Digital Rights Management (DRM)

Verfahren, die helfen Rechte an virtuellen Waren durchzusetzen

**Vorlesung im Wintersemester 2011/2012 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**

Windows Media DRM und andere

***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

- **Fairplay von Apple**
- **iPhone Apps**
- **Windows Media Rights Manager**
- **Amazons Kindle**

FairPlay - das DRM bei Apple iTunes

Was ist FairPlay?

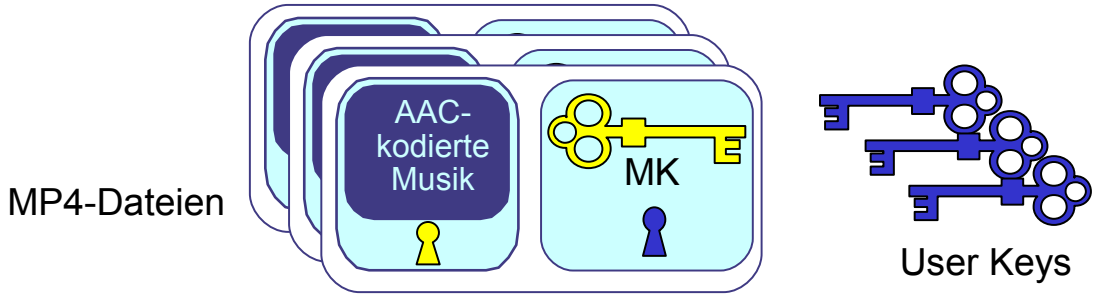
- *DRM-System von Apple Computer*
- *Bis März 2009 im Einsatz*
- *Basiert auf Entwicklungen von Veridisc*
- *In die QuickTime Technologie integriert*
- *Wird im iPod, in der iTunes Software (für Mac und PC) und im iTunes Music Store benutzt*
- *Alle im iTunes Music Store gekauften Dateien sind mit FairPlay kodiert (geschützt)*
- *Verschlüsselte AAC (Advanced Audio Coding – Nachfolger von MP3) kodierte Dateien (typischerweise 128 KBit/s)*
- *Die Datei können nur auf autorisierten Computer abgespielt werden*

Einschränkungen bei iTunes

- **Folgende Nutzungsrechte hat Apple festgelegt:**
  - ***Die Musikstücke dürfen auf beliebig viele iPods kopiert werden***
  - ***Die Musik darf gleichzeitig auf 5 (zuerst waren es 3) autorisierten Computern abgespielt werden***
  - ***Die Musik darf beliebig oft als eine Standard Audio-CD gebrannt werden***
    - *Die CD kann zwar dann in ein ungeschütztes Format wie MP3 „geripped“ werden. Dabei entstehen aber Artefakte (Transcoding)*
    - *Ein bestimmte Playlist darf maximal 7 mal (zuerst waren es 10 mal) auf CD gebrannt werden. Danach muss die Liste umsortiert werden.*
- **Und für Videoverleih:**
  - ***Nach dem ersten mal ansehen, kann das Video noch weitere 48h angesehen werden.***

FairPlay ist ein einfaches DRM

- *Es gibt keine Rechtebeschreibung. Die festgelegten Rechte sind in der iTunes Software und QuickTime einprogrammiert.*
- *Die Standard MP4-Dateien enthalten AAC-kodierte Audiodaten, die mit AES durch den Master Key (MK) verschlüsselt sind. Der Master Key (MK) entspricht dem CEK.*
- *Der MK befindet sich in der MP4-Datei. Er ist mit dem User Key (UK) verschlüsselt.*



- *Bei Kauf wird auf dem Server ein zufälliger UK erzeugt, dort gespeichert und an die iTunes Software des Nutzer gesendet. Die iTunes Software speichert die UKs verschlüsselt.*
- *Auf den iPod werden MP4-Dateien und UKs übertragen*

How it works

- **Aus http://en.wikipedia.org/wiki/FairPlay (Restored am 19.1.2007; war am 8.11.06 von 203.115.82.38 gelöscht worden, inzwischen wieder online)**

FairPlay is a fairly simple implementation of DRM techniques. FairPlay-protected files are regular MP4 container files with an encrypted AAC audio stream. The audio stream is encrypted using the Rijndael algorithm in combination with MD5 hashes. The master key required to decrypt the encrypted audio stream is also stored in encrypted form in the MP4 container file. The key required to decrypt the master key is called the "user key."

Each time a customer uses iTunes to buy a track a new random user key is generated and used to encrypt the master key. The random user key is stored, together with the account information, on Apple's servers, and also sent to iTunes. iTunes stores these keys in its own encrypted key repository. Using this key repository, iTunes is able to retrieve the user key required to decrypt the master key. Using the master key, iTunes is able to decrypt the AAC audio stream and play it.

When you authorize a new computer, iTunes sends a unique machine identifier to Apple's servers. In return it receives all the user keys that are stored with the account information. This ensures that Apple is able to limit the number of computers that are authorized and makes sure that each authorized computer has all the user keys that are needed to play the tracks that it bought.

When you deauthorize a computer, iTunes will instruct Apple's servers to remove the unique machine identifier from their database, and at the same time it will remove all the user keys from its encrypted key repository.

The iPod also has its own encrypted key repository. Every time a FairPlay-protected track is copied onto the iPod, iTunes will copy the user key from its own key repository to the key repository on the iPod. This makes sure that the iPod has everything it needs to play the encrypted AAC audio stream.

At this time, it looks like the restrictions mentioned above are hard-coded into QuickTime and the iTunes application, and not configurable in the protected files themselves.

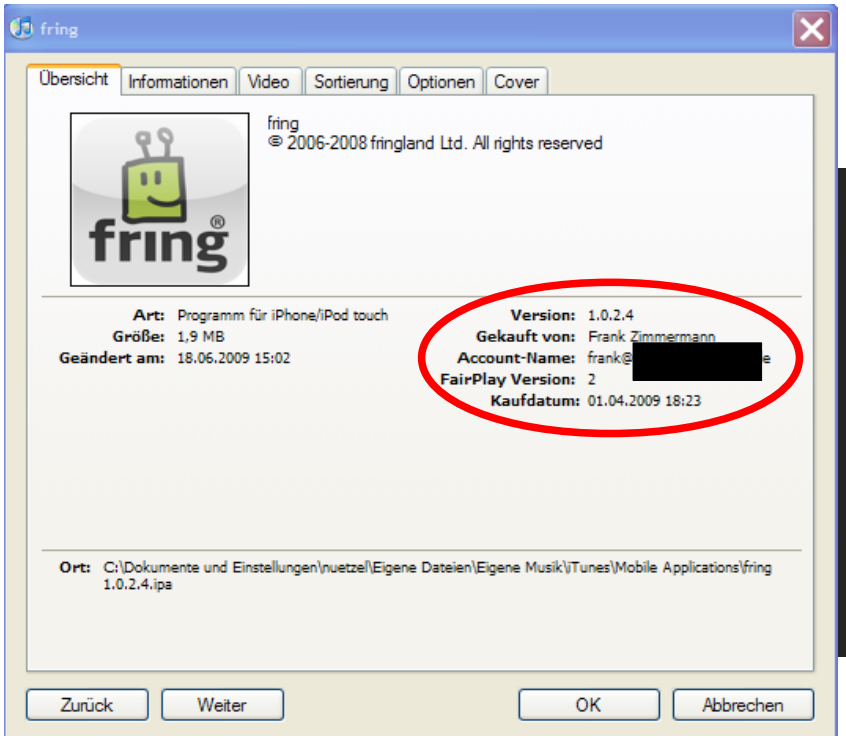
Der Apple AppStore für das iPhone

- **Apple kontrolliert die Verteilung von Software**
  - *Der Vertrieb von iPhone Software erfolgt analog zur Musik*
  - *Apple betreibt hierfür den AppStore*
  - *Apple behält sich vor Software abzulehnen*
  - *Am AppStore vorbei kann die Software nur an registrierte (oder gehackte, Jail-Break) iPhones ausgeliefert werden*

- **Mit dem iPad kommt auch iBooks ...**

Ein gescheiterter Kopierversuch

- **Apps sind auch mit Fairplay geschützt**
  - *Im File (in iTunes) ist der Name und E-Mail-Adresse des Käufers*
  - *Die Nutzdaten sind verschlüsselt und signiert*
  - *Jail-Break modifiziert das Betriebssystem des iPhone*

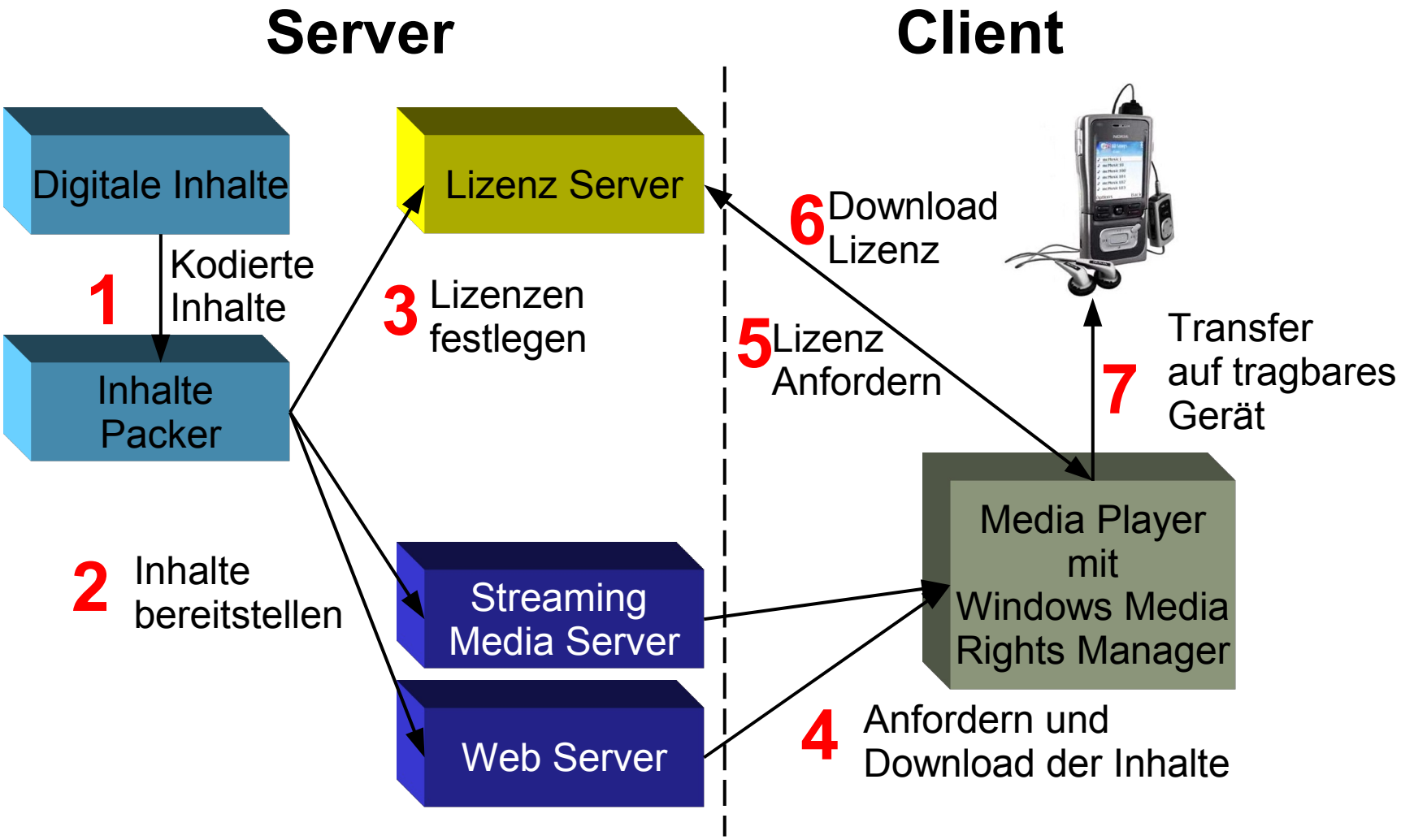


Windows Media Rights Manager [1]

- **Windows Media DRM …**
  - *… ist ein voll ausgebautes DRM-System mit Client- und Server-Komponenten und hohen Sicherheitsanforderungen.*
  - *Die Anwendung von Mircosoft‘s DRM ist Mircosoft‘s Formate Windows Media Audio WMA und Windows Media Video WMV beschränkt.*
  - *Der DRM-Controller in den Windows Media Player integriert.*
  - *Aktuell in der Version 11 für Windows XP und Vista verfügbar*

  - *Server-Komponenten (Lizenz-Server) benötigen Windows 2003 Server.*
  - *Umsetzungen für tragbare (unconnected) Geräte (z.B. Nokias N95)*

Windows Media Rights Manager [2]

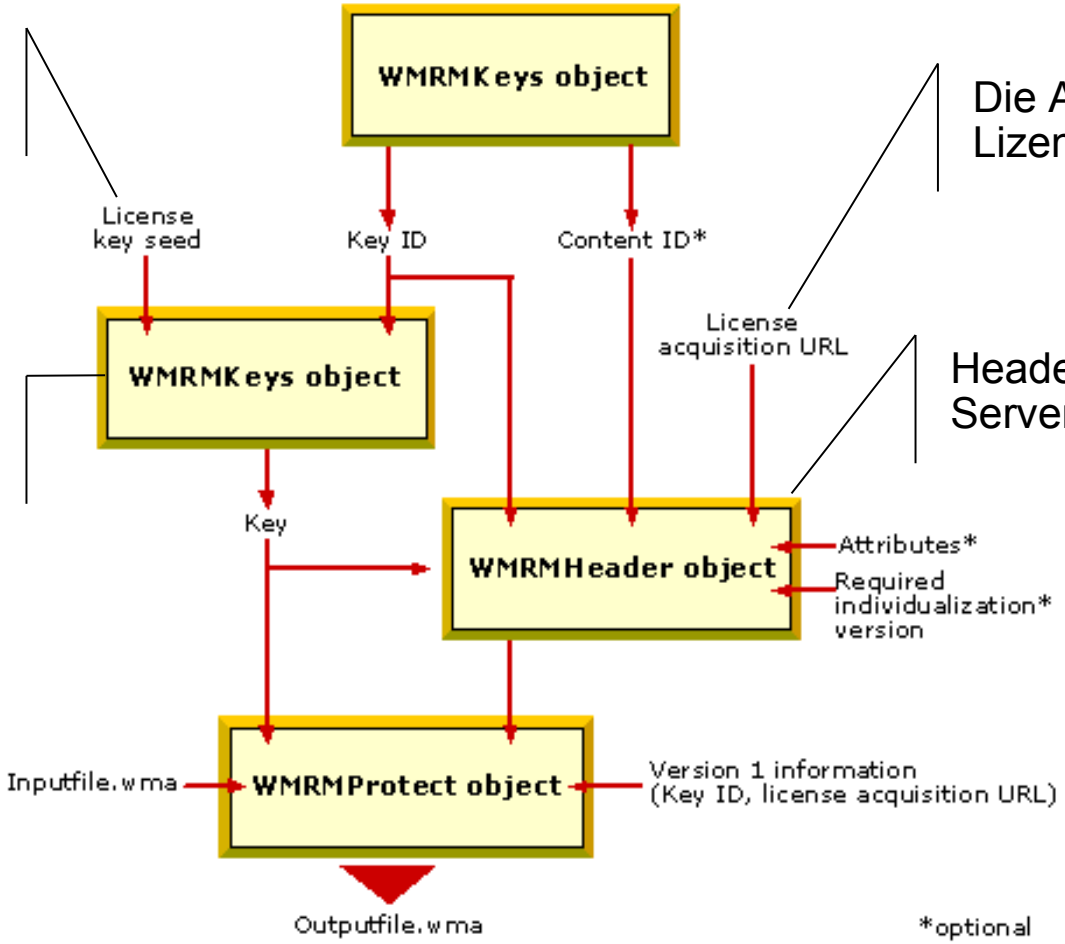


Der Inhalte-Packer

- **Im Header stehen KeyID und License acqui. URL**

Seed:
Geheimer Startwert
für die Schlüsselbildung

Schlüsselbildung nach
geheimen Verfahren
aus Seed und Key ID



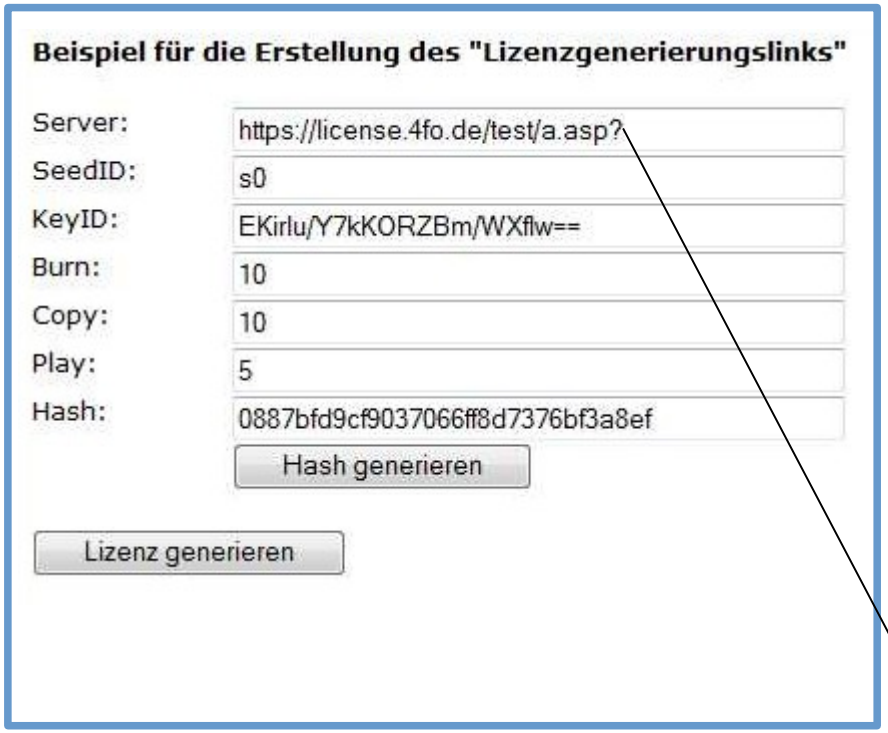
Die Adresse des
Lizenz-Servers

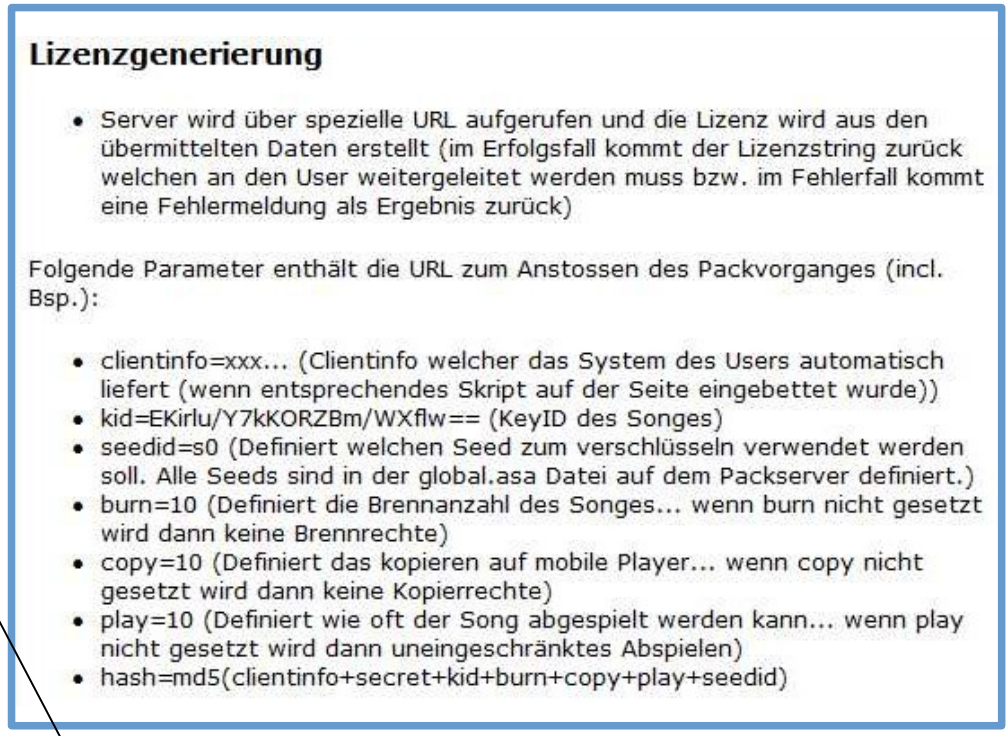
Header ist digital vom
Server signiert

Lizenzgenerierung

Unser Test-System für Windows Media DRM

- *Key wird aus Seed und KeyID berechnet*

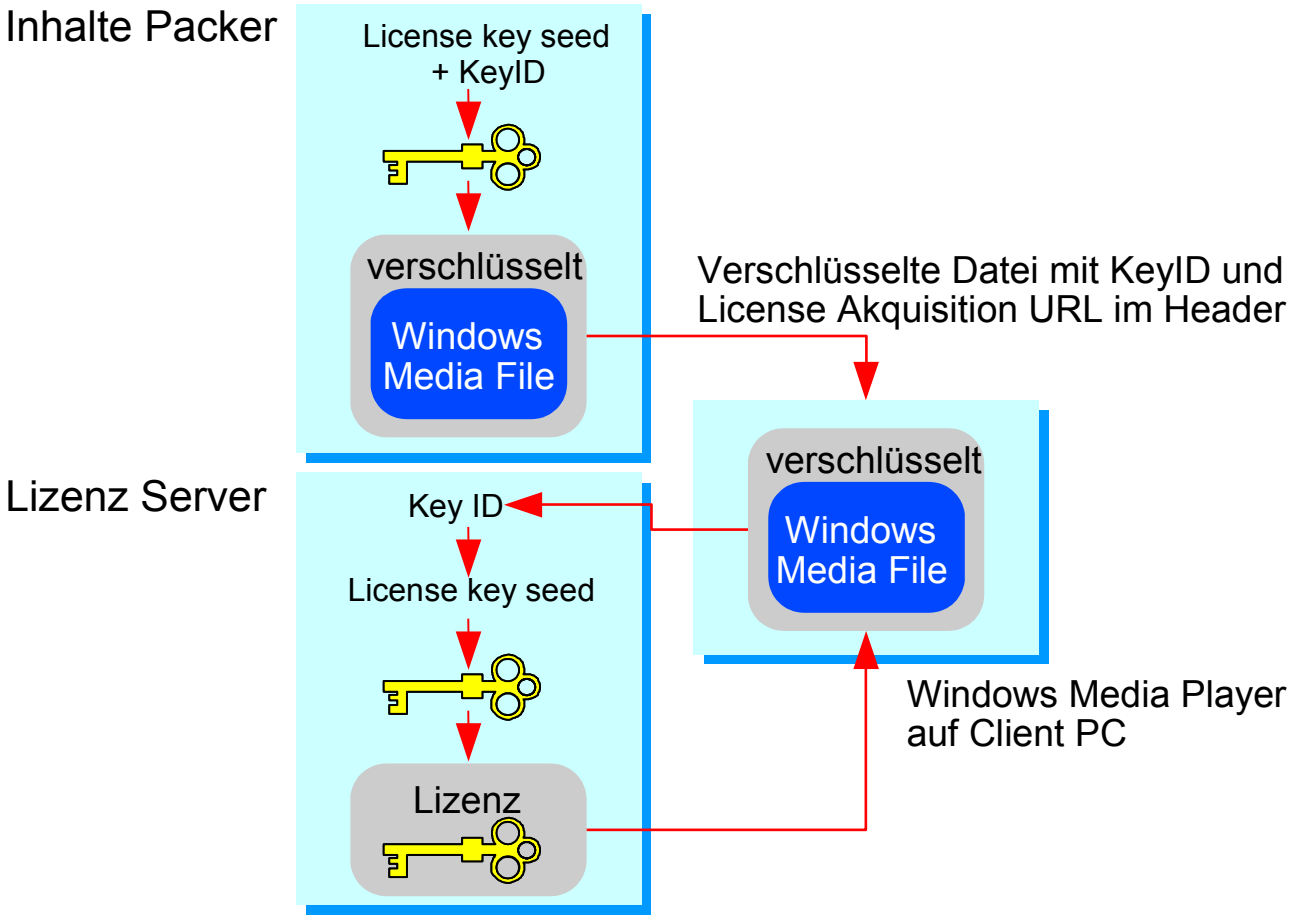




Die Adresse des Lizenz-Servers
License acquisition URL

Die Key-ID

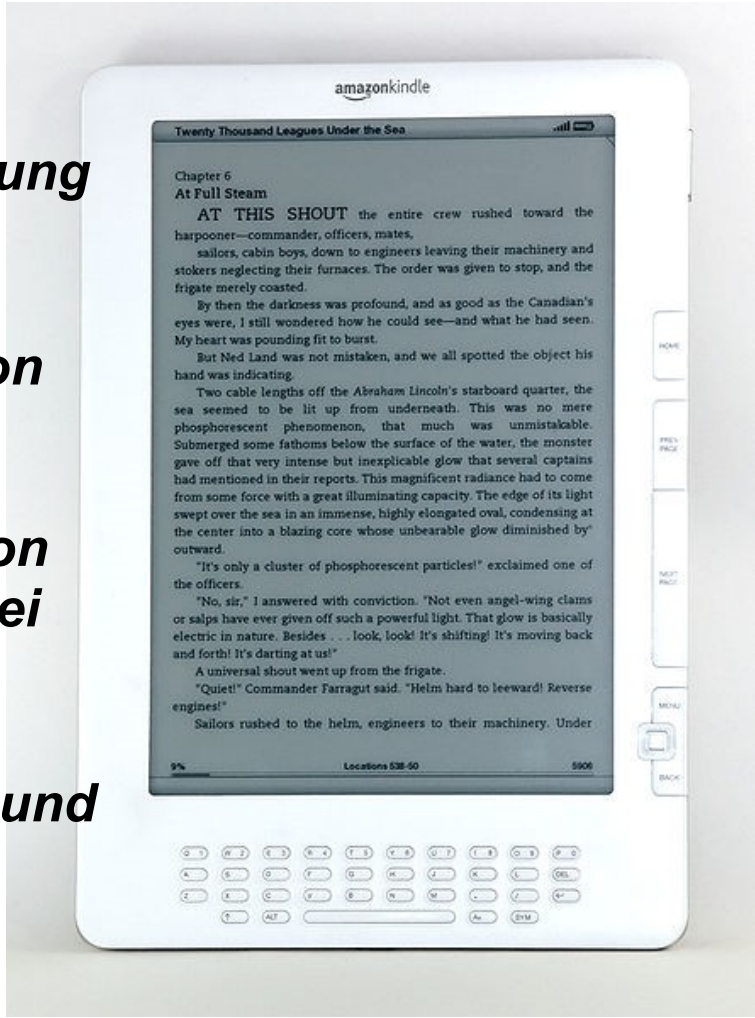
Der Lizenz-Server berechnet den Schlüssel



Amazons Kindle

Amazons E-Book-Reader

- *Der Bildschirm basiert auf der Technologie des elektronischen Papiers. Keine Hintergrundbeleuchtung und soll auch im Sonnenlicht gut zu lesen sein.*
- *Über das sogenannte Whispernet von Sprint Nextel können in den USA E-Books, Zeitschriften und Zeitungen direkt aus dem Webshop von Amazon gekauft oder abonniert werden. Dabei fallen keine zusätzlichen Übertragungsentgelte an.*
- *Die gekauften Bücher, Zeitschriften und Zeitungen werden durch DRM geschützt.*



Adobe Digital Editions

- **Überblick**
  - ***Software zum Betrachten DRM-geschützter E-Books und baut auf der Adobe Flash-Technologie auf. Eignet sich zum Lesen und Verwalten von E-Books, elektronischen Zeitungen und Magazinen.***
  - ***Basis EPUB (Akronym für electronic publication) ist ein offener Standard für E-Books vom International Digital Publishing Forum (IDPF)***
- **Einsatz in der Online Buchausleihe (Onleihe)**
  - ***Z.B. Thüringer Bibliotheksnetz: www.thuebibnet.de***
- **Eingesetztes DRM**
  - ***ADEPT DRM (CEK: AES, RSA Schlüsselpaar)***
  - ***2009 wurde Angriff beschrieben:***
    Circumventing Adobe ADEPT DRM for EPUB
    http://i-u2665-cabbages.blogspot.com/2009/02/circumventing-adobe-adept-drm-for-epub.html

Nächste Vorlesung

- **Open Mobile Alliance DRM 2.0**
  - ***www.openmobilealliance.org***
  - ***Ein offener Standard in der Version 2.0***
  - ***DCF – DRM Content Format***
  - ***ROAP – Rights Object Acquisition Protocol***
  - ***Rechte Objekte***
  - ***Domains***
  - ***Superdistribution***
  - ***Transaction Tracking (optional)***
  - ***Abo-Modelle***

Weitere Informationen

- *Jürgen Nützel: Die informatorischen Aspekte virtueller Güter und Waren, Oktober 2006 im Universitätsverlag Ilmenau, www.juergen-nuetzel.de/habilitation.html*
- *http://en.wikipedia.org/wiki/FairPlay#How_it_works*
- *http://developer.apple.com/iphone/program/*
- *http://en.wikipedia.org/wiki/App_Store*
- *http://en.wikipedia.org/wiki/Jailbreak_(iPhone)*
- *www.microsoft.com/windows/windowsmedia/de/drm/features.aspx*
- *Amazon Kindle: www.amazon.com/kindle*
- *http://en.wikipedia.org/wiki/Amazon_Kindle*
- *http://de.wikipedia.org/wiki/Adobe_Digital_Editions*
- *Circumventing Adobe ADEPT DRM for EPUB: http://i-u2665-cabbages.blogspot.com/2009/02/circumventing-adobe-adept-drm-for-epub.html*