arbido

2006/4 Elektronisches Publizieren – Informationsspezialisten als Mittler zwischen zwei Welten

Büttner Stephan,

Tags: loi droit d'auteur, audiovisuel,

Digital Rights Management und Co.: Wo bleibt der Nutzer zwischen DRM, Trusted Computing und gesetzlichem Rahmen?

Schon mal passiert? Sie gestalten eine Audio-CD zum Geburtstag eines Freundes. Dazu stellen Sie eine Kompilation aus Titeln gekaufter CDs und legal bei einem Musikportal erworbener Titel zusammen. Beim Brennen erhalten Sie eine Fehlermeldung: «„ Brennen nicht mo?glich. Ihre Lizenz ist abgelaufen. Bitte erneuern Sie Ihre Lizenz!“». Das ist ein durchaus typisches Szenario fu?r Digital Rights Management.

Digital Rights Management (DRM) sowie vertrauenswu?rdige Hard- und Software (Trusted Computing, TC) sind Themen, die seit einiger Zeit z.T. sehr kontrovers diskutiert werden. Insbesondere werden die Mechanismen des Digital Rights Management und des Trusted Computing oft miteinander vermischt und auf das Thema Kopierschutz reduziert. Der gesetzliche Rahmen, die Urheberrechtgesetze, werden davon wiederum isoliert wahrgenommen.

Tatsa?chlich besteht das eigentliche Problem, zumindest fu?r den Nutzer, aber in der Kombination von DRM-Mechanismen, hard- und softwarebasierten TC-Komponenten sowie den neuen Urheberrechtsgesetzen.

Dazu sei zuna?chst ein kurzer U?berblick u?ber die technischen Komponenten von DRM-Systemen sowie von TC gegeben.

Digital Rights Management

Eine allgemein gu?ltige und anerkannte Definition fu?r DRM gibt es z.Z. nicht. Allen Definitionsversuchen gemein ist, dass mit DRM die Rechte an digitalen Inhalten kontrolliert und verwaltet werden sollen.

Zwei der bekannteren Definitionen belegen dies.

Nach Bechtold[Bechtold, S. Vom Urheber- zum Informationsrecht. Implikationen des Digital Rights Management. C.H. Beck Vlg. 2002. – 458 S.] steht DRM «fu?r eine Vielzahl unterschiedlicher technischer und rechtlicher Pha?nomene, die alle miteinander zusammenha?ngen».

Kuhlmann/Gehring formulieren es a?hnlich als «eine Kombination aus Technologien, Rechtsvorschriften und Gescha?ftsmodellen zur Kontrolle und Verwertung von digitalen Informationsgu?tern»[Kuhlmann, D.; Gehring, A.; Trusted Platforms, DRM, and Beyond. In: Lecture Notes in Computer Science, Springer Berlin/ Heidelberg. – 2003.].

Es ist wichtig, zu betonen, dass es sich nicht um das Management digitaler Rechte handelt.

DRM und TC haben sehr wohl unterschiedliche inhaltliche Wurzeln und sind auch zeitlich unabha?ngig voneinander entstanden.

DRM im eigentlichen Sinne hat seine Wurzeln in den 1990er-Jahren und entstand im Gefolge des zunehmenden digitalen Vertriebs geistigen Eigentums. Urheber bzw. Verwerter suchten nach geeigneten Vertriebswegen und Gescha?ftsmodellen fu?r digitale Inhalte. Man kann verschiedene Generationen bei der Entwicklung der Kerntechniken von DRM unterscheiden.

Der *1. Generation* ging es im Wesentlichen um Fragen wie – IP-basierter Zugriffsschutz – Verschlu?sselungsverfahren

– Dabei wird zwischen symmetrischen und asymmetrischen Verfahren unterschieden.

– Bei den symmetrischen Verfahren werden sowohl die verschlu?sselten digitalen Inhalte als auch der Schlu?ssel zur Dechiffrierung an den Nutzer u?bertragen.

– Bei den asymmetrischen Verfahren werden je ein Verschlu?sselungsschlu?ssel und ein Entschlu?sselungsschlu?ssel generiert.

So wird DRM auch heute noch oft verstanden! Es ist jedoch weitaus mehr.

In der *2. Generation* kam dann die Objektidentifizierung hinzu, im Wesentlichen mit der Beschreibung und Identifizierung durch Metadaten.

- Nach der Art der Einbettung der Metadaten in die Medien wird unterschieden:

– Direkt im Datei-Vorspann wie bei Dublin Core Metadata Initiative,

– im Dokument verteilt wie bei den digitalen Wasserzeichen,

– in einer Metabeschreibungssprache wie die eXtensible rights Markup Language (XrML), eine Erweiterung des XML-Standards um Rechtebestimmungen,

– in einer Datenbank, mit der eine unabha?ngige Identifizierung des Nutzers mo?glich ist, wie beim digitalen Fingerabdruck oder der Seriennummerregistrierung.

Die *3. Generation* konnte dann sowohl den Zugriff kontrollieren als auch Informationen u?ber die Nutzung sammeln. Bei den hardwarebasierten DRM-Technologien werden die Endgera?te dahingehend gesichert, dass ein Abgreifen der digitalen Inhalte nicht mo?glich ist.

Beispiele sind:

– Dongles: kleine Hardwareadapter, die auf eine Schnittstelle des Computers gesteckt werden. In den Dongles befinden sich Schlu?ssel, ohne die kein Zugriff auf die digitalen Inhalte mo?glich ist.

– Smartcards: Karten, in denen ein beschreibbarer Chip integriert ist. Der Chip entha?lt Daten, ohne die kein Zugriff auf die digitalen Inhalte mo?glich ist. Anwendung finden Smartcards u.a. in Telefonkarten, Mobiltelefonen, Krankenversicherungskarten usw.

Die Hersteller versuchten sich auch mit softwarebasierten DRM-Systemen: Es bleibt jedoch (bisher) bei Stand-Alone-Lo?sungen (z.B. Real-Player, Windows Media Player).

Fu?r weiterfu?hrende Aussagen zu den DRM-Techniken s.u.a. bei Bu?ttner[Bu?ttner, St. Rechte und Vertrauen sichern: «Digital Rights Management und Trusted Computing». In: Handbuch Erfolgreiches Management von Bibliotheken und Informationseinrichtungen. Verlag Dasho?fer. 2004, Kap. 9.4.1.].

Bei den in der Praxis angewendeten DRM-Systemen sind meist mehrere Komponenten anzutreffen.

Fu?r den *Anwender* wichtige Komponenten und die dahinterstehenden Technologien zeigt *Tab. 1* (aus Bu?ttner, in Anlehnung an Bechtold).

DRM-Systemarchitektur

Das Spektrum der am Markt befindlichen DRM-Systeme ist weit – Registrierung, Lizenzierungen, Kopierschutz usw. Allen liegt jedoch eine a?hnliche DRM-Systemarchitektur zugrunde.

Die DRM-Systemarchitektur besteht aus drei Komponenten: Content-Server, Lizenz-Server und Nutzer.

1. Laden von digitalen Inhalten (Content-Package) durch den Nutzer. Der Container entha?lt das verschlu?sselte urheberrechtliche Werk sowie zusa?tzliche Informationen wie Lizenzbedingungen, Urheberangaben usw.

2. Aktivierung des DRM-Controller bei Aufruf der Datei (Abgleich mit den Nutzungsbedingungen).

3. U?bertragung der notwendigen Daten vom DRM-Controller zum Lizenz-Server.

4. Identifizierung des Nutzers vom Lizenz-Server.

5. Abgleich der Nutzungsrechte auf dem Lizenz-Server mit den vom Nutzer angeforderten.

6. Ggf. finanzielle Transaktion.

7. Erstellen einer personalisierten Lizenz vom Lizenz-Server

8. Lizenz wird an den Nutzer gesendet

9. Entschlu?sselung des digitalen Inhalts vom DRM-Controller, Freigabe der Wiedergabe an die gewu?nschte Anwendung und Kontrolle der in der Lizenz vereinbarten Nutzungsbedingungen.

10. Endgera?t startet die Wiedergabe.

Trusted Computing

Und was wird nun unter vertrauenswu?rdigen Systemen verstanden? Pearson[Pearson, S. Trusted Computing Platforms. Prentice Hall PTR, New York, 2003.] hat dazu formuliert: «A Trusted Platform is one containing a hardware-based subsystem devoted to maintaining trust and security between machines.»

Interessant ist die Betonung, dass es um die Sicherheit und das Vertrauen *zwischen* Maschinen gehe.

Das Bemu?hen um vertrauenswu?rdige Systeme ist nicht neu, sondern geht zuru?ck bis in die 1960er[1].

Gehring beschreibt TC wie folgt: «A tool for making the behaviour of computer systems more predictable, by enforcing rules on users and processes (i.e., mandatory access control), trusted computing creates ample opportunity for ruling out undesirable effects of software – and software users. At the same time it empowers parties controlling access to the rule-making process to forcing users to comply with their private interests, and to cut out competitors, when attempting to access, and use, system resources.» Gehring, R.A., 2006: Trusted computing for digital rights management. INDICARE Monitor, Vol. 2, No.12, February 2006; online verfu?gbar unter http://www.indicare.org/tiki-read_article.php?articleId=179, [2]

Hier wird sehr klar auf Regeln, Richtlinien gesetzt. Diese Regeln werden von den Anbietern (Hardware, Firmware und Software) gemacht.

Hinter vielen aktuellen TC-Anwendungen steht die Trusted Computing Group (TCG), ein Unternehmen, das 2003 aus der TCPA (Trusted Computer Platform Alliance) entstand. In diesem Unternehmen sind viele Hard- und Softwareunternehmen vereinigt wie AMD, Hewlett Packard, IBM, Intel, Microsoft, Sony und Sun. Das TCG-Konzept war zuna?chst hardwarebasiert. U.a. von Microsoft (MS) wurde das softwarebasierte Konzept, das «trustworthy computing» entwickelt.

Hardwarebasiertes Trusted Computing

Kernbausteine bei hardwarebasierten TC sind das TPM-Modul (Trusted Platform Modul) und das Core Root of Trust Measurement (CRTM)

– Das TPM ist ein spezieller Chip, der auf dem Mainboard eingebaut wird und eine *hardware* seitige Unterstu?tzung fu?r die Ver- und Entschlu?sselung darstellt und zur sicheren Abspeicherung von Passwo?rtern und Schlu?sseln dient. Das TPM entspricht einer Smartcard, ist jedoch nicht an einen konkreten Benutzer, sondern im Unterschied dazu fest an ein System gebunden.

– Das Core Root of Trust Measurement (CRTM) ist eine *BIOS-Erweiterung*.

Die Funktionsweise:

1. Bei Inbetriebnahme des PC ruft das BIOS das CRTM auf.

2. Das CRTM u?berpru?ft, ob das TPM aktiviert ist.

– Ist das TPM deaktiviert, wird der Bootvorgang «normal» fortgesetzt.

3. Ist das TPM aktiviert, wird die Rechnerkonfiguration analysiert.

4. Die Rechnerkonfiguration wird berechnet.

– Beim Aktivieren jeder Hard- oder Softwarekomponente wird ein Hash-Wert gebildet (Platform Configuration).

5. Sicherung eines Hash-Werts der Gesamtkonfiguration im TPM.

Im Ergebnis der positiven Pru?fung wird die Systemkonfiguration als vertrauenswu?rdig und sicher deklariert. Sollte der Hash-Wert vera?ndert sein, kann dies zum Betriebsabbruch des PC fu?hren.

Nach anhaltender Kritik kann der Anwender beide Komponenten deaktivieren, was zuna?chst nicht vorgesehen war (es geht um die Durchsetzung von Regeln des *Anbieters*!). Seit der Spezifikation 1.7 sind auch pseudonyme Nutzungsformen mo?glich.

Softwarebasiertes Trusted Computing

Microsoft (MS) arbeitet seit Jahren an einer softwarebasierten Sicherheitskomponente, die interessanterweise ihrerseits z.T. auf den TCG-Spezifikationen aufbaut. Im kommenden Betriebssystem VISTA ist von den jahrelangen Anku?ndigungen nicht sehr viel u?brig geblieben. Im Wesentlichen sind dies:

- User Account Protection (UAP)

- Die Anwendungen werden (im Normalfall) mit eingeschra?nkten Zugriffsrechten gestartet, d.h., den Anwendungen wird ein Schreibzugriff auf die Systemkonfiguration verwehrt – sie werden in einen Virtual Store im Windows-Verzeichnis umgeleitet. Damit ko?nnen Anwendungen keinen oder nur begrenzten Schaden anrichten. Letztlich ist dies ein Rudiment aus dem Compartment-Ansatz, dem Abschottungsprinzip von Microsoft (fu?r weiterfu?hrende Aussagen dazu

User Rights Management – die Lo?sung?

Wo bleibt nun der Nutzer, welchen Gestaltungsraum haben Bibliotheken und Informationseinrichtungen bei dem Zusammenwirken aller Komponenten?

Neben den schon teilweise dargelegten Problemen sind durchaus wesentliche Potenziale erkennbar.

Authentizita?t und Integrita?t

Die Gewa?hrleistung von Authentizita?t und Integrita?t digitaler Dokumente war bisher schon fu?r Bibliotheken und Informationseinrichtungen wichtig. Mit dem einsetzenden Paradigmenwechsel zu digitalen Medien wird dies jedoch essenziell.

Im Kontext der Entwicklung des Web 2.0, in dem das Netzwerk als Plattform agiert, sind webbasierte Anwendungen nur sinnvoll bzw. durchsetzbar, wenn Offenheit *und* Sicherheit, also die Vertrauenswu?rdigkeit, gewa?hrleistet ist. Gleiches gilt auch fu?r die weltweiten E-Science- oder Grid-Aktivita?ten.

Gemeinsame Ressourcenverwaltung, kollaboratives Arbeiten, Schaffung einer webbasierten publikationsunterstu?tzenden Infrastruktur basiert auf Offenheit, aber eben auch auf Vertrauenswu?rdigkeit.

Wahrung der Urheberrechte

Bibliotheken und Informationseinrichtungen treten zunehmend auch als Anbieter digitaler Inhalte auf, z.B. als Betreiber eines E-Verlages oder Preprint-Servers usw. Hier sind neue Mo?glichkeiten der Informationsbeschaffung und -bereitstellung, neue Vertriebsformen z.B. fu?r Audiodateien bereits im Einsatz.

Nutzerfreundliches Urheberrecht/User Rights Management

Die USA waren die Vorreiter bei der Anpassung des Urheberrechts an die Mo?glichkeiten, die digitale Medien ero?ffnen. Erinnert sei an den Digital Millennium Copyright Act[Digital Millenium Copyright Act H.R.2281. Online: http://thomas.loc.gov/cgi-bin/query/z?c105:H.R.2281.ENR:, (letzter Zugriff: 2.11.2006).].

Um hier einen Ausgleich, eine Balance «wieder» herzustellen, gibt es dort Bestrebungen, die Nutzerrechte zu sta?rken. So wurde z.B. 2003 und nochmals 2005 ein Digital Media Consumers' Rights Act (DMCRA) in das Repra?sentantenhaus eingebracht [3], (letzter Zugriff: 2.11.2006).. Ziel dieses Gesetzesentwurfs sei es: «to restore the ability of consumers to use copyrighted material lawfully» The Digital Media Consumers' Right Act of 2003, Hearing. H.R. 107, May 12, 2004, Serial No. 108–109..

In den EU-La?ndern ist der erste verpflichtende Korb der Novellierung des Urheberrechts im Rahmen der Umsetzung der EU-Richtlinie zum Urheberrecht in der Informationsgesellschaft in Kraft getreten. Z. Z. wird sehr intensiv um den zweiten Korb gerungen, also um die Regelungen, die den Mitgliedsstaaten u?berlassen wurden. Dabei geht es u.a. um:

– die o?ffentliche Zuga?nglichmachung fu?r Unterricht und Forschung,

– die Privatkopie,

– die Vergu?tung der Urheber usw.

In Deutschland setzt sich das Aktionsbu?ndnis «Urheberrecht fu?r Bildung und Wissenschaft» Aktionsbu?ndnis «Urheberrecht fu?r Bildung und Wissenschaft». Online: http://www.urheberrechtsbuendn.../, (letzter Zugriff: 2.11.2006). sehr aktiv dafu?r ein, dass das Urheberrecht nicht ausschliesslich zu einem Instrument der Kommerzialisierung von Wissen wird, insbesondere im Bildungs- und Wissenschaftsbereich.

Nach den vorliegenden Entwu?rfen soll es den Bibliotheken untersagt sein, elektronische Dokumente zu verteilen, wenn der Markt diese Dokumente ebenfalls anbietet, bzw. eine Bereitstellung digitaler Dokumente soll erst dann mo?glich sein, wenn kein kommerzielles Angebot vorliegt (§52a, §52b).

Grundlegende Voraussetzung wissenschaftlichen Arbeitens ist jedoch der freie und faire Zugang zu Wissen. Sollten diese wissenschaftsfeindlichen und innovationshinderlichen Gesetze tatsa?chlich in Kraft treten, wird Open Access so wichtig wie nie zuvor!

Es muss allerdings gefragt werden, ob Bibliotheken und Informationseinrichtungen dafu?r wirklich geru?stet sind?

Open Access wird zwar von den Bibliotheken unterstu?tzt, konnte sich aber bei den Wissenschaftlern noch nicht in breiter Front durchsetzen Deutsche Forschungsgemeinschaft: Publikationsstrategien im Wandel? Ergebnisse einer Umfrage zum Publikations- und Rezeptionsverhalten unter besonderer Beru?cksichtigung von Open Access Weinheim: Wiley-VCH, 2005..

Bibliotheken und Informationseinrichtungen sind deshalb gut beraten, sich diesem Aspekt wesentlich sta?rker als bisher zuzuwenden, insbesondere auch Marketing bei den Nutzern zu betreiben. Einzelne Forschungsorganisationen haben schon Vorarbeiten dazu gemacht (z.B. Helmholtz-Gemeinschaft Deutscher Forschungszentren). Diverse Diplomarbeiten zeugen auch von dem u?berdurchschnittlichem Interesse der Studierenden an dieser Problematik.

Literaturverzeichnis

– Aktionsbu?ndnis «Urheberrecht fu?r Bildung und Wissenschaft». Online: http://www.urheberrechtsbuendnis.de **(letzter Zugriff: 2.11.2006)**

– Bechtold, S. Vom Urheber- zum Informationsrecht. Implikationen des Digital Rights Management. C.H. Beck Vlg. 2002. 458 S.

– Bu?ttner, St. Rechte und Vertrauen sichern: «Digital Rights Management» und «Trusted Computing». In: Handbuch Erfolgreiches Management von Bibliotheken und Informationseinrichtungen. Verlag Dasho?fer. 2004, Kap. 9.4.1.

– Deutsche Forschungsgemeinschaft: Publikationsstrategien im Wandel? Ergebnisse einer Umfrage zum Publikations- und Rezeptionsverhalten unter besonderer Beru?cksichtigung von Open Access. Weinheim: Wiley-VCH, 2005

– The Digital Media Consumers' Right Act of 2003, Hearing. H.R. 107, May 12, 2004, Serial No. 108–109

– Digital Millennium Copyright Act H.R. 2281.Online: http://thomas.loc.gov/cgi-bin/query/z?c105:H.R.2281.ENR: **(letzter Zugriff: 2.11.2006)**

– Digital Media Consumers'Rights Act. Online: http://thomas.loc.gov/cgi-bin/query/D?c109:43:./temp/~c109ipDg9k: **(letzter Zugriff: 2.11.2006)**

– Gehring, R.A., 2006: Trusted computing for digital rights management. INDICARE Monitor, Vol. 2, No. 12, February 2006. Online: *http://www.indicare.org/tiki-r...*

– Himmelein, G. Baustelle Sicherheit-Microsoft krempelt seine Sicherheitsinitiative NGSCBum. In: c't 2004, Heft 12. – S. 43–46

– Kuhlmann, D.; Gehring, A.Trusted Platforms, DRM, and Beyond. In:Lecture Notes in Computer Science, Springer Berlin/Heidelberg. – 2003

– Mu?ller-Maguhn, M.Hundertprozentige Sicherheit durch TCG?Schutz vor wem In: Symposium «Trusted Computing Group» Berlin, 3.7.2003. Online: *http://ftp.gnumonks.org/pub/co...* (letzter Zugriff: 2.11.2006)

– Pearson, S. Trusted Computing Platforms. Prentice Hall PTR, New York, 2003

– Rosenblatt, W.; Trippe, W.; Mooney, S. Digital Rights Management: Business and Technology. John Wiley Vlg. – Chichester 2001. – 300 S.

– Seiler, M. Vista-Verschlu?sselung kein Allheilmittel, Computerwoche 2006, 21.

– The Trusted Computing Group (TCG): TCG Architecture Overview. Online: https://www.trusted-computinggroup.org/downloads/TCG_1_0_Architecture_Overview.pdf (letzter Zugriff: 30.10.2006)

1 s. Gehring, A.; Kuhlmann, D. (2003).

2 .

3 Digital Media Consumers' Rights Act. Online: http://thomas.loc.gov/cgi-bin/query/D?c109:43:./temp/~c109ipDg9k:

Stephan Büttner

Fachhochschule Potsdam Fachbereich Informationswissenschaften