Digital Rights Management (DRM)

Verfahren, die helfen Rechte an virtuellen Waren durchzusetzen

**Vorlesung im Sommersemester 2010 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**

Rechte und ihre formale Notation

***Folien stellen ein zusätzliches Informationsangebot für die Teilnehmer der Vorlesung dar.
Die Vorlesung richtet sich an Studierende der Informatik,
der Ingenieurinformatik, Wirtschaftsinformatik, Medienwirtschaft,
Angewandten Medienwissenschaft und Medientechnik.***

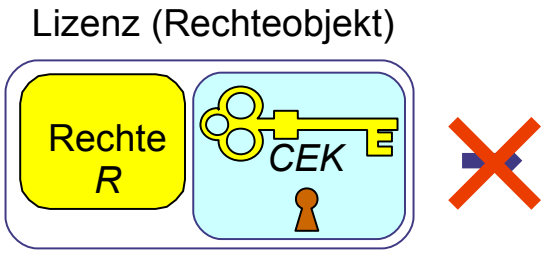
Diese Folien und weitere Informationen unter: www.juergen-nuetzel.de/drm_lecture.html

Überblick

- **Nutzungsrechte**
- **Mögliche Nutzungsrechte**
- **Spezielle Geschäftsmodelle**
- **Rechtebeschreibungssprachen**
- **Stammbau der Rechtebeschreibungssprachen**
- **MPEG-21**
- **Beispiel: ODRL**

Lizenzen (oder Rechteobjekte)

- **Lizenzen enthalten den Schlüssel und eine Rechtebeschreibung**



  - ***Verschlüsselte Nutzdaten sind ohne Lizenz wertlos***
  - ***Rechtebeschreibung legt die zulässige Nutzungsart (abspielen) und Nutzungsdauer (3 mal) fest***
  - ***Verschlüsselte Nutzdaten können und sollen kopiert werden***
  - ***Lizenzen sind an das Endgerät gebunden (Weitergabe unmöglich oder wirkungslos)***

Rechte und Rechtebeschreibung [1]

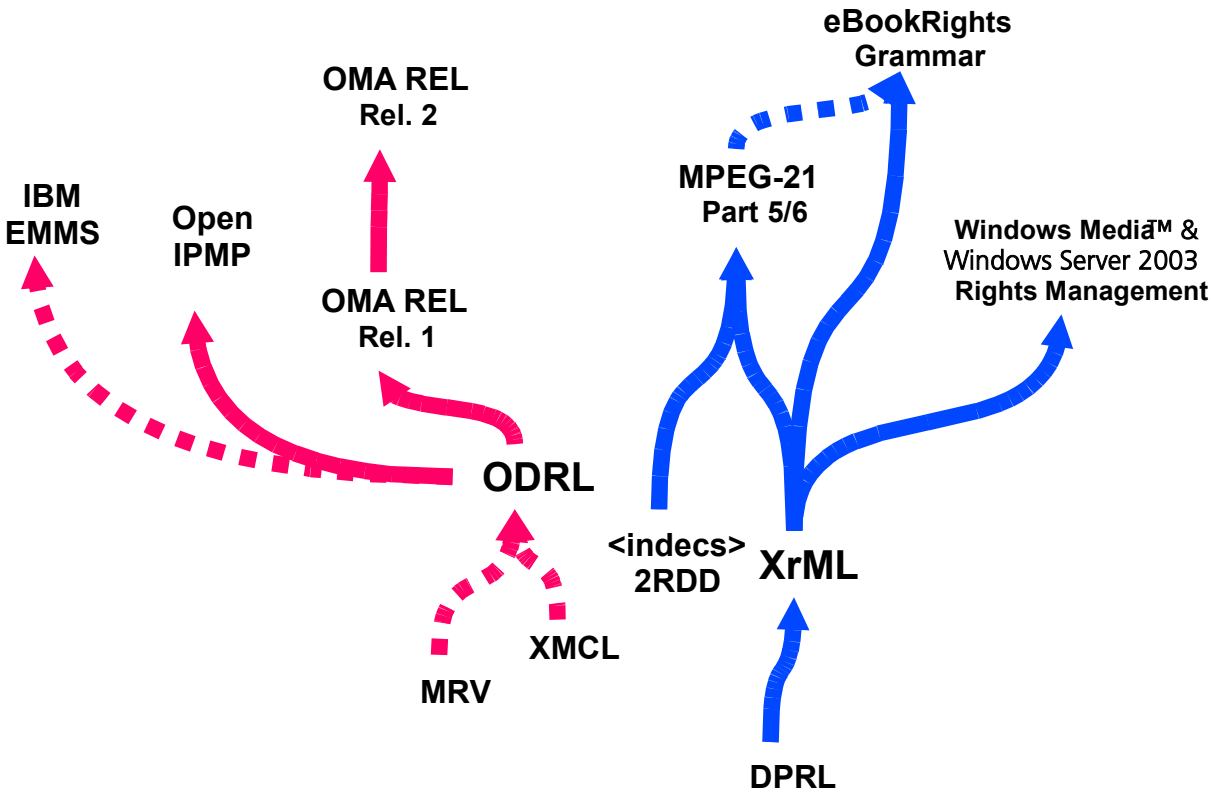
- **Rechtebeschreibung (Rights Expression)**
  - ***Einem Nutzer wird das Recht gewährt unter einer definierten Bedingung eine bestimmte (virtuelle) Ware in einer definierten Art und Weise zu nutzen.***
  - ***Rechte sind an eine bestimmte Ware (Datei) und einen bestimmten Nutzer (Endgerät) gebunden***
  - ***Rechte sind in einer speziellen Sprache, der Rechtebeschreibungssprache (Rights Expression Language, REL) notiert.***
  - ***Rechte und REL müssen maschinenlesbar sein***
  - ***REL basiert auf XML (eXtensible Markup Language)***
  - ***Der DRM-Controller interpretiert die Rechte und setzt sie technisch durch***

Rechte und Rechtebeschreibung [2]

- **Mögliche Nutzungsrechte**
  - *Abspielen (Anzahl, Zeitraum …)*
  - *Auf Audio-CD brennen*
  - *Auf tragbares Gerät (Anzahl) übertragen*
  - *Drucken (Texte, Bilder)*
- **Weitere Möglichkeiten**
  - *Rechte können voneinander abhängen (Stammlizenzen!)*
  - *Verschiedene Rechte für eine Ware (Probelizenzen!)*

Rechtebeschreibungssprachen

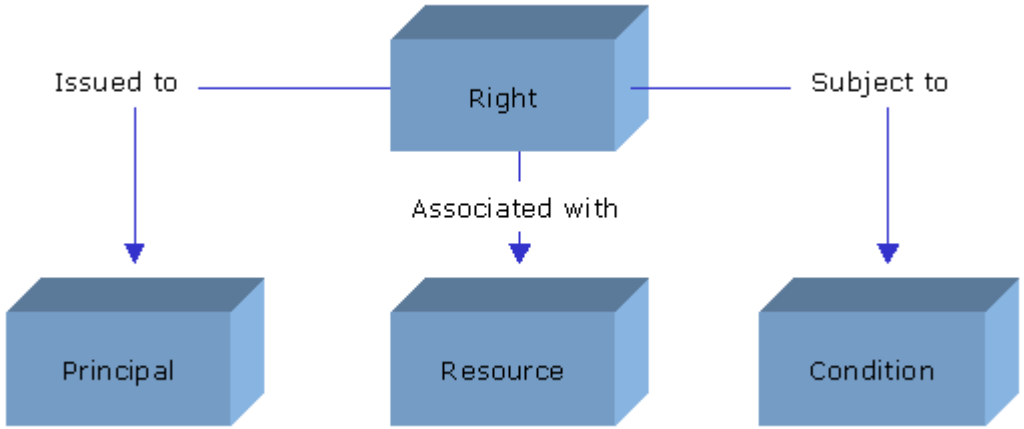
- **Stammbau der Rechtebeschreibungssprachen**
  - ***Unterschiedliche REL Standards: ODRL, XrML, MPEG-21 …***



MPEG-21

Multimedia Framework

- ***MPEG-21 Teil 5 Rights Expression Language***



  - *The principal to whom the grant is issued*
  - *The right that the grant specifies*
  - *The resource to which the right in the grant applies*
  - *The condition that must be met before the right can be exercised*
- ***MPEG-21 Teil 6 Rights Data Dictionary***

Beispiel ODRL

- **Open Digital Rights Language (ODRL)**
  - *ODRL v1.1 wird bei der Open Mobile Alliance (OMA) eingesetzt (Mobile Profile)*
- **Elemente**
  - *<rights>*
  - *<agreement> <asset>*
  - *<context> <version> <uid>*
  - **<digest> <DigestMethod>**
  - *<KeyInfo> <EncryptedKey> <xenc:EncryptionMethod> <CipherData> <RetrievalMethod>*
  - *<permission> <play> <display> <execute> <print> <export>*
  - *<constraint> <count> <timed-count> <datetime> <interval> <accumulated> <individual> <system>*
  - *<inherit>*

```
<o-ex:rights
 xmlns:o-ex="http://odrl.net/1.1/ODRL-EX"
 xmlns:o-dd="http://odrl.net/1.1/ODRL-DD"
 xmlns:oma-dd="http://www.openmobilealliance.com/oma-dd"
 xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
 xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
 o-ex:id="C.1">
 <o-ex:context>
  <o-dd:version>2.0</o-dd:version>
  <o-dd:uid>RightsObjectID</o-dd:uid>
 </o-ex:context>
 <o-ex:agreement>
  <o-ex:asset>
  <o-ex:context>
   <o-dd:uid>ContentID</o-dd:uid>
  </o-ex:context>
  <o-ex:digest>
   <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
   <ds:DigestValue>DCFHash</ds:DigestValue>
  </o-ex:digest>
  <ds:KeyInfo>
   <xenc:EncryptedKey>
    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#kw-aes128"/>
    <ds:KeyInfo>
     <ds:RetrievalMethod URI="REKReference"/>
    </ds:KeyInfo>
    <xenc:CipherData>
     <xenc:CipherValue>EncryptedCEK</xenc:CipherValue>
    </xenc:CipherData>
   </xenc:EncryptedKey>
  </ds:KeyInfo>
  </o-ex:asset>
  <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>
 </o-ex:agreement>
</o-ex:rights>
```

Die Erlaubnis etwas 3 mal abzuspielen

Policy-Oriented Web

Nach Renato Ianella:
http://www.virtualgoods.org/2009/PolicyOrientedWeb.pdf

- **User Generated Content (UGC)**
  - *Nutzer stellen eigene Inhalte (Fotos, Videos ...) ins Web*
  - *Plattformen wie Wikipedia, YouTube, Flickr ... ermöglichen anderen Nutzer den Zugriff auf UGC*
  - *Konsumenten von UGC wissen oft nicht, welche Rechte bestehen*
  - *Nutzer wissen oft nicht, was die Plattform-Betreiber mit dem User-Content machen können.*
- **Policies regeln die Rechte am UGC**
  - *Nutzer können die Verwendung ihrer Inhalt begrenzt über Policies steuern*
  - *Jede Plattform hat andere Möglichkeiten*
  - *Policies werden nur angezeigt, nicht technisch erzwungen*
  - *Reicht das in Zukunft???*

Nächsten zwei Vorlesungen

- **Public-Key-Kryptographie**
  - ***Grundprinzip***
  - ***Anwendungen bei DRM***
  - ***Geheime Übertragung des CEK***
  - ***Zertifikate***
  - ***Digitale Signatur***
  - ***Hash-Funktion***
  - ***RSA-Verfahren***

Weitere Informationen

- *Jürgen Nützel: Die informatorischen Aspekte virtueller Güter und Waren, Oktober 2006 im Unversitätsverlag Ilmenau, www.juergen-nuetzel.de/habilitation.html*
- *Jürgen Nützel: Digital Rights Management (Seite 28 - 49), in Die Privatkopie, herausgegeben von Frank Fechner, 2007, Universitätsverlag Ilmenau, ISBN 978-3-939473-06-0, http://www.db-thueringen.de/servlets/DocumentServlet?id=7543*
- *www.openmobilealliance.org*
- *ODRL: www.odrl.net*
- *MPEG-21: www.chiariglione.org/mpeg/standards/mpeg-21/mpeg-21.htm*