Systeme für das Management digitaler Rechte

Die Autoren

Thomas Hess
Vural Ünlü

Prof. Dr. Thomas Hess
Vural Ünlü, MBA, BA (Hons.)
Ludwig-Maximilians-Universität München
Institut für Wirtschaftsinformatik
und Neue Medien
Ludwigstraße 28
80539 München
089 2180-6390
{thess | uenlue}@bwl.uni-muenchen.de
http://www.wi.bwl.uni-muenchen.de

Kernpunkte

Medienunternehmen bzw. Produzenten von geistigem Eigentum stehen derzeit vor existenziellen Bedrohungen, weil werthaltige Inhalte unkontrolliert vervielfältigt werden und direkte Erlöse damit zumindest nicht mehr in gewohntem Maße generiert werden können. Digitale-Rechte-Management-Systeme (DRMS) versprechen eine Eindämmung dieser Problematik durch die Implementierung technischer Schutzmaßnahmen und versprechen zudem neue Optionen bei der Gestaltung von Erlösmodellen. Die Autoren skizzieren eine grundlegende Architektur von DRMS, geben einen Überblick über den Entwicklungsstand von DRMS aus funktionaler Perspektive, beschreiben die zu Grunde liegenden Basistechnologien und stellen exemplarisch drei am Markt verfügbare Lösungen vor. Folgende Ergebnisse werden erarbeitet:

- DRMS bieten Zugangs- und Nutzungssteuerung sowie Nutzungsabrechnung und unterstützen die Verfolgung von Rechtsverletzungen.
- DRMS stellen dem Nutzer ausgewählten Content zur Verfügung, greifen auf Lizenzdaten zurück und generieren Abrechnungsdaten.
- Die genannten Funktionen lassen sich durch die Kombination bekannter Verschlüsselungsverfahren mit neuen, medienspezifischen Verfahren zur Definition von Rechten und zur Markierung mittels digitaler Wasserzeichen erreichen.

Bei der Implementierung eines konkreten DRMS muss neben der technologischen Perspektive auch die wirtschaftliche Dimension ins Kalkül gezogen werden. Letztendlich ist ökonomisch zu entscheiden, welcher technische Schutzgrad im konkreten Fall sinnvoll ist.

Stichworte: Digitale-Rechte-Management-Systeme, Verschlüsselungsverfahren, digitale Wasserzeichen, Rechtedefinitionssprachen, Medienunternehmen

1 Einleitung

Medienunternehmen stellen Inhalte über ein Medium bereit und erzielen so direkte und indirekte Erlöse: direkte Erlöse für die Bereitstellung der Inhalte an sich sowie indirekte Erlöse von Werbetreibenden für die Generierung von Aufmerksamkeit [ScHe02, 38–45]. Das Verhältnis zwischen direkten und indirekten Erlösen ist je nach Mediengattung unterschiedlich: Während ein Buchverlag fast 100 % seiner Umsätze über direkte Erlöse generiert, erhält ein Free-TV-Sender 100 % über Werbung und verwandte Erlöse [Wirt01, 19].

Direkte Erlöse lassen sich nur generieren, wenn die Kosten für die Weitergabe von Inhalten (dem so genannten Content [AnHe03]) prohibitiv hoch sind. In den letzten Jahren sind diese Kosten immer weiter gesunken. Fotokopierer haben das Kopieren von Zeitschriften und Zeitungen verbilligt, Videorekorder haben das Mitschneiden von Fernsehsendungen vereinfacht und CD-Brenner haben das Vervielfältigen von CDs erleichtert. Auf Peer-to-Peer-(P2P-)Architektur basierende Tauschbörsen haben zudem den Austausch von Bild-, Text- und Audiodateien stark erleichtert [ScFi02]. Durch verbesserte Bandbreiten wird in absehbarer Zeit auch der Austausch von Videodateien in Spielfilmlänge möglich sein [HeAS02].

In Rechte-Management-Systemen für digitale Inhalte, den so genannten *Digitalen-Rechte-Management-Systemen (DRMS)*, sehen Medienunternehmen und die anbietende Softwareindustrie nun einen wichtigen Ansatzpunkt, die unkontrollierte Weitergabe von Content zu unterbinden und sich so direkte Erlösquellen zu sichern. Gerade im Musikbereich ist dies schon heute höchst relevant, da ein Teil der signifikanten Umsatzrückgänge in der Branche auf die Verletzung von Urheberrechten zurückgeführt wird. So ging laut des globalen

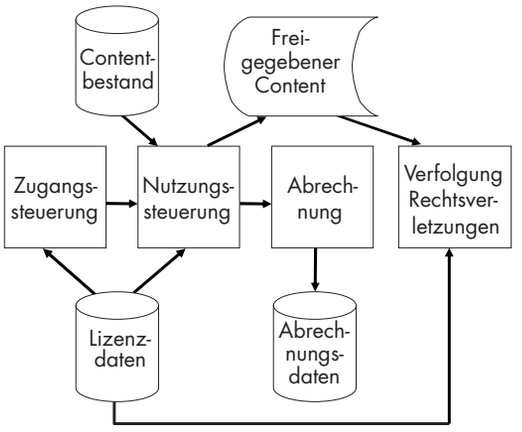

Bild 1 Logischer Aufbau eines DRMS

Plattenfirmenverbands IFPI der weltweite Musikumsatz im ersten Halbjahr 2003 im Vergleich zum Vorjahr um 10,9 % zurück, vorrangig wegen des Geschäfts mit Raubkopien [IFPI03]. Sicherlich steht die Steuerung der Weitergabe von Content im Zentrum der Konzeption von DRMS. Daneben wird aber auch erwartet, dass derartige Systeme neue Optionen bei der Gestaltung von Erlösmodellen eröffnen [Buhs01, 389], so z. B. durch eine technisch bisher nicht mögliche nutzenabhängige Abrechnung oder durch verbesserte Formen der Preisdifferenzierung.

Ziel des nachfolgenden Beitrags ist es, einen Überblick über den Entwicklungsstand von DRMS vor dem Hintergrund der beiden genannten Ziele zu geben. Den Einstieg liefert eine Skizze der Architektur von DRMS in Abschnitt zwei. In Kapitel drei findet sich eine Darstellung der wichtigsten Funktionen von DRMS. Die hinter diesen Funktionen liegenden Basistechniken werden in Abschnitt vier dargestellt. Ohne eine detaillierte Analyse der Basistechniken lässt sich der Entwicklungsstand von DRMS nicht fundiert einschätzen. Ergänzend werden in Kapitel fünf drei ausgewählte DRMS-Lösungen der Praxis präsentiert. Mit einem kurzen Fazit und einer Einordnung der Ergebnisse in Kapitel sechs schließt dieser Übersichtsbeitrag ab.

Abzugrenzen sind DRMS von konventionellen *Rechte-Management-Systemen (RMS)*, welche auf eine Steigerung der administrativen Effizienz im Umgang mit Lizenzrechten und -abrechnungen abzielen. Auch bei Content, der nicht digitalisiert vorliegt, stellt sich die Frage nach dem Rechtemanagement, wenn auch gegenüber digitalisiertem Content in eingeschränkter Form: Nur vorhandene Lizenzrechte können vertrieben werden, denn andernfalls drohen empfindliche Schadensersatzansprüche sowie Reputationsverlust. RMS werden mittlerweile sowohl von spezialisierten Anbietern als auch von Enterprise-Resource-Planning-Anbietern angeboten und zurzeit in vielen Medienunternehmen eingesetzt.

2 Architektur eines DRMS

DRMS sollten vorrangig die Weitergabe von Content kontrollierbar machen. Im Kern geht es damit um den gesteuerten Zugriff auf Content. DRMS müssen daher insbesondere Funktionen zur Zugangs- und zur Nutzungssteuerung bereitstellen. Während es der Zugangssteuerung um eine Einschränkung des Personenkreises („Wer?“) geht, steht bei der Nutzungssteuerung die Art der Nutzung („Wie?“) im Mittelpunkt. Beide Funktionen greifen auf Lizenzdaten zu, die in unterschiedlicher Granularität bis auf die Ebene von Nutzern verfeinert werden können. Auf Basis der Informationen aus der Zugangssteuerung sowie weiterführender Lizenzdaten löst die Nutzungssteuerung aus dem gesamten Content-Bestand dediziert Content für einen Nutzer frei.

Schlagen diese vorbeugenden Maßnahmen zur Durchsetzung von Urheberrechten fehl bzw. werden sie bewusst nicht implementiert, bieten sich noch nachgelagerte Aktivitäten an, die zumindest die Verfolgung von Rechtsverletzungen unterstützen können und damit – im Idealfall – Auskunft über die Lizenzrechte geben müssten. DRMS sollen dies durch eine entsprechende Funktion wirksam unterstützen.

In zweiter Linie sollen DRMS neue Optionen bei der Gestaltung von Erlösmodellen eröffnen. DRMS können diese einerseits durch die Bereitstellung einer Abrechnungsfunktion unterstützen. Die mithilfe der Abrechnungsfunktion erfassten Nutzungsdaten werden gesammelt und können dann von einem Abrechnungssystem beliebiger Art (wie z. B. einem Micropayment-System) weiterverarbeitet werden. Andererseits soll die bereits erwähnte Funktion zur Unterstützung der Nutzungssteuerung die gruppen- oder sogar personenbezogene Differenzierung von Rechten und Preisen unterstützen. In Bild 1 ist der logische Aufbau eines DRMS im Überblick dargestellt.

Bezüglich der physischen Verteilung der Systemkomponenten lässt sich kein generelles Bild zeichnen. Notwendig ist hierbei aufseiten des Inhalteanbieters ein Backend-DRMS, welches Medienprodukte vor Auslieferung an Endkunden mit Metainformationen anreichert und verschlüsselt, und ein Frontend-DRMS, das endkundenseitig die Sicherheitsziele durchsetzt. Zur Darstellung einer anbieterseitigen Lösung (Backend-Lösung) und zweier kundenseitiger Lösungen (Frontend-Lösungen) sei auf Abschnitt 5 verwiesen.

In Abschnitt drei werden die genannten Funktionen von DRMS einzeln vorgestellt. Bezüglich der Speicherung von Content sei auf [Lehn01, 81–92; Rawo02] verwiesen. Lizenz- und Abrechnungsdaten sind klassische kaufmännische Daten. Spezifika ergeben sich hier weniger durch deren Strukturierung, sondern vielmehr durch die Notwendigkeit der Standardisierung. In Abschnitt 4.3 wird dieser Aspekt noch einmal aufgegriffen.

3 Funktionen von DRMS

3.1 Zugangssteuerung

Ziel dieser Funktion ist es sicherzustellen, dass der Zugang zu unautorisierten Kopien verwehrt wird bzw. nur berechtigte Personen und Endgeräte Zugriff zu legal erworbenen Medienprodukten erhalten.

Im ersten Fall kann dies durch Zugriffsfilter bzw. Blockingverfahren realisiert werden, bei denen der Zugriff auf illegal kopierte Inhalte unterbunden wird [KöKS97]. Gängige Verfahren sind z. B. DNS-Umleitung, URL-Blocking und Proxy-Filterung. Beispiel für ein gescheitertes Filtersystem

ist das von der Musikindustrie propagierte Rights Protection System, welches bei deutschen Internetprovidern mit Auslandsanbindung implementiert werden sollte, um Zugriffe auf illegale ausländische Inhalte zu verhindern.

Im zweiten Fall kann der Zugriff auf legalen Content neben dem berechtigten Subjekt auch hinsichtlich Zeitpunkt und Standort eingegrenzt werden. Hierbei wird der Benutzer im ersten Schritt mittels eines Authentifizierungsverfahrens identifiziert. Aus technischer Sicht gibt es unterschiedliche Lösungsansätze: Das Spektrum an Verfahren reicht von Passwörtern (z. B. Software-ID) oder Hardware-Authentifikation (z. B. X509 oder CPU) bis hin zu biometrischen Verfahren [ArFB00; Schn01, 127–141]. Hierbei besteht ein Zielkonflikt zwischen Stichhaltigkeit der Identifikation und Implementierungskosten: Passwörterbasierte Systeme sind zwar einfach und kostengünstig zu implementieren, aber durch eine einfache Weitergabemöglichkeit der alphanumerischen Zeichenfolge leicht überwindbar. Im anderen Extremfall können biometrische Verfahren einen Benutzer durch biologische Merkmale eindeutig identifizieren, aber der Implementierungsaufwand für Medienanwendungen ist prohibitiv hoch.

3.2 Nutzungssteuerung

Der isolierte Einsatz der Zugangssteuerung ist eine unzureichende Schutzmaßnahme. Ist der Zugang zu Medienprodukten einmal gegeben und befindet sich der Content im Machtbereich des Benutzers, kann nicht mehr kontrolliert werden, was der Nutzer nachträglich damit macht. Aus diesem Grund ist es wichtig, dass die Nutzungsüberwachung der Medienprodukte bis in die Privatsphäre des Nutzers erweitert wird. Es muss kontrolliert werden, zur Durchführung welcher Aktionen der Benutzer nach Erhalt des Medienproduktes berechtigt ist. Insbesondere soll das unautorisierte Kopieren und die Weitergabe an Unberechtigte unterbunden werden.

Hierzu müssen die durchzuführenden Operationen durch spezielle, autorisierte Frontend-DRMS endkundenseitig freigegeben werden. Voraussetzung hierfür ist, dass das Frontend-DRMS über die Nutzungseinräumung an einem konkreten Medienprodukt informiert ist. Diese Aufgabe übernehmen Rechte-Management-Informationen, welche als Metainformationen von einem Backend-DRMS vor der Auslieferung mit dem Medienprodukt versehen werden. Ist die Nutzung personenbezogen, liegen die Metainformationen primär aufseiten des Backend-DRMS. Bei endgerätegebundenem Konsum liegen diese vorrangig beim Frontend-DRMS bzw. kombiniert bei hybriden Nutzungskonzepten, wie z. B. bei iTunes.

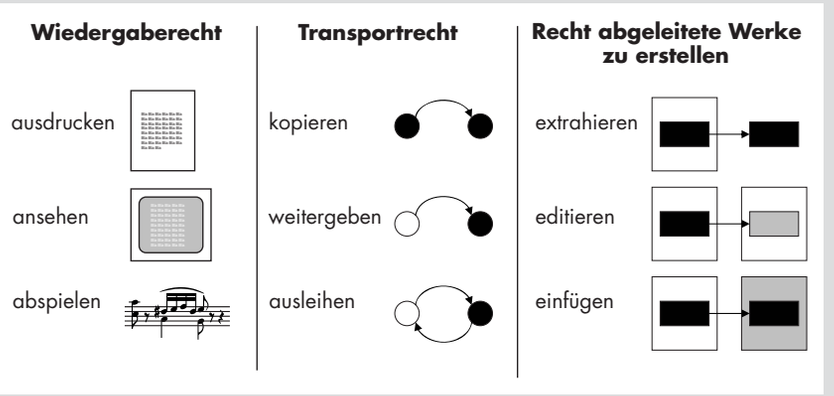

Bild 2 Umfang der Rechtegewährung [RoTM02, 62]

Das in Bild 2 abgebildete Rechtemodell kann folgende drei fundamentale Verfügungsformen einräumen [RoTM02, 62; Stef96]:

(1) Wiedergaberecht (ausdrucken, ansehen und abspielen)
(2) Transportrecht (kopieren, weitergeben und ausleihen)
(3) Recht, abgeleitete Werke zu erstellen (extrahieren, editieren und einfügen)

So könnte beispielsweise das Ausdrucken und die Ausgabe eines Dokumentes auf dem Bildschirm erlaubt (als positive Wiedergaberechte), aber die Weitergabe durch einen lokalen Speicherschutz unterbunden werden (als Einschränkung der Transportrechte). In ihrer einfachsten Form umfassen Nutzungssteuerungssysteme damit einen simplen Kopierschutzmechanismus (wie z. B. beim Digital Audio Tape (DAT) oder beim DVD-Standard). In der Regel ist es jedoch nicht das Ziel, das Kopieren völlig zu unterbinden, sondern Kopiervorgänge im Sinne einer Kopierkontrolle steuern zu können.

Zugangs- und Nutzungssteuerung stellen zusammen die Ausschließbarkeit vom Konsum sicher und verhindern somit, dass sich Medienprodukte zu perfekten öffentlichen Gütern entwickeln.

3.3 Nutzungsabrechnung

DRMS ermöglichen nicht nur einen umfassenden Schutz, sondern durch den existierenden direkten Endkundenkontakt auch die Etablierung *nutzungsabhängiger Erlösmodelle* (Pay-per-View, Pay-per-Click etc.). Einher geht die Absicht seitens der Medienindustrie, zukünftig verstärkt nicht den Besitz, sondern mehr die Nutzung von Informationsgütern in Rechnung zu stellen [RoTM02, 28–29]. Der Konsum von Medienprodukten wird analog zur Strom- und Gasabrechung gehandhabt, mit der alle *Stakeholder* zufrieden gestellt werden können: Konsumenten von Medienprodukten erfreuen sich dabei an einer verursachungsgerechteren Bezahlung und können Medienprodukte selektiv und in Kleinstmengen erwerben. Inhalteanbieter erhoffen sich eine weitgehende Abschöpfung der Konsumentenrente. Der Gesetzgeber sieht im Preisdifferenzierungspotenzial einen wohlfahrtsförderlichen Mechanismus.

Technisch gesehen ist bei der Einzelnutzungsabrechnung eine enge Verzahnung von Systemkomponenten auf Anbieter- und auf Nutzerseite erforderlich. Ein DRMS kann im Idealfall die Nutzung der Inhalte in Echtzeit detailliert mitprotokollieren und diese Informationen per Rückkanal an das Abrechnungssystem des Anbieters weitergeben. Neben der Protokollierungsfunktion und Rückkanalfähigkeit sind zusätzlich auch die Integration von E-Commerce- und sicheren Zahlungssystemen notwendig [SaSc03]. Offenheit gegenüber bestehenden und neuen Geschäftsmodellen ist zusätzlich erstrebenswert.

In einem weitergehenden Superdistributions-Ansatz von Ryoichi Mori und Brad Cox werden aus Konsumenten auch Vertriebsmitarbeiter, welche in Netzwerken (z. B. in Rahmen von P2P-Architekturen) Medienprodukte an Interessierte empfehlen

und bei erfolgreicher Vermittlung Lizenzzahlungen für die Urheber sowie auch eine Kommission für sich selbst generieren können [MoKa90; Cox96]. Durch Kombination der technischen Schutzmaßnahmen von DRMS, den Distributionsmöglichkeiten von P2P-Netzwerken und cleveren Anreizmechanismen erhofft man sich attraktive Geschäftsmodelle [GeAn02].

3.4 Verfolgung von Rechtsverletzungen

Die Einschränkung der Verwendungskontrolle stellt sicherlich eine Beschneidung der gewohnten Nutzungsmöglichkeiten dar, bietet jedoch für bestimmte Medienprodukte und Kundengruppen einen wirkungsvollen Schutz. Dennoch ist ein vollkommener Schutz nicht durchsetzbar: Auch wenn die technischen Schutzmöglichkeiten den Angriffstechniken und -werkzeugen der Hacker einen Schritt voraus bleiben sollten, besteht weiterhin das fundamentale „Problem der analogen Lücke", d. h. die Möglichkeit, Analogkopien hochwertig zu digitalisieren und mindestens eine Kopie mit den daraus resultierenden Schneeballeffekten über technische Netzwerke zu verbreiten. Das führt dazu, dass früher oder später mit der Erhältlichkeit von nicht legal erworbenen Medienprodukten zu rechnen ist und Inhalteanbieter auch illegale Kopien identifizieren sowie Rechtsverletzungen verfolgen müssen.

Dementsprechend erweitert sich der notwendige Aktionsradius von Inhalteanbietern nicht nur auf vorbeugende, sondern auch auf reaktive Maßnahmen im Kampf gegen unautorisierte Kopien. Diese beugen zwar nicht direkt Rechtsverletzungen vor, können aber durch den Abschreckungseffekt einen Beitrag zur Vermeidung von Rechtsverletzungen leisten. Vorraussetzung für die Identifizierung von unerlaubten Kopien sind bewusst gesetzte Markierungen oder die Abwesenheit von Markierungen als Zeichen für kompromittierte Medienprodukte. Es lassen sich auch hier verschiedene Verfahren unterscheiden:

Zu den schwachen Markierungsverfahren zählen das *Labeling* und das *Tatooing*, welche im ersten Fall die urheberrechtlichen Informationen in bestimmten Abschnitten des Medienprodukts (üblicherweise im Header) platzieren und im letzteren Fall einen Copyright-Vermerk sicht- bzw. hörbar in das Medienprodukt einfügen. Diese Verfahren sind entweder leicht überwindbar, weil die Metainformationen nicht versteckt werden, oder die Qualität des Medienproduktes und somit die Zahlungsbereitschaft stark reduziert wird. Zu den harten Markierungsverfahren zählen *Wasserzeichen*, welche die versteckte Einbettung von Metadaten in Medienprodukte ermöglichen (siehe Abschnitt 4.3).

Die Identifikation von illegal kopierten Medienprodukten kann automatisiert durch Internet-Suchroboter erfolgen, welche anhand der charakteristischen Bitmuster eines Medienprodukts und (gesetzter bzw. fehlender) Markierungen illegal verbreitete Inhalte bzw. den ursprünglichen Käufer (bei digitalen Fingerabdrücken) aufspüren können [KaPe00, 104].

4 Basistechniken für DRMS

Zugangs- und Nutzungssteuerung funktionieren nur, wenn deren Umgehung so schwer wie möglich gemacht wird. Techniken zur *Verschlüsselung* unterstützen dies. Scheitern derartige Schutzmechanismen oder werden sie bewusst außer Acht gelassen, sollten *Wasserzeichen* greifen. Beide Techniken – und auch die nicht näher beschriebene *Abrechnungsfunktion* – setzen umfangreiches Wissen über die eingeräumten Zugangs- und Nutzungsrechte voraus, die mithilfe von *Rechtedefinitionssprachen* flexibel beschrieben werden können. Während Verschlüsselungsverfahren zu den mittlerweile bewährten Kerntechniken der IT-Sicherheit zählen, sind Wasserzeichen und Rechtedefinitionssprachen speziell für Medienanwendungen entwickelte Techniken. Alle drei Techniken sind nachfolgend skizziert – zur Vereinfachung isoliert, obwohl die drei Techniken natürlich sehr stark ineinander greifen. Als vertiefende Lektüre zu DRMS-Schutztechniken empfiehlt sich [PfFK02].

4.1 Verschlüsselung

Um Medienprodukte vor unberechtigter Nutzung, Veränderung oder Verfälschung zu schützen, müssen die übertragenen Inhalte verschlüsselt sein, sodass die Besitzübernahme und Weitergabe von chiffrierten Datenpaketen für einen „feindlichen" Nutzer wertlos sind.

Kryptographische Techniken stellen die ausgereifteste Basistechnik dar und werden in offen gelegte symmetrische, asymmetrische sowie hybride Verfahren und in geheim gehaltene Verfahren unterteilt [PfFK02, 20–22]. Bei *symmetrischen Verfahren* benutzt der Sender und Empfänger denselben Schlüssel zur Ver- und Entschlüsselung des Inhalts. Jedoch erfordert dies eine sichere Übertragung des Schlüssels und einen hohen Aufwand bei der Generierung und Übermittlung von Schlüsseln. Unter den etablierten Standards finden sich z. B. DES (Data Encryption Standard) bzw. Triple-DES, AES (Advanced Encryption Standard) und IDEA (International Data Encryption Standard) [Schn01, 80–84]. Bei Anwendungen von *asymmetrischen Verfahren* (auch: *Public-Key-Verfahren*) erfolgt die Ver- und Entschlüsselung der Information mit unterschiedlichen (öffentlichen und privaten) Schlüsselpaaren [BeSW01, 10–12]. Notwendig wird eine so genannte Public-Key-Infrastruktur, welche die öffentlichen Schlüssel der kommunizierenden Parteien verwaltet. Vorteilhaft gegenüber den symmetrischen Verfahren ist, dass das Sicherheitsrisiko bei der Übermittlung des Schlüssels vermieden und die Schlüsselverteilung vereinfacht wird. Allerdings sind diese Systeme auch deutlich rechenintensiver und erfordern eine öffentliche Verwaltungsinfrastruktur. Die bekanntesten Vertreter sind RSA und ElGamal. Eine konkrete Anwendung ist die *digitale Signatur*, welche mittels einer umgekehrten asymmetrischen Verschlüsselung die Authentizität einer Person nachweist [Schn01, 90–91]. Bei *hybriden Verfahren* wird die zu verschlüsselnde Information symmetrisch chiffriert und dieser Schlüssel im Anschluss asymmetrisch verschlüsselt. Dadurch verringert sich sowohl der Rechenaufwand als auch das Sicherheitsrisiko bei der Schlüsselübermittlung. Schließlich existieren noch *geheim gehaltene Verfahren*, welche sich durch nicht standardisierte sowie nicht veröffentlichte Sicherungsdesigns auszeichnen und eine zusätzliche Hürde für den Angreifer darstellen können. Dagegen sprechen jedoch mögliche Sicherheitslücken durch fehlende Expertenwürdigung und rechtliche Probleme. So sicher auch das Design eines Verschlüsselungsverfahrens ist, kann es durch das Durchsuchen des endlichen Schlüsselraumes (auch Brute-Force-Angriff) gebrochen werden. Mit steigender Rechenleistung bei gleichzeitig sinkenden Kosten, einer höheren Werthaltigkeit und längeren Halbwertszeit des Contents muss daher dementsprechend auch die Schlüssellänge und die Performanz der Frontend-DRMS erweitert werden.

Kryptographische Verfahren kommen insbesondere im Rahmen der Zugriffs- und Nutzungskontrolle sowie der sicheren Abrechnung zum Einsatz: digitale Signaturen stellen die Authentizität des Berechtigten sicher und sind eine wesentliche Vorraus-

setzung für eine wirksame Zugangskontrolle. Eine effiziente Nutzungskontrolle, welche die lokale Speicherung der Mediendaten ausschließlich in verschlüsselter Form zulässt und die entschlüsselten Datenströme nur *just-in-time* und lediglich für den benötigten Abschnitt bereitstellt, wird durch so genannte *digitale Container* realisiert. Im Rahmen *elektronischer Zahlungssysteme* helfen Verschlüsselungsverfahren (insbesondere das Secure-Electronic-Transaction-(SET-)System) bei der sicheren Übertragung von sensiblen Abrechnungsdaten (z. B. Kreditkartennummern) über das Internet. Weiterhin können symmetrische Authentifikationssysteme im Rahmen von so genannten Challenge-Response-Verfahren einen Beitrag zur Identifikation und Ausschaltung (*device revocation*) von manipulierten DRMS-Clients und damit gegen unautorisierten Medienkonsum leisten [BeSW01, 26–28].

4.2 Digitale Wasserzeichen

Ziel der verschiedenen Wasserzeichenverfahren ist es, Metainformationen unwiderruflich mit einem Medienprodukt zu verbinden. Zu unterscheiden sind drei Varianten:

(1) Bei *sichtbaren Wasserzeichen* wird eine klar erkennbare Copyright-Markierung an das zu schützende Objekt angebracht, was die nicht autorisierte Nutzung unattraktiv machen soll und in jedem Fall zu einem (wenn auch manchmal marginalen) Qualitätsverlust führen kann. Nach dem legitimen Kauf eines Medienprodukts werden sichtbare Wasserzeichen nach Möglichkeit entfernt bzw. unsichtbare Wasserzeichen neu eingesetzt.

(2) In (*unsichtbar-)robusten Wasserzeichen* werden rechtebezogene Informationen im Content „versteckt", d. h. unsichtbar gespeichert und untrennbar mit dem Werk verbunden. Derartige Informationen werden häufig zur Überprüfung von Zugangs- und Nutzungsrechten und für Abrechnungszwecke genutzt. Gelegentlich umfassen robuste Wasserzeichen auch Informationen zum Lizenznehmer. Im letzten Fall spricht man von digitalen Fingerabdrücken [Ditt00, 115–134], die sich zur Rechtsverfolgung einsetzen lassen.

(3) *(Unsichtbar-)fragile Wasserzeichen* dienen dem Nachweis der Unverfälschtheit (Unversehrtheit und Integrität). Hierbei wird überprüft, ob eine Mediendatei durch Angriffe manipuliert wurde. Dabei sollen fragile Wasserzeichen nur gegen Verarbeitungsoperationen (Komprimierung, Skalierung etc.) robust sein, während bei inhaltlichen Änderungen (z. B. Bildmanipulationen) das Wasserzeichen zerstört werden soll [Ditt00, 135–147]. Daher lassen sich fragile Wasserzeichen für die Verfolgung von Rechtsverletzungen einsetzen.

Sowohl bei den robusten als auch bei den unsichtbaren Wasserzeichen kommen steganographische Algorithmen zum Einsatz. Ergänzend sei erwähnt, dass es noch immer nicht abschließend gelungen ist, intelligente Angriffe gegen Wasserzeichen wirklich auszuschließen [Ditt00, 149–153].

4.3 Rechtedefinitionssprachen

Rechtedefinitionssprachen erlauben die Beschreibung des Umfangs der eingeräumten Rechte und der gewählten Form der Abrechnung. Hierzu werden für jedes Medienprodukt durch das DRMS alle für einen Kunden erwerbbaren bzw. erworbenen Nutzungsmöglichkeiten abgebildet und mit Preisen hinterlegt [Guth03]. Je nachdem wie umfangreich die Rechtedefinitionssprache ist, können Nutzungsrechte differenziert abgebildet und abgerechnet werden: Nutzungszeitraum, -häufigkeit, -qualität (Bild- und Hörqualität), -operationen (drucken, ändern, kopieren etc.) und weitere Bedingungen bzw. Einschränkungen (geographischer, sprachlicher oder endgerätespezifischer Natur) können granular definiert werden und ermöglichen eine zielgerichtete Nutzungskontrolle [RoTM02, 60–77]. Rechtedefinitionssprachen sollen dabei idealtypischerweise alle denkbaren (also sowohl bestehende als auch neue) Rechtedimensionen über alle Auswertungsformen, Medienformen (Print, Audio, Bewegtbild) und Abrechnungsmodalitäten in maschinenlesbarer Form abbilden.

Die Möglichkeit der individuellen Steuerung und Abrechung des Konsums ermöglicht digitale und nutzungsabhängige Geschäftsmodelle, welche bisher bei analogen Medien undenkbar waren. Die hierfür benutzte Sprache kann entweder proprietär oder offen sein. Eine offene und damit standardisierte Sprache ist notwendig, wenn eine plattformübergreifende, interoperable Nutzung anvisiert wird. Beispiele für etablierte Standards sind die durch die *Organisation for the Advancement of Structured Information Standards (OASIS)* vorangetriebene *eXtensible rights Markup Language (XrML)* sowie die von der *Open Mobile Alliance (OMA)* entwickelte *Open Digital Rights Language (ODRL)* [Guth03, 105–106]. Das XrML-Datenmodell besteht aus vier Entitäten sowie deren Beziehungen zueinander. Die dargestellte Hauptbeziehung zwischen den vier Entitäten wird durch die so genannte *Grant Assertion* definiert, bestehend aus „*Principal*" (Lizenznehmer), „*Right*" (Nutzungsumfang), „*Resource*" (lizenziertes Werk) und „*Condition*" (Vorbedingung, die erfüllt sein muss bevor das Recht ausgeübt werden kann) [o.V.02].

Rechteinformationen können entweder mittels steganographischer Verfahren untrennbar an die Medienprodukte angefügt oder separat zu diesen geliefert werden. Der Vorteil der ersten Variante ist, dass es zu keiner ungewünschten Entkopplung zwischen Medienprodukt und Nutzungskontrollinformationen kommt. Bei der zweiten Form können Rechteinformationen flexibler geändert werden, was dezentralen Geschäftsmodellen (insb. Superdistribution) entgegenkommt.

Ähnlich wie bei Verschlüsselungstechniken kommen Rechtedefinitionssprachen im Rahmen von DRMS umfassend zum Einsatz: Sie unterstützen mittels Einbringung von Kundeninformationen die Zugangssteuerung, indem das lokale Abgreifen der Medienprodukte nur vorab autorisierten Nutzern gestattet wird. Primärzweck ist jedoch die Realisierung einer flexiblen Nutzungssteuerung sowie einer nutzungsabhängigen Abrechnung durch Rechte- und Abrechnungsinformationen.

In Tabelle 1 ist der funktionale Beitrag der drei dargestellten Techniken noch einmal im Überblick dargestellt. Die Darstellung ist nicht vollständig, sondern will lediglich zeigen, dass Basistechniken nicht isoliert, sondern kombiniert eingesetzt werden müssen, um die funktionalen Anforderungen zu realisieren. Eine effiziente Nutzungssteuerung wird z. B. erst durch die Kombination aller drei Kerntechniken erzielt.

5 DRMS-Lösungen am Markt

Am Markt steht mittlerweile eine Vielzahl von Standardlösungen bereit. Ein ausführlicher Marktüberblick findet sich z. B. in [FrKa04]. Nachfolgend sind drei populäre Lösungen kurz skizziert.

Die *Electronic-Media-Management-System-(EMMS-)Suite* von IBM zielt als

Tabelle 1 DRMS Funktionen-Techniken-Matrix

Funktionen Techniken	Zugangssteuerung	Nutzungssteuerung	Management von Rechtsverletzungen	Nutzungsabrechnung
Verschlüsselung	Authentifizierungsverfahren (z. B. Digitale Signatur)	Nutzungsfreigabe durch Content-Entschlüsselung (z. B. symmetrische Verschlüsselungsverfahren)	Ausschalten von manipulierten DRMS-Clients (Device Revocation nach Challenge-Response-Verfahren)	Sichere Zahlungsverfahren (z. B. SET-Verfahren)
Digitale Wasserzeichen	Robuste Wasserzeichen zur Authentifizierungsprüfung	Robuste Wasserzeichen zur Durchsetzung des Kopierschutzes	Fragile Wasserzeichen zum Integritätsnachweis	Robuste Wasserzeichen zur Authentifizierungsprüfung
Rechtedefinitionssprachen	Abbildung autorisierter Nutzer/ Endgeräte	Abbildung von Verfügungsrechten	Abbildung autorisierter Nutzer/ Endgeräte	Abbildung Einzelabrechnungsinformationen

Backend-DRMS-Lösung nicht primär auf den endkundenseitigen Schutz (wie in den beiden nachfolgend beschriebenen Produkten), sondern bereitet den Content in geschützter und mit Metadaten angereicherter Form zur Auslieferung an ein Frontend-DRMS vor. Dennoch ermöglicht ein Software-Development-Kit die Entwicklung von EMMS-kompatibler Client-Abspielsoftware, wobei auch Standard-Clients (z. B. RealPlayer) unterstützt werden. EMMS besteht aus insgesamt sieben kombinierbaren Backend-Modulen und ist Bestandteil der „DB2 Content Management"-Produktfamilie. Das Angebot umfasst den Schutz aller Medienformate sowohl im innerbetrieblichen als auch im Vertriebskontext. Basierend auf einer Preparation- und Mastering-Komponente wird der Content auf Anbieterseite vorbereitet und mittels eines Hosting-Services und einer E-Commerce-Applikation elektronisch vertrieben. Für Rechteintermediäre werden auch kaufmännische Module, welche beispielsweise den gesamten Abrechnungszyklus managen, angeboten. Die Ausführungsumgebung ist Java, die Rechtedefinition erfolgt im XML-Format, wodurch eine unternehmensindividuelle und flexible Zugangs- und Nutzungssteuerungssprache mit Abrechnungsfunktionen entwickelt werden kann. Weiterhin werden eine geographische Steuerung sowie eine Tracking-Funktion bereitgestellt. EMMS verwendet Verschlüsselungstechniken im Verbund mit digitalen Containern. Wasserzeichentechniken werden für Audio-Inhalte angeboten.

Der kostenlos erhältliche *Microsoft Windows Media Player* (aktuell mit der 9-Reihe) ist eine Audio- und Bewegtbild-Abspielsoftware und damit eine mehr auf die Nutzerseite fokussierte Lösung, welche seit 1999 standardmäßig auf nahezu allen Windows-Rechnern installiert ist und den *Microsoft Media Rights Manager* mit DRM-Funktionalitäten enthält [Prun03]. Bild 3 veranschaulicht den Datenfluss in der Microsoft-Lösung und ordnet dabei auch die logischen Komponenten Anbietern bzw. Nachfragern zu. Im logisch ersten Schritt wird der digitale Content verschlüsselt. Nun folgt die Distribution der geschützten Mediengüter durch Bereitstellung auf einem Web- bzw. Streaming-Server zum Download (Schritt 2). Es erfolgt keine Zugriffssteuerung, d. h., die Dateien können frei und ohne Authentifizierung herunter geladen werden (Schritt 3), weil der verschlüsselte Content ohne Lizenzschlüssel wertlos ist. Dieser wird separat vom verschlüsselten Content über einen Lizenzserver bereitgestellt und vertrieben (Schritt 4). Über diesen können sich Kunden authentifizieren und Lizenzen erwerben (Schritt 5). Die Anfrage nach einer Lizenz erfolgt automatisch, wenn ein Kunde versucht, über den Client auf den geschützten Inhalt zuzugreifen. Nachdem der Kunde eine Lizenz erworben hat, kann er die gewünschte Datei abspielen, wobei die Nutzung der Dateiinhalte natürlich den in der Lizenz festgelegten Regeln unterliegt. Lizenzen sind an ein Frontend-DRMS gebunden und können nicht auf einem anderen Frontend-DRMS ohne Lizenzneuerwerb genutzt werden.

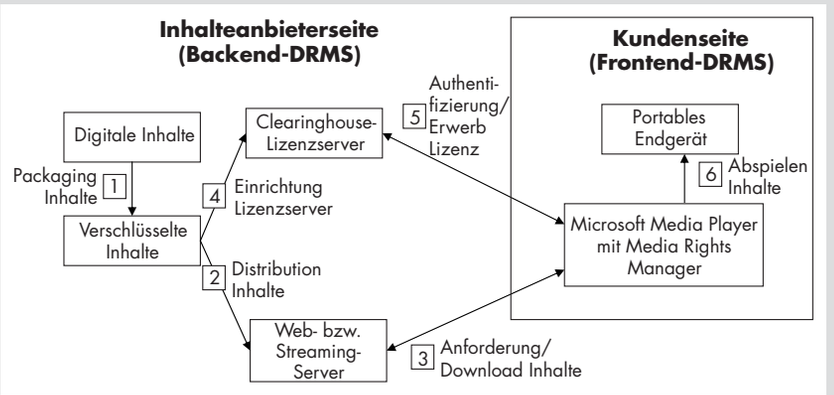

Bild 3 Architektur des Microsoft Windows Media Players [Prun03]

Der Media Rights Manager unterstützt eine differenzierte Nutzungssteuerung. Neben der zeitlichen Begrenzung der Nutzung von Inhalten kann auch die Anzahl der Abspielvorgänge und eine Kopierfreigabe auf CD-Speicher festgelegt werden. Wenn Lizenzen erforderlich werden, können Prüfung und Erwerb im Hintergrund erfolgen. Im Kern setzt der Media Rights Manager auf folgende Schutztechniken: Die Verschlüsselung im proprietären wma-Format erfolgt über gängige Verfahren, wie z. B. Triple-DES und RSA. Inhalteanbieter können den Benutzern vor der Nutzung des Contents vorschreiben, den Media Player zu individualisieren (z. B. mittels einer CPU-Identifikation) und so durch den Content an den individualisierten Media Player zu binden. Automatisierte Online-Updates, welche manipulierte Media Player säubern und ein Analogwandlungsver-

fahren, welches das Abgreifen der entschlüsselten Datenflüsse in der Soundkarte unterbindet, stellen weitere Sicherheitskomponenten dar [FrKa04, 158–160].

Mithilfe der *Multimedia Home Plattform (MHP)* wurde durch das European Telecommunications Standards Institute ein Standard für interaktives Fernsehen mit Internetzugang geschaffen. Im Regelfall wird MHP in einer Set-Top-Box realisiert und ist damit – genauso wie der Media Rights Manager – ebenfalls als nutzerseitige Lösung einzustufen. MHP ist eine auf der Java-Plattform basierte Middleware, welche zwischen Betriebssystem und Anwendungen eingebunden ist. Bei der Verwendung von Set-Top-Boxen als Endgerät in Kombination mit einem so genannten Subscriber-Management-System als Lizenzverwaltungssystem auf Anbieterseite wird eine differenzierte Zugangs- und Nutzungssteuerung durch den Ausschluss von nicht autorisierten Nutzern und unberechtigtem Nutzungsumfang ermöglicht. Durch die zunehmend verbreitete Rückkanalfähigkeit werden nutzungsabhängige Abrechnungsmodelle denkbar. Der Inhalteanbieter überträgt dabei einen codierten Datenstrom an alle Kunden. Mithilfe einer speziell ausgegebenen Chipkarte, auf der sich i. d. R. der Schlüssel befindet, kann ein Kunde diesen Datenstrom decodieren und damit entsprechend seine Rechte nutzen. Welcher Kryptostandard dabei konkret eingesetzt wird (üblicherweise symmetrische Verfahren wie Triple-DES, AES, IDEA), richtet sich nach dem jeweiligen Anbieter. Im Rahmen der MHP-Standards werden bei der Übertragung des Bewegtbilds zusätzlich spezielle Java-Applets (so genannte Xlets) übertragen, welche in einer abgesicherten „Sandbox"-Umgebung ausgeführt werden [PfFK02, 30]. Das Sicherheitskonzept ähnelt dem von Java, da Xlets mittels Public-Key-Infrastruktur digital signiert sein können und bei Annahme auf den vollen Funktionsumfang von MHP Zugriff nehmen können. MHP-konforme Xlets können vielfältige Anwendungen wie z. B. interaktive Shoppinglösungen und On-Demand-Services umfassen.

6 Fazit und Einordnung

DRMS versprechen die Implementierung eines umfassenden Schutzschemas durch die Kombination und Integration der drei Basistechniken Verschlüsselung, Wasserzeichen und Rechtedefinitionssprachen zu vorbeugenden (Zugriffs- und Nutzungssteuerung) und reaktiven (Management von Rechtsverletzungen) Zwecken. Zusätzliche Abrechnungsfunktionen lassen nutzungsabhängige Erlösströme möglich erscheinen. Detaillierte Informationen über den Nutzer eröffnen zumindest technisch auch weitergehende Formen der Preisdifferenzierung. Bei den aktuellen Angeboten der Softwareindustrie handelt es sich sowohl um anbieter- als auch nutzerseitig fokussierte Lösungen.

Trotz eines inzwischen umfangreichen Angebotes an DRMS-Lösungen zögern Inhalteanbieter überwiegend noch, ihre hochwertigen Inhalte digital anzubieten. Sicherlich müssen in Pilotprojekten erst Erfahrungen mit der neuen Klasse von Systemen gewonnen werden [ÜRHF03]. Daneben ist aber auch eine weitergehende Zurückhaltung zu erkennen. Eine Ursache könnte in der noch unklaren Reaktion des Gesetzgebers auf die neuen technischen Optionen liegen. Es bestehen Konflikte zum Urheber-, Datenschutz- und Wettbewerbsrecht mit möglicherweise negativen Wohlfahrtseffekten [PiFi03, 294–295], die eine rechtliche Einschränkung bestimmter DRM-Funktionen rechtfertigen [Bech02, 375] und kostspielige Anpassungen von DRMS-Installationen bedingen könnten. Aus technischer Sicht ist die Unsicherheit geringer, welches auf die Reife der zu Grunde liegenden Forschungs- und Entwicklungsarbeit zurückzuführen ist. Dies gilt insbesondere für die Verschlüsselungstechnologie, während bei den digitalen Wasserzeichen wie angedeutet noch Grundlagenforschung notwendig ist. Neben den Sicherheitszielen müssen Inhalteanbieter aber auch kundenseitige Interessen berücksichtigen. Ein zentrales Defizit bestehender DRMS liegt in fehlender *Interoperabilität*, d. h. in Inkompatibilität zwischen konkurrierenden DRM-Plattformen und damit zusammenhängend in eingeschränkter Mobilität. Dies bedeutet, dass noch immer Rechte nicht personenbezogen, sondern lediglich geräteabhängig eingeräumt werden können und sich nicht frei zwischen den Endgeräten übertragen lassen. Voraussetzung für eine breite Kundenakzeptanz sind jedoch offene DRMS, welche eine Vielzahl von Technik- und Content-Standards (wie z. B. Medienformate, Dokumentenidentifikation, Rechtedefinitionssprachen und andere Metadaten) unterstützen. Der Einsatz standardisierter Rechtedefinitionssprachen ist ein wichtiger Schritt um die notwendige Interoperabilität zu gewährleisten.

Technische Schutzmaßnahmen stellen jedoch keine ultimative Lösung für die aktuellen Nöte der Medienindustrie dar. Ein absoluter Schutz ist zum einen nicht möglich, zum anderen wirtschaftlich nicht sinnvoll: Technische Schutzmaßnahmen ermöglichen zwar die Nutzungsausschließung von Trittbrettfahrern, führen jedoch zugleich zu höheren Kosten entlang der gesamten Wertschöpfungskette und möglicherweise zu einer Nutzenminderung auf der Konsumentenseite [ÜnHe03]. Auch hat sich die Hoffnung auf eine Erschließung von Kleinstbeträgen durch derzeit noch prohibitiv hohe Transaktionskosten (insb. Abrechnungskosten) nicht realisiert. Ein interessanter Ansatz findet sich im iTunes Music Store von Apple, der u. a. kontrollierte Kopien für den Eigengebrauch und die beschränkte Weitergabe von Rechten erlaubt [vWH03].

Abstract

Digital Rights Management Systems

Media companies and producers of intellectual property are currently threatened with massive information product piracy. Digital Rights Management Systems (DRMS) offer technical copyright protection measures to protect content against digital piracy. The authors give an overview about the status quo of DRMS from a functional, technical and architectural perspective. Apart from purely technological issues, it is also essential to take the economic aspects of DRMS into consideration. The trade-off between content protection and total cost of ownership of a DRMS installation will require the determination of a suitable level of technical copyright protection for a given context.

Keywords: Digital Rights Management, Encryption, Digital Watermarks, Rights Expression Languages, Media Company

Als Schlussfolgerung ist festzuhalten, dass die DRMS und ihre Basiskomponenten reifer werden und perspektivisch innerhalb der DRM-Industrie mit weiteren Standardisierungserfolgen und einer klaren Position des Gesetzgebers zu rechnen ist. Aufseiten der Inhalteanbieter ist eine sinnvolle Balance zwischen Inhalteschutz und Kundennutzen zu schaffen und das betriebswirtschaftliche Kalkül zu verfeinern, d. h. der ökonomische Beitrag einer Investition in DRM-Technologie zu prüfen. Die Klärung dieser Punkte ist eine wesentliche Bedingung, damit Inhalteanbieter ihren häufig zu beobachtenden Attentismus aufgeben und digitale Produktangebote bereitstellen.

Literatur

[AnHe03] *Anding, Markus; Hess, Thomas:* Was ist Content? Zur Definition und Systematisierung von Medieninhalten. In: Arbeitsberichte des Instituts für Wirtschaftsinformatik und Neue Medien der LMU München, Nr. 5/2003, München, 2003.

[ArFB00] *Arnold, Michael; Funk, Wolfgang; Busch, Christoph:* Technische Schutzmaßnahmen multimedialer Daten. In: *Dittrich, Robert (Hrsg.):* Beiträge zum Urheberrecht: Österreichische Schriftenreihe zum gewerblichen Rechtschutz. Manz, Wien 2000.

[Bech02] *Bechtold, Stefan:* Vom Urheber- zum Informationsrecht. Implikationen des Digital Rights Management. C.H. Beck, München 2002.

[BeSW01] *Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus-Dieter:* Moderne Verfahren der Kryptographie. Vieweg, Braunschweig, Wiesbaden 2001.

[Buhs01] *Buhse, Willms:* Systematisierung von Geschäftsmodellen für Online-Musik unter Berücksichtigung von Marktunsicherheiten. WIRTSCHAFTSINFORMATIK 43 (2001) 4, S. 383–391.

[Cox96] *Cox, Brad:* Superdistribution: Objects as Property on the Electronic Frontier. Addison-Wesley, New York 1996.

[Ditt00] *Dittmann, Jana:* Digitale Wasserzeichen. Springer, Berlin u. a. 2000.

[FrKa04] *Fränkl, Gerald; Karpf, Philipp:* Digital Rights Management Systeme – Einführung, Technologien, Recht, Ökonomie und Marktanalyse. pg Verlag, München 2004.

[GeAn02] *Gehrke, Nick; Anding, Markus:* Peer-To-Peer Business Model for the Music Industry. In: *Monteiro, J. L. et. al. (Hrsg.):* Towards the Knowledge Society. Proceedings of the 2nd IFIP Conference on eCommerce, eBusiness and eGovernment. Kluwer Academic Publishers, Lissabon 2002, S. 243–257.

[Guth03] *Guth, Susanne:* Rights Expression Languages. In: *Becker, Eberhard. et al. (Hrsg.):* Digital Rights Management: Technological, Economic, and Legal and Political Aspects. Springer Verlag, Heidelberg 2003, S. 101–112.

[HeAS02] *Hess, Thomas; Anding, Markus; Schreiber, Matthias:* Napster in der Videobranche? Erste Überlegungen zu Peer-to-Peer-Anwendungen für Videoinhalte. In: *Schoder, Detlef; Fischbach Kai; Teichmann, René (Hrsg.):* Peer-To-Peer (P2P) Ökonomische, technologische und juristische Perspektiven. Springer Verlag, Berlin u. a. 2002, S. 25–40.

[IFPI03] *International Federation of the Phonographic Industry:* Global sales of recorded music down 10.9% in the first half of 2003. http://www.ifpi.org/site-content/press/20031001.html, 2003–10-01, Abruf am 2003-11-1.

[KaPe00] *Katzenbeisser, Stefan; Petitcolas, Fabien A. P.:* Information Hiding: Techniques for Steganography and Digital Watermarking, Artech House, Boston, London 2000.

[KöKS97] *Köhntopp, Marit; Köhntopp, Kristian; Seeger, Martin:* Sperrungen im Internet. In: Datenschutz und Datensicherheit 21 (1997) 11, S. 626–631.

[Lehn01] *Lehner, Franz:* Einführung in Multimedia. Gabler Verlag, Wiesbaden 2001.

[MoKa90] *Mori, Ryoichi; Kawahara, Masaji:* Superdistribution: The Concept and the Architecture. In: The Transactions of the IEICE 73 (1990) 7, S. 1133–1146.

[o.V.02] *O. V.:* XrML 2.0 Technical Overview. http://www.xrml.org/reference/XrMLTechnicalOverviewV1.pdf, 2002-03-08, Abruf am 2003-11-01.

[PfFK02] *Pfitzmann, Andreas; Federrath, Hannes; Kuhn, Markus:* Anforderungen an die gesetzliche Regulierung zum Schutz digitaler Inhalte unter Berücksichtigung der Effektivität technischer Schutzmechanismen. Studie im Auftrag des dmmv e.V. und des VPRT e.V., 2002.

[PiFi03] *Picot, Arnold; Fiedler, Marina (2003):* Impacts of DRM on Internet based Innovation. In: *Becker, Eberhard et al. (Hrsg.):* Digital Rights Management: Technological, Economic, and Legal and Political Aspects. Springer Verlag, Heidelberg 2003, S. 288–300.

[Prun03] *Pruneda, Andrea:* Using Windows Media Encoder to Protect Content. http://www.microsoft.com/windows/windowsmedia/howto/articles/ProtectContent.aspx, 2003-03-01, Abruf am 2003-11-01.

[Rawo02] *Rawolle, Joachim:* Content Management integrierter Medienprodukte – Ein XML-basierter Ansatz. Deutscher Universitätsverlag, Wiesbaden 2002.

[RoTM02] *Rosenblatt, Bill; Trippe, Bill; Mooney, Stephen:* Digital Rights Management: Business and Technology. M&T Books, New York 2002.

[SaSc03] *Sadeghi, Ahmad-Reza; Schneider, Markus:* Electronic Payment Systems. In: *Becker, Eberhard et al. (Hrsg.):* Digital Rights Management: Technological, Economic, and Legal and Political Aspects. Springer Verlag, Heidelberg 2003, S. 113–137.

[ScFi02] *Schoder, Detlef; Fischbach, Kai:* Peer-to-Peer. WIRTSCHAFTSINFORMATIK 44 (2002) 6, S. 587–589.

[ScHe02] *Schumann, Matthias; Hess, Thomas:* Grundfragen der Medienwirtschaft. 2. Aufl., Springer, Berlin 2002.

[Schn01] *Schneier, Bruce*: Secrets and Lies – IT-Sicherheit in einer vernetzten Welt. Wiley-VCH Verlag, Weinheim 2001.

[Stef96] *Stefik, Mark:* Letting Loose the Light: Igniting Commerce in Electronic Publication. In: *Stefik, Mark (Hrsg.):* Internet Dreams: Archetypes, Myths, and Metaphors. MIT Press, Cambridge 1996, S. 219–255.

[ÜnHe03] *Ünlü, Vural; Hess, Thomas:* The optimal level of technical copyright protection: A game-theoretic approach. In: Working Paper of the Institute of Information Systems and New Media at the Munich School of Management, Nr. 9/2003, Munich 2003.

[ÜRHF03] *Ünlü, Vural; Rauchfuß, Frank; Hess, Thomas; Faecks, Wolf-Ingomar:* Rechtemanagement als Lösungsansatz aus dem Digitalen Dilemma. Gemeinsame Studie der LMU München und Cap Gemini Telecom Media & Networks Dtl., München 2003.

[vWHe03] *von Walter, Benedikt; Hess, Thomas:* iTunes Music Store: Eine innovative Dienstleistung zur Durchsetzung von Property-Rights im Internet. WIRTSCHAFTSINFORMATIK 45 (2003) 5, S. 541–546.

[Wirt01] *Wirtz, Bernd W.:* Medien- und Internetmanagement. Gabler, Wiesbaden 2001.