

Digital Rights Management (DRM)

Verfahren, die helfen Rechte an virtuellen Waren durchzusetzen

**Vorlesung im Wintersemester 2011/12 an der
Technischen Universität Ilmenau von
Privatdozent Dr.-Ing. habil. Jürgen Nützel,
Vorstand der 4FriendsOnly.com Internet Technologies AG (4FO AG)
JN (at) 4FO (dot) DE**



Motivation und Überblick

***Diese Folien dienen der Einführung in die Vorlesung.
Weitere Folien liefern ergänzende/vertiefende Informationen.
Die Vorlesung richtet sich an Studierende der Informatik,
der Ingenieurinformatik, Wirtschaftsinformatik, Medienwirtschaft
Angewandten Medienwissenschaft und Medientechnik.***

Diese Folien und weitere Informationen unter: www.juergen-nuetzel.de/drm_lecture.html

Der Dozent Jürgen Nützel



- **Geb. 1967 in Schweinfurt, verheiratet, 2 Kinder**
- **Historie**
 - *Promotion 1999, Habilitation 2006*
 - *Privatdozent für Informatik (seit 2006)*
 - *Mitgründer und Vorstand der 4FO AG (seit 2000)*
- **4FO AG (4FriendsOnly AG), www.4FO.de**
 - *Ausgründung der TU Ilmenau und Fraunhofer IDMT*
 - *Implementierungspartner der Intershop AG*
 - *Betreiber der MP3-Download-Plattform www.PotatoSystem.com (zusammen mit Fraunhofer)*
 - *Betreiber des Internet-Bezahlsystems www.Paybest.de*
 - *OMA DRM 2.0 Implementierung mit Fraunhofer IIS*
 - *E-Commerce-Software-Entwicklung (Implementationspartner der Intershop AG)*
 - *Entwicklung von Apps für iPhone, Android ...*

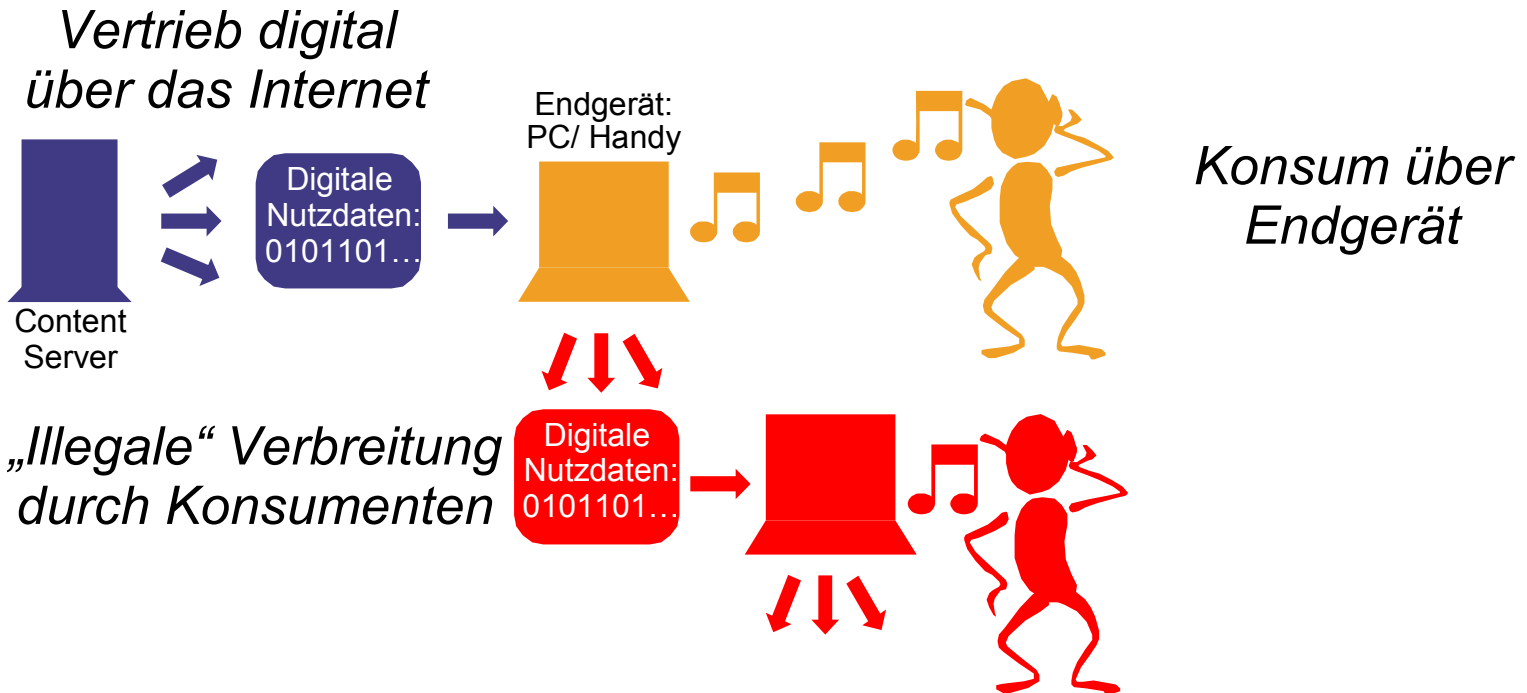
Lernziele



- ***Bedeutung digitalisierter virtueller Waren***
- ***Die technische Hintergründe***
 - *Aufwand und Nutzen*
 - *Folgen der DRM Technik*
- ***Die ökonomischen und rechtlichen Rahmenbedingungen***
 - *Nicht alles ist erlaubt bzw. sinnvoll*
- ***Konkrete DRM Systeme verstehen und anwenden***
 - *DRM Systeme anwenden*
 - *DRM Systeme umsetzen*
- ***Alternative Ansätze kennenlernen***

Motivation – Virtuelle Waren

□ Beispiel: Musik-Download

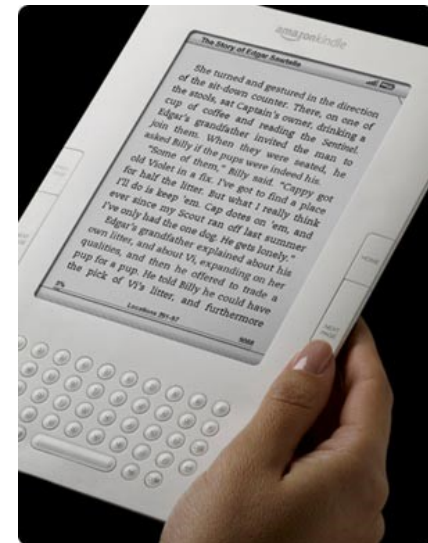


- ***Auch der Konsument kann die Ware verteilen***
- ***Die Anbieter fürchten daher um ihre Geschäftsmodelle (Free-Rider-Problem)***

Motivation – Neue Geräte



- **Neuartige Mobiltelefone**
 - Einsatz mehrerer DRM Systeme
 - Z.B. Nokia Serie 60 Reihe (ca. 2006)
- **Oder: iPhone**
 - DRM für Musik, Video und Software
- **Apples iPad**
 - In-App-Payment
 - DRM in jeder App möglich
- **Amazons Kindle**
 - E-Books, E-Paper

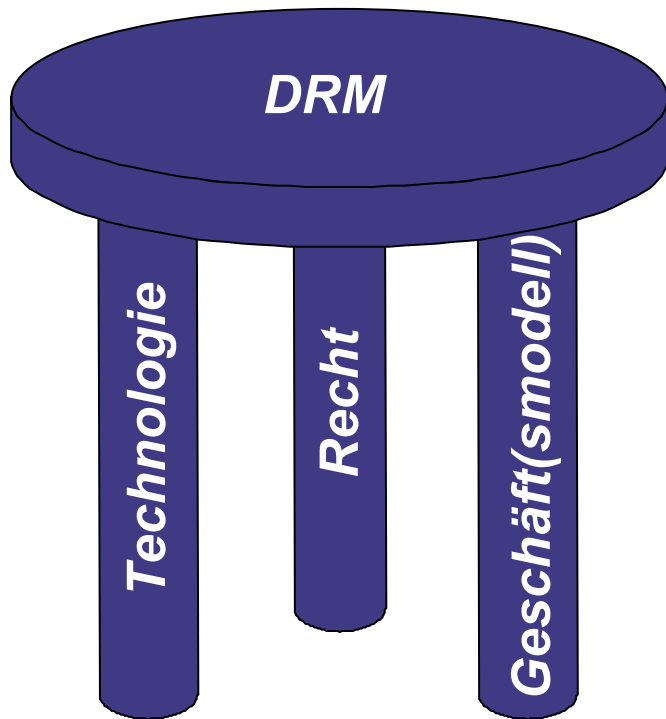


Weitere Termine

- 2. Unterschiedliche Sichten und Definitionen**
- 3. Wirtschaftliche und rechtliche Aspekte**
- 4. Technische Grundprinzipien**
- 5. Rechte und ihre formale Notation**
- 6. Public-Key-Kryptographie (in 2 Teilen)**
- 7.**
- 8. DRM-Referenz-Modell**
- 9. Windows Media DRM, Apple & andere**
- 10. Open Mobile Alliance (OMA) DRM Standard 2.0**
- 11. Wasserzeichen und Fingerprinting**
- 12. Wiederholung, Zusammenfassung und Vertiefung**
- 13. Klausur**

Unterschiedliche Sichten & Definitionen

2. Vorlesung



- *Virtuelle Waren und ihre „Probleme“*
- *DRM ist nicht nur Technik*
- *DRM ist nicht gleich Kopierschutz*
- *Es gibt keine einheitliche Definition für DRM*
- *Positive und negative Sicht auf DRM*

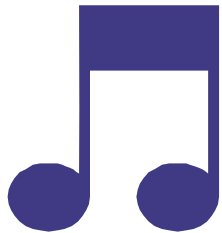
3. Vorlesung

- *Öffentliche versus private Güter*
- *Unterschiedliche Erlösmodelle*
- *Alte und neue Geschäftsmodelle*
- *Urheberrecht im Wandel der Zeit*



Technische Grundprinzipien

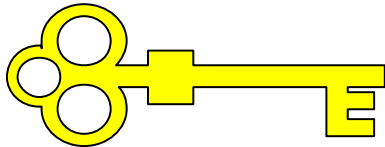
4. Vorlesung



=

0110
1110
1010

- *Verschlüsselung der Nutzdaten*
- *Symmetrische Verschlüsselung*
- *Kontrolle des Schlüssels CEK auf dem Endgerät*
- *Lizenzen mit Rechten und Schlüssel*
- *Sichere Speicherung der Lizenzen*



=

0111
0011
1110

Rechte und ihre formale Definition

5. Vorlesung

„Dieses Stück darf dreimal
abgespielt werden“



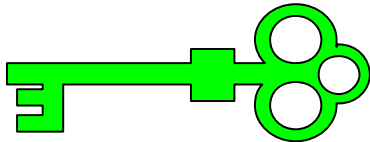
- **Nutzungsrechte**
- **Mögliche Nutzungsrechte**
- **Spezieller Geschäftsmodelle**
- **Rechtebeschreibungssprachen**
- **MPEG-21, ODRL, XrML**

```
<o-ex:permission>  
  <o-dd:play>  
    <o-ex:constraint>  
      <o-dd:count>3</o-dd:count>  
    </o-ex:constraint>  
  </o-dd:play>  
</o-ex:permission>
```

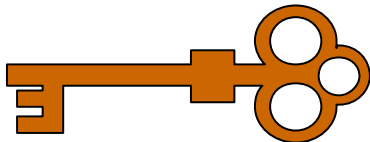
Public-Key-Kryptographie

6. Vorlesung (in 2 Teilen)

Public Key



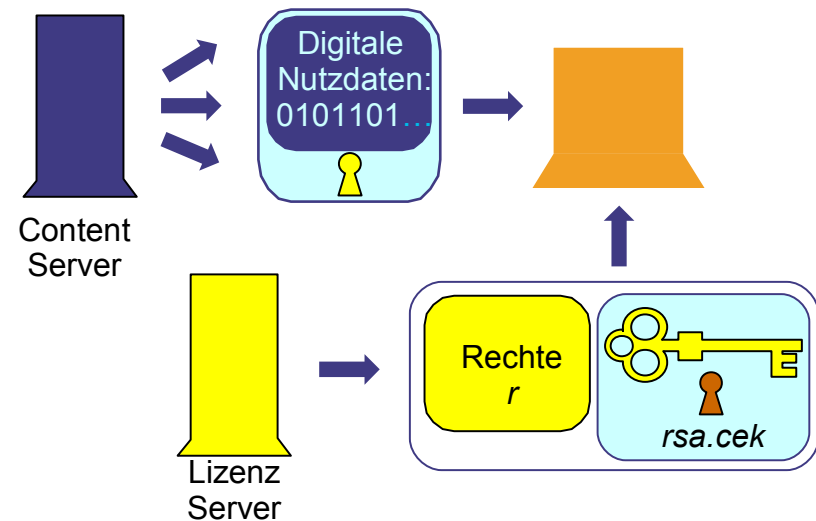
Private Key



- *Anwendungen (bei DRM)*
- *Geheime Übertragung des CEK*
- *Zertifikate*
- *Digitale Signatur*
- *Hash-Funktion*
- *RSA-Verfahren*

DRM-Referenz-Modell

7. Vorlesung



- Grundsätzlicher Aufbau eines DRM-Systems der 2. Generation
- Lizenz-Server (Rights Issuer)
- Content-Server
- DRM Agent (im Endgerät)
- Typische Abläufe

Windows Media, Apple & andere Systeme

8. Vorlesung



- *Windows Media Rights Manager*
- *Amazons Kindle*
- *Mögliche Geschäftsmodelle*
- *Apple's FairPlay in iTunes*
 - *DRM weiterhin für Filme?*
 - *Auch im iPhone und iPad für Software*
 - *Mit In-App-Payment DRM für alle neuen Inhalte?*
- *HD+*

Open Mobile Alliance (OMA) DRM 2.0

9. Vorlesung



- www.openmobilealliance.org
- *Offener Standard in der Version 2.0*
- *DCF – DRM Content Format*
- *ROAP – Rights Object Acquisition Protocol*
- *Rechte Objekte*
- *Domains*
- *Superdistribution*
- *BCAST*

Wasserzeichen-Verfahren und Fingerprinting-Technologien

10. Vorlesung

- ***Was steckt hinter den Wasserzeichen-Verfahren***
- ***Illegale Verbreitung nicht verhindern aber erkennen können.***
- ***Welche Möglichkeiten bietet die Fingerprinting-Technologie***
- ***Black-List Systeme für Online-Plattformen***

Weitere Informationen

- **Wikipedia zu DRM:**
http://en.wikipedia.org/wiki/Digital_rights_management
- **OMA DRM Standard Version 2.0:**
www.openmobilealliance.org/Technical/release_program/drm_v2_0.aspx
- **Microsoft Windows Media DRM:**
windows.microsoft.com/de-DE/windows-vista/Windows-Media-Player-DRM-frequently-asked-questions
- **Wikipedia zu Kindle:** http://en.wikipedia.org/wiki/Amazon_Kindle
- **Wikipedia zu Apple's FairPlay DRM:**
<http://en.wikipedia.org/wiki/FairPlay>
- **Rosenblatt, Trippe, Mooney: Digital Rights Management, 2001, John Wiley & Sons**
- **Jürgen Nützel: Die informatorischen Aspekte virtueller Güter und Waren, Oktober 2006 im Universitätsverlag Ilmenau, www.juergen-nuetzel.de/habilitation.html**