
DRM-Techniken und ihre Grenzen

Rüdiger Grimm

Technische Universität und

Fraunhofer-Institut für Digitale Medientechnologie IDMT

Ilmenau

„DRM – Distribution u. Schutz digitaler Medien-Information“
Fachkonferenz Münchner Kreis

München, 22. April 2004



Fraunhofer
Institut
Digitale
Medientechnologie



Technische
Universität
Ilmenau

DRM-Techniken und ihre Grenzen

Überblick

- Rechte und ihre Durchsetzung
- Exkursion: Technische DRM Ansätze
- Das Dilemma: Interessenkonflikt zwischen Anbieter und Nutzer
- LWDRM
 - Grundidee
 - Eigenschaften
- Weitere Alternativen: Anreizsysteme „Potato“
- Zusammenfassung

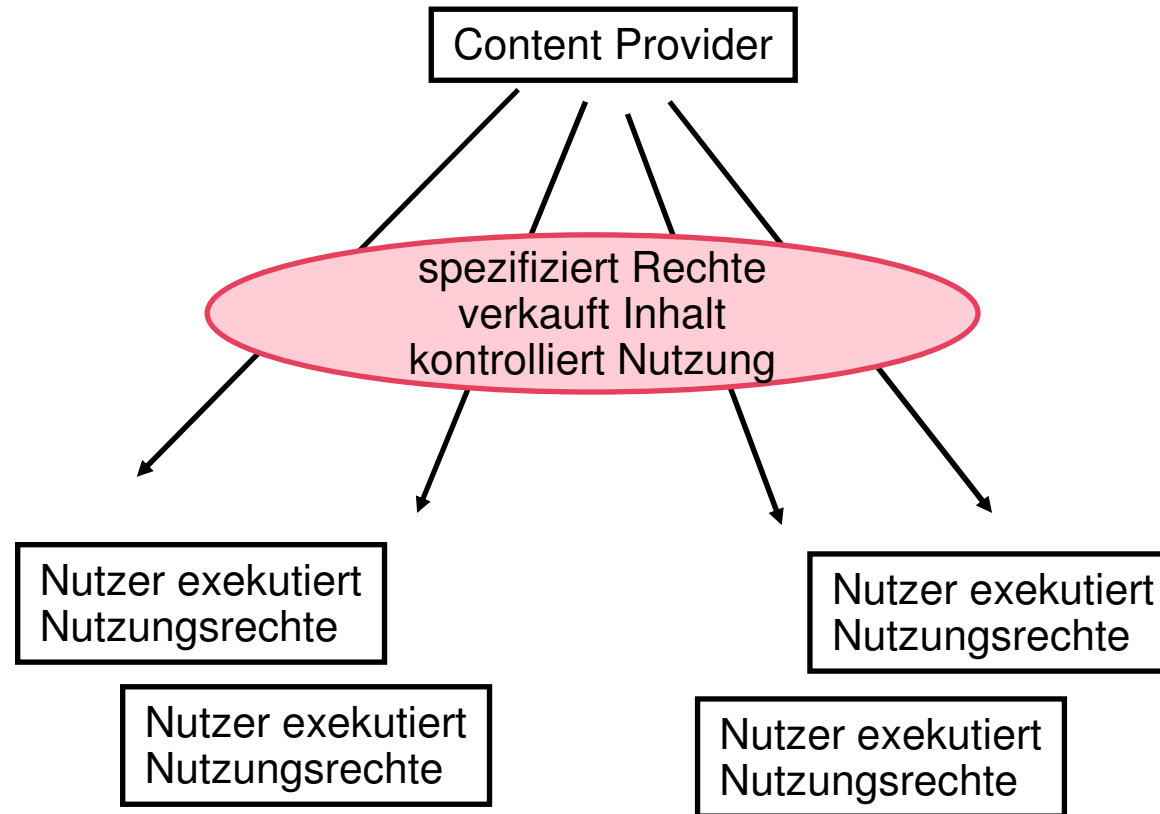


DRM-Techniken und ihre Grenzen

- Rechte und ihre Durchsetzung
- Exkursion: Technische DRM Ansätze
- Das Dilemma: Interessenkonflikt zwischen Anbieter und Nutzer
- LWDRM
 - Grundidee
 - Eigenschaften
- Weitere Alternativen: Anreizsysteme „Potato“
- Zusammenfassung

DRM-Techniken und ihre Grenzen

Rechte und Durchsetzung



DRM-Techniken und ihre Grenzen

Rechte und Nutzungsregeln

- Rechte im Medienformat codiert
- Rechte als „Nutzungsregeln“ im Endgerät exekutiert

- Kopierschutz
- Nutzungsbegrenzung

- Qualitätseinbuße (Kopien, Pre-Listening)
- Anzahl Kopien (Weitergabe)
- Anzahl Abspielen (Zahl)
- Nutzungszeit (Zeit)
- Nutzungsumgebung (Raum)

DRM-Techniken und ihre Grenzen

High-level model DRM

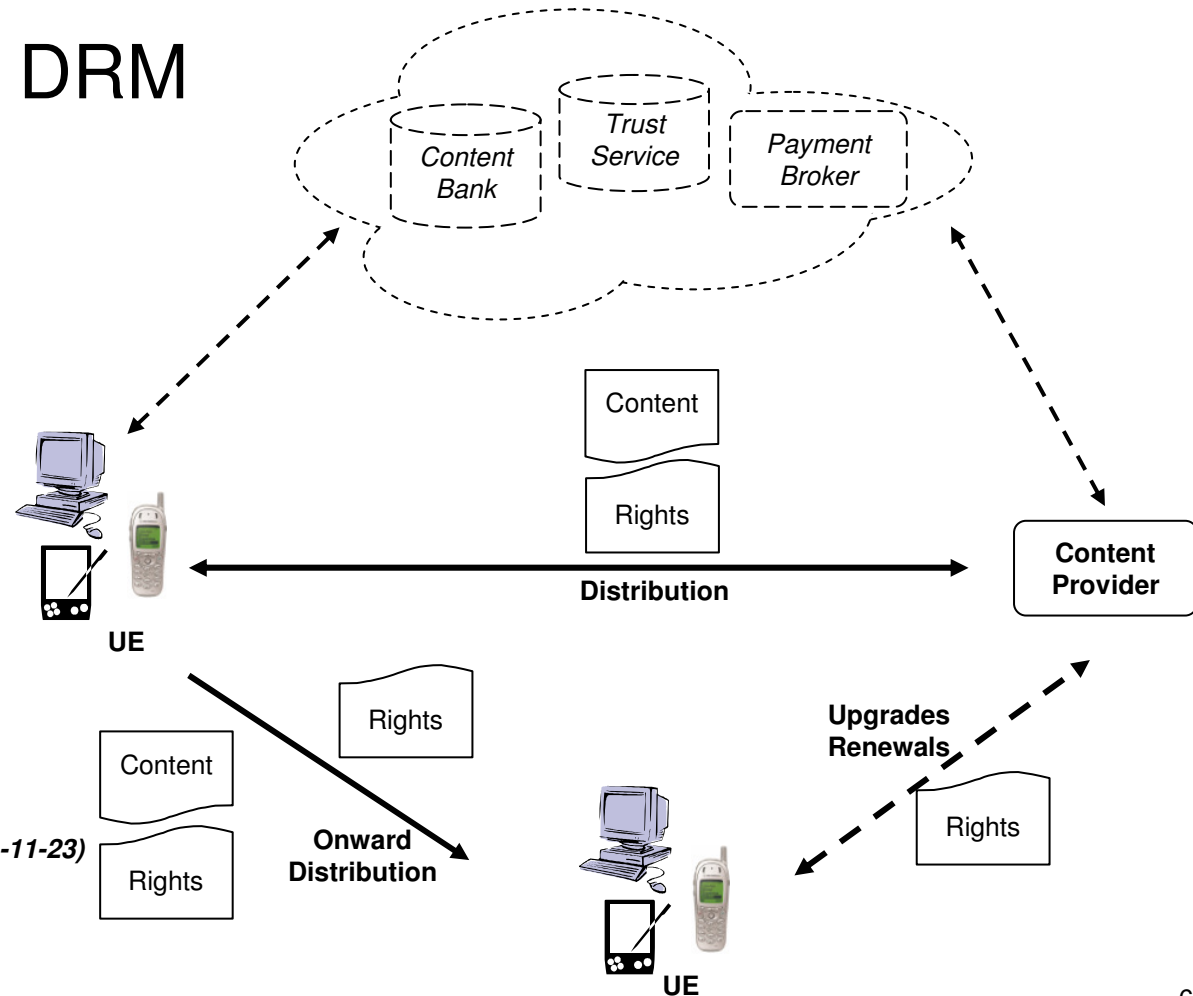


Figure 1, page 7 in: 3GPP S1-01 1197 V0.0.0 (2001-11-23)
Proposed Stage 1, Release 6, Nov 2001

DRM-Techniken und ihre Grenzen

- Rechte und ihre Durchsetzung
- **Exkursion: Technische DRM Ansätze**
- Das Dilemma: Interessenkonflikt zwischen Anbieter und Nutzer
- LWDRM
 - Grundidee
 - Eigenschaften
- Weitere Alternativen: Anreizsysteme „Potato“
- Zusammenfassung



DRM-Techniken und ihre Grenzen

Ausgangslage: keine einheitliche DRM-Technologie

- Kein dominanter **Anbieter**
 - MS, RealNetworks, IBM/EMMS, Apple/iTunes, etc...
- Uneinheitliche **Medienformate**
 - MP3, WAV, AIF, MPEG-1/2/4/7/21, etc...
 - HTML, PDF, GIF, TIFF, JPEG, etc...
 - RealAudio, RealVideo, Windows Media, QuickTime 4, etc...
- Proprietäre DRM-**Metadata**
- *Vgl. dagegen:*
 - **Betriebssysteme:** Windows/Linux/Macintosh
 - **Kommunikation:** TCP/IP, HTTP
 - **Hyperfiles Präsentation:** HTML/Netscape/IE

8 / 24



DRM-Techniken und ihre Grenzen

Standardisierbare Bereiche

- Nicht standardisierbar:
 - Wasserzeichen
 - technische Komponenten (z.B. DRM controllers)
- Standardisierbar:
 - Protokolle
 - Dateiformate (bereits misslungen)
 - Metadaten (z.B. Content Ids, Rechte)
 - Encryption

DRM-Techniken und ihre Grenzen

Standards (Beispiele)

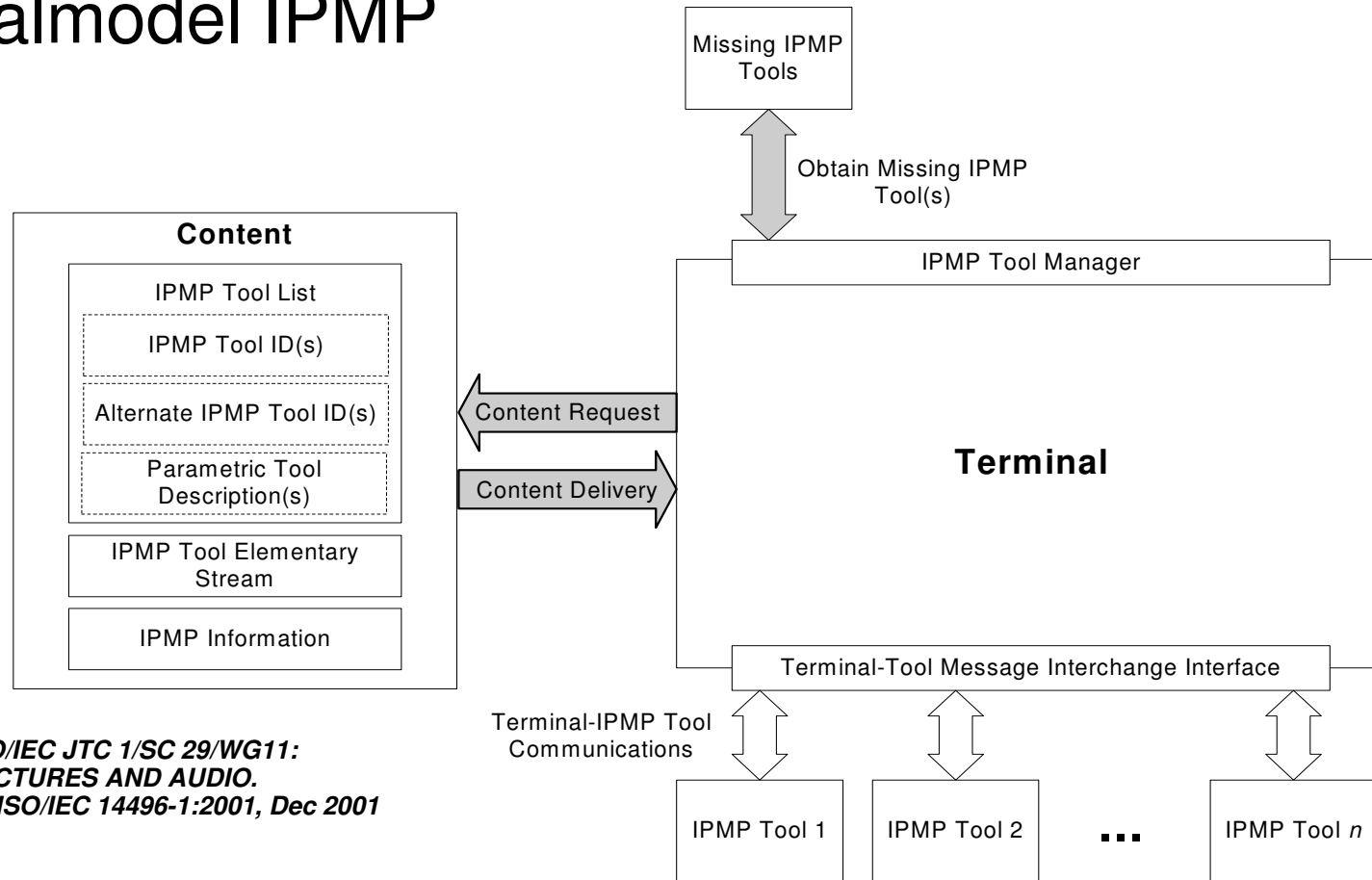
- Identifikation: ISBN, DOI
- Publisher-Publisher Protocol ICE
 - Vignette Corp., Murdoch Internet News Services
- Metadata Rights Spec Languages: XrML, ODRL, ...
 - XrML: Mark Stafik, Xerox Parc, MS, aber Patent-geschützt
 - XCML: RealNetworks and Anti-MS, aber keine Implementierung
 - ODRL: Australia/Pacific Rim, aber kein Einfluss
- DRM Modell, Technologie: SDMI
 - RIAA, „Big 5“, alle Technology Companies
 - nicht PC, Players, LWM (licensed compliant module), Watermarks
 - zerbrochen an Konflikten unter den Teilnehmern
- DRM Modell, Technologie: IPMP
 - MPEG-Model (Intertrust, Optibase)

10 / 24



DRM-Techniken und ihre Grenzen

Terminalmodel IPMP



*IPMP Ad-hoc Group, ISO/IEC JTC 1/SC 29/WG11:
CODING OF MOVING PICTURES AND AUDIO.
Study of Text of PDAM ISO/IEC 14496-1:2001, Dec 2001*

DRM-Techniken und ihre Grenzen

- Rechte und ihre Durchsetzung
- Exkursion: Technische DRM Ansätze
- **Das Dilemma: Interessenkonflikt zwischen Anbieter und Nutzer**
- LWDRM
 - Grundidee
 - Eigenschaften
- Weitere Alternativen: Anreizsysteme „Potato“
- Zusammenfassung

DRM-Techniken und ihre Grenzen

Interessen versus Durchsetzung

- Contentprovider haben Interesse an Rechtedurchsetzung
- Contentprovider formulieren Rechte (Policies)
- Rechte schränken Nutzung ein

- *Last der Durchsetzung bei Nutzern*

- Nutzer haben Interesse an Private Use
- Nutzer umgehen Rechte

Möglichkeiten der Rechtedurchsetzung

Nutzer verhalten sich rechtmäßig aufgrund

1. Technische Durchsetzung:

- Nutzer *können nicht* anders

2. Identifizierbarkeit, Verfolgbarkeit

- Nutzer *trauen sich nicht* anders
- Fehlverhalten bringt Nachteile / Wohlverhalten lohnt sich

3. Anreize

- Nutzer *wollen* es nicht anders
- Wohlverhalten lohnt sich

DRM-Techniken und ihre Grenzen

- Rechte und ihre Durchsetzung
- Exkursion: Technische DRM Ansätze
- Das Dilemma: Interessenkonflikt zwischen Anbieter und Nutzer
- **LWDRM**
- Weitere Alternativen: Anreizsysteme „Potato“
- Zusammenfassung

DRM-Techniken und ihre Grenzen

LWDRM[®] - Grundidee

- Ziele
 - Benutzerinteressen wahren (Fair-Use, Privacy)
 - Kein Klartext beim User (Inhalte verschlüsseln)
 - Bei Missbrauch Nachverfolgbarkeit ermöglichen

Grundidee

- Ein Kunde darf Inhalte veröffentlichen, wenn er bereit ist, diese digital zu signieren
- Ansonsten werden die Inhalte lokal an das Abspielgerät gebunden

DRM-Techniken und ihre Grenzen

LWDRM Eigenschaften

Local
Media File

- Nach Download ist Content mit lokalem Schlüssel verschlüsselt an Endgerät gebunden

Signed
Media File

- Nach Wahl des Nutzers kann er LMF befreien, indem er es signiert

Sicherheit/
Privacy

- Zertifikat enthält pseudonymisierte Benutzerinformationen
- Zertifikat enthält Schlüssel zum Entschlüsseln
- SMF kann frei kopiert und transferiert werden
- Indem man SMF konsumiert, verifiziert man seine Herkunft

17 / 24

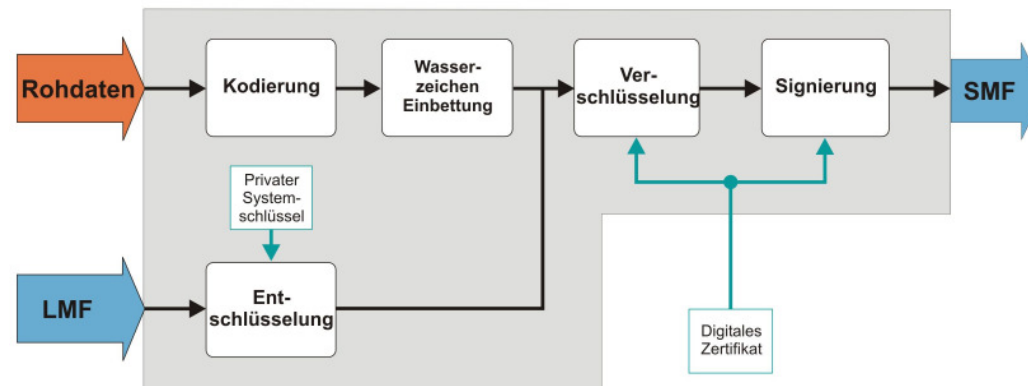


DRM-Techniken und ihre Grenzen

Profile von LWDRM[®] (3)

Signing Profile

- Erzeugung von Inhalten des signierten Formats
- Umwandlung des lokalen Formats in das signierte Format (evtl. Erwerb einer Lizenz notwendig)
- Registrierung bei einer Zertifizierungsstelle notwendig, da Zertifikat benötigt wird
- Wiedergabe auf allen Abspielgeräten möglich



DRM-Techniken und ihre Grenzen

- Rechte und ihre Durchsetzung
- Exkursion: Technische DRM Ansätze
- Das Dilemma: Interessenkonflikt zwischen Anbieter und Nutzer
- LWDRM
- **Weitere Alternativen: Anreizsysteme „Potato“**
- Zusammenfassung

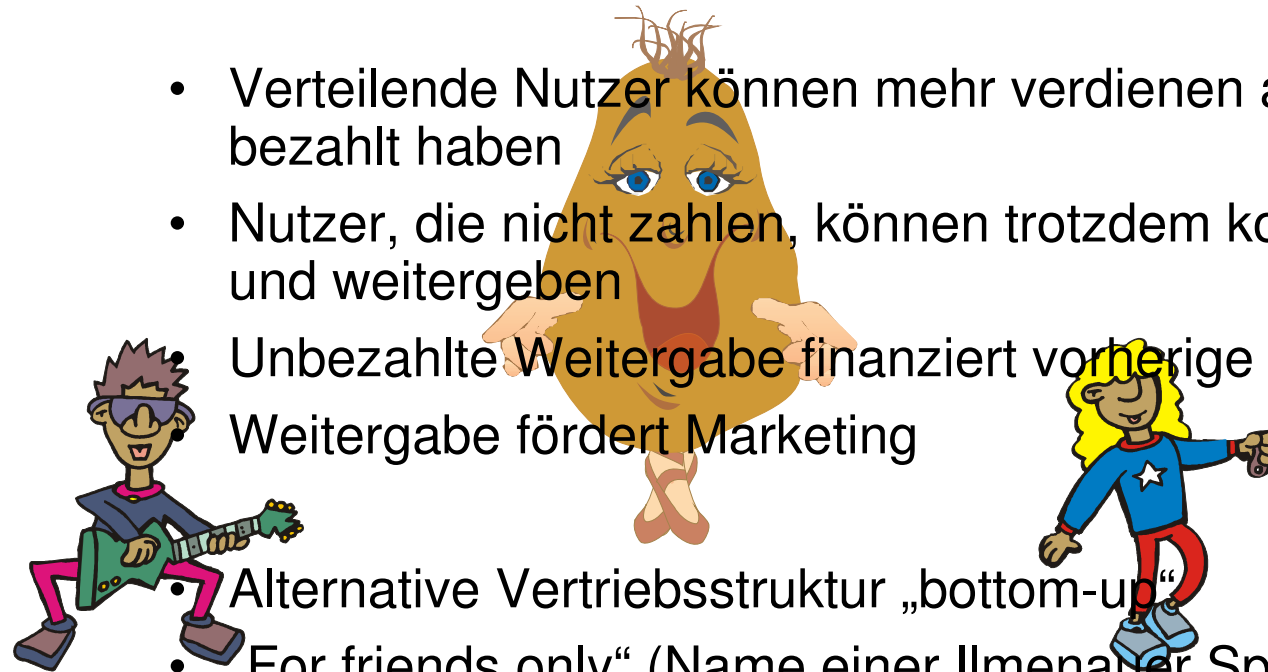
DRM-Techniken und ihre Grenzen

Anreize

- Provision
 - Nutzer verdienen mit
- Services
 - Nutzer bekommen mehr:
 - Cover, Infos, Alben
 - „vom Radio/Konzert/Kneipe zum Album“
- Qualität
- Community
 - Nutzer bekommen Kontakt zu anderen Nutzern (Matching Service)

DRM-Techniken und ihre Grenzen

Potato – „Pretty Good Distribution“

- 
- Verteilende Nutzer können mehr verdienen als sie bezahlt haben
 - Nutzer, die nicht zahlen, können trotzdem konsumieren und weitergeben
 - Unbezahlte Weitergabe finanziert vorherige Zahler
 - Weitergabe fördert Marketing
 - Alternative Vertriebsstruktur „bottom-up“
 - „For friends only“ (Name einer Ilmenauer Spin-off-Firma mit vergleichbaren Ideen für Spiele, Lernmodule)
 - Open Source in www.4fo.de

21 / 24

DRM-Techniken und ihre Grenzen

Potato-Anwendungen

- Musikmarketing
- Junge Musik
- Musiksendungen im Radio
- Konferenzliteratur (Autoren wollen Verteilungsrechte behalten)
- Levels in Spielen mit verteilten Autoren

- Testphase mit GEMA und lokalen Providern
- www.potatosystem.com

22 / 24



Fraunhofer
Institut
Digitale
Medientechnologie



Technische
Universität
Ilmenau

ruediger.grimm@tu-ilmenau.de
22. April 2004

DRM-Techniken und ihre Grenzen

Zusammenfassung

- Klassische DRM Systeme nur Teil-Lösung:
 - sichere (?) aber eingeschränkte Nutzung
 - Konflikt zwischen Anbieter und Nutzer zerstört Vertrauen in Markt
- Alternativen zur technischen Durchsetzung:
 - Fair Use unterstützen
- LWDRM:
 - Verantwortung der Nutzer
- Potato:
 - Anreize für Nutzer

DRM-Techniken und ihre Grenzen

Vielen Dank für Ihre Aufmerksamkeit!

**Fragen ?
Diskussion!**

