, H. R. (1999): „The Art of Standards Wars“, California Management Review 41, S. 8-32.

Shy, O. (2001): „The Economics of Network Industries“, Cambridge University Press.

Shy, O.; Morgan, P. B. (2000): „Undercut-Proof Equilibria“, http://econ.haifa.ac.il/~ozshy/conhot71.pdf (Aufruf: 19.02.2004)

Stähler, P. (2002): „Geschäftsmodelle in der digitalen Ökonomie : Merkmale, Strategien und Auswirkungen“, Köln.

Stiller, A. (2004): „Prozessorengeflüster“, in: c't 2/2004.

TCG-Backgrounder (2003):
http://www.trustedcomputinggroup.org/downloads/TCG_Backgrounder.pdf (Aufruf 05.12.2004).

TCG-Current Members (2004):
https://www.trustedcomputinggroup.org/about/members/ (Aufruf: 05.01.2004).

TCG Main Specification Version 1.1b:
https://www.trustedcomputinggroup.org/downloads/Main_TCG_Architecture_v1_1b.zip (Aufruf: 23.02.2004).

TCG PC Specific Implementation Specification Version 1.1:
https://www.trustedcomputinggroup.org/downloads/TCG_PCSpecificSpecification_v1_1.pdf (Aufruf: 23.02.2004).

TCG Software Stack Specification Version 1.1:
https://www.trustedcomputinggroup.org/downloads/TSS_Version__1.1.pdf (Aufruf: 23.02.2004).

TCG TPM Specification Version 1.2 (2003a): „Design Principles“, https://www.trustedcomputinggroup.org/downloads/tpmwg-mainrev62_Part1_Design_Principles.pdf (Aufruf: 23.02.2004).

TCG TPM Specification Version 1.2 (2003b): „Structures of the TPM“, https://www.trustedcomputinggroup.org/downloads/tpmwg-mainrev62_Part2_TPM_Structures.pdf (Aufruf: 23.02.2004).

TCG TPM Specification Version 1.2 (2003c): „TPM Commands“, https://www.trustedcomputinggroup.org/downloads/tpmwg-mainrev62_Part3_Commands.pdf (Aufruf: 23.02.2004).

TCG TPM v1.2 Specifications Changes (2003): https://www.trustedcomputinggroup.org/downloads/TPM_1_2_Changes_final.pdf (Aufruf: 23.02.2004).

TCPA Membership (2004), http://www.trustedcomputing.org/home/membership/ (Aufruf: 06.03.2004).

Varian, H. R. (2003): „Economics of Information Technology“, http://www.sims.berkeley.edu/~hal/Papers/mattioli/mattioli.pdf (Aufruf: 19.01.2004).

Varian, H. R. (2002): „New chips can keep a tight rein on consumers, even after they buy a product“, in: New York Times, 4. Juli, http://www.sims.berkeley.edu/~hal/people/hal/NYTimes/2002-07-04.html (Aufruf: 21.02.2004).

Varian, H. R. (2001): „High-Technology Industries and Market Structure“, http://www.sims.berkeley.edu/~hal/Papers/structure.pdf (Aufruf: 19.01.2004).

Varian, H. R. (1998): „Markets for Information Goods“, http://www.sims.berkeley.edu/~hal/Papers/japan/japan.pdf (Aufruf: 19.01.2004).

Varian, H. R. (1997): „Versioning Information Goods“, http://www.sims.berkeley.edu/~hal/Papers/version.pdf (Aufruf: 19.01.2004).

Ward, J. (2004): „Keine Hintertüren – Interview mit Jim Ward, Leiter der Trusted Computing Group“, in: c’t 01/2004, S. 76-77.

Wave Systems (2004): „Trusted Computing Group (TCG) Compliant Solutions”, http://www.wavesys.com/products/ets.html (Aufruf: 10.03.2004).

Weitzner, D., Herman, M., Peterson, S., Piotrowski, T., Rein, B., Plotka Workman, H. (2001): „W3C Patent Policy Framework Working Draft“, http://www.w3.org/TR/2001/WD-patent-policy-20010816/#def-RAND (Aufruf: 04.02.2004).

Wikipedia (2004): Kooperation, http://de.wikipedia.org/wiki/Kooperation (Aufruf: 13.02.2004).

Wild, O. (2003): Enforcer Homepage, http://enforcer.sourceforge.net (Aufruf: 11.03.2004).

Zerdick, A. (2001): „Die Internet-Ökonomie“, 3. Auflage, Berlin et al.

Ehrenwörtliche Erklärung

Versicherung

Ich versichere hiermit, dass ich die vorliegende Arbeit selbständig und nur unter Benutzung der angegebenen Literatur und Hilfsmittel angefertigt habe. Wörtlich übernommene Sätze und Satzteile sind als Zitate belegt, andere Anlehnungen hinsichtlich Aussage und Umfang unter den Quellenangaben kenntlich gemacht. Die Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen und ist nicht veröffentlicht.

Ort, Datum: _____

Unterschrift: _____