



Fachhochschule Bonn-Rhein-Sieg

# Neue Konzepte zur Sicherung von Urheberrechten aus dem Blickwinkel des Datenschutzes

4. Dezember 2005

Daniel Müller  
Karsten Reineck

Studienarbeit zur Erlangung eines Leistungsnachweises im 5. Semester für Recht/Rechtinformatik

*„Copyright and freedom of speech cannot coexist.  
One of them has to go.“*

Ian Clarke  
(Entwickler der P2P-Börse „Freenet“)

## Inhaltsverzeichnis

1.	Kurzdarstellung.....	4
2.	Gesetzliche Lage.....	5
2.1.1.	Urheberrecht .....	5
2.1.2.	Recht auf Privatkopie .....	5
2.1.3.	Bundesdatenschutzgesetz .....	6
3.	Digital Rights Management.....	8
3.1.	Einleitung.....	8
3.2.	Technische Voraussetzung und Umsetzung .....	9
3.2.1.	Versuche, DRM zu umgehen .....	10
3.3.	Vorteile des DRM für Rechteinhaber und Nutzer.....	11
3.4.	Nachteile des DRM für den Nutzer .....	11
3.5.	Probleme des Datenschutzes.....	12
3.6.	Nutzerprofile vs. Schutz der Privatsphäre.....	13
4.	Verschiedene Konzepte des DRM.....	14
4.1.	Einleitung.....	14
4.2.	Pay-TV.....	14
4.3.	Audiokopierschutz .....	15
4.3.1.	XCP .....	15
4.3.2.	MediaMax.....	17
4.4.	Microsoft Windows Media Rights Manager.....	18
4.4.1.	Vorgehensweise bei Windows Media DRM.....	18
4.4.2.	Secure Audio Path.....	20
4.4.3.	Musicload .....	20
4.5.	Apple FairPlay .....	22
4.5.1.	Datenschutz bei Apple FairPlay .....	22
4.6.	Adobe DRM Activator .....	23
4.6.1.	Datenschutz bei Adobe und bei der Adobe-ID .....	24
4.7.	Trusted Computing .....	24
4.7.1.	Trusted Computing für DRM-Systeme.....	25
4.7.2.	Next-Generation Secure Computing Base für DRM .....	25
4.7.3.	Gefahren des Trusted Computing .....	26
4.8.	HD-DVD & Blu-ray Disc.....	28
4.8.1.	AACs.....	28
4.8.2.	Gefahren des AACs .....	29
5.	Fazit und Ausblick.....	30
6.	Abbildungen.....	32
7.	Literaturverzeichnis.....	33

## 1. Kurzdarstellung

Diese Ausarbeitung zum Thema „Neue Konzepte zur Sicherung von Urheberrechten aus dem Blickwinkel des Datenschutzes“ beschäftigt sich mit aktuellen sowie zukünftigen Maßnahmen zum Schutz des Urheberrechts.

Zunächst wird ein Blick auf die gesetzliche Lage geworfen, dazu zählen die Maßnahmen des Gesetzgebers zum Thema Urheberrecht und welche Rechte zum Schutz der Privatsphäre existieren.

Das zweite Kapitel gibt dann einen Überblick darüber, was man sich unter einem digitalen Rechtemanagement (DRM) vorzustellen hat und welche technischen Voraussetzungen diese mitbringen. In diesem Zusammenhang wird auch kurz aufgedeckt, welche Versuche es gibt, solche Systeme zu umgehen und wie dies verhindert wird. Basierend auf diesen Erkenntnissen werden die Vor- und Nachteile von DRM aufgezeigt, zu denen auch der unzureichende Datenschutz gehört.

Gegenstand des darauf folgenden Kapitels sind sowohl aktuelle DRM-Systeme als auch Zukunftsmodelle, die unter Datenschutzaspekten kritisch betrachtet werden. Dazu zählen bereits etablierte Schutzmaßnahmen aus dem Pay-TV-Bereich, aus dem Musikbereich in Form von Audiokopierschutz und Online-Musikdistribution sowie dem Schutzmanagement bei digitalen Büchern (eBooks). Zukünftige Konzepte werden anhand von Trusted Computing und dem digitalen Rechtemanagement, welches beim DVD-Nachfolger HD-DVD bzw. Blu-ray Disc zum Einsatz kommen soll vorgestellt. Der Fokus wurde dabei weniger auf die technische Beschreibung sondern vielmehr auf die Erklärung der Vorgehensweise dieser Systeme und den daraus resultierenden Gefahren für die Privatsphäre gesetzt.

Ein abschließendes Fazit und ein kurzer Ausblick, womit man in Zukunft zu rechnen hat und worauf man bereits heute achten sollte, bilden den Schluß dieser Arbeit. DM

## 2. Gesetzliche Lage

### 2.1.1. Urheberrecht

Das Urheberrechtsgesetz wurde ursprünglich im Jahre 1965 in der Bundesrepublik Deutschland eingeführt. „Das Urheberrecht schützt den Urheber in seinen geistigen und persönlichen Beziehungen zum Werk und in der Nutzung des Werkes.“ (§ 11 UrhG). Es wurde seit seiner Einführung schon mehrmals aktualisiert und zuletzt trat am 13. September 2003 der „Erste Korb“ der Novellierung des Urheberrechts in Kraft. Damit wurde im Wesentlichen die neue EU-Richtlinie zum Thema „Urheberrechtsschutz in der Informationsgesellschaft“ (2001/29/EG) umgesetzt. Alles, was die Richtlinie nicht zwingend vorschreibt, sondern den Mitgliedstaaten zur Regelung überlässt, blieb dem "Zweiten Korb" vorbehalten. Dieser „Zweite Korb“, der sich unter anderem noch weitergehend mit dem Recht auf die Privatkopie auseinandersetzt, steht momentan noch aus.

Mit dem ersten Teil der Novellierung wurde aber bereits der Schutz des geistigen Eigentums an die neuen Anforderungen, bedingt durch die rasante Entwicklung des Internets als Vertriebsplattform, angepasst. <sup>DM</sup>

### 2.1.2. Recht auf Privatkopie

Zentrale Vorschriften für die Frage, ob in Zukunft noch Kopien von Datenträgern zu privaten Zwecken hergestellt werden dürfen, finden sich in den §§53 und 95a ff. UrhG. §53 UrhG hält dabei zunächst ausdrücklich daran fest, dass Kopien zum privaten Gebrauch erlaubt bleiben. Ergänzt wurde diese Regelung durch die bisher schon geltende Rechtslage, dass Kopien nur dann zulässig sind, wenn sie nicht offensichtlich aus einer illegal hergestellten Vorlage stammen, wie man sie vorwiegend in Internet Tauschbörsen findet.

Eine sehr kontroverse Änderung betrifft den §95a ff. UrhG. Hiernach darf nämlich auch der private Nutzer Kopien zum eigenen Gebrauch grundsätzlich nur dann herstellen, wenn er dazu eine technisch wirksame Schutzvorrichtung nicht umgeht. Zum einen stellt sich hier die Frage, wie man eine „technisch wirksame Schutzvorrichtung“ überhaupt definiert und zum anderen, weshalb technisch wirksame Schutzvorrichtungen überhaupt des Schutzes bedürfen? „Sind unwirksame techni-

sche Schutzvorrichtungen nicht schutzwürdig?“ hinterfragt z. B. auch der Landesbeauftragte für Datenschutz und für das Recht auf Akteneinsicht in Brandenburg, Alexander Dix in einem Symposium zum Thema „DRM und Alternativen“ [DIX01]. Gemeint sind hiermit natürlich auch andere Schutzvorrichtungen, wie sie beispielsweise bei Pay-TV in Form von Zugangskontrollsystemen zu finden sind und die vor dem steigenden Anteil an Piraterie durch gefälschte Zugangskarten geschützt werden sollen. In erster Linie betrifft diese Änderung aber das Recht auf die Privatkopie und brisanterweise auch das Recht auf Meinungs- und Informationsfreiheit, da schon das Bereitstellen von Informationen zum Umgehen dieser Schutzvorrichtungen gesetzwidrig ist. <sup>DM</sup>

### 2.1.3. Bundesdatenschutzgesetz

Das deutsche Bundesdatenschutzgesetz (BDSG) besteht seit 1978 und regelt zusammen mit den Datenschutzgesetzen der Bundesländer und anderen bereichsspezifischeren Regelungen den Umgang mit personenbezogenen Daten, die in IT-Systemen oder manuell verarbeitet werden.

Das BDSG gliedert sich in sechs Abschnitte. So regelt der erste Abschnitt (§§1 - 11) die allgemeinen Vorschriften, die auch essentiell für die weiteren Regelungen sind. Für die öffentlichen Stellen, aber z. T. auch für private Unternehmen entscheidend ist der zweite Abschnitt (§§12 - 26), während der dritte Abschnitt (§§27 - 32) rein für die privaten Unternehmen von Bedeutung ist. Der vierte Abschnitt (§§39 - 42) enthält Sondervorschriften, Abschnitt fünf (§§43 - 44) regelt die Buß- und Strafgeldvorschriften und im letzten Abschnitt (§§45 - 46) finden sich Übergangsvorschriften. Entscheidend für die weitere Betrachtung von den aktuell technisch möglichen Schutzmaßnahmen und den Planungen zum Schutz des Urheberrechts aus dem Blickwinkel des Datenschutzes sind die Vorschriften aus dem ersten Abschnitt.

Das Gesetz umschreibt seine Zweckbestimmung in § 1 Abs. 1 wie folgt: „Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.“

Das Persönlichkeitsrecht wird abgeleitet aus den Grundrechten der Verfassung. In Artikel 1 Abs. 1 des Grundgesetzes heißt es: „Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist die Verpflichtung aller staatlichen Gewalt.“ Und weiter steht in Artikel 2 Abs. 1 Grundgesetz: „Jeder hat das Recht auf freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.“ Diese beiden Grundsätze bilden also die Grundlage des Datenschutzes.

Das Bundesverfassungsgericht hat im so genannten Volkszählungsurteil vom 15. Dezember 1983 herausgestellt: „Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“ [BVG01]. Damit ist gemeint, dass jeder Einzelne ein Recht auf informationelle Selbstbestimmung hat, um somit seine Privatsphäre zu erhalten. Jeder hat das Recht zu wissen, wer was wann über ihn weiß.

DM

### **3. Digital Rights Management**

#### **3.1. Einleitung**

Bei Digital Rights Management (DRM) handelt es sich um ein System, mit technischen Mitteln das gesetzlich festgelegte Urheberrecht durchzusetzen und den Anbietern digitaler Inhalte eine Möglichkeit der Abrechnung zu geben.

Der Schutz des Urheberrechts hat in den letzten Jahren immer mehr an Bedeutung gewonnen, denn es wird immer einfacher, multimediale Inhalte ohne Qualitätsverlust zu kopieren und zu verbreiten. Die Ursachen liegen im technischen Fortschritt auf Seiten der Software, Hardware und Vernetzung.

Softwareseitig erlauben z. B. Komprimierungsverfahren wie MP3 für Audio- und DivX für Videodaten die Reduzierung der Daten auf eine bequem zu übertragende Dateigröße. Immer preiswertere Hardware (sowohl Medien wie DVD-Rohlinge als auch DVD-Brenner oder tragbare MP3-Player) unterstützt das Kopieren und Archivieren geschützter Inhalte. Letztendlich hat auch die fortlaufende Ausbreitung des Internets in jeden ‚modernen‘ Haushalt und die Nutzung von Filesharing-Tools wie eMule, mit dem sich (kostenlos und illegal) jegliche Art digitalen Inhalts (Software, Musik, Video, Bücher, ...) herunterladen lässt, dazu geführt, dass sich u. a. Softwarehersteller und Musikindustrie zusammengesetzt haben, dem entgegen zu wirken.

DRM ist ein Schritt in diese Richtung: Es ermöglicht den Anbietern digitaler Inhalte die Nutzung ihres Angebots mit technischen Mitteln zu kontrollieren und damit die Nutzer zur Zahlung zu veranlassen. Dies ist nicht der erste Versuch: Schon seit den 80er Jahren versuchen z. B. Software-Hersteller durch Schutzmaßnahmen die Missachtung des Urheberrechts zu bekämpfen und die Musikindustrie durch Kopierschutzverfahren CDs ‚unkopierbar‘ zu machen. Diese Schutzmaßnahmen hatten eine gemeinsame Schwäche: Sie basierten meist ausschließlich auf Software. Dadurch war es versierten ‚Crackern‘ möglich, den Schutz zu umgehen. Heute existieren Mechanismen, die Inhalte software- und hardwareseitig schützen. Diese sind nicht mehr so einfach durch Manipulation der Software auszuhebeln, da die Hardware auf diese Weise nicht umgangen werden kann; dieser Weg wird heute beschritten. KR

### **3.2. Technische Voraussetzung und Umsetzung**

Voraussetzung für die Durchsetzung des DRM sind verschiedene technische Hilfsmittel. Dazu zählen z. B. digitale Wasserzeichen, mit denen einzelne Inhalte eindeutig ‚beschriftet‘ und so identifizierbar werden. Wird der Inhalt unrechtmäßig kopiert, wird auch das Wasserzeichen kopiert und somit transparent, vom wem die Kopie stammt. Bei einem digitalen Wasserzeichen handelt es sich um digitale Informationen, die so in einen digitalen Inhalt (wie ein Bild oder ein Musikstück) eingebettet werden, dass die Veränderungen zum Original zu gering sind, um vom menschliche Auge bzw. Ohr wahrgenommen zu werden. Dabei ist das Wasserzeichen so stark mit dem Inhalt ‚verknüpft‘, dass die Entfernung den Inhalt zerstören würde.

Das wichtigste technische Hilfsmittel ist die Verschlüsselung. Ein verschlüsselter Inhalt bleibt so lange unbrauchbar, bis er entschlüsselt wird. In einem auf DRM basierenden System liegt der Inhalt immer nur in verschlüsselter Form vor, z. B. auf einem zentralen Server. Ein weiterer Server ist für die Verwaltung der Rechte zuständig. Dieser kennt alle Benutzer und weiß, welcher Nutzer welchen Inhalt ansehen oder abspielen darf. Es gibt DRM-Verfahren, die offline funktionieren. Zur Zeit sind jedoch noch sicherere Verfahren in der Entwicklung, die nur funktionieren, wenn man eine Verbindung mit dem Internet hat. Letztere Verfahren funktionieren wie folgt:

Möchte ein Nutzer auf einen bestimmten Inhalt zugreifen, z. B. ein Musikstück wiedergeben, meldet sich die Wiedergabesoftware bei dem lokalen DRM-Dienst. Dieser fragt zum einen den eigentlichen Inhalt vom Inhaltserver ab, zum anderen wendet er sich an den Rechteserver. Dieser überprüft nach erfolgreicher Authentifizierung ob der Nutzer das Recht hat, das Stück abzuspielen und ggf. den korrekten Schlüssel zum Entschlüsseln des Inhalts übermittelt hat. Wenn der Nutzer das Recht hat, das Stück abzuspielen, ist der DRM-Dienst in der Lage, den Inhalt mittels des übertragenen Schlüssels zu entschlüsseln und kann das abspielfähige Stück an die Wiedergabesoftware weiterleiten. In allen anderen Fällen lässt sich das Musikstück nicht abspielen, da es nicht entschlüsselt werden kann. Auch wenn das Stück auf den lokalen Computer heruntergeladen wurde bleibt es unbrauch-

bar, solange das Stück nicht rechtmäßig erworben und damit der entsprechende Schlüssel vorgelegt wird.

Heute sind (noch) Verfahren gebräuchlich, die keine ständige Verbindung ins Internet benötigen. Sie haben den Vorteil, dass man nur einmalig eine Verbindung ins Internet herstellen muss, bei der alle relevanten Informationen, die zum Abspielen benötigt werden, heruntergeladen werden. Ein großer Nachteil aus Sicht der Anbieter ist es, dass sie nicht nachträglich auf die geschützten Daten zugreifen können um sie z. B. im Falle einer unrechtmäßigen Aktivität zu sperren. KR

### 3.2.1. Versuche, DRM zu umgehen

Ein Musikstück wird vom Inthalteserver so verschlüsselt, dass es nur mit dem privaten Schlüssel des Käufers entschlüsselt werden kann. Wenn also die Datei z. B. über ein Filesharing-Tool unrechtmäßig verbreitet wird, sind auch die Kopien nur mit dem privaten Schlüssel des Käufers abspielbar. Ein unrechtmäßiger Besitzer kann diese Datei zwar auch auf seinem Computer speichern, diese aber mit seinem privaten Schlüssel nicht entschlüsseln und somit abspielen.

Wenn auch der private Schlüssel des Käufers über das Internet verbreitet wird, wäre es theoretisch möglich, das Stück damit wieder zu entschlüsseln. Aber es ist davon auszugehen, dass der Inthalteanbieter dies früher oder später mitbekommt und dann den Schlüssel als ungültig deklariert. Dadurch wäre weder der Käufer noch der unrechtmäßige Besitzer in der Lage, das Musikstück abzuspielen. Diese Maßnahme wird den Käufer davon abhalten so zu handeln. Eine weitergehende Methode ist den Schlüssel in Hardware zu implementieren; ein Ansatz den die Trusted Computing Group (TCG) verfolgt. In diesem Fall ist ein Musikstück tatsächlich nur auf einem spezifischen Computer abspielbar, der die richtige Hardwarekomponente besitzt. Der Schlüssel wird dabei in die Komponente so ‚eingebrennt‘, dass er nicht ausgelesen oder kopiert werden kann.

Auch den Versuch DRM zu umgehen, indem der Käufer das entschlüsselte Stück verbreitet, verhindert ein vollständig auf DRM basierendes System: Wie anfangs erwähnt liegen die Inhalte immer nur in verschlüsselter Form vor. Erst in letzter Instanz – nämlich vor der tatsächlichen Wiedergabe – werden die Daten explizit für

die Wiedergabe entschlüsselt. Die DRM-fähige Wiedergabesoftware erlaubt es nicht, den Inhalt unverschlüsselt zu speichern. KR

### **3.3. Vorteile des DRM für Rechteinhaber und Nutzer**

Die Vorteile für den Rechteinhaber liegen auf der Hand: Er ist mittels DRM in der Lage zu kontrollieren, wer sich z. B. ein Musikstück (oder das Recht ein Musikstück zu hören) gekauft hat und kann nur den rechtmäßigen Käufern erlauben, dieses Stück auf einem speziellen Gerät abzuspielen. Wenn das Stück unrechtmäßig kopiert wurde, fehlt dem neuen Besitzer das Recht das Stück abzuspielen. Auch er müsste es rechtmäßig kaufen, da die Kopie sich nicht abspielen lässt. Ein vollständig auf DRM basierendes System würde so den Raubkopien ein Ende bereiten. ‚Vollständig‘ daher, weil ein nur teilweise DRM-sicheres Verfahren das gesamte System untergraben könnte, denn es gäbe dann die Möglichkeit das System zu umgehen. Die gegenwärtigen Verfahren lassen sich noch alle umgehen, da die heute aktuellen Betriebssysteme und die zugrunde liegende Hardware nicht DRM-fähig sind (siehe dazu z. B. Apple FairPlay).

Die Vorteile für den Nutzer sind nicht offensichtlich: In einer perfekt vernetzten Welt könnte man sich vorstellen, dass der Nutzer gar nicht mehr lokal eine Datei mit dem Musikstück speichern muss, er kauft nur noch das Recht, ein bestimmtes Stück abzuspielen. Dieses liegt zentral auf einem über das Internet erreichbaren Server. Der Nutzer könnte von überall auf der Welt über seinen Computer, sein Laptop, sein Handy, oder seinen tragbaren MP3-Player auf sein Musikstück zugreifen, sofern er sich zuvor als rechtmäßiger Nutzer an den Geräten authentifiziert. Er müsste sich nicht mehr um die Archivierung kümmern und keinen großen lokalen Speicher mehr haben, sondern nur noch DRM-fähige Abspielgeräte. KR

### **3.4. Nachteile des DRM für den Nutzer**

Leider haben DRM-Systeme für den Nutzer nicht nur Vorteile. Zu den größten Nachteilen zählen geringere Benutzerfreundlichkeit und die Einschränkung bei der Nutzung für private Zwecke.

Die Benutzerfreundlichkeit nimmt dadurch ab, dass z. B. bei jedem Öffnen eines mittels DRM geschützten Inhalts erst die Rechte an diesem Inhalt überprüft werden

müssen. Zum einen könnte je nach Verfahren dafür eine Verbindung zum Internet unabdingbar sein, zum anderen kostet die Überprüfung Zeit und Ressourcen und damit auch Geld. Viel schlimmer ist der Gedanke, dass bei Ausfall einer Teilkomponente (z. B. die Server auf Anbieterseite, die lokale Verbindung ins Internet, ein Fehler im Betriebssystem oder im DRM-Dienst usw.) das gesamte System versagt. Dies liegt daran, dass ein DRM-System nicht funktionieren kann, wenn alles erlaubt wäre, was nicht verboten ist. Stattdessen arbeitet es so restriktiv, dass grundsätzlich alles verboten ist, was nicht explizit erlaubt ist. In diesem Fall wäre das geschützte Musikstück nicht abspielbar. Man stelle sich aber eine Situation vor, in der alle möglichen Arten von Dokumenten geschützt sind, so z. B. auch Word-Dokumente, die durch solch einen Fehler nicht mehr zu öffnen wären. Ein derartiger Ausfall könnte im privaten Bereich lästig sein, wenn sich beispielsweise die Bachelorarbeit nicht mehr öffnen lässt, im wirtschaftlichen Bereich könnte ein Fehler allerdings einen ganzen Betrieb lahm legen. KR

### **3.5. Probleme des Datenschutzes**

In dem oben beschriebenen Szenario muss vor jedem Abspielen eines Musikstückes die Identität des Hörers überprüft und das Recht kontrolliert werden, dass von ihm angeforderte Stück abspielen zu dürfen.

Der Anbieter muss dazu immer wissen, welche Stücke ein bestimmter Nutzer hören darf; in einem Online DRM-System kann er sogar detailliert feststellen, wer welches Stück wann und wie oft gehört hat. Der Anbieter ist somit in der Lage, ein Profil über den persönlichen Musikgeschmack und das persönliche Hörverhalten eines Nutzers erstellen zu können.

Anhand solch eines Profils kann der Anbieter ein sehr individuelles Werbeangebot zusammenstellen, z. B. zum neuesten Album der Lieblingsband, die ihrerseits im Profil vermerkt ist.

Dieses Datenschutzproblem tritt bei nahezu allen Systemen auf. Es gibt allerdings auch Systeme, die eine Pseudonymisierung erlauben, d. h. ein Nutzer kann sich hinter einem oder mehreren Synonymen verbergen. Allerdings stellt die Pseudonymisierung im Internet immer ein Problem dar, denn letztendlich ist jeder Computer im Internet über seine IP-Adresse eindeutig identifizierbar. Ob diese vom Anbie-

ter ausgewertet wird liegt immer beim Anbieter des Dienstes. Auch wenn man seine wahre Identität hinter einem Pseudonym verbirgt, ließe sich so die tatsächliche Identität herausbekommen. KR

### **3.6. Nutzerprofile vs. Schutz der Privatsphäre**

Man bekommt also passende Werbung zugeschickt: „Ist doch praktisch!“ – In gewisser Weise schon, denn Nutzerprofile erlauben es Anbietern, gezielt auf die Bedürfnisse des Nutzers eingehen zu können: sachverwandten Themen können vorgestellt, interessante und möglicherweise günstigere Angebote offeriert werden.

Man muss sich die Frage stellen: „Will ich das wirklich? Will ich Prospekte über Babyprodukte zugeschickt bekommen, nachdem ich zehn Monate nach dem Onlinekauf eines Schwangerschaftstests ein Kinderschlaflied heruntergeladen habe?“ Letztendlich sollte die Entscheidung bei jedem Einzelnen liegen, wie er diese Frage beantworten möchte.

Das Problem liegt hier bei dem ‚sollte‘. Bei manchen DRM-Systemen kann man sich frei entscheiden, wie viele persönliche Daten man preisgeben möchte, bei anderen hat man jedoch nicht die Wahl, sondern wird technisch bzw. systembedingt dazu gezwungen, gewisse Informationen mitzuteilen. In diesem Fall bleibt nur die Alternative, dieses DRM-System nicht zu benutzen.

Im folgenden Kapitel werden wir detailliert auf verschiedene aktuelle DRM-Systeme eingehen und jeweils beschreiben, inwieweit die Betreiber Wert auf diese Thematik legen. KR

## **4. Verschiedene Konzepte des DRM**

### **4.1. Einleitung**

Einige DRM-Systeme sind in der Entwicklungsphase und noch nicht marktreif, andere haben sich schon längst auf dem Markt durchgesetzt. Im Folgenden werden wir auf einige der heute aktuellen DRM-Systeme eingehen, die teilweise bereits verwendet, oder sich in absehbarer Zeit auf dem Markt etablieren werden. Bei manchen handelt es sich nicht explizit um Verfahren zur Durchsetzung des DRM, sondern nur um Grundlagen, die ein DRM-System nutzen könnte. KR

### **4.2. Pay-TV**

Als erstes Beispiel eine aus datenschutzrechtlicher Sicht gelungene Implementierung eines DRM-Systems: das Bezahlfernsehen. Bedingt durch die unidirektionale Architektur des Kabelnetzes ist es dem Betreiber nicht möglich, in Echtzeit Informationen über das Fernsehverhalten eines Nutzers zu erfahren. Er hat lediglich die Möglichkeit, Daten in das Kabelnetz einzuspeisen, kann aber keine Informationen daraus lesen, da kein Rückkanal vorhanden ist.

Der Pay-TV-Betreiber stellt Schlüssel in Form von Chipkarten zur Verfügung. Auf diesen Karten ist lediglich vermerkt, welche einzelnen Sender ein Benutzer ‚gekauft‘ hat und damit sehen darf. Es bleibt ihm verborgen, welche einzelnen Sendungen der Nutzer tatsächlich sieht, womit es ihm auch nicht möglich ist, ein Profil über dessen Fernsehverhalten zu erstellen.

Bei dem hier beschriebenen System handelt es sich um das ursprüngliche Pay-TV-Konzept, wie es beispielsweise von Premiere verwendet wird. Mittlerweile gibt es neue Ansätze: Zwar ändert sich generell nichts daran, dass das Kabelnetz unidirektional ist, jedoch ist mittlerweile jede Chipkarte (z. B. die von Premiere) eindeutig identifizierbar. Dadurch haben Pay-TV-Betreiber die Möglichkeit, einzelnen Nutzern bestimmte Sendungen freizuschalten. Das funktioniert so, dass ein Nutzer per Internet oder Telefon eine bestimmte Sendung für eine bestimmte Uhrzeit gegen Gebühr einkauft (z. B. bei ‚Premiere Direkt‘). Zusammen mit der eigentlichen Bildinformation werden dann Entschlüsselungsinformationen mitgesendet, die nur von

denen gelesen werden können, die vorher die Sendung bestellt/bezahlt haben. Dadurch können Pay-TV-Betreiber Nutzungsprofile ihrer Kunden erstellen. KR

### **4.3. Audiokopierschutz**

Die einfachste und älteste Form eines DRM wird bei kopiergeschützten Audio-CDs eingesetzt. Da CD-Brenner Mitte der 90er Jahre immer erschwinglicher wurden und Internet-Tauschbörsen immer mehr Zulauf fanden, sah sich die Musikindustrie gezwungen, ihre CDs mit einem Kopierschutz zu versehen.

Alle Kopierschutzsysteme setzen auf eine manipulierte CD Struktur, um der Hard- und/oder Software ein fehlerhaftes Produkt vorzutäuschen, das nicht gelesen, abgespielt oder vervielfältigt werden kann. Dazu wird auf der CD neben dem Audiobereich noch eine Daten-Session hinzugefügt und dem Inhaltsverzeichnis der CD (Table of Content, TOC) falsche Angaben für die Sektoren und Abschnitte gegeben. Die bekanntesten Kopierschutzverfahren, die auf diese Art arbeiten, sind Cactus Data Shield 200, Key2Audio oder Laserlock. Somit entsprechen diese CDs auch nicht mehr dem im „Red-Book“ festgehaltenen ANSI-Standard, den die beiden Unternehmen Sony und Philips Anfang der 80er Jahre festgelegt haben [PHI01]. Seit dem 1. November 2003 müssen solche kopiergeschützten CDs nach § 95 UrhG entsprechend gekennzeichnet werden.

HiFi CD-Player berücksichtigen gemäß dem Red-Book-Standard nur die erste Session einer CD mit dem Audioteil und haben somit keine Probleme mit der Wiedergabe. Da aber in vielen neueren Playern, vor allem in DVD-Playern, Computer-Hardware eingesetzt wird, kommt es auch dort immer häufiger zu Problemen.

Mit der Zeit wurden weitere Maßnahmen entwickelt und auf dem Markt etabliert, die zumindest das Abspielen im PC ermöglichen. Dazu werden im Daten-Teil komprimierte Versionen der Musik abgelegt, die nicht der gewohnten HiFi-Qualität entsprechen, und diese lassen sich dann am PC abspielen. DM

#### **4.3.1. XCP**

Das international agierende Plattenlabel SonyBMG hat 2005 in Amerika zwei Kopierschutzmaßnahmen eingesetzt, die noch einen Schritt weiter gehen.

Ein Verfahren stammt von der britischen Firma First4Internet und nennt sich ‚XCP‘ („Extended Copy Protection“). Derartig geschützte Audio-CDs starten auf Microsoft Windows Rechnern via Autostart automatisch beim Einlegen der CD oder nach manuellem Start der `autostart.exe` eine Softwareinstallation. In der Lizenzbedingung, die zunächst eingeblendet wird und bestätigt werden muss, ist die Rede von einer Abspielsoftware [Vgl. SON01]. Diese Abspielsoftware soll es dem Nutzer ermöglichen, die Audio-CD am PC anzuhören und bis zu 3 digitale Kopien davon anzufertigen. Bei der Softwareinstallation wird aber auch ein spezieller Filtertreiber für das CD-ROM Laufwerk installiert, der den Zugriff auf das Laufwerk kontrolliert. Darüber hinaus versteckt diese Software ihre zugehörigen Dateien, Verzeichnisse, Prozesse und Registrierdatenbank-Schlüssel und sogar global alles, was den Präfix `$sys$` trägt, vor dem Benutzer [Vgl. SYS01]. Derartige Eingriffe in das Betriebssystem sind allgemein als „Rootkit“ bekannt, die ihre (illegalen) Aktivitäten ebenfalls vor dem Computernutzer verbergen. Auf diese Art und Weise könnte sich nun auch andere Schadsoftware durch die entsprechende Namensgebung tarnen und unbemerkt vom Nutzer agieren. „The hiding techniques used by the DRM software can be abused by less technical malware authors to hide their backdoors and other tools. If a malware names its files beginning with the prefix \"\$sys\$\", the files will also be hidden by the DRM software. Thus it is very inappropriate for commercial software to use these techniques.“ [FSE01].

Bei jeder Nutzung der CD im PC wird außerdem durch die Abspielsoftware selbständig und unwissend vom Nutzer Kontakt zu einem Server aufgebaut, bei der Uhrzeit, IP-Adresse und eine eindeutige Nummer der CD (Album-ID) übermittelt werden. Berichten der Herstellerfirma zufolge dient diese Datenübermittlung lediglich dazu, weiterführende Informationen zum Künstler und ein CD-Cover abzurufen [Vgl. SYS02]. Dadurch ist es für den Anbieter aber auch möglich, unbemerkt ein Nutzungsprofil anzulegen.

Diese Software enthält keine Möglichkeit der Deinstallation und wird auch nicht in der Software-Liste der Systemsteuerung aufgeführt. Zum Deinstallieren der Software hat SonyBMG nach den ersten Kundenbeschwerden zunächst ein spezielles Kontaktformular bereitgestellt, über das man einen Uninstaller anfordern konnte. Dieser ActiveX-basierte Uninstaller brachte jedoch auch wieder einige Sicherheits-

lücken zutage, wie Edward W. Felton und Alex Haldermann, Professoren für Informatik an der Princeton-Universität herausgefunden haben [Vgl. FEL01]. In der Zwischenzeit haben Antiviren-Hersteller wie Sophos reagiert und bieten sichere und effektive Säuberungstools an [Vgl. SOP01]. Auch SonyBMG hat mittlerweile auf die wachsenden Beschwerden und die ersten Sammelklagen in Amerika reagiert und eine Rückrufaktion für die betroffenen CDs gestartet [Vgl. SON02]. Die ursprünglich für 2006 geplante Einführung dieses Kopierschutzes in Europa wurde vorerst auf Eis gelegt. Dennoch betont SonyBMG: „Wir stehen zum Einsatz von Technologie zum Inhalte-Schutz als ein wichtiges Werkzeug, um unsere Urheberrechte und die unserer Künstler zu schützen“ [DPA01] DM

#### 4.3.2. MediaMax

Das zweite Verfahren stammt von der amerikanischen Firma ‚SunComm Technologies‘ und trägt die Bezeichnung ‚MediaMax‘.

Hier reicht ebenfalls das Einlegen der Audio-CD in einen Windows-Rechner mit aktiviertem Autostart bzw. manueller Start der `autostart.exe`, um die Softwareinstallation zu starten. Bei diesem Verfahren wird jedoch ohne Rückfragen, auch bei Ablehnen der Lizenzbedingung, ein CD-ROM Treiber zur Überwachung der CD-Aktivität auf dem Rechner installiert. Dieses Inhaltsmanagement-Programm soll die Anzahl der digitalen Kopien regeln und ein Abspielen des Audio-Teils am PC ermöglichen. Eine Möglichkeit der Deinstallation ist aber auch bei dieser Software nicht gegeben.

Genau wie XCP von First4Internet ist auch diese Software datenschutztechnisch bedenklich, da auch hier bei jedem Abspielvorgang im PC unbemerkt Kontakt zu einem Server aufgebaut wird, der das unbeobachtete Erstellen von Nutzungsprofilen begünstigt.

Dieser Kopierschutz wird zum gegenwärtigen Zeitpunkt zumindest im amerikanischen Raum weiterhin eingesetzt und es bleibt abzuwarten, ob hier ebenfalls seitens SonyBMG eingelenkt wird oder ob dieser Kopierschutz auch demnächst hierzulande auf Audio-CDs zu finden sein wird. DM

#### **4.4. Microsoft Windows Media Rights Manager**

Microsoft stellt mit dem ‚Windows Media Digital Rights Management‘ (WMMR), welches fester Bestandteil des Windows Media Player ist, das momentan am weitesten verbreitete DRM bereit. Mit dem WMMR Software Development Kit stellt Microsoft alle Funktionen bereit, die für den Einsatz dieses Systems notwendig sind [Vgl. MIC01].

Der erste Punkt ist Sicherheit („Security“), d. h. alle Mediendateien im Windows-Media-Format können verschlüsselt und mit restriktiven Abspielbedingungen verknüpft werden. Dazu zählen z. B. minimale Sicherheitsanforderungen an das Abspielgerät, um somit nur bestimmten, von Microsoft zertifizierten Playern die Wiedergabe zu gestatten.

Daneben gibt es die so genannten „Robust Features“ des WMMR, zu denen z. B. die Möglichkeit zählt, Mediendateien eine Reihe an individuellen Rechten mitzugeben. Das fängt bei der einfachen Kontrolle, ob eine Wiedergabe überhaupt möglich ist an und geht so weit, bis ins Detail die Nutzungsrechte für eine Datei definieren zu können. Auf diese Art und Weise kann man Lizenzen zu Vermarktungszwecken gleich kostenlos mitliefern, die nur eine beschränkte Gültigkeit haben. Dem Kunden kann man anschließend die Möglichkeit geben, eine weitere Nutzungslizenz zu erwerben. Damit muss der eigentliche Inhalt vom Kunden nur einmal heruntergeladen werden.

Zuletzt gibt es die Skalierbarkeit („Scalability“), d. h. die Möglichkeit, die verschiedenen Funktionen des WMMR auf unterschiedliche Systeme zu verteilen. Da das System von Microsoft auf Komponenten basiert, lässt es sich z. B. in ein bereits existierendes System eines Online-Anbieters integrieren und sorgt dann dort für das Lizenzmanagement. <sup>DM</sup>

##### **4.4.1. Vorgehensweise bei Windows Media DRM**

Die grundsätzliche Vorgehensweise bei Windows Media DRM setzt sich aus 5 Schritten zusammen [Siehe dazu MIC02 und Abbildung 1]:

- Verpacken („Packaging“): Im ersten Schritt wird das digitale Medium im WMA- (Audio) bzw. WMV-Format (Video) gespeichert und dabei verschlüsselt. Der

zugehörige Schlüssel zum Entsperrern wird ebenfalls verschlüsselt in einer Lizenzdatei abgelegt, die separat vertrieben wird.

- Verteilung („Distribution“): Die verpackte Mediendatei kann dann zum Download auf einer Webseite angeboten werden, auf CD vertrieben oder als Stream auf einem Medienserver bereitgestellt werden. Eine Weitergabe dieser Datei unter Freunden und Bekannten ist dabei möglich, da die zugehörige Lizenzdatei unabhängig davon erworben wird.
- Einrichten eines Lizenzservers („Establishing a license server“): Der Inhabeanbieter wählt einen Lizenzaussteller („license clearing house“) aus, der die spezifischen Lizenzrechte oder -regeln speichert und die Lizenzdienste des Windows Media-Rechte-Managers implementiert. Der Lizenzaussteller sorgt dann für die Authentifizierung des Benutzers und seiner Lizenzanforderung.
- Lizenzerwerb („License acquisition“): Um eine geschützte Mediendatei zu benutzen, muss sich der Kunde zunächst einen gültigen Lizenzschlüssel zum Entsperrern der Datei besorgen. Dieser Vorgang findet automatisch statt, wenn der Kunde z. B. versucht, eine geschützte Mediendatei das erste Mal abzuspielen. Dazu wird der Benutzer dann entweder an eine Registrierungsseite weitergeleitet, auf der Benutzerinformationen eingegeben werden müssen oder eine Zahlung getätigt werden muss, oder er bekommt die Lizenz automatisch von einem Lizenzaussteller zugestellt.
- Wiedergeben der digitalen Mediendatei („Playing the digital media file“): Zum Abspielen einer Windows Media Datei wird ein Player mit Windows Media DRM Unterstützung benötigt. Der Benutzer kann dann die Datei gemäß der in der Lizenz enthaltenen Regeln oder Rechte wiedergeben. Lizenzen können unterschiedliche Rechte aufweisen, wie z. B. Startzeiten und -daten, Dauer und begrenzte Operationen. Dazu zählt dann beispielsweise auch die Möglichkeit, die Datei auf ein tragbares Gerät zu kopieren. Ein Übertragen der Lizenzdatei auf einen anderen Computer ist dabei nicht möglich. Wenn ein Benutzer eine verpackte digitale Mediendatei an einen Freund sendet, muss dieser eine eigene Lizenz erwerben, um die digitale Mediendatei nutzen zu können. <sup>DM</sup>

#### 4.4.2. Secure Audio Path

Microsoft hat auch an die Sicherheitsanforderung innerhalb des Client-Rechners, auf dem die Datei letztendlich genutzt wird, gedacht. So stellt eine Technologie namens „Secure Audio Path“, die erstmalig bei Windows ME eingeführt worden ist sicher, dass ein digitales Mitschneiden der Audio-Datei im Rechner nicht möglich ist [Vgl. MIC03]. Ein mögliches Angriffsszenario wäre sonst das Speichern des entschlüsselten Audio-Streams auf dem Weg zur Ausgabe durch die Soundkarte mittels eines speziellen Plug-Ins im Computer. In der Vergangenheit gab es schon Fälle, das auf diese Weise eine ungeschützte Kopie in digitaler verlustfreier Qualität möglich war, indem man die Ausgabe des Audio-Streams anstatt zur Soundkarte in ein so genanntes „File-Writer“-Plug-In, also zum Schreiben in eine Datei umgeleitet hat.

Das wird dadurch unterbunden, dass in Zukunft eine durch Microsoft zertifizierte Komponente alle weiteren beteiligten Komponenten, darunter auch der eigentliche Soundkarten-Treiber, dahingehend überprüft, ob diese ebenfalls von Microsoft zertifiziert sind. Als Konsequenz daraus wird das Entschlüsseln der Mediendatei trotz gültiger Lizenz durch die Microsoft-Technologie verweigert, sollten nicht autorisierte oder gefährdete Komponenten erkannt werden. Welche Komponenten als gefährdet eingestuft werden, entscheidet dabei allein Microsoft. Schon seit Jahren werden Hardware-Treiber durch das Windows Hardware Quality Lab (WHQL) gegen entsprechende Gebühren überprüft und zertifiziert. Hardware-Treiber, die ein solches Zertifikat nicht tragen, werden von Microsoft pauschal als sicherheitsgefährdend eingestuft. Der Nutzer wird hierauf beim Installieren der jeweiligen Hardware hingewiesen. DM

#### 4.4.3. Musicload

Ein populäres Beispiel für den Einsatz von Microsofts DRM ist das Musikportal „Musicload“ von T-Online.

Um eine Musikdatei bei Musicload zu erwerben, muss man sich zunächst über das Anmeldeformular bei diesem Dienst anmelden. Dabei werden personenbezogene Daten, wie Name und Anschrift, erfasst und in einem weiteren Schritt wird man zur Eingabe der Abrechnungsdaten gebeten. Hierbei wird zwar auch die Möglichkeit

einer Gutscheineinlösung gegeben, also einer Prepaid-Möglichkeit, die Angabe der personenbezogenen Daten erfolgt jedoch in allen Fällen. „Füllen Sie bitte alle Felder aus. Ihre Postadresse brauchen wir z. B. für die Abrechnung, die E-Mail Adresse für die Bestellbestätigung.“ [MUS01]. Ein anonymes Abrufen der Medieninhalte ist dabei genauso wenig gegeben, wie eines der Grundprinzipien des Datenschutzes, nämlich die Datensparsamkeit. Schließlich sind die personenbezogenen Daten im Falle eines Prepaid Kaufes genauso wenig notwendig wie für die Durchsetzung des WMRM.

Entscheidet man sich zum Kauf einer Musikdatei bei Musicload erwirbt man in der Regel eine unbegrenzte Anzahl an Abspielvorgängen, eine beschränkte Anzahl an Brennmöglichkeiten auf CD und beschränkte Übertraggelegenheiten auf ein portables Endgerät. Und genau bei der Brennmöglichkeit sieht man auch einen Schwachpunkt dieses DRM, da sich auf diese Weise das gesamte System umgehen lässt. Man erhält dadurch die Möglichkeit, seine geschützten Musikdateien auf eine ungeschützte CD zu kopieren, um sie von dort unbegrenzt anzuhören oder nochmals zu kopieren und damit die Möglichkeit einer unbeschränkten Weitergabe an Freunde und Bekannte. In Konflikt mit dem geltenden deutschen Urheberrecht stößt man hierbei nicht, da die gebrannte CD in keiner Weise mit einem technisch wirksamen Kopierschutz ausgestattet ist. In diesem Zusammenhang sollte nicht unerwähnt bleiben, dass Musicload sogar damit wirbt, dass man seine legal erworbenen Musikdateien auf CD brennen und verschenken kann und bietet dafür auch gleich die passenden Cover zum Download an [Vgl. MUS02].

Musicload bietet darüber hinaus auch die Möglichkeit an, eine erworbene Lizenz 3-mal herunterzuladen und somit auf drei verschiedenen PCs einzusetzen [Vgl. MUS03]. Dazu werden alle erworbenen Lizenzen des Benutzers sechs Monate lang im Benutzerkonto gespeichert. Ein typisches Szenario wäre also der Einsatz auf dem heimischen Desktop-PC, dem tragbaren Notebook und dem Firmen-PC. Alle drei Systeme müssen dabei selbstverständlich mit einem WMRM kompatiblen Player ausgestattet sein. <sup>DM</sup>

#### **4.5. Apple FairPlay**

Apple verwendet als DRM-System sein eigenes so genanntes ‚Apple FairPlay‘ Verfahren. Dieses soll – man beachte die Reihenfolge – „fair zu den Künstlern, zur Musikindustrie und zum Nutzer“ [APP01: „fair to the artist, to the record companies and to you“] sein. Apple definiert als ‚fair für den Nutzer‘ die Möglichkeit, ein Musikstück auf maximal fünf Geräten abspielen zu können, wobei es sich unbegrenzt mit dem Apple-eigenen Abspielgerät ‚iPod‘ synchronisieren lässt. Ein vielleicht auf den ersten Blick faires Verfahren, das allerdings bei genauerer Betrachtung einige Nachteile mit sich bringt:

So ist es z. B. nicht möglich, über den iTunes Music Store gekaufte Musikstücke auf anderen MP3-Playern abzuspielen und auch auf den iPod lassen sich ohne (legale) Tricks keine ‚fremden‘ (d. h. nicht über den iTunes Music Store gekaufte) Musikstücke aufspielen.

Die technische Implementierung des DRM ähnelt der von Microsoft, denn auch hier besteht die Möglichkeit, aus iTunes heraus CDs zu brennen. Da der CD-Standard nicht DRM-fähig ist, wird durch das Brennen der DRM-Schutz aufgehoben. Wird anschließend der Schritt umgekehrt und werden von der CD wieder MP3-Dateien hergestellt, erhält man DRM-freie MP3-Dateien. Kritiker werfen Apple daher vor, es ginge ihnen weniger um den Schutz der Inhalte, als vielmehr um die Marktmacht gegenüber den Hauptkonkurrenten Microsoft und Sony, denn mit der zunehmenden Verbreitung der iPods und der Nutzung der iTunes nimmt die Zahl der Musikstücke zu, die nicht mit anderen Playern außer denen von Apple abspielbar sind. Ausgetragen wird dieser Kampf auf dem Rücken der Verbraucher, die sich mit Kopierschutz- und DRM-Verfahren herumärgern müssen, die auf den ersten Blick lästig sind, da sie die Nutzung erschweren, und die auf den zweiten Blick weder den Künstlern, noch der Musikindustrie oder den Nutzern dienen, da sich der DRM-Schutz relativ leicht umgehen lässt. KR

##### **4.5.1. Datenschutz bei Apple FairPlay**

Apple speichert, je nach Art der Kommunikation mit dem Kunden, jede persönliche Information, die entsprechend angefallen ist. Dazu zählen beispielsweise das Surfverhalten bei Webseitenbesuchen und die für uns interessante Erfassung persönli-

cher Daten bei der Nutzung von Produkten und Leistungen, so z. B. bei der Nutzung der iTunes. Apple erfasst die Daten, um den Kunden „einen bequemen Zugriff auf unsere Produkte und Services zu ermöglichen und ein optimales Leistungsangebot zu unterbreiten“ [APP02]. Außerdem betont Apple: „Es werden von Ihnen stets nur solche Auskünfte erbeten, die für die jeweilige Situation relevant sind“ [APP02]. Liest man sich jedoch die Datenschutzerklärung genauer durch, findet man auch Angaben darüber, dass erfasste Informationen nicht nur zum Vorteil des Kunden, sondern auch zu Werbezwecken eingesetzt werden. Des Weiteren werden auch Informationen zu Marktforschungszwecken erfasst, z. B. Angaben über den Beruf unter dem Vorwand „den Kunden besser kennen zu lernen“ [APP02].

Welche Informationen speziell bei den iTunes erfasst werden lässt sich nicht herausbekommen; da FairPlay auf DRM beruht, muss Apple jedoch genau speichern, welche Nutzer welche Musikstücke gekauft haben. Ferner ist festzuhalten, dass alle Kundenaktivitäten auf der iTunes Webseite aufgezeichnet werden.

Dies alles sind Erfassungsmaßnahmen, auf die der Kunde keinen Einfluss hat. Apple geht sogar noch einen Schritt weiter und bietet auf der iTunes Webseite die Möglichkeit, sich eine so genannte Apple ID einzurichten, die einen Nutzer eindeutig identifiziert und eine noch bequemere Nutzung der iTunes verspricht. Dazu wird ein Profil mit dem Namen, der Telefonnummer, der E-Mail-Adresse und ggf. der Anschrift oder der Kreditkartennummer des Kunden angelegt. Surft man nun auf der Seite, ist man jederzeit identifizierbar und kann nach Eingabe des persönlichen Kennworts direkt neue Produkte kaufen oder Bestellungen aufgeben.

Trotz diverser Erfassungsmaßnahmen weist Apple in der Datenschutzerklärung darauf hin, dass der Kunde auf der Webseite die Möglichkeit hat, sich alle erfassten Daten wie gekaufte Produkte, Kontaktaufnahmen zu Vertriebspartnern und dem Kundendienst und alle persönlichen Daten zukommen zu lassen. KR

#### **4.6. Adobe DRM Activator**

Die Firma Adobe Systems, bekannt geworden durch ihr portables Dokumentenformat PDF, verfügt mittlerweile ebenfalls über ein DRM-System, mit dem sich PDF-Dokumente digital schützen lassen. Adobes DRM Activator dient in erster Li-

nie dem Schutz der Urheberrechte von Autoren bzw. Herausgebern von eBooks, es lassen sich aber auch selbst erstellte Dokumente schützen.

Wenn man digital geschützte Dokumente betrachten möchte, muss sowohl der Adobe Reader als auch Acrobat aktiviert sein. Für die Aktivierung muss man sich entweder mit einem .net Passport von Microsoft identifizieren oder mit der Adobe-ID. Erst nach der Identifizierung ist es möglich, die geschützten Dokumente auf andere persönliche Geräte zu kopieren und dort zu öffnen. Dabei ist die gemeinsame Verwendung von Dokumenten auf sechs Geräte beschränkt. KR

#### 4.6.1. Datenschutz bei Adobe und bei der Adobe-ID

Auch bei Adobe werden bei Webseitenbesuchen diverse Informationen gespeichert wie Surfverhalten, Browsertyp, Betriebssystem, Prozessorgeschwindigkeit und IP-Adresse [Vgl. ADO02]. Anders als bei Apple betont Adobe jedoch, dass diese Informationen nicht in Verbindung mit personenbezogenen Daten gebracht werden.

Interessanterweise kommt in der Datenschutzerklärung von Adobe [ADO02] kein einziges Mal der Begriff der Adobe-ID vor. Welche Informationen anzugeben sind, erfährt man nur, wenn man sein Adobe Produkt registriert oder explizit eine Adobe-ID anlegt. Beim Erstellen einer Adobe-ID ist die Angabe des Landes, des Namens und der E-Mail-Adresse zwingend erforderlich. Ist die Adobe-ID angelegt, ist man über diese eindeutig identifizierbar. Zusätzlich kann man noch weitere Informationen angeben: Dazu zählen Anschriften und Zahlungsmöglichkeiten für Online-Bestellungen aber auch persönliche Daten über den Beruf, die allerdings freiwillig sind. Bei der Produktregistrierung, die bei der Nutzung des DRM Activator vorgeschrieben ist, ist auch im Profil vermerkt, welche Produkte man gekauft und registriert hat. KR

#### 4.7. **Trusted Computing**

Trusted Computing (oder auch Trustworthy Computing, wie es von Microsoft genannt wird [Vgl. MIC04]) ist ein Konzept, eine sichere und zuverlässige Arbeit mit Computern zu gewährleisten. Dieses Konzept hat zunächst nichts mit dem Schutz von Urheberrechten zu tun. Dennoch bietet Trusted Computing (TC) mittels der

dazugehörigen Hardware, dem so genannten Trusted Platform Module (TPM), das von der Trusted Computing Group (TCG) entwickelt wird, eine stabile Grundlage, auf welcher DRM-Systeme aufsetzen können. Zu den Mitgliedern der TCG zählen Marktführer wie Microsoft und die Prozessorhersteller Intel und AMD. Früher war TC unter anderen Namen bekannt, dazu zählen Trusted Computing Platform Alliance (TCPA), Palladium oder aktuell die Next Generation Secure Computing Base (NGSCB). Wie man es auch bezeichnen möchte, es handelt sich prinzipiell immer um ein Verfahren des TC. Schon die Vielzahl der verschiedenen Begriffe führt zu einer Unübersichtlichkeit auf diesem Gebiet, die den Endbenutzer bereits bei der Recherche entmutigen kann. Ob dies mit Absicht geschehen ist, kann in dieser Arbeit weder belegt noch widerlegt werden. KR

#### 4.7.1. Trusted Computing für DRM-Systeme

Kritiker des TC behaupten, dass der ‚sichere Computer‘ nur als Vorwand benutzt wird, ein System auf dem Markt zu etablieren, mit dem es Firmen möglich sein wird dem Raubkopieren ein Ende zu bereiten und die Endbenutzer zum Kauf ihrer Produkte zu zwingen. Unzählige Internetseiten wettern geradezu gegen TC und werfen der Industrie vor, den Benutzern die Kontrolle über den eigenen Computer zu entziehen [Vgl. AND01]. Von Seiten der TCG und ihrer Mitglieder werden diese Vorwürfe jedoch dementiert. Fakt bleibt: „DRM-Systeme könnten die hardwarebasierten manipulationsresistenten Trusted-Computing-Mechanismen in den Bereichen der Verschlüsselung, Integritäts- und Authentizitätsprüfung, der Schlüsselverwaltung sowie der Durchsetzung von Zugangsrechten nutzen.“ [BEC03, S. 25] TC im Bereich der DRM-Systeme wird im Rahmen von Vermarktungsstrategien völlig neue Perspektiven eröffnen: Eine DRM-fähige DVD könnte z. B. nur am Wochenende abspielbar sein oder man kauft eine Musik-CD zur Probe, die sich nur 3-mal abspielen lässt, nur bei Gefallen müsste der Rest des Kaufpreises gezahlt werden. KR

#### 4.7.2. Next-Generation Secure Computing Base für DRM

Next-Generation Secure Computing Base (NGSCB) ist Microsofts Ansatz, DRM Technologien in seinen Systemen einzuführen. Bereits 1999 startete Microsoft das

Projekt als Gründungsmitglied der Trusted Computing Platform Alliance (TCPA). 2003 wurde dann NGSCB als Nachfolger vorgestellt, offiziell weil die TCPA aus organisatorischen Gründen handlungsunfähig war. Unbestätigten Informationen zufolge war TCPA durch negative Pressemitteilungen in schlechtes Licht gerückt und man entschied sich deshalb für einen neuen Namen.

Wie bereits in Kapitel 2 erläutert, ist es zwingend notwendig, dass ein DRM-System vollständig auf DRM-fähigen Komponenten beruht, da sonst eine Umgehung des Systems möglich wird. Dies beginnt bei der Hardware, hier setzt NGSCB auf das Trusted Platform Module (TPM), setzt sich fort über den Boot-Prozess des PCs und das Starten des Betriebssystems und mündet letztendlich in der Anwendung. Jede dieser Komponenten muss voll DRM-fähig sein, damit das System nicht umgangen werden kann. Microsofts neues Betriebssystem Windows Vista (Codename Longhorn) wird NGSCB integrieren und TPM unterstützen [Vgl MIC05]. Die gesamte Architektur von NGSCB zu erläutern würde den Rahmen dieser Ausarbeitung sprengen. Es sei hier nur kurz erwähnt, dass sich Microsofts neues Betriebssystem in zwei Bereiche aufteilen lässt: Den Standard-Bereich, der dem vergleichsweise unsicheren Windows entspricht, wie wir es heute kennen, und dem sicheren Bereich, in dem z. B. Hardwarezugriffe nur über einen speziellen sicheren Kernel (den so genannten Nexus) erlaubt sind. [Siehe dazu OBE01 und Abbildung 2]

Aus dem Blickwinkel des DRM betrachtet, endet die Hardware-Seite jedoch nicht beim TPM, sondern beginnt erst dort. Je nach Anwendung müssen alle beteiligten Hardwarekomponenten DRM-fähig sein: Wenn ein Kinofilm gekauft wurde, um ihn auf dem heimischen PC anzusehen muss auch die Grafikkarte DRM-fähig sein, wenn ein Musikstück abgespielt werden soll muss dementsprechend die Soundkarte DRM-fähig sein. Gleiches gilt auch für Chipsätze, den Prozessor und sogar alle computerinternen Busse für Datenübertragung, denn jede ungeschützte Hardware stellt ein potentiell Sicherheitsrisiko dar. KR

#### 4.7.3. Gefahren des Trusted Computing

Im Folgenden wird ein mögliches Szenario provokativ geschildert. Es ist übertrieben dargestellt, soll dabei aber die Möglichkeiten des TC offen legen und kritisch

beleuchten. Ob TC überhaupt als Grundlage für DRM genutzt wird bzw. werden kann ist noch unklar.

Wir gehen davon aus, dass TC sich auf dem Markt durchgesetzt hat. Die Ergebnisse, die Google auf einem TC-fähigen PC liefert, unterscheiden sich massiv von denen auf einem ‚unsicheren‘ Browser, da sich Webseiten wichtiger Unternehmen aus Sicherheitsgründen nur noch mit einem TC-fähigen Browser ansehen lassen. Open Source Software gibt es schon lange nicht mehr, da es sich die Benutzer-gemeinde nicht leisten kann, ihre Produkte bei Microsoft auf ihre Sicherheit hin überprüfen zu lassen und auch TC-Gegner mussten mittlerweile auf TC-fähige PCs umsteigen, da sie sonst unfähig wären, sichere E-Mails zu lesen, die sie von ihren Kollegen zugeschickt bekommen. Die Kontrolle über Dateien muss von einer zentralen Stelle geregelt werden, die weiß, wer auf welche Daten zugreifen kann. Man stelle sich die politische Macht dieser zentralen Stelle vor, die – davon kann ausgegangen werden – in Amerika angesiedelt sein wird. So könnte im Kriegsfall angeordnet werden, dass Microsoft alle Word-Dokumente, die nicht von amerikanischen Word-Versionen erstellt wurden, sperren oder sogar sämtliche Computer feindseliger Nationen als ‚unsicher‘ einstufen soll, sodass diese nicht mehr booten. Wie bereits erwähnt, ist dieses Szenario sehr überzogen dargestellt. Aber es sollte deutlich geworden sein, welche gefährlichen Möglichkeiten TC eröffnet. Die eingebaute TC Hardware zu deaktivieren wäre eine Option, aber dann ließen sich sämtliche TC Programme nicht mehr starten bzw. TC Dokumente nicht mehr öffnen. Man hätte also einen lauffähigen TC-freien Computer, könnte damit aber nicht mehr vernünftig arbeiten.

Grundsätzlich lässt sich sagen, dass sich TC und NGSCB noch in der Entwicklungsphase befinden. Wie letztendlich die Realisierung aussieht, bleibt abzuwarten. Ob Microsoft tatsächlich die Kontrolle über den eigenen PC übernehmen wird, ist auch fraglich. Es bleibt jedoch festzuhalten, dass aus technischer Sicht die aktuelle Entwicklung in die Richtung geht, dass man die Herrschaft über den eigenen Computer in Teilen wird aufgeben müssen. Die Musikindustrie hat jedenfalls großes Interesse daran, möglichst schnell jeden PC der Welt ‚sicher‘ zu machen. KR

#### 4.8. HD-DVD & Blu-ray Disc

Nachdem der DVD-Kopierschutz Content Scrambling System (CSS) bereits wenige Wochen nach Erscheinen geknackt worden ist, hat die Unterhaltungsindustrie für die DVD-Nachfolger HD-DVD & Blu-ray Disc erhöhte Anforderungen an das Verschlüsselungssystem gestellt. <sup>DM</sup>

##### 4.8.1. AACS

Grundlage für beide Systeme ist das Advanced Access Content System (AACS), für das die Advanced Access Content System License Administration (AACS LA) bereits die Spezifikationen veröffentlicht hat [Vgl. AAC01]. Zu der AACS LA gehören Vertreter der Medien-, Hard- und Softwareindustrie, darunter Firmen wie Microsoft, Intel, Sony und Warner Bros.

Bei AACS handelt es sich um ein dynamisches Kopierschutzkonzept, das auch ein umfassendes Rechtemanagement mit sich bringt. Für die Verschlüsselung der digitalen Inhalte kommt ein offenes kryptographisches Verfahren zum Einsatz: Eine als sicher geltende symmetrische AES Verschlüsselung mit einem 128 Bit langen Schlüssel. Der Schlüssel zum Entsperren der Inhalte („Media Key“ -  $K_m$ ) wird vom Abspielgerät aus seinem eigenen Geräteschlüssel („Device Key Block“) und einem Schlüssel vom Medium („Media Key Block“ - MKB) ermittelt. Wird nun eine erworbene Disc kopiert, so erzeugt das Aufzeichnungsgerät einen neuen individuellen Schlüssel aus den Informationen, die im Leermedium hinterlegt sind. Auf diese Weise läßt sich die Anzahl der Kopien, anders als im bisherigen DVD-Format, regulieren und die Wiedergabe der Kopien auf bestimmte Geräte einschränken.

Beim AACS sollen sich, anders als beim CSS, kompromittierte Geräteschlüssel sperren lassen. Sollte sich ein hinterlegter Schlüssel in einem bestimmten Player aufgrund unzureichender Sicherung knacken lassen, so sind die Anbieter der Medien in der Lage, diesen Geräteschlüssel in ihren kommenden Veröffentlichungen zu sperren. Das hat für die betroffenen Player oder die Software dann zur Folge, dass sie die Discs der kommenden Generationen nicht mehr abspielen können. „If a set of Device Keys is compromised in a way that threatens the integrity of the system, an updated MKB can be released that causes a device with the compromised set of Device Keys to be unable to calculate the correct  $K_m$ . In this way, the

compromised Device Keys are “revoked” by the new MKB.“ [AAC02] Auf diese Weise haben die Produzenten die volle Kontrolle, auf welchen Geräten ihre Filme abgespielt und aufgenommen werden können. Eine zentrale Autorisierungsstelle soll dabei sicherstellen, dass jede veröffentlichte Disc auch wirklich eine aktuelle Liste mit den annullierten Schlüsseln enthält.

Das Rechtemanagement von AACS legt genau fest, auf welche Arten sich eine Disc abspielen lässt und ob es dabei zeitliche Begrenzungen gibt. Die Ausgabe des Audio- und Videostroms wird genauestens reguliert und bisher ist es vorgesehen, dass entsprechende HDTV („High Definition Television“) Geräte nur digital verschlüsselt per HDCP („High-bandwidth Digital Content Protection“) angesteuert werden können. Analoge Ausgänge werden vom Rechtemanagement entweder ganz abgeschaltet oder auf eine niedrige Auflösung herunterskaliert. DM

#### 4.8.2. Gefahren des AACS

Durch das sensible Schlüsselmanagement bei AACS lässt sich auch schnell ein Horrorszenario herleiten: Gelingt es einem versierten Cracker, einen AACS-Geräteschlüssel zu knacken und öffentlich zu machen, könnte ein immenser wirtschaftlicher Schaden für den Hersteller des betroffenen Gerätes entstehen, da dessen Player von einem auf den anderen Tag unbrauchbar werden. Die Besitzer solcher Geräte würden dann ebenfalls in die Röhre schauen, da sie unfreiwillig Opfer einer solchen Attacke geworden wären. DM

## 5. Fazit und Ausblick

Die Ziele des Digital Rights Management liegen auf der Hand: Der Urheber soll für seine Arbeit gerecht entlohnt und das unerlaubte Vervielfältigen verhindert werden. Leider berücksichtigen heutige DRM-Systeme den Datenschutz nur unzureichend, denn eine Registrierung mit Angabe von personenbezogenen Daten ist bei allen Systemen zwingend erforderlich. Die Anbieter behaupten meist, dass anonyme oder pseudonyme Zugänge technisch und wirtschaftlich unzumutbar seien. Unserer Meinung nach ist dieses Argument jedoch sachlich falsch, da durchaus Pre-paid-Systeme denkbar wären mit denen eine anonyme Nutzung möglich wäre.

Viele Nutzer der Dienste haben auch kein Problembewusstsein für die Risiken durch den Verlust der Privatsphäre und sind auf diesem Gebiet wenig sensibilisiert. Sie wissen meist nicht, dass sie Auskunft über ihre Person und ihre Gewohnheiten weitergeben mit denen sich Anbieter ein vollständiges Profil erstellen können. Dieses Profil lässt sich von der Industrie zu zielgerichteten Marketingzwecken verwenden. Ein nicht zu unterschätzendes Missbrauchspotenzial geht von weniger seriösen Unternehmen aus, die z. B. anhand des Kaufs bestimmter Literatur aus dem Gesundheitswesen auf den Gesundheitszustand des Kunden schließen könnten. Seriöse Unternehmen sind sich ihrer Verpflichtung gegenüber dem Kunden zur Aufklärung datenschutzrechtlicher Aspekte durchaus bewusst, überfluten ihn hierbei aber mit seitenlangen Datenschutzerklärungen, die voll von juristischen und technischen Fachbegriffen sind. Das trägt dazu bei, dass diese meist ungelesen akzeptiert werden.

Bei allen Systemen stehen die Interessen der Inhabergebiet im Vordergrund. Dies äußert sich unter anderem dadurch, dass jeder Anbieter ein proprietäres Verfahren entwickelt und versucht auf dem Markt durchzusetzen. Für den Kunden ergeben sich hierdurch Einschränkungen in der Benutzerfreundlichkeit, da für jedes System eigene Software und ggf. sogar eigene Hardware notwendig ist; eine Einigung der Anbieter auf einen gemeinsamen Standard ist nicht abzusehen.

Die Versuche der ehrlichen Kunden sich den Restriktionen, die sich aus dem DRM ergeben, zu entziehen, um sich beispielsweise ein legal gekauftes Musikstück im

Autoradio anzuhören, werden dabei auch vom Gesetzgeber verhindert. Dieser verbietet das Umgehen eines technisch wirksamen Kopierschutzes.

Aufgrund der genannten Gründe fehlt es vielen Endanwendern an Vertrauen in die neue Technologie.

Es wird nur dann gelingen diese Vorbehalte auszuräumen, wenn DRM-Systeme datenschutzgerechter gestaltet werden und nicht nur die Rechte der Urheber im Vordergrund stehen, sondern auch auf die Bedürfnisse der Nutzer eingegangen wird. Es empfiehlt sich schon heute, sich mit DRM-Systemen auseinander zu setzen, denn diese werden unserer Meinung nach immer mehr an Bedeutung gewinnen. Haben sich diese etabliert, so wird ggf. über die Auflösung der Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte (GEMA) nachzudenken sein, da die Rechteinhaber bereits durch das DRM-System vergütet wurden. DM+KR

## 6. Abbildungen

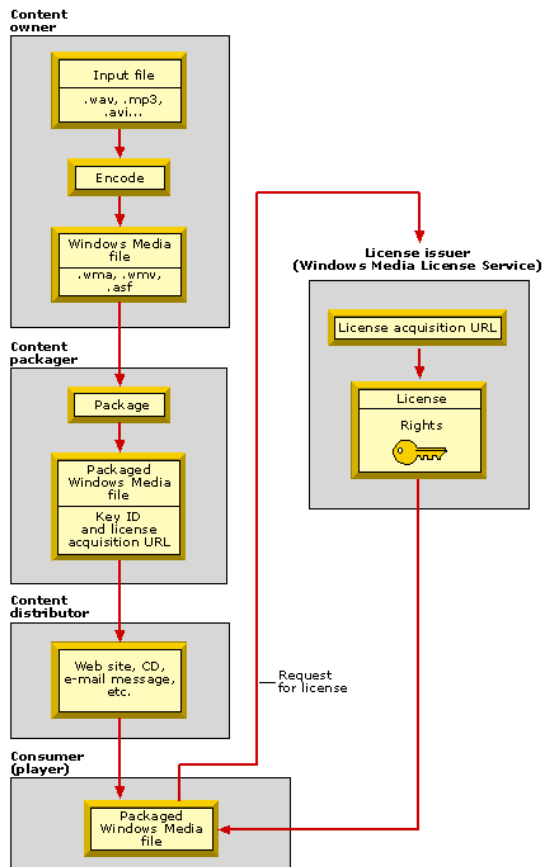


Abbildung 1: Funktionsweise des Windows Media Rights Management (WMRM) [MIC06]

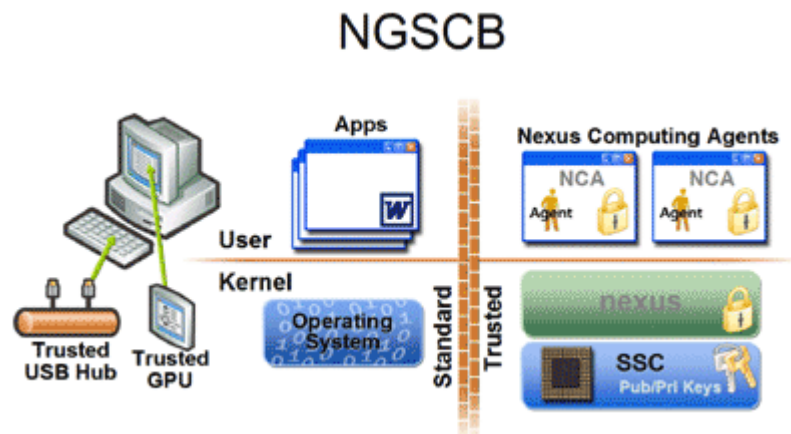


Abbildung 2: Next-Generation Secure Computing Base (NGSCB) [MIC07]

## 7. Literaturverzeichnis

- [AAC01] Advanced Access Content System: Specifications, <http://aacsla.org/specifications/specifications.htm>, 2005
- [AAC02] Advanced Access Content System: Introduction and Common Cryptographic Elements v0.90, [http://aacsla.org/specifications/AACS\\_Spec-Common\\_0.90.pdf](http://aacsla.org/specifications/AACS_Spec-Common_0.90.pdf), 2005
- [ADO01] Adobe Systems: Hilfe für Adobe DRM Actovator, <https://aractivate.adobe.com/eden/edenui.asp?command=showhelp&argument=1>, 2003
- [ADO02] Adobe Systems: Online Privacy Policy, <http://www.adobe.com/misc/privacy.html>, 2005
- [AND01] Anderson, R.: 'Trusted Computing' Frequently Asked Questions, <http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html>, Cambridge 2003
- [APP01] Apple Computer: Apple Support – iTunes Music Store Customer Service, <http://www.apple.com/lu/support/itunes/authorization.html>, 2005
- [APP02] Apple Computer: Apple Strategie zum Schutz der Persönlichkeitsrechte, <http://www.apple.com/de/legal/privacy/>, 2005
- [BEC01] Bechtold, S.: Vom Urheber- zum Informationsrecht, München, 2002
- [BEC02] Bechtold, S.: The Present and Future of Digital Rights Management – Musings on Emerging Legal Problems, in Digital Rights Management: Technological, Economic, Legal and Political Aspects, 2003, S. 597-654
- [BEC03] Bechtold, S.: Trusted Computing: rechtliche Probleme einer entstehenden Technologie, [http://www.jura.uni-tuebingen.de/bechtold/2005\\_20online.pdf](http://www.jura.uni-tuebingen.de/bechtold/2005_20online.pdf), Bonn 2005
- [BVG01] BVerfGE 65, 1: Volkszählungsurteil, <http://www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm>, 1983
- [BYG01] Bygrave, L. A.: Digital Rights Management and Privacy — Legal Aspects in the European Union, in Digital Rights Management: Technological, Economic, Legal and Political Aspects, 2003, S. 418-446
- [DIX01] Dix, A.: Datenschutz und DRM, <http://netzspannung.org/tele-lectures/series/DRM>, 2005
- [DPA01] dpa: Sony setzt Produktion von CDs mit XCP-Kopierschutz aus, <http://www.sueddeutsche.de/computer/artikel/277/64213/>, 14.11.2005
- [FEL01] Felton, E.: Don't Use Sony's Web-based XCP Uninstaller, <http://www.freedom-to-tinker.com/?p=926>, 2005
- [FIR01] First4Internet Ltd.: XCP, <http://www.xcp-aurora.com/xcp.aspx>, 2005
- [FSE01] F-Secure: XCP DRM Software, [http://www.f-secure.com/v-descs/xcp\\_drm.shtml](http://www.f-secure.com/v-descs/xcp_drm.shtml), 2005
- [MIC01] Microsoft Corporation: Windows Media Rights Manager 10.1 SDK, <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wmrm10/htm/windowsmediarightsmanagersdk.asp?frame=true>, 2005
- [MIC02] Microsoft Corporation: How does Windows Media DRM work?, [http://www.microsoft.com/windows/windowsmedia/drm/faq.aspx#drmfq\\_1\\_4](http://www.microsoft.com/windows/windowsmedia/drm/faq.aspx#drmfq_1_4), 2005
- [MIC03] Microsoft Corporation: What is Secure Path?, [http://www.microsoft.com/windows/windowsmedia/drm/faq.aspx#drmfq\\_2\\_7](http://www.microsoft.com/windows/windowsmedia/drm/faq.aspx#drmfq_2_7), 2005
- [MIC04] Microsoft Corporation: Trustworthy Computing, <http://www.microsoft.com/mscorp/twc/default.mspix>, 2005
- [MIC05] Microsoft Corporation: Next-Generation Secure Computing Base, <http://www.microsoft.com/resources/ngscb/default.mspix>, 2005
- [MIC06] Microsoft Corporation: Understanding How Windows Media Rights Manager Works, <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wmrm10/htm/howwindowsmediarightsmanagerworks.asp>, 2005
- [MIC07] Microsoft Corporation: Microsoft Discusses Details of Next-Generation Secure Computing Base, <http://www.microsoft.com/presspass/features/2003/may03/05-07NGSCB.mspix>, 2003
- [MUS01] Musicload: Anmeldung, <http://www.musicload.de/login>, 2005
- [MUS02] Musicload: Cover, <http://www.musicload.de/special?pageid=43>, 2005
- [MUS03] Musicload: Nutzungsrechte, <http://www.musicload.de/help?pageid=28>, 2005
- [OBE01] Obert, T.: Next Generation Secure Computing Base, in Datenschutz und Datensicherheit, 2005, S. 521-525

- [PHI01] Philips Electronics N.V.: Intellectual Property & Standards,  
<http://www.licensing.philips.com/information/cd/audio/>, 2005
- [SON01] SonyBMG: EULA, <http://www.sysinternals.com/blog/sony-eula.htm>, 2005
- [SON02] SonyBMG: XCP, <http://cp.sonybmg.com/xcp/customerletter.html>, 2005
- [SOP01] Sophos: Virus disinfection, <http://www.sophos.co.uk/support/disinfection/rkprf.html>, 2005
- [SUN01] SunComm International: MediaMax, <http://www.sunncomm.com/Brochure>, 2005
- [SYS01] SysInternals: Mark's Blog,  
<http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html>, 2005
- [SYS02] SysInternals: Mark's Blog,  
<http://www.sysinternals.com/blog/2005/11/sonys-rootkit-first-4-internet.html>, 2005