Karl-Heinz Rödiger

Fachbereich 3
Mathematik/Informatik

Über die Folgen eines durchgängigen DRM für Bildung und Wissenschaft

Hamburg, den 24. November 2006

Universität Bremen

Architektur eines DRMS

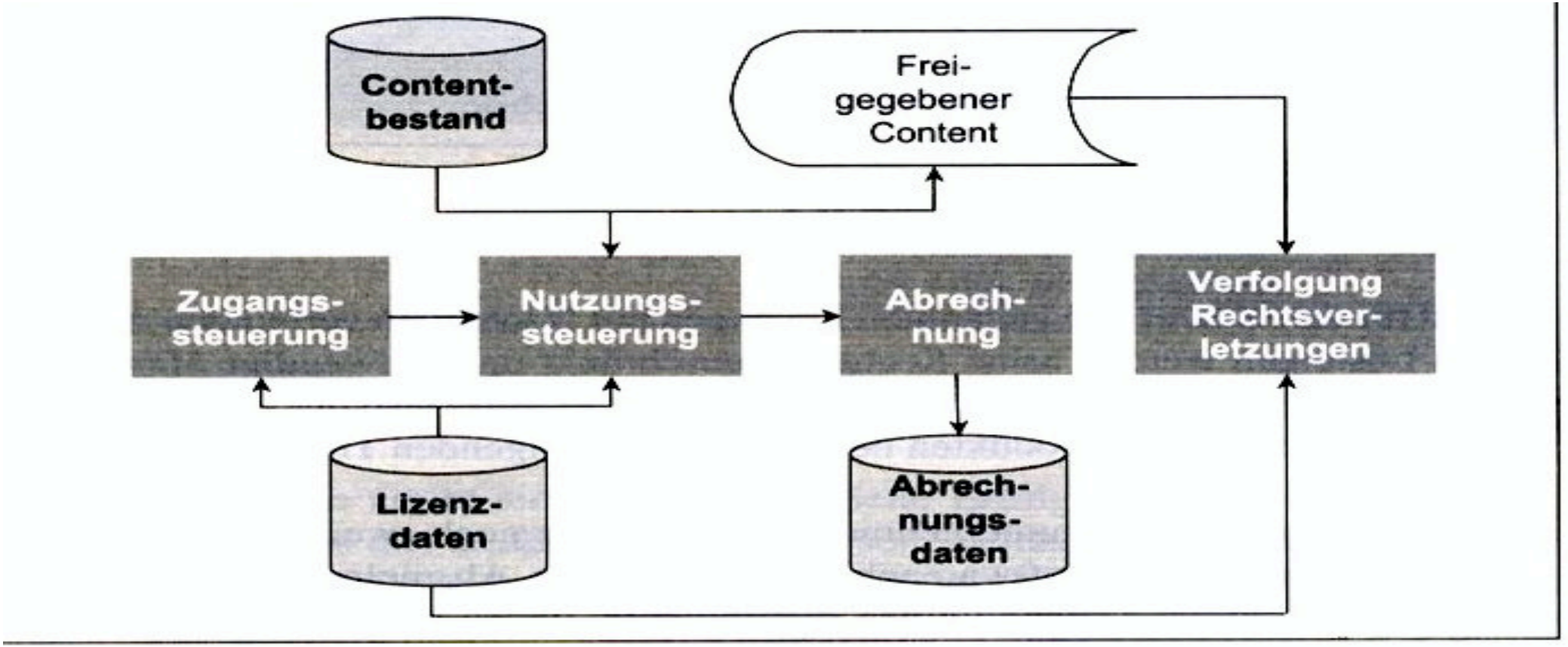


Bild 6: Architektur von DRMS (Vgl. Hess / Ünlü (2004))

Digital Rights Management (DRM)

„DRM bezeichnet den Einsatz der zur Verfügung stehenden Mittel durch Rechteinhaber zum Schutz geistigen Eigentums im digitalen Format“ (Arlt 2006).

DRM hat

- ökonomische
- juristische
- technische Aspekte

Digital-Rights-Management-Systeme (DRMS)

Anwendungssysteme zur Administration, Durchsetzung, zum Vertrieb und zur Abrechnung von Lizenzrechten

Funktionen

- Zugangssteuerung
- Nutzungssteuerung
- Nutzungsabrechnung
- Nutzungskontrolle

Digital-Rights-Management-Systeme (DRMS)

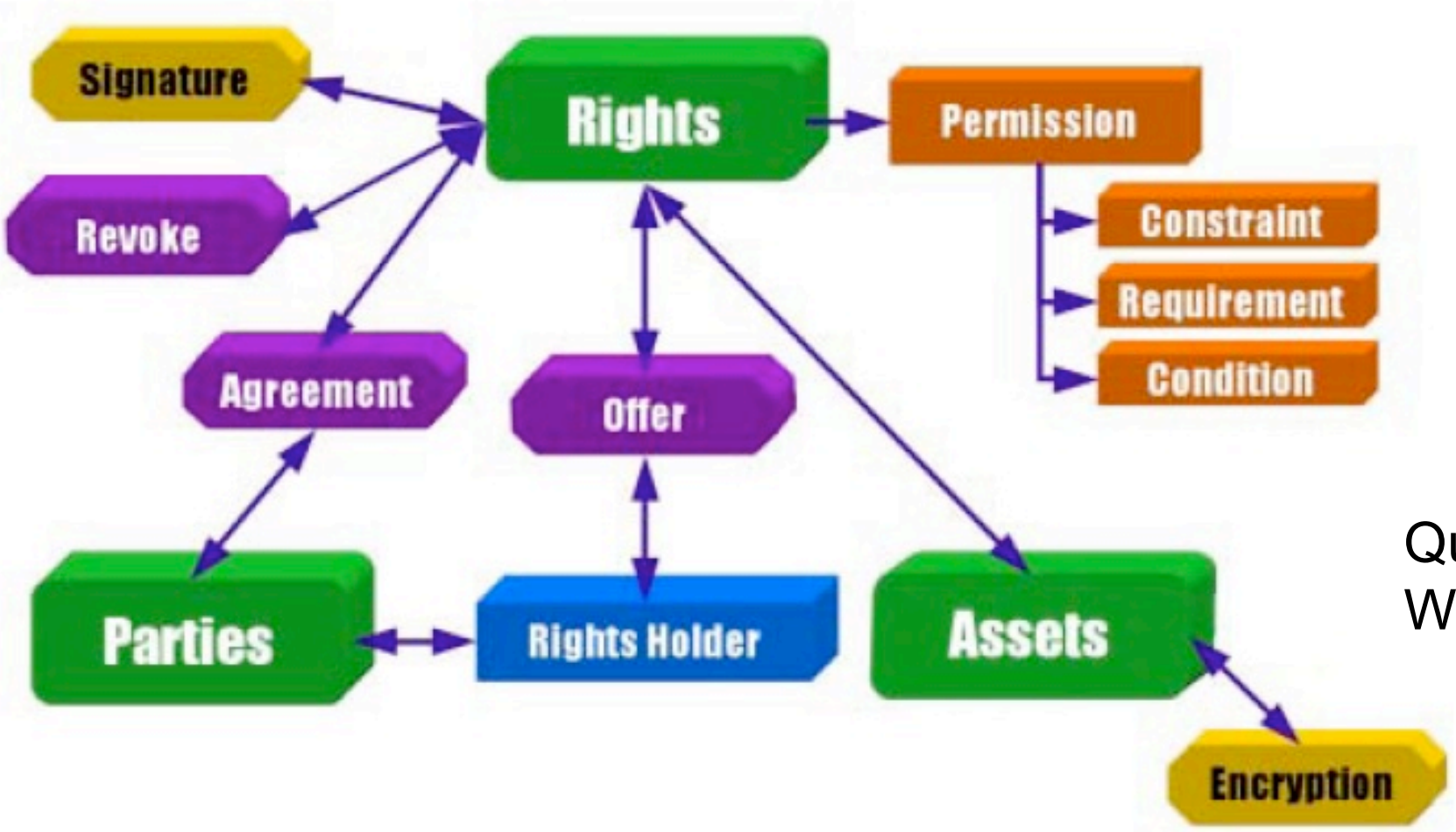
Techniken

Verschlüsselung: kryptografische Verfahren

Digitale Wasserzeichen: (Un-)sichtbare Wz., digitaler Fingerabdruck

Rechtedefinitionssprachen: MPEG21-REL, ODRL, XrML

Open Digital Rights Language (ODRL)



Quelle:
W3C

Open Digital Rights Language (ODRL)

Permission: Angebote und Vereinbarungen bez. Assets

Constraint: Rechtebeschränkung z.B. Wiedergabegerät

Requirement: Voraussetzungen für die Berechtigung

Condition: Bedingungen für den Entzug der Berechtigung

Offer: Vom Rights Holder eingeräumte besondere Rechte

Agreement: Vereinbarung über besondere Rechte

Context: Metainformationen zum Asset („Vermögenswert“)

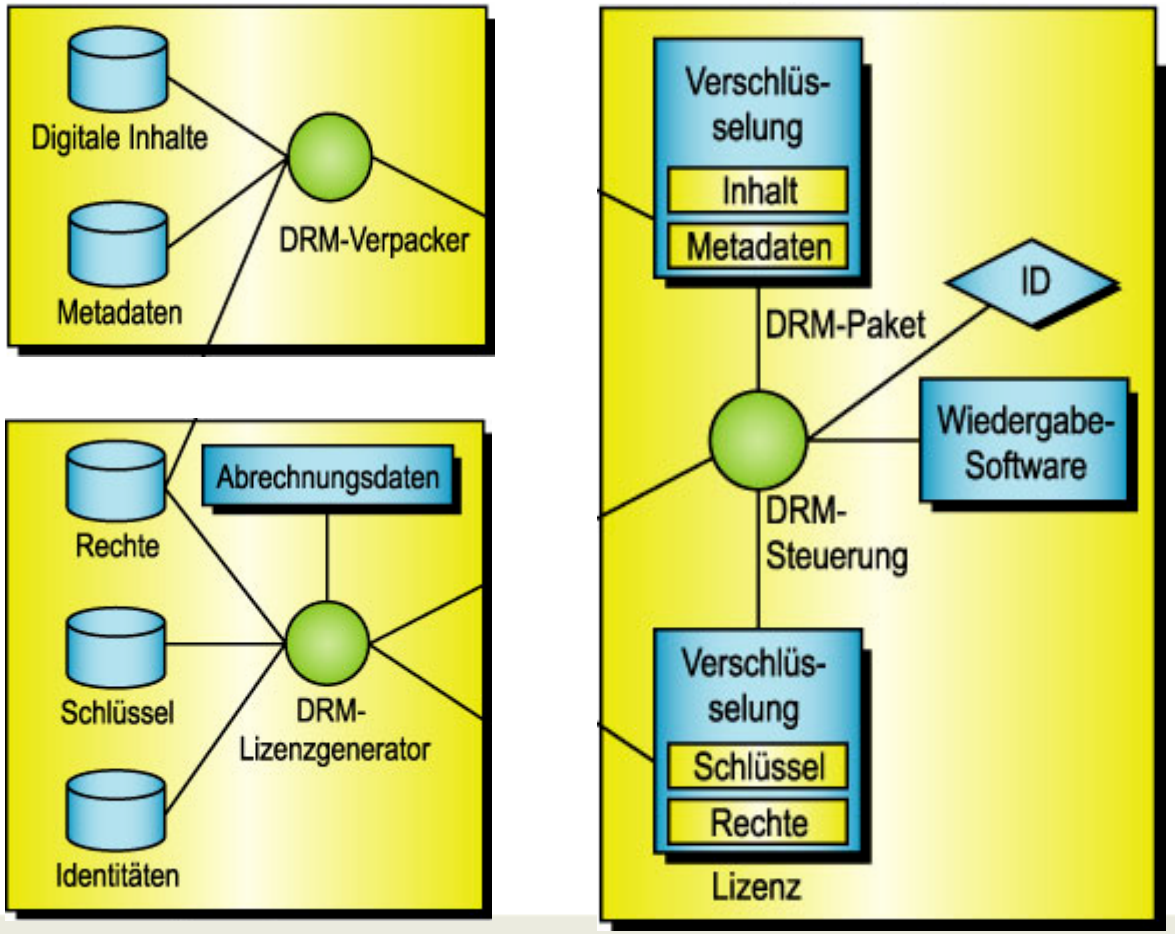
Revoke: Rückruf

Security: Digitale Signatur, Schlüssel

Architektur eines DRMS

Content-Server

Lizenz-Server



Client

Architektur eines DRMS

Der Content-Server verwaltet die zu schützenden digitalen Inhalte und verschlüsselt diese mit Hilfe des DRM-Verpackers.

Die DRM-Steuerung ermittelt die Benutzererkennung und fordert vom Lizenz-Server notwendige Lizenz an.

Der Lizenz-Server erzeugt aus den Identitäten und Rechtebeschreibungen die entsprechenden Lizenzen, zusammen mit den zugehörigen Schlüsseln für die Benutzer-Authentifizierung und Content-Entschlüsselung.

Digital-Rights-Management-Systeme (DRMS)

Funktionen und DRMS-Techniken

- Zugangssteuerung: Zugriffsfilter, Authentifizierung, Verschlüsselung
- Nutzungssteuerung: Rechtedefinitionssprachen, Verschlüsselung
- Nutzungsabrechnung: Rechtedefinitionssprachen
- Nutzungskontrolle: Digitale Wasserzeichen, Rechtedefinitionssprachen

Digital-Rights-Management-Systeme (DRMS)

Nutzungssteuerung

- Wiedergaberecht: ansehen, abspielen, drucken
- Transportrecht: kopieren, ausleihen, weitergeben
- Recht, Derivate zu erstellen: extrahieren, editieren, einfügen

DRMS

werden derzeit hauptsächlich bei Filmen oder Musik eingesetzt.

- **Windows Media DRM von Microsoft**
  verwenden viele Online-Shops wie Musicload.

- **OMA DRM der Open Mobile Alliance**
  wird von Mobilfunkanbietern für Klingeltöne, Bilder sowie für mobile Musik- und Fernsehübertragungen eingesetzt.

- **FairPlay von Apple**
  für iTunes

Digital Rights Management (DRM)

Umstritten, wegen

- Eingriffs in Verbraucherrechte (Privatkopie, Regionen-Code)
- Eingriffs in Datenschutzrechte (Lizenzierung, Digitaler Fingerabdruck)

Schwachpunkt

- Schlüssel in Reichweite von Benutzern, Entschlüsselung im Prozessor eines PC (Bspl. CSS; Ähnliches ist bei HDDVD und Blu-Ray-Disk zu erwarten)

„Knacken“ eines Schlüssels ist verboten.

DRM: Digital Restriction Management, Digitale Rechte-Minimierung

Trusted Computing (TC)

Basis: Trusted Platform Module (TPM),
kryptografischer Koprozessor

Zuständig für

- kryptografische Verfahren
- sichere Speicherung von Schlüsseln

Vielfach schon in Laptops vorhanden,
bislang kaum von Software genutzt.

Windows Vista setzt Teile der TC-Spezifikation um.

Trusted Computing (TC)

TC-Betriebssysteme können

- Programme und Daten an eine Hardware binden;
- die Ausführung fremder Software verhindern.

Folge:

- Kontrollverlust
- Einschränkung der Interoperabilität
- Verletzung des Datenschutzes
- Realisierung von DRM

Trusted Computing (TC)

Offiziell: Schutz vor Viren und anderer Schadsoftware

Real: Sicherung der Interessen von Content-Anbietern

Folgen von DRM und TC

Content-Anbieter können Rechte durchsetzen und verfolgen (Wasserzeichen, Revocation)

Bildung und Wissenschaft werden in ihrer Arbeit behindert:

- kompliziertere Nutzung
  --> Installation eines DRMS, Mittelbeschaffung, Bezahlung

- Elektronische Leseplätze
  --> Beschränkung mittels DRM durchsetzbar

- Privatkopie
  --> Verbot qua Gesetz

Folgen von DRM und TC

- Schutzfristen
  --> Was passiert nach Auslaufen von Schutzfristen?

- Archivierung
  --> Das DRMS muss ggf. mit archiviert werden.

- Nachhaltigkeit
  --> Wer stellt sicher, dass DRM Geschütztes noch benutzt werden kann, wenn der Anbieter nicht mehr existiert?

- Datenschutz
  --> Wer schützt die Daten, die der Lizenzserver sammelt?

„Originale brauchen Kopien“

Positionspapier der
Gesellschaft für Informatik e.V. (GI)
zur Novellierung des Urheberrechts

http://www.gi-ev.de/fileadmin/redaktion/Download/GI-Position_Urheberrecht2006.pdf

7 Forderungen der GI

1 DRM und TC

Kein Einsatz von DRM und TC bei rechtmäßig erworbenen Inhalten

2 Open Access

Anerkennung des Rechts auf Informationsfreiheit, Bekenntnis zum Prinzip des offenen Zugangs

3 Zugang zu Literatur

Entfristung des § 52a, elektronischer Zugriff von allen Arbeitsplätzen auf die Bibliotheksbestände, Erhalt von Subito

7 Forderungen der GI

4 Privatkopie

Recht auf Privatkopie auch bei technisch geschütztem Inhalt

... und als Denkanstoß: Urheberumlage

Umlage abhängig von der Online-Übertragungsrate, Einzug und Verteilung durch eine Verwertungsgesellschaft

7 Forderungen der GI

1 Digital Rights Management (DRM) und Trusted Computing (TC)

Auch wenn DRM und TC gegenwärtig weitgehend wirkungslos sind, dürfen diese Techniken nicht dazu eingesetzt werden, die private und bibliothekarische Nutzung rechtmäßig erworbener Inhalte zu behindern. Archivierung, Herstellung von Interoperabilität auch mit Open Source-Systemen oder beispielsweise die Privatkopie einer Audio-CD zur Nutzung im PKW erfordern oft den Bruch eines Kopier- oder Abspielschutzes.

7 Forderungen der GI

DRM und TC (Forts.)

Mittels DRM geschützte Inhalte müssen daher per Gesetz analog zu ungeschützten Inhalten zur Nutzung freigegeben werden, auch wenn dazu gegebenenfalls ein DRM gebrochen werden muss. Andererseits soll es weiterhin verboten bleiben, urheberrechtlich geschütztes Material über Tauschbörsen zu verbreiten, unabhängig davon, ob dafür eine Schutzmaßnahme umgangen wurde.