Zeitschrift: Arbido

Herausgeber: Verein Schweizerischer Archivarinnen und Archivare; Bibliothek Information Schweiz

Band: - (2006)

Heft: 4: Elektronisches Publizieren - Informationsspezialisten als Mittler zwischen zwei Welten = Publication électronique - les spécialistes en information et documentation , médiateurs entre deux mondes = Pubblicazione elettronica - gli specialisti dell'informazione e della documentazione quali mediatori tra due mondi

Artikel: Digital rights management und Co. : wo bleibt der Nutzer zwischen DRM, Trusted computing und gesetzlichem Rahmen

Autor: Büttner, Stephan

DOI: https://doi.org/10.5169/seals-769677

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

Stephan Büttner
Fachhochschule Potsdam
Fachbereich Informationswissenschaften

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 möglich. Ihre Lizenz ist abgelaufen. Bitte erneuern Sie Ihre Lizenz!&#8220». Das ist ein durchaus typisches Szenario für Digital Rights Management.

Digital Rights Management (DRM) sowie vertrauenswürdige 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.

Tatsächlich besteht das eigentliche Problem, zumindest für den Nutzer, aber in der Kombination von DRM-Mechanismen, hard- und softwarebasierten TC-Komponenten sowie den neuen Urheberrechtsgesetzen.

Dazu sei zunächst ein kurzer Überblick über die technischen Komponenten von DRM-Systemen sowie von TC gegeben.

Digital Rights Management

Eine allgemein gültige und anerkannte Definition für 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[1] steht DRM «für eine Vielzahl unterschiedlicher technischer und rechtlicher Phänomene, die alle miteinander zusammenhängen».

Kuhlmann/Gehring formulieren es ähnlich als «eine Kombination aus Technologien, Rechtsvorschriften und Geschäftsmodellen zur Kontrolle und Verwertung von digitalen Informationsgütern»[2].

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 unabhängig 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 Geschäftsmodellen für 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
- Verschlüsselungsverfahren
  - Dabei wird zwischen symmetrischen und asymmetrischen Verfahren unterschieden.
    - Bei den symmetrischen Verfahren werden sowohl die verschlüsselten digitalen Inhalte als auch der Schlüssel zur Dechiffrierung an den Nutzer übertragen.
    - Bei den asymmetrischen Verfahren werden je ein Verschlüsselungsschlüssel und ein Entschlüsselungsschlüssel 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 unabhängige Identifizierung des Nutzers möglich ist, wie beim digitalen Fingerabdruck oder der Seriennummerregistrierung.

Die *3. Generation* konnte dann sowohl den Zugriff kontrollieren als auch Informationen über die Nutzung sammeln. Bei den hardwarebasierten DRM-Technologien werden die Endgeräte dahingehend gesichert, dass ein Abgreifen der digitalen Inhalte nicht möglich ist.

Beispiele sind:

- Dongles: kleine Hardwareadapter, die auf eine Schnittstelle des Computers gesteckt werden. In den Dongles befinden sich Schlüssel, ohne die kein Zugriff auf die digitalen Inhalte möglich ist.
- Smartcards: Karten, in denen ein beschreibbarer Chip integriert ist. Der Chip enthält Daten, ohne die kein Zugriff auf die digitalen In-

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

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

halte möglich 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-Lösungen (z.B. Real-Player, Windows Media Player).

Für weiterführende Aussagen zu den DRM-Techniken s.u.a. bei Büttner[3].

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

Für den *Anwender* wichtige Komponenten und die dahinterstehenden Technologien zeigt *Tab. 1* (aus Büttner, in Anlehnung an Bechtold).

DRM-Systemarchitektur

Das Spektrum der am Markt befindlichen DRM-Systeme ist weit – Registrierung, Lizenzierungen, Kopierschutz usw. Allen liegt jedoch eine ähnliche 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 enthält das verschlüsselte urheberrechtliche Werk sowie zusätzliche Informationen wie Lizenzbedingungen, Urheberangaben usw.
2. Aktivierung des DRM-Controller bei Aufruf der Datei (Abgleich mit den Nutzungsbedingungen).
3. Übertragung 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. Entschlüsselung des digitalen Inhalts vom DRM-Controller, Freigabe der Wiedergabe an die gewünschte Anwendung und Kontrolle der in der Lizenz vereinbarten Nutzungsbedingungen.
10. Endgerät startet die Wiedergabe.

Komponente	Kurzbeschreibung	Technologien (Beispiele)
Zugangs- und Nutzungskontrolle	Kontrolle des Zugangs zu den digitalen Inhalten und deren Nutzung	• Verschlüsselungsverfahren • Kopierkontrollsysteme • Passwortzugang
Schutz der Authentizität und Integrität	• Nachweis der Identität des Urhebers/Autors und der Echtheit des Datenmaterials (*Authentizität*) • Schutz vor unautorisierter Veränderung (*Integrität*)	• Digitale Signatur • Digitale Wasserzeichen
Identifizierung durch Metadaten	Dauerhafte Identifizierung und inhaltliche Beschreibung der • digitalen Inhalte und Rechteinhaber • Rechtespezifikationen • Nutzer	○ Dublin Core ○ Digitale Wasserzeichen ○ XrML ○ Digitaler Fingerabdruck ○ Seriennummerregistrierung
Manipulationssichere Hard- und Software	Manipulationssichere Ausstattung von Endgeräten und Anwendersoftware	• Hardware ○ Dongles ○ Smartcards • Software ○ Windows Media Player ○ Real One Player
Suchsysteme	Suche nach • bereits hergestellten illegalen Kopien digitaler Inhalte • veränderten Inhalten (*Integritätsverletzungen*) • Nutzerregistrierungen	• Digitale Wasserzeichen • Digitaler Fingerabdruck
Zahlungssysteme	Bezahlung für die Nutzung digitaler Inhalte ○ Preismodelle: Pay per use, Subskription	• Secure Electronic Transaction-System (SET) • Micropayment
Integrierte e-commerce Systeme	Unterstützung der Vertragsabwicklung • Vertragsanbahnung • Vertragsaushandlung • Bestellung • Rechnung	• Electronic Data Interchange (EDI) • XML-basierte Systeme

Tab. 1: Komponenten und Technologien im DRM (Büttner, 2004).

Trusted Computing

Und was wird nun unter vertrauenswürdigen Systemen verstanden? Pearson[4] 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 Bemühen um vertrauenswürdige Systeme ist nicht neu, sondern geht zurück bis in die 1960er[5].

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 compe-

3 Büttner, St. Rechte und Vertrauen sichern: «Digital Rights Management und Trusted Computing». In: Handbuch Erfolgreiches Management von Bibliotheken und Informationseinrichtungen. Verlag Dashöfer. 2004, Kap. 9.4.1.

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

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

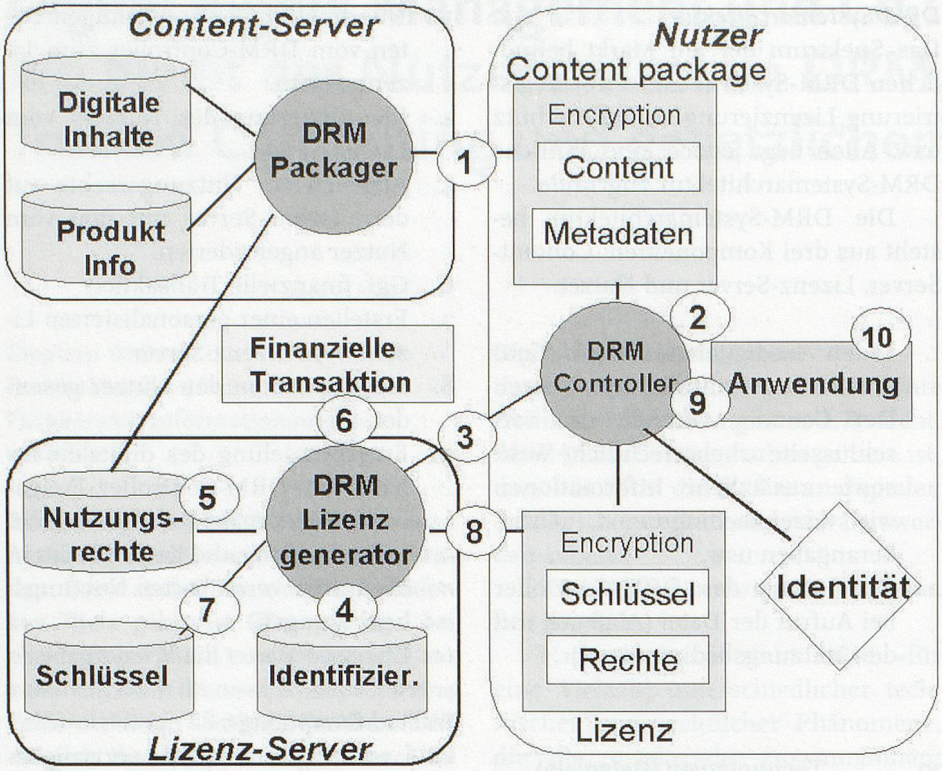

Abb. 1: DRM-Systemarchitektur (nach Rosenblatt; Trippe; Mooney)[6].

titors, when attempting to access, and use, system resources.»[7]

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 zunächst 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 Unterstützung für die Ver- und Entschlüsselung darstellt und zur sicheren Abspeicherung von Passwörtern und Schlüsseln 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 überprüft, 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 Prüfung wird die Systemkonfiguration als vertrauenswürdig und sicher deklariert. Sollte der Hash-Wert verändert sein, kann dies zum Betriebsabbruch des PC führen.

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

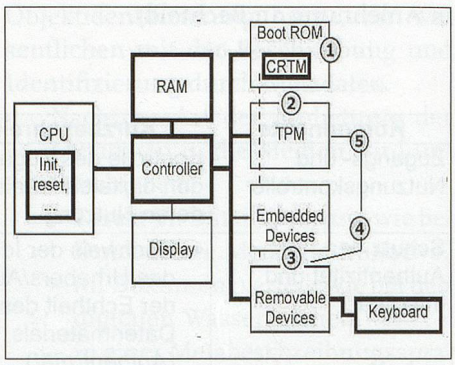

Abb. 2: Architektur des TC (bearbeitet nach der TCG-Specification, Rev 1.2[8]).

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 Ankündigungen nicht sehr viel übrig geblieben. Im Wesentlichen sind dies:

- User Account Protection (UAP)
  - Die Anwendungen werden (im Normalfall) mit eingeschränkten Zugriffsrechten gestartet, d.h., den Anwendungen wird ein Schreibzugriff auf die Systemkonfiguration verwehrt – sie werden in einen Virtual Store im Windows-Verzeichnis umgeleitet. Damit können Anwendungen keinen oder nur begrenzten Schaden anrichten. Letztlich ist dies ein Rudiment aus dem Compartment-Ansatz, dem Abschottungsprinzip von Microsoft (für weiterführende Aussagen dazu

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

7 Gehring, R.A., 2006: Trusted computing for digital rights management. INDICARE Monitor, Vol. 2, No.12, February 2006; online verfügbar unter *http://www.indicare.org/tiki-read_article.php?articleId=179*

8 The Trusted Computing Group (TCG): TCG Architecture Overview URL: *https://www.trustedcomputinggroup.org/downloads/TCG_1_0_Architecture_Overview.pdf* (letzter Zugriff: 30.10.2006)

s. z.B.[9]). Mit diesem, nun doch (noch?) nicht realisierten Ansatz wäre es möglich, dass nur proprietäre Anwendungen erlaubt wären – der Anbieter also bestimmt, mit welcher (lizenzierten) Anwendung eine (lizenzierte) Datei geöffnet wird.

- Secure Startup Full Volume Encryption
  - Mit dieser Technik wird das Verschlüsseln von Festplatten ermöglicht. Damit wäre ein verloren gegangener oder gestohlener PC bzw. eine Festplatte wertlos, da vor unberechtigtem Zugriff geschützt. Nach dem Start wird die Festplatte im Hintergrund verschlüsselt (wahlweise 128 oder 256 bit). Das Chiffrieren erfolgt über die dieser Technik zugrunde liegende Bitlocker-Software. Zusätzlich ist es für den Anwender möglich, den TPM-Chip zu aktivieren. Damit soll sichergestellt werden, dass nur berechtigte Personen auf das System zugreifen können[10].

Geht es also beim DRM-Konzept um die Durchsetzung von Rechten, bieten die TC-Ansätze die Fähigkeit, vom Anbieter vorgegebene Nutzungsrichtlinien, Regeln durchzusetzen.

Was zunächst zu unterschiedlicher Zeit und aus unterschiedlichen Beweggründen entwickelt wurde, kann im Zusammenspiel

TC + DRM + Recht

durchaus zum Problem werden. Die Hardware kontrolliert die Software. Die Software kontrolliert den Benutzer[11], und der Benutzer hat nur bedingt Zugriff auf die Schlüssel. Der rechtliche Rahmen, der z.Z. die Verwertungsinteressen der Informationswirtschaft in den Vordergrund stellt, «vollendet» diese Kombination zulasten der Nutzer.

User Rights Management – die Lösung?

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.

Authentizität und Integrität

Die Gewährleistung von Authentizität und Integrität digitaler Dokumente war bisher schon für Bibliotheken und Informationseinrichtungen wichtig. Mit dem einsetzenden Paradigmenwechsel zu digitalen Medien wird dies jedoch essenziell.

Die Hardware kontrolliert die Software. Die Software kontrolliert den Benutzer, und der Benutzer hat nur bedingt Zugriff auf die Schlüssel. Der rechtliche Rahmen, der z.Z. die Verwertungsinteressen der Informationswirtschaft in den Vordergrund stellt, «vollendet» diese Kombination zulasten der Nutzer.

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 Vertrauenswürdigkeit, gewährleistet ist. Gleiches gilt auch für die weltweiten E-Science- oder Grid-Aktivitäten.

Gemeinsame Ressourcenverwaltung, kollaboratives Arbeiten, Schaffung einer webbasierten publikationsunterstützenden Infrastruktur basiert auf Offenheit, aber eben auch auf Vertrauenswürdigkeit.

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 Möglichkeiten der Informationsbeschaffung und -bereitstellung, neue Vertriebsformen z.B. für Audiodateien bereits im Einsatz.

Nutzerfreundliches Urheberrecht/User Rights Management

Die USA waren die Vorreiter bei der Anpassung des Urheberrechts an die Möglichkeiten, die digitale Medien eröffnen. Erinnert sei an den Digital Millennium Copyright Act[12].

Um hier einen Ausgleich, eine Balance «wieder» herzustellen, gibt es dort Bestrebungen, die Nutzerrechte zu stärken. So wurde z.B. 2003 und nochmals 2005 ein Digital Media Consumers' Rights Act (DMCRA) in das Repräsentantenhaus eingebracht[13]. Ziel dieses Gesetzesentwurfs sei es: «to restore the ability of consumers to use copyrighted material lawfully»[14].

In den EU-Ländern 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 überlassen wurden. Dabei geht es u.a. um:

- die öffentliche Zugänglichmachung für Unterricht und Forschung,
- die Privatkopie,
- die Vergütung der Urheber usw.

In Deutschland setzt sich das Aktionsbündnis «Urheberrecht für Bildung und Wissenschaft»[15] sehr aktiv dafür ein, dass das Urheberrecht nicht ausschliesslich zu einem Instrument der Kommerzialisierung von Wissen wird, insbesondere im Bildungs- und Wissenschaftsbereich.

---

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

10 Seiler, M. Vista-Verschlüsselung kein Allheilmittel, Computerwoche 2006, 21

11 Müller-Maguhn, M. Hundertprozentige Sicherheit durch TCG? Schutz vor wem? In: Symposium «Trusted Computing Group» Berlin, 3.7.2003, online: *http://ftp.gnumonks.org/pub/congress-talks/tcg2003-berlin/day2/papers/02_huntertprozentige_it_sicherheit-ccc-maguhn.pdf* (letzter Zugriff: 2.11.2006)

12 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)

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

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

15 Aktionsbündnis «Urheberrecht für Bildung und Wissenschaft». Online: *http://www.urheberrechtsbuendnis.de/* (letzter Zugriff: 2.11.2006)

Nach den vorliegenden Entwürfen 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 möglich 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 tatsächlich in Kraft treten, wird Open Access so wichtig wie nie zuvor!

Es muss allerdings gefragt werden, ob Bibliotheken und Informationseinrichtungen dafür wirklich gerüstet sind?

Open Access wird zwar von den Bibliotheken unterstützt, konnte sich aber bei den Wissenschaftlern noch nicht in breiter Front durchsetzen[16].

Die Gewährleistung von Authentizität und Integrität digitaler Dokumente war bisher schon für Bibliotheken und Informationseinrichtungen wichtig. Mit dem einsetzenden Paradigmenwechsel zu digitalen Medien wird dies jedoch essenziell.

Bibliotheken und Informationseinrichtungen sind deshalb gut beraten, sich diesem Aspekt wesentlich stärker als bisher zuzuwenden, insbesondere

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

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 überdurchschnittlichem Interesse der Studierenden an dieser Problematik.

contact:
st.buettner@fh-potsdam.de
http://www.fh-potsdam.de/~buettner

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

Literaturverzeichnis

- Aktionsbündnis «Urheberrecht für 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.
- Büttner, St. Rechte und Vertrauen sichern: «Digital Rights Management» und «Trusted Computing». In: Handbuch Erfolgreiches Management von Bibliotheken und Informationseinrichtungen. Verlag Dashöfer. 2004, Kap. 9.4.1.
- Deutsche Forschungsgemeinschaft: Publikationsstrategien im Wandel? Ergebnisse einer Umfrage zum Publikations- und Rezeptionsverhalten unter besonderer Berücksichtigung 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-read_article.php?articleId=179*
- Himmelein, G. Baustelle Sicherheit – Microsoft krempelt seine Sicherheitsinitiative NGSCB um. 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
- Müller-Maguhn, M. Hundertprozentige Sicherheit durch TCG? Schutz vor wem? In: Symposium «Trusted Computing Group» Berlin, 3.7.2003. Online: *http://ftp.gnumonks.org/pub/congress-talks/tcg2003-berlin/day2/papers/02_hundertprozentige_it_sicherheit-ccc-maguhn.pdf* (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-Verschlüsselung kein Allheilmittel, Computerwoche 2006, 21.
- The Trusted Computing Group (TCG): TCG Architecture Overview. Online: *https://www.trustedcomputinggroup.org/downloads/TCG_1_0_Architecture_Overview.pdf* (letzter Zugriff: 30.10.2006)