Georg-August-Universität Göttingen
Institut für Wirtschaftsinformatik
Professor Dr. Matthias Schumann

WI2 WIRTSCHAFTSINFORMATIK II

Platz der Göttinger Sieben 5
37073 Göttingen
Telefon: + 49 551 39 - 44 33
+ 49 551 39 - 44 42
Telefax: + 49 551 39 - 97 35
www.wi2.wiso.uni-goettingen.de

Arbeitsbericht Nr.08/2004
Hrsg.: Matthias Schumann

Lutz Seidenfaden/Svenja Hagenhoff

Absatz digitaler Produkte und Digital Rights Management

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AAC	Advanced Audio Coding
COS	Content Owner Sponsoring
CRF	Content Reference Forum
DRM	Digital Rights Management
DRMS	Digital Rights Management System(e)
EMMS	Electronic Media Management System
I&K	Information und Kommunikation
ISP	Internet Service Provider
MPEG	Motion Picture Expert Group
ORDL	Open Digital Rights Language
P2P	Peer-to-Peer
PDF	Portable Document Format
REL	Rights Expression Language
RSVP	Realtime Reservation Protocol
RTCP	Realtime Control Protocol
RTP	Realtime Transport Protocol
RTSP	Realtime Streaming Protocol
TCG	Trusted Computing Group
TCPA	Trusted Computing Platform Association

1 Einleitung

Mit der Zunahme von Internetanschlüssen weltweit hat die Distribution digitaler Produkte an Bedeutung gewonnen. Hervorzuheben sind vor allem die Möglichkeiten der Disintermediation, also der Ausschaltung von Handelsstufen bzw. Intermediären im Distributionsprozess und den damit verbundenen Veränderungen in der Wertschöpfungskette.

Populäre Peer-to-Peer-Applikationen wie WinMx (http://www.winmx.com), Gnutella (http://www.gnutella.com) oder KaZaa (http://www.kazaa.com), mittels derer Inhalte beinahe jeglicher Art bezogen werden können, haben zudem den Ruf nach Mechanismen zur Wahrung des Urheberrechts laut werden lassen. Die wirtschaftlichen Auswirkungen der nahezu kostenlosen Distribution digitaler Güter sind anhand sinkender Abverkaufszahlen und damit einhergehenden Umsatzeinbrüchen in der Entertainment-Branche eindrucksvoll dargelegt[1].

Unter dem Schlagwort Digital Rights Management (DRM), sind jüngst zahlreiche Initiativen gegründet worden, die den Schutz des Urheberrechts von digitalen Produkten zum Ziel haben[2].

Der vorliegende Arbeitsbericht klärt in Kap. 2 die grundlegenden Begriffe, Eigenschaften und Technologien im Zusammenhang mit digitalen Gütern. Weiterhin werden traditionelle Erlösmodelle der Distribution digitaler Güter dargestellt (vgl. Kap. 3). Digital Rights Management wird in Kap. 4 behandelt. Dazu werden eine Begriffsdefinition gegeben, grundlegende Konzepte vorgestellt und aktuelle Technologien erörtert sowie aktuelle DRM-Systeme im Überblick dargestellt. Der Arbeitsbericht schließt mit einer Zusammenfassung (vgl. Kap. 5).

[1] vgl. ifpi (2004), S. 1; Es gibt jedoch kritische Stimmen, die behaupten, dass die Umsatzeinbußen nicht nur durch Raubkopieren („piracy“) sondern ebenfalls durch Innovationsdefizite im Hinblick auf Organisations- und Vertriebsformen seitens der Unterhaltungsindustrie verursacht werden. Vgl. dazu Kuhlen (2003), S. 118ff.

[2] z.B. Content Reference Group (http://www.crforum.org/), Trusted Computing Platform Association (http://www.trustedcomputing.org/home), Trusted Computing Group (http://www.trustedcomputing group.org/)

2 Grundlagen: Digitale Produkte

Die Verwendung des Begriffs „digitale Produkte“ ist in der wissenschaftlichen Literatur uneinheitlich, da sich dieser auf digitale Gütern, digitale Dienstleistungen und Informationsgütern beziehen kann. Um ein allgemeines Verständnis des Untersuchungsgegenstandes zu ermöglichen, wird in 2.1 eine (mögliche) Definition (vgl. 2.1.1) vorgenommen und grundlegende Eigenschaften digitaler Produkte erläutert (vgl. 2.1.2).

2.1 Definition und Begriffsabgrenzung

Digitale Produkte sind allgemein recht eindeutig gegenüber physischen Produkten abgrenzbar. Das grundlegendste Unterscheidungskriterium zwischen physischen und digitalen Produkten ist die Immaterialität[3].

Physische Produkte werden hier nicht betrachtet, da sie keinen digitalen Anteil haben, d.h. nicht durch Datenströme repräsentiert werden können. Sie sind folglich materiell. Vielmehr sollen an dieser Stelle die digitalen Güter betrachtet werden, die aufgrund ihrer Immaterialität vollständig elektronisch handelbar sind.

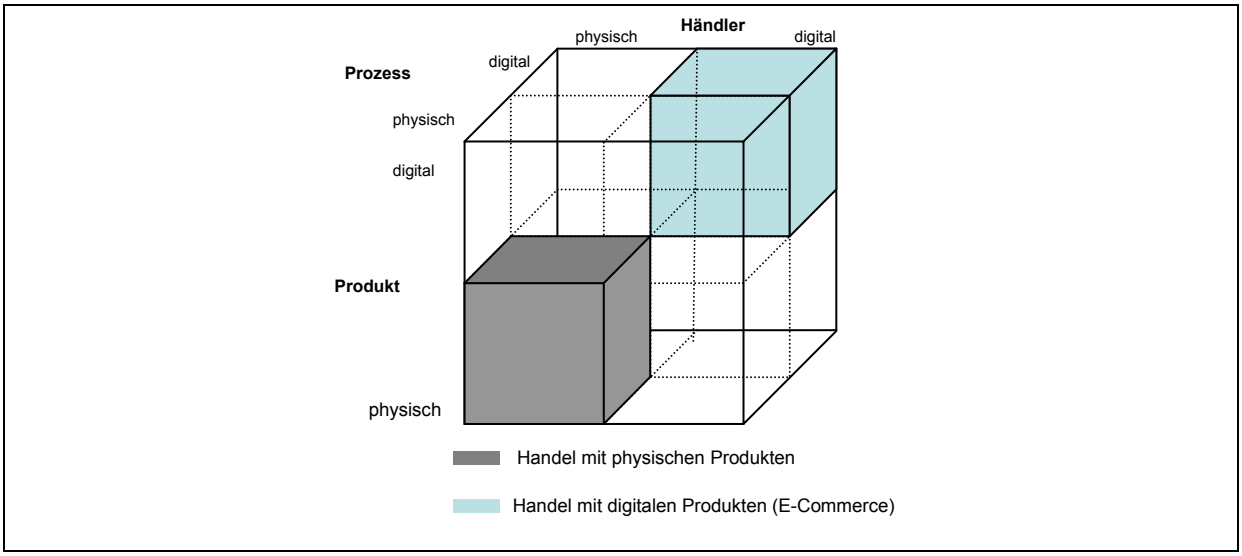

Abbildung 2-1: Einordnung von vollständig digitalem und traditionellem Handel[4]

Dies bedeutet, dass neben dem gehandelten Gut (z.B. ein Musiktitel), auch der Handelsprozess (z.B. Suche, Kaufabwicklung und Distribution über das Internet) und der Makler (z.B. ein elektronisches Wertpapierhandelssystem) elektronisch sind (vgl. Abb. 2-1)[5].

[3] vgl. Löbbecke (1999), S. 1
[4] vgl. Löbbecke (1999), S. 2
[5] vgl. Luxem (2001), S. 14, Brandtweiner (2000), S. 31, Barkai (2002), S. 62

Dieses Verständnis deckt sich weitgehend mit dem Begriff des Online Delivered Content (ODC), der als „data, information, and knowledge traded on the internet or other online means“[6] verstanden wird und sich auf Online-Magazine, -Datenbanken und (Online-)Beratung, etc. bezieht. In beiden Definitionen ist die, durch die Digitalisierbarkeit bedingte, Möglichkeit der Distribution über ein Netzwerk das entscheidende Kriterium[7]. Dies impliziert eine Loslösung des Inhalts von einem physischen Trägermedium.

Die Definition des ODC fasst die Produktgruppen digitale Informationsgüter, digitale Güter und digitale Dienstleistungen zusammen, deren Unterschiede erklärungsbedürftig erscheinen:

- Digitale Informationsgüter werden ausschließlich ihres Inhalts wegen gekauft[8]. Das Trägermedium ist dabei unerheblich. Beispiele sind wissenschaftliche Publikationen, eBooks, Tageszeitungen und Musik in elektronischer Form.
- Digitale Güter im engeren Sinn sind immaterielle Güter, die ihrer Funktion wegen gekauft werden, der Inhalt jedoch keine oder nur eine untergeordnete Rolle spielt. Als Beispiel kann Software angeführt werden, die dem Nutzer eine gewisse Funktionalität bietet, dieser jedoch nicht an der der Funktionalität zugrunde liegenden Programmierung interessiert ist.
- Digitale Dienstleistungen benötigen, wie traditionelle Dienstleistungen auch, die Mitwirkung des Kunden („externer Faktor“). Darin unterscheiden sich die digitalen Dienstleistungen von den digitalen Produkten und digitalen Informationsgütern. Beispiele hierfür sind Beratungsdienste z.B. von Versicherungen und Banken, die online geführt werden. Ohne die Angabe der Kundenwünsche dürfte eine sinnvolle Beratung nicht möglich sein.

Im Folgenden wird der Fokus der Untersuchung auf die digitalen Informationsgüter und die digitalen Güter gelegt, die unter dem Term „digitale Produkte“ subsumiert werden. Sie weisen einige charakteristische Eigenschaften auf[9]:

Erstens sei die *Nicht-Abnutzbarkeit* genannt. Dies bedeutet, dass digitale Güter keinerlei Abnutzung unterliegen, wie es üblicherweise bei physischen Produkten zu beobachten ist. Die Unterscheidung zwischen neuem und altem (z.B. Second Hand) Produkt entfällt, da die Produktqualität mit der Zeit nicht abnimmt.

Zweitens ist die vergleichsweise einfache *Veränderbarkeit* von digitalen Produkten hervorzuheben. Diese bezieht sich jedoch nicht auf Abnutzung durch Benutzung, sondern auf willentliche Veränderungen wie z.B. die gezielte Veränderung von Programmcode. Dadurch wird es möglich, mit geringem Aufwand Produktvarianten zu erstellen, die neue Nachfrage auf dem Absatzmarkt nach sich ziehen.

Drittens ist die einfache *Reproduzierbarkeit* von digitalen Produkten zu nennen. In der Literatur wird in diesem Zusammenhang von „first copy costs“ gesprochen, also jenen Kosten, die bei der Erstellung des ersten Exemplars des digitalen Produktes entstehen[10]. Die Grenzkosten für die Erstellung von wei-

[6] Löbbecke (1999), S. 1
[7] ähnlich Brandtweiner (2000), S. 33
[8] vgl. Brandtweiner (2000), S. 37
[9] vgl. Luxem (2001), S. 24, Brandtweiner (2000), S. 34
[10] vgl. Varian (1998), S.5, Brandtweiner (2000), S.146 , Grimm (2003), S. 94

teren Kopien des digitalen Produktes sind, im Gegensatz zu physischen Produkten, vernachlässigbar gering (bzw. tendieren gegen Null)[11]. Ökonomisch bedeutet dies, dass sich eine Fixkostendegression einstellt, da sich alle hergestellten Stücke nur noch die Produktionskosten teilen und daher die Kosten pro Stück drastisch abnehmen („economies of scale"). Dieser Effekt ist bei digitalen Gütern umso größer, da die Investitionen in Produktionsanlagen für digitale Produkte im Gegensatz zu Anlagen für die Herstellung physischer Produkte relativ gering sind. Da (fast) keine Kapazitätsgrenze existiert, entfallen zudem noch weitere Investitionen, die sonst bei einer Ausweitung der Produktion bei physischen Produkten notwendig wären.

Durch diese Eigenschaften ergeben sich eine Reihe von ökonomischen Fragestellungen. Zunächst muss geklärt werden, ob digitale Produkte als knappe, private und damit marktfähige, oder als öffentliche bzw. freie Güter einzuordnen sind. Für eine Einordnung als freie Güter spricht die einfache Reproduzierbarkeit, die es ermöglichen sollte, die Nachfrage nach einem Gut zu einem gegebenen Zeitpunkt zu befriedigen. Es entsteht also kein Knappheitseffekt, wie dies bei knappen Gütern der Fall ist. Für eine Einordnung als öffentliches Gut spricht, dass die Nutzung des Gutes unabhängig von der Anzahl der Nutzer ist, bzw. die Nutzung des Gutes durch eine Person nicht die Nutzung des Gutes durch eine andere Person einschränkt („Nichtrivalität beim Konsum"). Damit digitale Produkte marktfähig werden, d.h. den Charakter von knappen und privaten Gütern annehmen, erscheint eine unterstützende Gesetzgebung (z.B. Urheberrechte) und die Durchsetzung dieser Rechte notwendig.

Ein anderer Aspekt betrifft die Preisbildung für digitale Produkte. Nimmt man die Preissetzung anhand der in der ökonomischen Theorie verbreiteten Methode, nach welcher der optimale Preis in der Höhe der Grenzkosten eines Gutes festzusetzen ist, vor, wäre der Preis aufgrund der einfachen Reproduzierbarkeit gleich Null. Die digitalen Produkte müssten demnach kostenlos erhältlich sein.

Der Markt für digitale Produkte muss folglich als unvollkommen angesehen werden[12], da der Preis für digitale Produkte über deren Grenzkosten liegt, staatliche Eingriffe notwendig und die digitalen Produkte nicht homogen sind[13].

2.2 Überblick über Distributionstechnologien

Distributionsarchitekturen für digitale Inhalte lassen sich allgemein in „infrastucture-based" und „Peer-to-Peer" Content Distribution unterteilen[14]. Erstere fügt sich in das traditionelle Client/Server-System ein, indem sie die zu verteilenden Inhalte auf einem oder mehreren zentralen Server(n) vorhält von dem diese vom Benutzer bei Bedarf abgerufen werden. Letztere funktionieren in der Regel ohne Zentralinstanz, da die Inhalte auf den teilnehmenden Peers verteilt vorgehalten werden („Peer-provided Con-

[11] vgl. Grimm (2003), S. 96
[12] vgl. dazu ausführlich Varian (1998)
[13] für Merkmale eines unvollkommenen Marktes vgl. Kortmann (2002)
[14] vgl. Padmanabhan et al. (2002), S. 1

tent“)[15]. Die Verschiedenartigkeit der Konzepte lässt vermuten, dass die Modelle sich in ihren Anwendungsgebieten und den eingesetzten Technologien unterscheiden.

2.2.1 Distributionstechnologien in der zentralen Architektur

Ein Beispiel für eine Technologie im Rahmen der zentralen Architektur stellt „Streaming Media“ dar, welche sich wie folgt beschreiben lässt: „Der Begriff Streaming Media bezeichnet eine Internet-Technologie, bei der Filme oder Sprache bzw. Musik in Echtzeit direkt aus dem Inter- oder Intranet abgespielt werden können“[16]. Hierbei werden die Multimediadaten (z.B. Audio- und Videodaten) als stetige Datenströme (Streams) erzeugt und verarbeitet. Die Daten liegen hierbei auf den zentralen Servern, die sie auf Anfrage von Nutzern bereitstellen. Streaming stellt hohe Anforderungen an die Hardware (insbesondere Bandbreite) und kann selbst die Kapazität großer Server schnell erschöpfen[17]. Dies resultiert vor allem daraus, dass Streaming Media an besondere Anforderungen hinsichtlich der Servicequalität (Quality of Service, QoS) gebunden ist[18]:

- **Bandbreite:** Unter Bandbreite versteht man die Geschwindigkeit mit der ein Multimedia-Stream transportiert wird. Die Bandbreite sollte bei der Distribution ausreichend und kontinuierlich hoch sein, um eine flüssige Übertragung zu gewährleisten.
- **Latenz:** Hierunter wird die Transportlaufzeit verstanden, also die Zeit, die ein Stream zwischen Sender und Empfänger unterwegs ist. Die Latenz von Multimedia-Streams sollte möglichst klein sein und nicht zu stark schwanken.
- **Verlustrate:** Die Verlustrate gibt an, wie viel Datenelemente verworfen werden, da sie nicht in der geplanten Auslieferungszeit den Empfänger erreicht haben und somit wertlos sind. Um Verlustraten möglichst gering zu halten, sind ausreichend große Zwischenspeicher (Buffer) vorzuhalten, welches häufig eine nicht akzeptable Inanspruchnahme von Ressourcen auf Clientseite darstellt.

Insbesondere um die Beanspruchung der Bandbreite (ca. 120 Mbps für einen TV-Video-Stream) während der Übertragung zu reduzieren, ist es üblich, Streams vor dem Versand zu komprimieren. Dies geschieht mit Hilfe sogenannter Codecs (kurz für compression/decompression), die Informationen über die Verarbeitung und Ausgabe der Streamdaten beinhalten und die Komprimierung auf Sender- und Empfängerseite vornehmen (vgl. Abb. 2-2).

[15] vgl. Miller (2001), S. 20
[16] Wegner / Bachmeier (2000), S. 13
[17] vgl. Gehrke et al. (2003), S. 2
[18] vgl. dazu Coulouris et al. (2002), S. 714

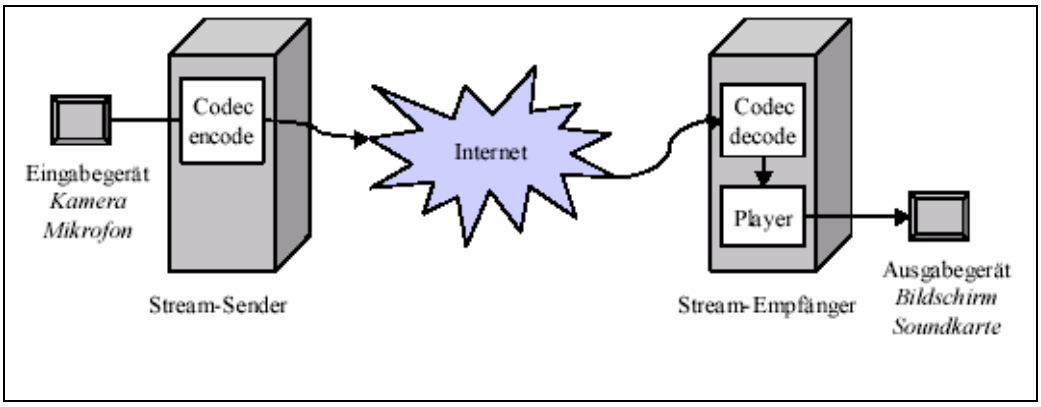

Abbildung 2-2: Versand eines Multimedia-Streams[19]

Gängige Medienformate wie MPEG-1,2,4 (Motion Picture Expert Group), AVI (Audio Video Interface), MOV (Apple Quicktime), DivX im Videobereich sowie MPEG-3 und AAC (Advanced Audio Coding) im Audiobereich, können so die Bandbreitenanforderungen um den Faktor 10 bis Faktor 100 reduzieren. Dies wird allerdings mit erhöhtem Rechenbedarf für die Kodier- bzw. Dekodiervorgänge bei Versand und Wiedergabe erkauft. Dies geschieht i.d.R mit Hilfe einer meist properitären Audio-Video-Players (Quicktime Player, Realplayer, DivX Player oder Windows Media Player), der das Abspielen von Audio- und Videodateien ermöglicht.

Für die Übertragung selbst werden spezielle, meist auf TCP/IP oder UDP/IP aufsetzende Protokolle benutzt. Diese Notwendigkeit ergibt sich, da TCP/IP in Ermangelung geeigneter Mechanismen zur Bandbreitenreservierung die nötige Servicequalität nicht bereitstellen kann[20]. Folgende Protokolle sind im Zusammenhang mit Streaming zu nennen:

- RTP[21]: Das paketorientierte Real Time Transport Protocol überträgt Informationen zum Typ des Streams (Audio/Video) zur Abspielzeit und weiteren Timing Anforderungen, d.h. dass es kein reines Transportprotokoll ist. Es kann jedoch die zeitgerechte Auslieferung der einzelnen Pakete eines Streams nicht garantieren, so dass die Servicequalität nicht garantiert werden kann.
- RTCP[22]: Das Real Time Control Protocol kontrolliert die Übertragung von RTCP-Paketen in einer RTP-Session und ermöglicht Feedback vom Empfänger an den Sender. Dies bedeutet, dass mit Hilfe von RTCP Informationen über den Datenfluß ausgetauscht werden.
- RTSP[23]: Das Real Time Streaming Protocol ist ein IETF Proposed Standard. RTSP ist auf der Applikationsebene angesiedelt auf der es Multimedia-Streams eröffnet und kontrolliert. RTSP bietet Funktionen, die im Zusammenhang mit Streaming-Systemen von Bedeutung sind. Dazu zählen sind das Zwischenspeichern (Caching) von Daten (ähnlich wie bei HTTP), das Wechseln des Servers innerhalb eines Streams (load balancing) und Synchronisation verschiedener Streams von mehreren Servern.

[19] Gehrke et al. (2003), S.4
[20] ähnlich Coulouris et al. (2002), S. 99
[21] vgl. RTP (2003) sowie Schulzrinne et al. (1996), S. 1- 13
[22] vgl. Schulzrinne et al. (1996), S. 15 -17
[23] vgl. RTSP (2004)

- RSVP[24]: Das Real Time Reservation Protocol ist für die Reservierung von Bandbreiten zuständig. Dafür wird auf den Routern, die zwischen Sender und Empfänger liegen, die benötigte Bandbreite reserviert, so dass eine bestimmte Servicequalität garantiert werden kann. Einschränkend ist zu bemerken, dass die bisher im Internet eingesetzten Router die Ressourcenreservierung nicht unterstützen[25].

Die vorgestellten Protokolle arbeiten dergestalt zusammen, dass per RTSP die Verbindung geöffnet wird, dann mittels RTP oder RTCP die Übertragung des vorgenommen wird. RSVP würde, wenn es zum Einsatz kommt, die Servicequalität durch die Reservierung benötigter Bandbreite gewährleisten. Der Durchbruch der Streaming Technologie wird in diesem Jahr (2004) erwartet, da dann die Anzahl der Breitbandanschlüsse genügt, um Skaleneffekte auf Seiten der Streaminganbieter realisieren zu können[26]. Dementsprechend erwartet man einen Anstieg des Traffic, der durch „Rich Media"-Anwendungen (zu denen Streaming zählt) hervorgerufenen wird (vgl. Abb 2-3).

Neben Streaming zählt natürlich auch das Beziehen von Inhalten jeglicher Art (z.B. per Download oder Email) von einem zentralen Anbieterserver zu den zentralen Distributionstechnologien. Die Anforderungen an Hardware und Bandbreite sind jedoch bei weitem nicht so hoch wie bei Streaming Media. Beispielsweise spielt beim Download einer Softwaredatei die Reihenfolge des Eintreffens der einzelnen Datenpakete keine Rolle, da die Software vor dem vollständigen Herunterladen ohnehin nicht verwendungsfähig ist. Daher werden in diesem Zusammenhang meist keine speziellen Protokolle (sondern TCP/IP oder FTP) verwendet, weshalb an dieser Stelle nicht darauf eingegangen werden soll.

2.2.2 Technologien in der dezentralen Architektur

Als dezentrale Distributionstechnologie ist z.B. das Peer-to-Peer-Filesharing zu nennen. Die Popularität von Filesharing-Applikationen war mit Beginn ihres Aufkommens sehr hoch, daher wird der Traffic nach Schätzungen in naher Zukunft nur marginal ansteigen (vgl. Abb. 2-3). Beim Filesharing liegen die Inhalte auf den teilnehmenden Peers verteilt. Jedes Peer stellt Funktionen zum Dateiversand, Empfang und zur Dateisuche bereit, ist also Client und Server zugleich. In dieser Architektur erhöht sich, durch den Wegfall einer zentralen Koordinationsinstanz hervorgerufen, der Koordinationsaufwand zwischen Peers und damit die Belastung des Netzes[27]. Das Problem im Gnutella-Netz lag in dessen Kommunikationsprotokoll begründet, welches durch ineffiziente Suchalgorithmen die Bandbreite überbeanspruchte.

Neuere Protokolle, wie z.B. Chord, implementieren allerdings Algorithmen, die Suchanfragen sehr effizient in logarithmischer Laufzeit durchführen und so die Belastung des Netzes minimieren[28]. Allgemein lassen sich die aktuellen Peer-to-Peer-Kommunikationsprotokolle in properitäre und offene Protokolle unterteilen (vgl. Tabelle 2-1).

[24] vgl. RSVP (2004)
[25] vgl. Gehrke et al. (2003), S. 5 und Ripeanu et al. (2003), S. 6
[26] vgl. Lainee et al. (2002), S. 3
[27] vgl. dazu Messungen im Gnutella Netz von Ripeanu et al. (2003) ,S. 6-7, Barkai (2002), S. 278
[28] vgl. Stoica et al. (2002)

Protokoll	properitär	offen	Client-Anwendung
Napster	X		Napster
Fasttrack	X		KaZaa
JXTA		X	JXTA
Gnutella		X	Gnutella
OpenFT		X	beliebiger Client
Jabber		X	beliebiger Client
eDonkey	X		eDonkey
WinMX	X		WinMX

Tabelle 2-1: Übersicht gängiger Peer-to-Peer-Protokolle

Während der Quellcode der properitären Protokolle nicht öffentlich und an bestimmte Client-Applikationen gebunden ist, sind die Protokollspezifikationen der offenen Protokolle frei zugänglich.

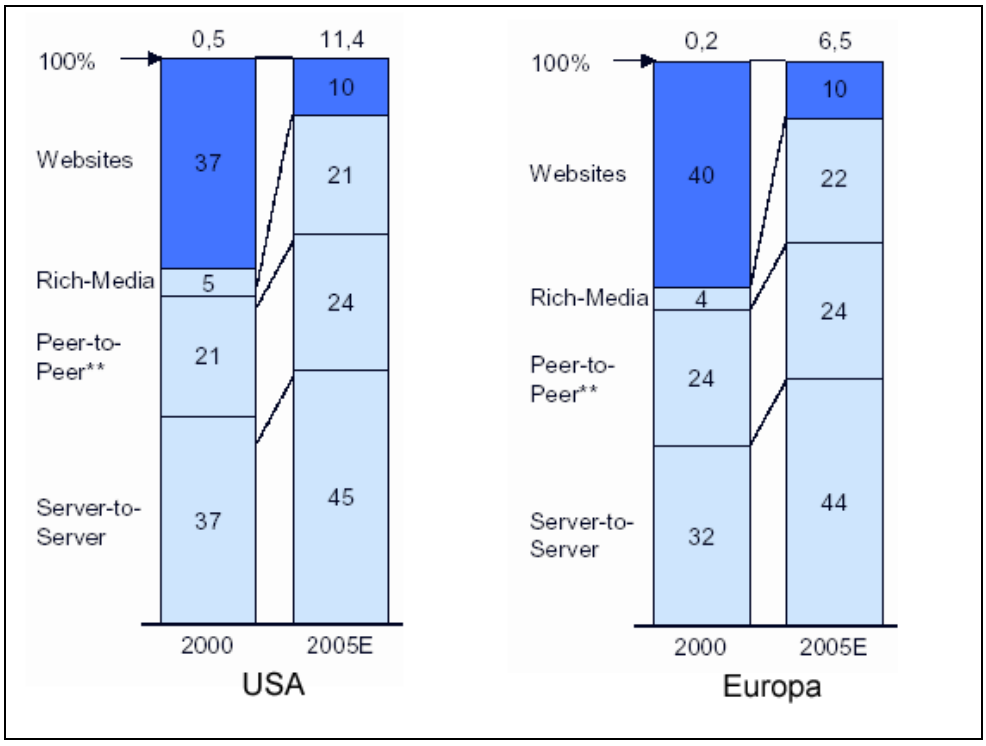

Abbildung 2-3: Übersicht über Traffic-Aufkommen in Europa und USA[29]

Neben der zusätzlichen Bandbreite, die durch den erhöhten Koordinationsaufwand hervorgerufen wird, sind auch die Bereiche Sicherheit, Vertrauen und Urheberrechtsverletzungen (vgl. Kap. 3) Problembereiche, da sich die dezentralen Strukturen schlechter kontrollieren lassen als ein zentralisiertes System. Einige Autoren sehen in der schweren Kontrollierbarkeit von P2P-Strukturen durch Autoritäten aber auch gerade den Vorteil von P2P-Distribution[30].

Vor dem Hintergrund der Entwicklung von P2P-Anwendungen zu einem kommerziell anerkannten, d.h. legalen Distributionskanal für digitale Inhalte ist fraglich, ob die mangelnde Kontrollierbarkeit dieser Entwicklung förderlich ist.

[29] entnommen aus Lainee et al. (2002), S. 2
[30] vgl. Miller (2001), S. 4-14;25

Das die beiden genannten Distributionsarchitekturen und die eingesetzten Technologien keine Antagonisten sind, zeigen Bestrebungen, Peer-to-Peer Umgebungen zum Verteilen von Streaming Media Datenströmen zu nutzen[31].

3 Grundlegende Erlösmodelle der Distribution digitaler Produkte

Ein Erlösmodell ist der Teil einer modellhaften Beschreibung eines Geschäfts (Geschäftsmodell), in dem dargelegt wird, aus welchen Quellen die Einnahmen des Unternehmens generiert werden[32]. Die Arbeit konzentriert sich auf Erlösmodelle, da im Rahmen dieses Arbeitsberichtes die Distribution erörtert wird und somit z.B. das die vorgelagerte Wertschöpfungsstufe beschreibende Produktionsmodell außer Betracht gelassen werden kann.

Aufgrund der etablierten Marktstrukturen besteht hinsichtlich der branchenspezifischen Geschäftsmodelle oft nur wenig Spielraum[33]. Die oben erläuterten technischen Möglichkeiten der Distribution digitaler Produkte (vgl. 2.2) eröffnen den Produzenten eine Chance, aus diesen etablierten Marktstrukturen auszubrechen und neue Erlösformen zu entwickeln, die erst durch digitale Produkte ermöglicht werden (z.B. Micropayment für Anzeigen und Inhalte im Internet, Pay-per-View-Modelle im digitalen Fernsehen). Allgemein können direkte und indirekte Erlösformen unterschieden werden, wie nachfolgend dargestellt wird. Aufgrund der Eigenschaften digitaler Produkte, insbesondere der einfachen Reproduzierbarkeit (vgl. 2.1.2) und der daraus resultierenden Möglichkeit zur kostengünstigen Distribution, wird angenommen, dass ein großer Teil der digitalen Produkte kostenfrei erhältlich sein wird[34]. Dies bringt die Anbieter dazu, einen Großteil des Erlöses über nicht-digitale Güter und Dienstleistungen, wie Beratung, Softwaretraining (sofern dieses nicht über Internet erfolgt) und kostenpflichtige Suchmaschinen zu erbringen, da diese nicht den Kostenstrukturen digitaler Produkte unterliegen (vgl. 2.1.1) und man sich dadurch eine Generierung von Erlösen erhofft.

3.1 Direkte Erlösmodelle

Im Rahmen von direkten Erlösmodellen werden die Erlöse aus dem Verkauf der digitalen Produkte generiert. Als Beispiele hierfür sind der Vertrieb von Lizenzen, die volumenabhängige Abrechnung und Abonnements zu nennen. Beim Vertrieb von Lizenzen werden Nutzungsrechte an verschiedenen Varianten des digitalen Produkts an die Nutzer verkauft. Hierbei sind (teilweise aufwendige) Mechanismen zu installieren, die den Missbrauch der Lizenzen durch Unautorisierte verhindern sollen. In dem Modell der Superdistribution[35] werden die digitalen Produkte zwar über eine unsichere öffentliche Infrastruktur schnell und einfach verteilt, idealerweise kann die Nutzung aber erst erfolgen, wenn man einen zum

[31] vgl. z.B. Gehrke et al. (2003) sowie Padmanabhan et al. (2002).
[32] vgl. Stähler (2001), S. 41
[33] vgl. Luxem (2001), S. 77
[34] vgl. Dyson (1995), S.1-2, Grimm (2003), S. 96
[35] vgl. zur Superdistribution im Kontext von Peer-to-Peer Rosenblatt et al. (2002), S. 29

Produkt passenden Schlüssel (Lizenz) vom Hersteller oder einem Clearing Center gegen Entgelt bezogen hat.

Somit wird eine schnelle Verbreitung der Produkte gewährleistet, ohne die Kontrolle der Nutzung aufzugeben[36]. Die Komplexität der Lizenzmodelle reicht von den einfachen Pay-per-view bzw. Pay-per-use-Modellen (z.B. für Videofilme), die nur variable Kosten beinhalten, bis hin zu Modellen, die die Nutzung von Produkten mehrfach und zeitabhängig erlauben.

Die volumenabhängige Abrechnung stellt dem Nutzer den Umfang des von ihm genutzten Produkts in Rechnung. Der Umfang lässt sich z.B. anhand des Datenvolumens, der Anzahl unterschiedlicher Produkte oder der Anzahl von Abfragen quantifizieren. Im Gegensatz zum Lizenzmodell erfolgt in diesem Fall die Abrechnung nicht für ein einzelnes Produkt, sondern über ein, oft zeitraumbezogenes, Produkt- bzw. Leistungsbündel. Dies setzt die detaillierte Protokollierung der Inanspruchnahme sowie die Verwaltung von Kundenkonten voraus[37].

Als ein von traditionellen Medien (insbesondere Printmedien) bekanntes Erlösmodell wurde das Abonnentenmodell in die Distribution digitaler Produkte integriert. Als einzigem der hier vorgestellten Erlösmodelle liegt dem Abonnentenmodell eine dauerhafte Geschäftsbeziehung zwischen Anbieter und Nutzer des digitalen Produktes zugrunde. Der Abnehmer (Abonnent) zahlt für die Nutzung zuvor determinierter Leistungen des Anbieters eine feste Gebühr pro Abrechnungszeitraum. Das Maß der Inanspruchnahme der Leistungen durch den Abonnenten ist dabei für die Abrechung unerheblich. Der Vorteil dieses Modells liegt in der Einfachheit der Abrechnung sowie der Regelmäßigkeit der Zahlungseingänge[38]. Weiterhin ist aufgrund der dauerhaften Beziehung zu identifizierbaren Abnehmergruppen eine gute Möglichkeit zur Personalisierung des Angebots gegeben, sofern vom Anbieter neben den Stammdaten auch Profile der Abnehmer generiert und verwaltet werden. In der Personalisierung (z.B. Begrenzung des Abonnents auf bestimmte Themengebiete) besteht die eigentliche Neuerung der Übertragung des Abonnentenmodells auf digitale Produkte, da eine Personalisierung von z.B. physischen Printmedien nicht wirtschaftlich zu realisieren war.

3.2 Indirekte Erlösmodelle

In den Bereich der indirekten Erlösmodelle, bei denen die Erlöse nicht direkt aus dem Verkauf des produzierten digitalen Produkts generiert werden, fällt die Angebotsfinanzierung durch Werbung. Bei diesem Modell versucht der Anbieter seine Kosten durch Werbeeinnahmen zu decken. Hierbei steht sein Angebot auf dem Werbe- und Anzeigenmarkt in Konkurrenz zu anderen Anbietern, die ebenfalls im Wettbewerb um Werbekunden stehen.

Um die Attraktivität eines digitalen Angebots zu messen, werden neben Website-Besuchen (Hits) auch die Zahl der Kunden sowie ggf. auch deren soziodemographische Merkmale herangezogen. Am attraktivsten für einen Werbekunden ist folglich das Angebot, das ihm eine garantierte Zahl von Nutzern mit

[36] vgl. o.V. (1998)
[37] vgl. Luxem (2001), S. 81
[38] vgl. Luxem (2001), S. 82

den von ihm gewünschten Merkmalen bereitstellt. Die Erlöse können auf unterschiedliche Weise generiert werden. Zum einen kann mit den Werbekunden ein Festpreis für die Einblendung im Angebot des Anbieters ausgehandelt werden. Der Festpreis hängt, wie oben erwähnt, von der Besucherzahl und der Attraktivität der Nutzer als Zielgruppe für den Werbekunden ab. Zum anderen kann eine variable Bezahlung vereinbart werden, die z.B. sich nach der Anzahl der Besuche des Angebots des Werbekunden bemisst, die über die geschalteten Werbebanner im Angebot des Anbieters vermittelt wurden. Nachteil dieses Modells ist die Tatsache, dass man mit seinem Angebot nicht nur auf einem Rezipientenmarkt, sondern zusätzlich noch auf einem Werbe- und Anzeigenmarkt im Wettbewerb steht („doppelter Markt“)[39]. Hierzu ist zu bemerken, dass der Erfolg auf dem Rezipientenmarkt oft auch eine hohe Attraktivität auf dem Werbe- und Anzeigenmarkt nach sich zieht, da eine entsprechend große Nutzerschaft in der Regel auch eine attraktive Zielgruppe für Werbemaßnahmen des Massenmarketing darstellt.

Durch eine entsprechend große Nutzerschaft wird ein weiteres indirektes Geschäftsmodell ermöglicht, das als „Erlöse aus dem Verkauf von demographischen Daten“ beschrieben werden kann. Die Erlöse werden hierbei durch den Verkauf von anbieterseitig gesammelten demographischen Daten der Nutzer an z.B. Marktforschungsinstitute generiert. Der Anbieter tritt hier als so genannter Infomediär auf[40]. Bei dem Verkauf sind nationale juristische Beschränkungen zu beachten, so dass nicht jede Kombination von Daten rechtmäßig verkauft werden kann.

Das Content Owner Sponsoring[41] (COS) stellt ein neueres Geschäftsmodell dar. Der Besitzer bzw. Hersteller des digitalen Produkts bezahlt für die Distribution seines Produkts, um einen möglichst hohen Verbreitungsgrad zu erreichen. Dies ist immer dann sinnvoll, wenn man erwartet, dass das digitale Produkt erhebliche positive Netzeffekte auslösen kann. Beispielsweise kann ein Hersteller sein Softwareprodukt bei upload.com (vgl. http://wwww.upload.com) gegen eine Gebühr registrieren lassen.

Direkt			**Indirekt**
nutzungsabhängig	*nutzungsunabhängig*		
	einmalig	wiederholend	
• Pay-per-View • Pay-per-Use	• einmalig zu erwerbende Lizenzen	• Abonnement bzw. zeitraumbezogene Lizenzen	• Content Owner Sponsoring • Verkauf von Nutzerdaten • Werbefinanzierte Angebote

Tabelle 3-1: direkte und indirekte Erlösmodelle

Die Software steht dann auf beliebten Websites (z.B. CNET Networks' download library mit ca. 2,5 Mio. Zugriffen täglich) zum Herunterladen bereit. Diesen Weg beschritt Adobe (http://www.adobe.com) mit

[39] vgl. Schumann / Hess (2000), S. 20
[40] vgl. z.B. Rose (1999), S. 164ff.;173
[41] vgl. Clarke (1999)

dem Produkt „Adobe Acrobat Reader“, der kostenlos erhältlich ist und das Portable Document Format (PDF) zum De-facto-Standard für den Dokumentenaustausch etabliert hat. Im Zuge dessen wurde die Software „Adobe Acrobat“ zum Erstellen von PDF-Dokumenten ein kommerzieller Erfolg. Tabelle 3-1 fasst die vorgestellten Geschäftsmodelle überblicksartig zusammen.

4 Digital Rights Management

Im Rahmen der Distribution digitaler Produkte hat die Frage des Urheberechtschutzes an Bedeutung gewonnen. Insbesondere das P2P-Filesharing unterläuft diesen systematisch und hat bereits zu Einbußen in der Musikindustrie geführt. Aus diesem Grund ist diese sehr stark an funktionsfähigen DRM-Systemen (DRMS) interessiert, die es ihr erlaubt, ihre bisherigen Geschäftsmodelle auch in einer digitalen Umwelt durchzusetzen. Aber auch in Business-to-Business (B2B)- Bereichen dürften DRMS künftig stärker zum Einsatz kommen.

In diesem Abschnitt wird zunächst der Begriff „Digital Rights Management“ (kurz: DRM) erläutert. Anschließend werden Anforderungen an DRM und die aktuell eingesetzten Technologien vorgestellt.

4.1 Begriffsklärung

Die Definitionen von DRM in der Literatur stellen sich recht heterogen dar. Während ein Autor DRM als *„type of server software developed to enable secure distribution – and perhaps more importantly to disable illegal distribution – of paid content over the Web […]“*[42]

definiert, fasst GRIMM den Begriff weiter und stellen fest:

„unter DRM versteht man Verfahren, die helfen Rechte an digitalen Waren so zu schützen, wie wir das von den an physische Medien gebundenen intellektuellen Erzeugnissen her gewöhnt sind. Kopie und Weitergabe sollen an die Regeln des Rechteinhabers, also des Warenanbieters (Content Provider) gebunden sein“[43].

Diese Definition präzisierend führt IANELLA an: *„DRM covers the description, identification, trading, protecting, monitoring and tracking of all forms of usages over both tangible and intangible assets […]“*[44] oder *„Rights Management that uses digital technology and applies to intellectual property in digital form“*. In diesem Zusammenhang ist Rights Management zu verstehen als: *„business processes that for legal and commercial purposes track rights, rightsholders, licenses, sales, agents, royalties and associated terms and conditions“*[45].

Der ersten Definition ist allerdings zu bescheinigen, dass sie zu kurz greift, da sie im Gegensatz zu der von IANELLA das Umfeld, in welchem DRM eingesetzt wird, außer Acht lässt. DRM kann bzw. muss (in

[42] o.V. (2002), S. 1
[43] Grimm (2003), S. 97
[44] Ianella (2001), S. 1
[45] Rosenblatt et al. (2002), S. 4

verschiedenen Varianten) auf allen Stufen der Wertschöpfungskette, von der Produktion des digitalen Gutes bis zu dessen Bezahlung und während der anschließenden Benutzung eingesetzt werden, wie dies in der Definition von GRIMM anklingt. In anderen Worten: DRM umfasst alle Handlungen die jemand mit dem jeweiligen Inhalt im Rahmen von Distribution und Nutzung vornimmt[46]. Zu der Definition von IANELLA ist ergänzend anzumerken, dass der Rechteinhaber weitere Distributoren zwischenschalten kann, die im Rahmen der ihnen verliehenen Rechte weitere verschiedene Rechte für den Inhalt definieren können. Es ist denkbar, dass der Rechteinhaber einem Distributor die Kopie und Weitergabe für einen Inhalt überträgt, dieser jedoch in Abhängigkeit von der Kundengruppe (Geschäfts- oder Privatkunden) die ihm übertragenen Rechte weiter einschränkt. Der Warenanbieter determiniert also nicht in jedem Fall die Regeln allein.

Aus den obigen Feststellungen lassen sich generische Aufgabenbereiche für DRM ableiten. Zum einen das Verwalten von digitalen Rechten, zum anderen das Durchsetzen von Urheberrechten mit digitalen Mitteln. In den erstgenannten Aufgabenbereich fallen die Identifizierung des Inhalts (zur eindeutigen Zuordnung zu Rechteinhabern), das Sammeln von Metadaten (zum Auffinden des gewünschten Inhalts durch den Benutzer), sowie das Entwickeln von Geschäftsmodellen für den Vertrieb der Inhalte.

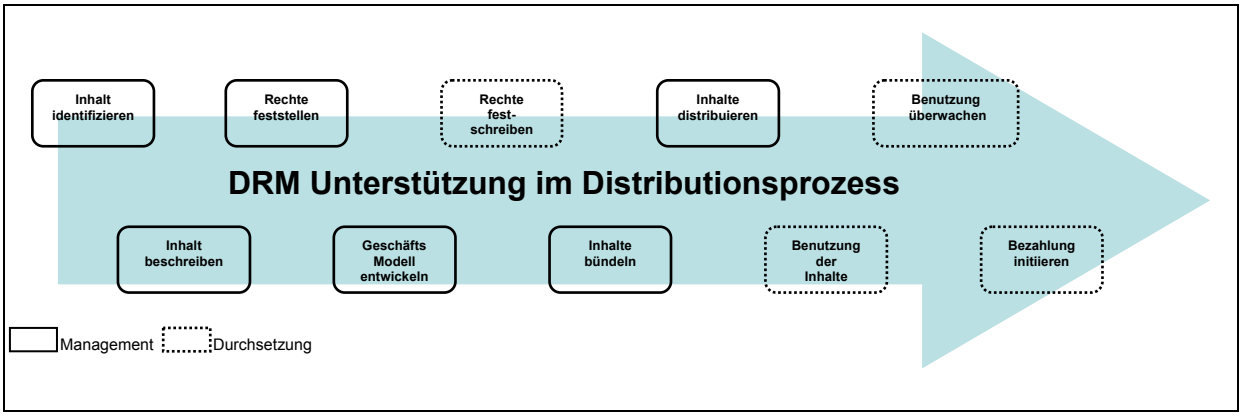

Abbildung 4-1: Schritte in der Distribution von Inhalten und DRM-Unterstützung[47]

Abbildung 4-1 zeigt die Schritte in der Distribution von digitalen Produkten, die von DRM Systemen unterstützt werden müssen und ordnet sie dem entsprechenden Aufgabenbereich zu.

In den Bereich der digitalen Durchsetzung von Urheberrechten fällt das Kontrollieren der Benutzung und Weitergabe des Inhalts durch Nutzer und Händler. Das heißt, dass ein DRM die Verwendung gemäß den Vorgaben des Rechteinhabers ermöglichen muss, andere Verwendungen und Manipulationen jedoch strikt zu verhindern hat.

[46] vgl. Rump (2003), S. 4, Rosenblatt et al. (2002), S. IX
[47] in Anlehnung an Rump (2003), S. 4

4.2 Anforderungen an DRM-Systeme (DRMS)

Aus den oben identifizierten Aufgabenbereichen lassen sich zunächst einige grundlegende[48] Anforderungen an DRMS ableiten[49].

Aus der Notwendigkeit zur begleitenden Unterstützung der gesamten Distributionskette resultiert die Forderung nach *Interoperabilität* von DRMS. Dies bedeutet, dass bestimmte Funktionen des DRMS auf den verschiedensten Plattformen, vom Multimediaserver beim Content Provider bis zum Handheld beim Endnutzer zur Verfügung stehen müssen, um eine kontrollierte Distribution zu garantieren. Weiterhin muss es für Nutzer möglich sein, den Inhalt auf verschiedenen Endgeräten zu verwenden (z.B. im Netzwerk zu Hause), ohne dass die Inhalte sofort der unkontrollierten Distribution per Internet zur Verfügung stehen. Da bisherige Geräte nur Software- und kaum bzw. keine Hardware-Unterstützung für DRM bieten, ist DRM zunächst auf den PC-Bereich beschränkt. Die Interoperabilität kann daher als derzeit nicht befriedigend gelöstes Problem angesehen werden, der Einführungsprozess der Hardware-Unterstützung steht erst am Anfang.

Weiterhin ist anzunehmen, dass DRMS - wie heutiger Kopierschutz auch - Ziel von Attacken sein wird. Da die Attackierungsmöglichkeiten sich ebenfalls über die gesamte Distributionskette erstrecken, müssen DRM besonders hohe Standards in punkto *Sicherheit* erfüllen.

Ziel dieser Attacken ist meist der unbefugte Zugriff („injection“)[50] auf den Inhalt unter Umgehung des Kopierschutzes bzw. der Zugriffsrechte. Dies ist zu verhindern, da bereits eine unerlaubte Kopie des Inhalts in einem Netzwerk ausreicht, um eine große Anzahl von Raubkopien zu ermöglichen. Dies ist unter anderem auf die einfache Reproduzierbarkeit und der nahezu kostenfreien Distribution digitaler Güter zurückzuführen (vgl. 2.1.2). Sicherheitsexperten haben daher folgende Kriterien identifiziert[51], die jedes DRMS erfüllen sollte:

1. es darf nicht auf einem globalen Geheimnis (z.B. einem allgemeingültigen Schlüssel) beruhen,
2. ein Versagen einzelner Systemteile darf nicht zur Unsicherheit des Gesamtsystems führen (d.h. kein „Single Point of Failure“) sowie
3. es besitzt die Fähigkeit, nach einem erfolgreichen Angriff die Sicherheitsmechanismen zu erneuern.

Eine weitere Anforderung an ein DRMS ist *Flexibilität.* Sie resultiert aus den verschiedensten Laufzeitumgebungen auf denen DRMS eingesetzt werden sollen. Dies wird u.a. durch immer kleiner werdende mobile Endgeräte forciert[52]. Die (im Vergleich zum PC) beschränkten Ressourcen derartiger Endgeräte sind in diesem Kontext zu berücksichtigen. Die Austauschbarkeit der Schutzmechanismen (z.B. Verschlüsselungsverfahren) ist neben dem Sicherheitsaspekt ebenfalls unter dem Gedanken der Flexibili-

[48] vgl. zu grundlegenden Anforderungen Gooch (2003), S. 5 ff.
[49] für einen umfangreichen Anforderungskatalog für Forschung und Bildung vgl. Martin et al. (2002)
[50] vgl. dazu Biddle et al. (2003), S. 352
[51] vgl. Gooch (2003), S. 21
[52] vgl. Sander (2002), S. 85

tät zu sehen. Während ältere DRMS die Lizenzen mit dem Inhalt bündelten und somit inflexibel waren, setzen neuere DRMS auf die Trennung von Lizenzen und Inhalt[53].

Bei allen Sicherheitsanforderungen ist zu bedenken, dass ein DRM nur die Akzeptanz der Nutzer findet, wenn die Sicherheitsmechanismen nicht einschränkend wirken. Das DRMS muss dem Nutzer den Umgang mit geschütztem („managed") Inhalt ebenso einfach ermöglichen, wie dies z.B. in einem ungeschützten P2P-Netzwerk der Fall ist. Diese Anforderung kann unter dem Stichwort *Nutzerfreundlichkeit* angesiedelt werden, wobei ein Zielkonflikt zwischen Sicherheit bzw. Zugriffsschutz und der Nutzerfreundlichkeit zu unterstellen ist.

4.3 Technische Grundlagen

Nachdem die Anforderungen an DRM-Systeme (DRMS) definiert wurden (vgl. 3.2) sollen nun Technologien vorgestellt werden, die die Grundlage für die noch vorzustellenden DRMS bilden. Streng genommen reichen die derzeitigen Anwendungsgebiete von DRMS von einfachen registrierungspflichtigen Angeboten (z.B. bei http://www.handelsblatt.com) über zahlungspflichtige Downloadangebote (z.B. http://www.proquest.co.uk) bis hin zu eher komplexen Print-on-Demand Angeboten. Diese Angebote beschreiben Rechte, implementieren jedoch keine Mechanismen zu ihrer Durchsetzung, sondern überlassen dies traditionellen Lizenzvereinbarungen. In diesem Abschnitt soll eine generische Architektur erörtert werden, die eine kontrollierte Distribution, d.h. die Durchsetzung von Rechten mittels Technologie ermöglichen. Die dabei eingesetzten technologischen Verfahren sind Verschlüsselungsmechanismen, digitale Wasserzeichen und Sprachen zur Modellierung von Rechten.

4.3.1 DRM Referenz Architektur

Zunächst soll eine technische DRM-Referenz-Architektur (vgl. Abb. 3-2) in ihre einzelnen Komponenten zerlegt und erörtert werden. Die identifizierbaren Komponenten sind[54]:

Inhaltsserver

Inhalte Repository

Hier werden die eigentlichen Inhalte und die sie beschreibenden Metadaten (z.B. interne Revisionsnummern o.ä.) vorgehalten. Die Inhalte können entweder schon in einem DRM-Format zur Distribution bereitstehen oder können auf Abruf in ein solches übertragen werden. Es ist hierbei denkbar, dass DRMS die simultane Unterstützung mehrerer Distributionskanäle vorsehen (z.B. Print und Internet).

[53] vgl. zu Nachteilen der Bündelung von Inhalten und Rechten Rosenblatt et al. (2002), S. 81ff.
[54] entnommen aus Rosenblatt et al. (2002), S. 80 - 83

Produktinformationen

Daten zu den einzelnen Produkten des Anbieters wie z.B. Preise, Marketingdaten, Formate, etc. sind hier abgelegt. Es bietet sich eine Integration von DRMS mit Shopsystemen an, so dass Eingaben in das Shopsystem direkt auch im DRMS verfügbar sind.

DRM Packer

Die Vorbereitung des Inhalts für die Distribution findet hier statt, d.h. er wird in ein DRMS-konformes Format übersetzt. Dies kann entweder vor Einlagerung des Inhalts in das Inhalte Repository stattfinden oder bei Abruf des Inhalts („on the fly"). Zusätzlich zum eigentlichen Inhalt enthält das fertige Paket noch DRMS bezogene Metadaten. Dazu gehören z.B. eine eindeutige Paketnummer zur Identifikation, Informationen zum Auffinden des Inhalts sowie die Spezifikation zum Umgang mit dem Inhalt. Eine zweite wichtige Aufgabe des DRM Packers ist also die Definition von Rechten, die der Anbieter dem Nutzer einräumen will.

Lizenzserver

Die Informationen über den Nutzer oder das Endgerät, welches den Inhalt benutzen möchte, die Identifikationsdaten des Inhalts sowie die dazugehörigen Rechte und deren Spezifikationen werden in Lizenzen festgehalten. Die Lizenzen werden vom DRM Packer erstellt und an den Lizenzserver weitergegeben. Gleichzeitig wird ein Schlüsselpaar generiert, das der späteren Identifikation von Nutzern sowie der Entschlüsselung von Inhalten dient. Beides wird separat gespeichert und ist über die oben genannten Identifikationsdaten eindeutig Inhalten zugeordnet. Weiterhin werden sog. Identitäten vorgehalten. Dies sind Daten über Nutzer, die gerade Rechte auf bestimmten Inhalten ausüben (z.B. ein Musikstück anhören oder einen Film anschauen). Aus diesen Daten werden dann die einzelnen Lizenzen generiert und an die jeweiligen Nutzer versandt.

DRM Client

Die Komponenten des DRM auf Nutzerseite sind der Controller, die Applikation zur Nutzung (Wiedergabe) des Inhalts und der Identifikationsmechanismus.

Die Controller-Komponente kann als eigenständige Software, innerhalb einer Applikation oder als Hardware realisiert werden. Ihre Aufgaben umfassen:

- Empfangen und Weiterleiten von Benutzeranforderungen
- Identitätsinformationen über den Nutzer sammeln und eine entsprechende Lizenz vom Lizenzserver holen
- Authentifikation der Wiedergabeapplikation auf Nutzerseite
- Management der Verschlüsselungsmechanismen, insbesondere Entschlüsselung des Inhalts

Die Wiedergabeapplikationen können grob in zwei Klassen unterteilt werden: die speziell für DRM geschriebenen Applikationen und die Applikationen, die das DRM zunächst modifizieren muss, um die Durchsetzung der Rechte zu garantieren. Erstgenannte haben den Vorteil dass sie mittels spezifischer Befehle relativ leicht „sicher" zu gestalten sind. Dem stehen jedoch zwei gewichtige Nachteile gegen-

über. Erstens muss die Applikation an die Nutzer distribuiert werden, zweitens ist eine Lernphase nötig, bevor die Nutzer die Applikation bedienen können. Zu letzteren zählen vor allem Plug-Ins, die für eine Reihe von Standardsoftware erhältlich sind. Mit ihrer Hilfe können aus DRM-Sicht unerwünschte Funktionen zur Modifikation bzw. Weiterverwendung des Inhalts (z.B. Drucken) unterdrückt werden. Der Vorteil dieses Ansatzes liegt vor allem darin, dass der Nutzer die gewohnte Applikation weiterbenutzen kann und damit sowohl die Distribution der kompletten Applikation, da nur das vergleichsweise kleine Plug-in distribuiert werden muss, als auch die Lernphase entfallen. Nachteilig ist zu bemerken, dass ein Plug-in nicht so sicher gestaltet werden kann wie eine speziell für DRM programmierte Applikation[55].

Die Identifikationskomponente identifiziert Geräte z.B. anhand einer vom DRM auslesbaren eindeutigen Seriennummer, die Hardwarehersteller in ihre Geräte einstellen[56]. Ein anderer Weg ist das generieren einer eindeutigen GeräteID aus den einzelnen Hardwarekomponenten des Endgeräts[57]. Eine Identifikation von Endgeräten anhand ihrer IP-Adresse kann in Zeiten dynamischer Adresszuweisungen durch die Internet Service Provider (ISP) vernachlässigt werden.

Ein idealtypischer Ablauf zum Abspielen einer Audio-/Videodatei kann wie folgt beschrieben werden:

(1) Der Nutzer erhält (z.B. per Download) den von ihm gewünschten Inhalt in einem verschlüsselten Container.

(2) Um den Inhalt benutzen zu können, wird eine Anfrage an den Lizenz Server gestellt, mit der Bitte bestimmte Rechte auf dem Inhalt ausüben zu dürfen. Diese Anfrage wird vom DRM Controller, unter Verwendung der Identiätsdaten sowie des Inhalts, generiert.

(3) Der DRM Controller kontaktiert den Lizenzserver und sendet die Anfrage.

(4) Der Lizenz Server überprüft den Nutzer anhand der gespeicherten Daten. Weiterhin werden die Rechte, die der Nutzer ausüben darf, anhand der Identifikationsdaten des Inhalts überprüft.

(5) Wenn nötig, wird eine finanzielle Transaktion veranlasst.

(6) Der Lizenzgenerator benutzt die gesammelten Identitätsdaten, Rechteinformationen und die Verschlüsselungsmechanismen, um eine Lizenz für den Nutzer zu generieren. Diese Lizenz ist verschlüsselt, um Missbrauch auszuschließen.

(7) Die Lizenz wird an den Client gesendet, auf dem weitere Authentifizierungsschritte ausgeführt werden (z.B. eine Überprüfung der Wiedergabeapplikation).

(8) Wenn die Authentifizierung abgeschlossen ist, kann der DRM Controller die Lizenz entschlüsseln. Mit den in der Lizenz enthaltenen Schlüsseln wird der Container mit dem Inhalt geöffnet.

(9) Der Inhalt wird von dem DRM Controller an die Wiedergabeapplikation übergeben und dort abgespielt.

[55] vgl. Rosenblatt et al. (2002), S. 85
[56] vgl. exemplarisch Fischer et al. (1999)
[57] vgl. dazu das Konzept der “Next Generation Secure Computing Base“ (NGSCB) von Microsoft (http://www.microsoft.com/resources/ngscb/default.mspx)

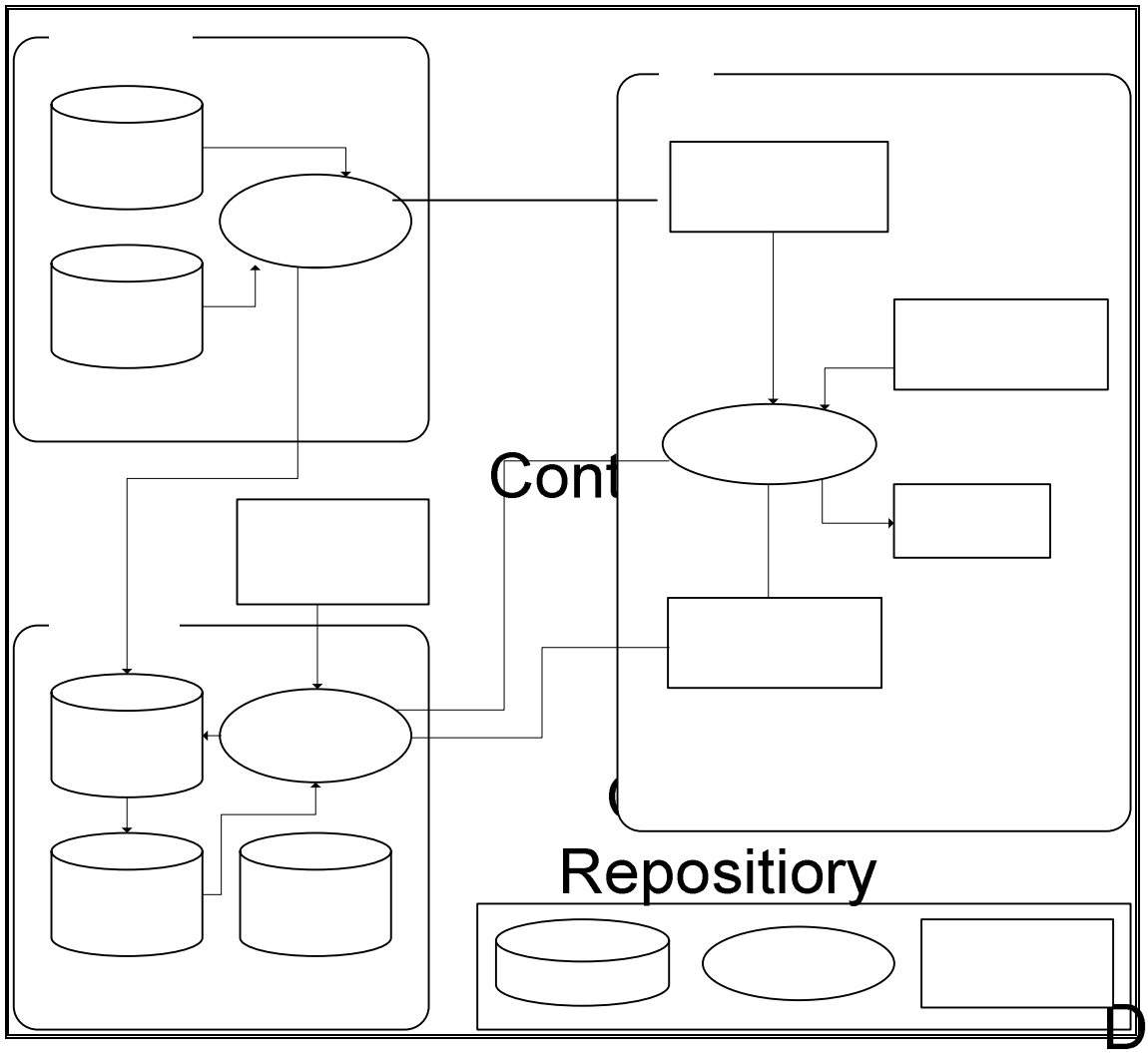

Abbildung 4-2: DRM Referenzarchitektur

4.3.2 Sprachen zur Modellierung von Rechten

Produkt
Informationen

Um eine kontrollierte Distribution digitaler Inhalte zu gewährleisten, ist es notwendig die Nutzungsrechte an digitalen Gütern informationstechnisch zu erfassen. Dies erfolgt mit Hilfe einer Rights Expression Language (REL), die vom DRM interpretierbar ist. Die z. Zt. bedeutsamsten REL sind die MPEG-21 REL sowie die Open Digital Rights Language (ODRL), die beide auf der Extensible Markup Language (XML) basieren.

MPEG-21 REL

Die MPEG-21 REL besteht aus den Modulen REL Core, REL Standard Extension und REL Content Extension. Das REL Core Modul stellt die grundlegenden Elemente für die Funktionalität der Sprache bereit, während die Standard Extension nützliche Erweiterungen bietet. Die REL Content Extension stellt die Multimediafähigkeit sicher.

Rechte werden mit Hilfe des Lizenzkonzepts abgebildet. Eine Lizenz kann als Container verstanden werden, der Berechtigungen, die ein Lizenznehmer von einem Lizenzgeber erhält, bündelt. Diese er-

finanzie
Transakt

mächtigen den Lizenznehmer bestimmte Rechte auf einem Produkt auszuüben, wenn die vorher definierten Bedingungen erfüllt sind. Einfache Bedingungen können Zeiträume oder Häufigkeit der Benutzung sein. MPEG-21 stellt ebenfalls Mechanismen zur eindeutigen Identifizierung von Berechtigten, d.h. Endnutzer oder Endgeräte bereit. Des Weiteren werden Zahlungsabwicklung, Verschlüsselung von Inhalten und digitale Signaturen unterstützt.

Open Digital Rights Language

ODRL modelliert Rechte mit Hilfe der Elemente Werk (Asset), Recht (Right) und Beteiligter (Party). Die Werke umfassen physische und digitale Inhalte. Rechte setzen sich aus Nutzungsrechten, Beschränkungen, Anforderungen sowie Bedingungen zusammen. Der Rechtebegriff bezieht sich im Gegensatz zur MPEG-21 REL nicht nur auf Nutzungsrechte, die für einen bestimmten Inhalt freigegeben wurden, sondern ist weiter gefasst. Unter Beteiligten versteht man Rechteinhaber und Konsumenten. Durch diese Elemente können Angebote, Übereinkünfte und Widerrufe abgebildet werden. Angebote werden den Konsumenten von Rechteinhabern unterbreitet und sind an bestimmte Werke gebunden. Sind die Beteiligten sich handelseinig, entsteht eine Übereinkunft, die der Lizenz in MPEG-21 ähnelt. Widerrufe können sich sowohl auf Angebote als auch auf Übereinkünfte beziehen. Da die Reihenfolge der Interaktionen beliebig ist, können mit ihrer Hilfe viele Geschäftsmodelle abgebildet werden. ODRL unterstützt einen einfachen Verschlüsselungsmechanismus zum Schutz von Werken und Rechtedefinitionen.

4.3.3 Mechanismen zum Schutz von digitalen Produkten

Um die modellierten Rechte wirksam durchsetzen zu können, bedarf es Schutzmechanismen. Nachfolgend werden die allgemein die Verschlüsselung sowie digitale Wasserzeichen vorgestellt.

Verschlüsselung

Wie bereits erwähnt, treffen die digitale Musik und die Lizenz in verschlüsselter Form beim Nutzer ein. Eine Verschlüsselung der digitalen Musik ist eine Voraussetzung für den Einsatz von DRMS, da ansonsten ungehindert eine direkte Wiedergabe mittels eines Hard- oder Softwaregerätes unter Umgehung des DRMS stattfinden kann.

Die Verschlüsselung kapselt die digitale Musik in ein Behältnis, sog. „Secure Container“, zu dem nur ein geheimer Schlüssel Zugang gewährt[58]. Dieser Schlüssel ist als Inhaltsschlüssel zu bezeichnen und üblicherweise selbst in verschlüsselter Form in der Lizenz enthalten. Aufgrund der Laufzeiteigenschaften ist der Inhaltsschlüssel symmetrisch. Gebräuchlich sind Blockverschlüsselungsverfahren wie Triple-DES. Somit ergibt sich vorliegend ein hybrides System. Es sind auch rein symmetrische Kryptosysteme für DRMS denkbar, besonders in individualisierten Geschäftsmodellen bieten hybride Systeme aber Vorteile[59]. Der Inhaltsschlüssel in der Lizenz muss zwingend selbst verschlüsselt sein. Für die Rechte in der Lizenz ist dies jedoch nicht erforderlich, hier genügt eine digitale Signatur, um Manipulationen

[58] vgl. Günnewig / Hauser (2002), S. 182, Spenger (2003), S. 79
[59] vgl. Spenger (2003), S. 78

auszuschließen. Manipulationen an der verschlüsselten Musikdatei sind durch Einweg-Hashfunktionen aufzudecken. ODRL benutzt einen durch den SHA-1-Algorithmus ermittelten „Digest Value“[60].

Die vorliegend eingesetzten Algorithmen sind bewährt und stellen in Kombination mit einer auf den Verwendungszweck abgestimmten Schlüssellänge hinreichend sichere Verfahren dar[61]. Werden andere bekannte und öffentlich verifizierte Algorithmen, wie z.B. AES oder IDEA, für die aktuell keine Kryptoanalyseverfahren bekannt sind, korrekt implementiert, so bieten diese ebenfalls ein akzeptables Sicherheitsniveau. Wird das gesamte Verschüsselungsverfahren vom Hersteller geheim gehalten und nicht nur der jeweilige Schlüssel, sog. Blackbox-Verfahren, kann dessen Qualität ohnehin nicht überprüft werden. Im diesem Zusammenhang ergibt sich eine besondere Problematik, da die Wirksamkeit einer technischen Schutzmaßnahme, zu denen die Verschlüsselung zu zählen ist, nach geltendem Recht (§§95a, 108b Abs.1 UrhG) objektiv zu bewerten ist. Der Rückgriff auf eine unabhängige Public-Key-Infrastruktur[62] erscheint aus denselben Gründen notwendig. Die Anwendung von Verschlüsselung in DRMS verfolgt konkurrierende Ziele. Dem Nutzer soll der Zugriff auf Daten erlaubt und verboten werden. In der Theorie lässt sich die Zielkonkurrenz durch die jeweils nur zeitweilige Erteilung von Zugriffserlaubnissen bzw. –verboten auflösen, in der Praxis gibt es konkrete Umsetzungsprobleme, die technisch nur schwer zu lösen sind. Das Hauptproblem liegt in der Schlüsselverwaltung und nicht in den verwendeten Algorithmen. Im konkreten Beispiel des von ODRL verwendeten „Encrypted Key“ bedeutet dies, dass „Encrypted Key“ rekursiv auf einen weiteren „Encrypted Key“ verweisen kann. Die Rekursion ist jedoch endlich. Also muss ein Schlüssel existieren, mit dem „Encrypted Key“ entschlüsselt wird, ein sog. „key-encryption-Schlüssel“[63]. Dieser Schlüssel kann grundsätzlich beim Musikanbieter oder in der Nutzersphäre aufbewahrt werden. Eine Aufbewahrung beim Anbieter ist auszuschließen, da eine sichere, abgeschirmte Online-Verbindung zu diesem aufgebaut werden müsste, was z.B. bei tragbaren MP3-Playern nicht möglich ist.

Verbleibt die Möglichkeit der Verwahrung in der Nutzersphäre, d.h. in seinem Wiedergabegerät, im DRMS Controller oder in anderer Soft- oder Hardware. Die Wahl des Verwahrungsortes muss verschiedene Aspekte berücksichtigen. Aus Sicherheitsgründen sollten Schlüssel häufiger ausgetauscht werden können, um das Risiko der Kompromittierung zu minimieren[64]. Eine Unterbringung in Software verursacht geringe Kosten, in Hardware entstehen hingegen hohe Kosten[65]. Es ist möglich, Aufspaltungsverfahren für Schlüssel zu verwenden, bei denen Schlüssel in verschiedene Teile zerlegt werden um sie dann auf Hard- und Software aufzuteilen. Damit lassen sich sowohl die Kosten für den Austausch senken als auch die Sicherheit reiner Hard- oder Softwarelösungen erhöhen[66].

Ein weiteres Problem besteht in der Anwendung der Verschlüsselung auf langfristig gespeicherte Daten. Wird ein „key-encryption-Schlüssel“ kompromittiert, muss er ausgetauscht werden. Alle betroffenen Lizenzen müssen erneut ausgestellt, alle Audiodaten müssen vernichtet, erneut übertragen und ge-

[60] vgl. Ianella (2002), S. 24
[61] vgl.Schneier (1996), S. 507
[62] Guth (2003), S. 153
[63] vgl. Schneier (1996), S. 208
[64] vgl. Schneier (1996), S. 216f.
[65] vgl. Feigenbaum (2003), S. 16
[66] vgl. Schneier (1996), S. 213

speichert werden. Deshalb muss die Schlüsselverwahrung auch über lange Zeit sehr sicher sein, ein vollständiger Schlüsselaustausch muss aus praktischen Gründen ausgeschlossen werden. Waren die Daten einmal, wenn auch nur kurzzeitig, unverschlüsselt verfügbar, ergeben sich für die Zukunft Möglichkeiten für „known-plaintext-Angriffe“[67]. Bei einem hohen Sicherheitsniveau muss die Entschlüsselung der digitalen Musik den Laufzeitanforderungen der konkreten Anwendung genügen, besonders darf sie eine qualitativ hochwertige Wiedergabe nicht beeinträchtigen.

Digitale Wasserzeichen

Digitale Wasserzeichen stellen einen speziellen Schutz in DRMS dar. Sie wirken unabhängig von den vorgenannten allgemeinen Schutzmechanismen[68] und haben ihren Ursprung in der Steganographie[69]. Ihr Einsatz ist deshalb notwendig, weil jedes Audiosignal letztlich die geschützte Sphäre des DRMS verlassen muss, damit der Nutzer es hört. „Ein nicht wahrnehmbares Wasserzeichen stellt ein transparentes, nichtwahrnehmbares Muster dar, welches in das Datenmaterial eingebracht wird. Dieses Muster wird dazu benutzt, entweder das Vorhandensein einer Kennzeichnung anzuzeigen oder Informationen zu codieren. Das Wasserzeichenverfahren nutzt geheime Informationen, wie zum Beispiel Schlüssel, und besteht aus einem Einbettungsprozess (Einbettungs- oder auch Markierungsalgorithmus) und einem Abfrageprozess (Abfragealgorithmus, Auslesen der Markierung). Das Wasserzeichenmuster ist meist ein Pseudorauschmuster und codiert die Wasserzeicheninformation“[70]. Während digitale Wasserzeichen im visuellen Bereich schon seit Beginn der neunziger Jahre Gegenstand zahlreicher Publikationen sind, wurden bisher in Bezug auf Audiodaten vergleichsweise wenige Verfahren veröffentlicht. Für digitale Wasserzeichen existieren zahlreiche Anwendungsmöglichkeiten. Im Kontext von Audiodaten können folgende Einsatzmöglichkeiten identifiziert werden:

(1) Die Überwachung von Radiostationen, bei der dem Abstrahlsignal Informationen hinzugefügt werden.

(2) Die Gewährleistung von Authentizität und Integrität der Audiodaten, wobei sog. fragile Wasserzeichen zum Einsatz kommen[71]. Etwaige Veränderungen am Wasserzeichen deuten auf Manipulationsversuche an den Daten hin.

(3) Die Zugriffskontrolle auf Audiodaten, die den Abspiel- bzw. Kopiervorgang in einem Hard- oder Softwaregerät nur dann zulässt, wenn ein authentisches Wasserzeichen existiert und der Nutzer dazu berechtigt ist.

(4) Die Überwachung und Rückverfolgung von Urheberrechtsverletzungen, wobei Audiodaten, die außerhalb der gültigen Distributionspfade entdeckt werden, in Wasserzeichen Informationen über den Urheber enthalten. Im Falle von Transaktionswasserzeichen ist hierin auch die Quelle der illegalen Kopien codiert.

---

[67] Schneier (1996), S. 260
[68] vgl. Fraunhofer (2002), S. 1
[69] vgl. Dittmann (2000), S. 16
[70] vgl. Fränkl / Karpf (2004), S. 20
[71] vgl. Bechtold (2002), S. 79

Die erste Anwendung ist in der Praxis verbreitet, aber hier nicht relevant. Für DRMS kommen die Anwendungen (2) bis (4) infrage. Informationen über die Lizenz sind durch Wasserzeichen in die Audiodaten eingebettet und somit fest mit den Audiodaten verbunden. Das DRMS erlaubt eine Nutzung nur bei unversehrtem Wasserzeichen unter den in der Lizenz festgelegten Bedingungen. Gelangen Audiodaten aus der Sphäre des DRMS, können der Urheber und letzte Lizenzinhaber dennoch eindeutig identifiziert werden. Auf digitale Fingerabdrücke wird hier nicht eingegangen.

Grundlegende Anforderungen an Audio-Wasserzeichen sind[72]: die Robustheit, die Unhörbarkeit, die Komplexität und die Kapazität. Demnach bedeutet Robustheit, dass die eingebrachte Information „zuverlässig aus dem Datenmaterial ausgelesen werden kann, auch wenn das Datenmaterial modifiziert (aber nicht vollständig zerstört) wurde“[73]. Beispiele für konkrete Modifikationen sind: Kompression und Quantisierung, Einbringen von Rauschen, Filtern, Samplepermutationen, Time-Stretching, Skalierung, nichtlineare Transformationen, Entfernen oder Einfügen einzelner Samples, Umwandlung in ein analoges Signal und Rückwandlung in ein digitales Signal, Verzerrung, Einbringen von Echoeffekten oder eine Veränderung der Frequenzanteile[74]. Die Unhörbarkeit ist gegeben, „wenn ein durchschnittliches […] Hörvermögen nicht zwischen markiertem Datenmaterial und Original unterscheiden kann“. „Komplexität: Beschreibt den Aufwand, der erbracht werden muß, die Wasserzeicheninformationen einzubringen und wieder auszulesen“[75]. Die Kapazität gibt an, „wieviel Informationen in das Original eingebracht werden können und wieviel Wasserzeichen parallel im Datenmaterial zugelassen bzw. möglich sind“[76]. Die Anforderungen stehen teilweise in einem konkurrierenden Verhältnis zueinander. Die Kapazität hängt von der Audiocharakteristik ab und geht zulasten der Unhörbarkeit und der Robustheit. Weiterhin kann die Komplexität in Konkurrenz zu den Laufzeitanforderungen der konkreten Einbettungsanwendung oder zum Abfrageprozess stehen[77]. Für die Verwendung in DRMS kann zusätzlich gefordert werden, dass eine Erkennung, Entfernung oder Fälschung von Wasserzeichen durch etwaige Angreifer nicht möglich ist und dass eine unparteiische Überwachung stattfindet[78].

4.4 Überblick über aktuelle DRM Systeme

Die Software iTunes 4 dient seit April 2003 für Apple- und seit Oktober für Windows-Nutzer als Client für den Apple Music Store und ermöglicht Musik auf das mobile Endgerät iPod zu übertragen. Geschützte Dateien vom Apple Music Store gelangen in MPEG-4-Containern zum Konsumenten. Das Format MPEG-4 ermöglicht über Erweiterungen ein DRM. Die Lizenzvergabe erfolgt über den Music Store. Zwar ist ein Abspielen geschützter Dateien nur durch iTunes bzw. QuickTime möglich, doch es können bis zu drei verschiedene Computer gleichzeitig dazu autorisiert werden, erworbene Dateien zu spielen. Brennvorgänge sind mit unverändertem Inhalt nur je zehnmal gestattet. Der Schutz der digita-

[72] vgl. Dittmann (2000), S. 25ff.
[73] Dittmann (2000), S. 25
[74] vgl. Dittmann (2000), S. 89
[75] Dittmann (2000), S. 26
[76] Dittmann (2000), S. 27
[77] vgl. Petitcolas (2003), S. 7
[78] vgl. Petitcolas (2003), S. 7 Dittmann (2000), S. 26ff., Cox et al. (2002), S. 31ff.

len Musikdateien geht dabei aber verloren, so dass eine anschließende Umwandlung in ein ungeschütztes Format möglich ist. Eine direkte Umwandlung geschützter Dateien in MP3 innerhalb von iTunes ist dagegen nicht möglich.

Ein bereits in der Musikindustrie eingesetztes System stellt IBM's Electronic Media Management System (EMMS) dar, welches weitgehend auf offenen Standards (z.B. Java und XML) aufbaut.

Helix DRM von Real Networks soll so ausgelegt sein, dass es jedes andere Medien-Format unterstützen kann. Dadurch ist es nicht mehr notwendig, für jedes Format einen Player mit properitärem DRM auf den Endgeräten zu installieren. Helix DRM bietet dazu zwei Varianten an, eine native Unterstützung als auch die Möglichkeit, Daten in einen sicheren Speicher zu transferieren. Geräte mit direkter Unterstützung können dann Inhalte direkt von Helix-DRM-Lizenz-Servern beziehen, der beispielsweise von Internet Service Providern (ISP) oder Musikanbietern betrieben wird.

Ein ähnliches Konzept verfolgen Philips und Sony, die von Intertrust ein DRMS entwickeln lassen, das ebenfalls endgeräteunabhängig arbeitet. Die Vorstellung des ersten Prototyps wird für Mitte dieses Jahres erwartet.

5 Zusammenfassung

Die Distribution digitaler Produkte nimmt stetig zu. Die technischen Möglichkeiten zu deren Distribution können grundsätzlich in zentralisierte und dezentralisierte Technologien unterteilt werden. Im Zusammenhang mit zentralisierten Technologien ist Streaming Media zu nennen, welches hauptsächlich zum Vertrieb von „Rich Media" Anwendungen (z.B. Videodaten) eingesetzt wird. Es ist anzunehmen, dass diese Technologie im kommerziellen Bereich weiterhin (z.B. im Marketingbereich durch Streaming-Werbung) an Bedeutung zunehmen wird. Im Gegensatz dazu sind dezentralisierte Peer-to-Peer-Systeme derzeit hauptsächlich in illegalen Tauschbörsen im Einsatz. Beide Distributionstechnologien können kombiniert werden doch derartige Systeme sind meistens noch im Prototypenstadium.

Traditionelle Erlösmodelle des Handels mit digitalen Produkten wie Abonnements, Lizenzmodelle und Erlöse durch Werbung scheinen bedroht bzw. können in den derzeitigen Absatzkanälen wegen mangelnder Kontrolle nicht durchgesetzt werden. Zu diesem Zweck werden Digital Rights Management Systeme (DRMS) entwickelt, die digitale Inhalte vor unerlaubter Nutzung, Manipulation und Weiterverbreitung schützen sollen. Deren Ziel ist die Wahrung des Urheberrechts durch kontrollierbare Absatzkanäle.

Die technologischen Grundlagen dieser Systeme sind Verschlüsselungsmechanismen und digitale Wasserzeichen, mit deren Hilfe der Inhalt sowie die vom Rechteinhaber mittels REL definierten Rechte, geschützt werden können. Das größte Problem von DRMS ist in erster Linie die Einschränkung der Verwendungsmöglichkeiten des Inhalts und damit eine geringere Nutzerfreundlichkeit.

Weitere Forschungsvorhaben sollten das Ziel haben, neue Geschäftsmodelle zu entwickeln, die eine kommerzielle Distribution über zentrale, im Kontext illegaler P2P Tauschbörsen, vor allem aber über dezentralen Technologien ermöglichen. Diese Geschäftsmodelle können DRM integrieren, jedoch

scheint dies nicht in allen Bereichen zwingend notwendig da mit DRM immer auch eine Nutzungseinschränkung einhergeht. Bei zu starker Einschränkung können anreizkompatible Erlösmodelle einen höheren Erfolg versprechen.

Literaturverzeichnis

Barkai (2002): Barkai, D.: Peer-to-peer computing: technologies for sharing and collaborating on the net, Hilsboro, Or., 2002.

Bechtold (2002): Bechtold, S.: Vom Urheber- zum Informationsrecht: Implikationen des Digital Rights Management, München, 2002.

Biddle et. al. (2003): Biddle, P., England, P., Peinado, M., Willman, B.: Darknet and the Future of Content Protection, in: E. Becker (Hrsg.): Digital Rights Management Technological, Economic, Legal and Political Aspects, Berlin [u.a.], 2003, S. 344 – 365.

Brandtweiner (2000): Brandtweiner, R.: Differenzierung und elektronischer Vertrieb digitaler Informationsgüter, Düsseldorf, 2000.

Clarke (1999): Clarke, R.: Electronic Services Delivery: From Broschure-Ware to Entry Points, http://www.anu.edu.au/people/Roger.Clarke/EC/ESD.html, 1999, Abruf am: 2004-03-16.

Coulouris (2002): Coulouris, G., Dollimore, J., Kindberg, T.: Verteilte Systeme: Konzepte und Design, München, 2002.

Cox et. al. (2002): Cox, I.J., Miller, M.L., Bloom, J.A.: Digital watermarking, San Francisco, Calif. [u.a.], 2002.

Dittmann (2000): Dittmann, J.: Digitale Wasserzeichen: Grundlagen, Verfahren, Anwendungsgebiete, Berlin [u.a.], 2000.

Dyson (1995): Dyson, E.: Intellectual Value, http://www.wired.com/wired/archive/3.07/dyson.html, 1995.

Feigenbaum (2003): Feigenbaum, J.: Digital Rights Management: ACM CCS-9 workshop, DRM 2002, Washington, DC, USA, November 18, 2002, Berlin [u.a.], 2003.

Fischer et. al. (1999) Fischer, S., Mi, J., Teng, A.: Pentium® III Processor Serial Number Feature Applications, http://www.intel.com/technology/itj/q21999/pdf/serial_number.pdf, 1999, Abruf am: 2004-03-16.

Fränkl/Karpf (2004): Fränkl, G., Karpf, P.: Digital Rights Management Systeme - Einführung, Technologien, Recht, Ökonomie und Marktanalyse, München, 2004.

Fraunhofer (2002): Fraunhofer Institut Integrierte Schaltungen: Audio Watermarking, http://www.iis.fraunhofer.de/amm/download/watermark.pdf, 2002, Abruf am: 2004-03-16.

Gehrke et. al. (2003): Gehrke, N., Burghardt, M., Schumann, M.: Divide et impera - ein Peer-to-Peer basiertes Geschäftsmodell für Streaming Media, in: Wirtschaftsinformatik 2003, (2003), S.467-490.

Gooch (2003): Gooch, R.: Requirements for DRM Systems, http://www.springerlink.com/media/m37uj6789cnqxha124e7/Contributions/A/9/3/7/A937V9P96C9FRM7R.pdf, 2003, Abruf am: 2004-03-16.

Grimm (2003): Grimm, R.: Digital Rights Management: Technisch-organisatorische Lösungsansätze, in: A. Picot (Hrsg.): Digital Rights Management, Berlin [u.a.], 2003, S. 93-107.

Günnewig/Hauser (2002): Günnewig, D., Hauser, T.: Musik im Hochsicherheitstrakt - Digital Rights Management - Stand der Dinge,in: C'T, (2002), S.182 - 185.

Guth (2003): Guth, S.: A Sample DRM System, in: Becker, E., Buhse, W., Günnewig, D., Rump, N. (Hrsg.): Digital Rights Management - Technological, Economic, Legal and Political Aspects, Berlin [u.a.], 2003, S. 150 -160.

Ianella (2001): Ianella, R.: Digital Rights Management (DRM) Architectures, http://www.dlib.org/dlib/june01/iannella/06iannella.html, 2001, Abruf am: 2004-03-16.

Ianella (2002): Ianella, R.: Open Digital Rights Language (ORDL) Version 1.1 - Specification, http://ordl.net/1.1./ORDL-11.pdf, 2002, Abruf am: 2004-03-16.

Ifpi (2004): ifpi: Bundesverband der phonographischen Wirtschaft e.V., http://www.ifpi.de/, 2004.

Kortmann (2002): Kortmann, W.: Mikroökonomik: anwendungsbezogene Grundlagen, Heidelberg, 2002, Abruf am: 2004-03-16.

Kuhlen (2003): Kuhlen, R.: Medienprodukte im Netz – Zwischen Kommerzialisierung und freiem Zugang, in: Picot, A. (Hrsg.): Digital Rights Management, Berlin [u.a.], 2003, S. 107 - 132

Lainee et. al. (2002): Lainee, F., de Boeck, P., Wilshire, M.: Internet Protocol Services: Vom Backbone zur Peripherie, http://www.digitaltransformation.de/pdf/2838988_digital_transformation_mdul5_isp.pdf, 2002, Abruf am: 2004-03-16.

Löbbecke (1999): Löbbecke, C.: Electronic Trading in On-line Delivered Content, http://www.mm.uni-koeln.de/loebbecke_pdf/Conf-036-1999-Electronic%20trading%20in%20On-Line.pdf, 1999, Abruf am: 2004-03-16.

Luxem (2001) Luxem, R.: Digital Commerce: Electronic Commerce mit digitalen Produkten, Lohmar [u.a.], 2001.

Martin et. al. (2002): Martin, M., Agnew, G., Boyle, J., McNair, J., Page, M., Rhodes, W.: DRM Requirements for Research and Education Discussion Paper, 2002.

Miller (2001): Miller, M.: Discovering P2P, San Francisco, 2001.

o.V. (1998): o.V.: A Piece of the Tick - Supporting the Commercial Redistribution of Electronic Information through Value Chains, http://www.intertrust.com/media/pdf/tick.pdf, 1998, Abruf am: 2004-03-16.

o.V. (2002): o.V.: Digital Rights Management, http://searchcio.techtarget.com/sDefinition/0,,sid19_ gci493373,00.html, 2002, Abruf am: 2004-03-16.

Padmanabhan (2002): Padmanabhan, P., Venkata, N., Wang, H.J., Chou, P.A.: Distributing Streaming Media Content Using Cooperative Networking, http://www.research.microsoft.com/~padmanab/papers/msr-tr-2002-37.pdf, 2002, Abruf am: 2004-03-16.

Petitcolas (2002): Petitcolas, F.A.P.: Digital watermarking: first international workshop, Seoul, Korea, November 21 - 22, 2002, Berlin [u.a.], 2003.

Ripeanu (2003): Ripeanu, A., Foster, I., Iamnitichi, A..: Mapping the Gnutella Network: Properties of Large-Scale Peer-to-Peer Systems and Implications for System Design, http://people.cs.uchicago.edu/~matei/PAPERS/ic.pdf, 2003, Abruf am: 2004-03-16.

Rose (1999): Rose, F.: The economics, concept, and design of information intermediaries: a theoretic approach, Heidelberg [u.a.], 1999.

Rosenblatt et. al. (2002): Rosenblatt, W., Trippe, W., Mooney, S.: Digital rights management: business and technology, New York, NA [u.a.], 2002.

RSVP (2004): RSVP Protocol Overview, http://www.isi.edu/div7/rsvp/overview.html, 2004, Abruf am: 2004-03-16.

RTP (2003): About RTP and the Audio-Video Transport Working Group, http://www.cs.columbia.edu/~hgs/rtp/, 2003, Abruf am: 2004-03-16.

RTSP (2004): Real Time Streaming Protocol (RTSP) Information and Updates, http://www.rtsp.org/, 2004, Abruf am: 2004-03-16.

Rump (2003): Rump, N.: Digital Rights Management Technological Aspects, in: Becker, E., Buhse, W., Günnewig, D., Rump, N. (Hrsg.): Digital Rights Management Technological Economical Legal and Political Aspects, Berlin [u.a.], 2003, S. 3 – 16.

Sander (2002): Sander, T.: Security and privacy in digital rights management: revised papers, Berlin [u.a.], 2002.

Schneier (1996): Schneier, B.: Angewandte Kryptographie: Protokolle, Algorithmen und Sourcecode in, Bonn [u.a.], 1996.

Schulzrinne et. al. (1996): Schulzrinne, H., Casner.., Frederick.., Jacobson..: RTP: A Transport Protocol for Real-Time Applications, http://www.ietf.org/rfc/rfc1889.txt?number=1889, 1996, Abruf am: 2004-03-16.

Schumann/Hess (2000): Schumann, M., Hess, T.: Grundfragen der Medienwirtschaft, Berlin [u.a.], 2000.

Spenger (2003): Spenger, G.: Authentication, Identification Techniques, and Secure Containers - Baseline Technologies, in: Becker, E., Buhse, W., Günnewig, D., Rump, N. (Hrsg.): Digital Rights Management: Technological, Economic, Legal and Political Aspects, Berlin [u.a.] 2003 S. 62 - 80.2003, 62 - 80.

Stähler (2001): Stähler, P.: Geschäftsmodelle in der digitalen Ökonomie: Merkmale, Strategien und Auswirkungen, Lohmar [u.a.], 2001.

Stoica et. al. (2002): Stoica, I.,Morris, R.,Liben-Novell, D., Karger, D., Kaashoek, F., Dabek, F., Balakrishnan, H.: Chord: A scalable Peer-to-Peer Lookup Protocol for Internet Applications, http://www.pdos.lcs.mit.edu/papers/chord:sigcomm01/chord_sigcomm.pdf, 2002.

Varian (1998): Varian, H.R.: Markets for Information Goods, http://www.sims.berkeley.edu/ ~hal/papers/japan/japan.pdf, 1998, Abruf am: 2004-03-16.

Wegner et. al. (2000): Wegner, R., Bachmeier, C.: Streaming Media im Business-Bereich: Echtzeitverfahren für das WWW, Boston, 2000.