Digital Rights Management (DRM)

Verfahren, die helfen Rechte an virtuellen Waren durchzusetzen

Probevorlesung am 27.10.2005
Dr.-Ing. Jürgen Nützel,
Juergen.Nuetzel@tu-ilmenau.de
Technische Universität Ilmenau

Diese Folien zeigen einen Ausschnitt und eine Zusammenfassung einer Vorlesungsreihe, die ab dem Sommersemester 2006 vom Autor für Studierende der Informatik, Wirtschaftsinformatik, Medientechnik und Medienwirtschaft angeboten wird.

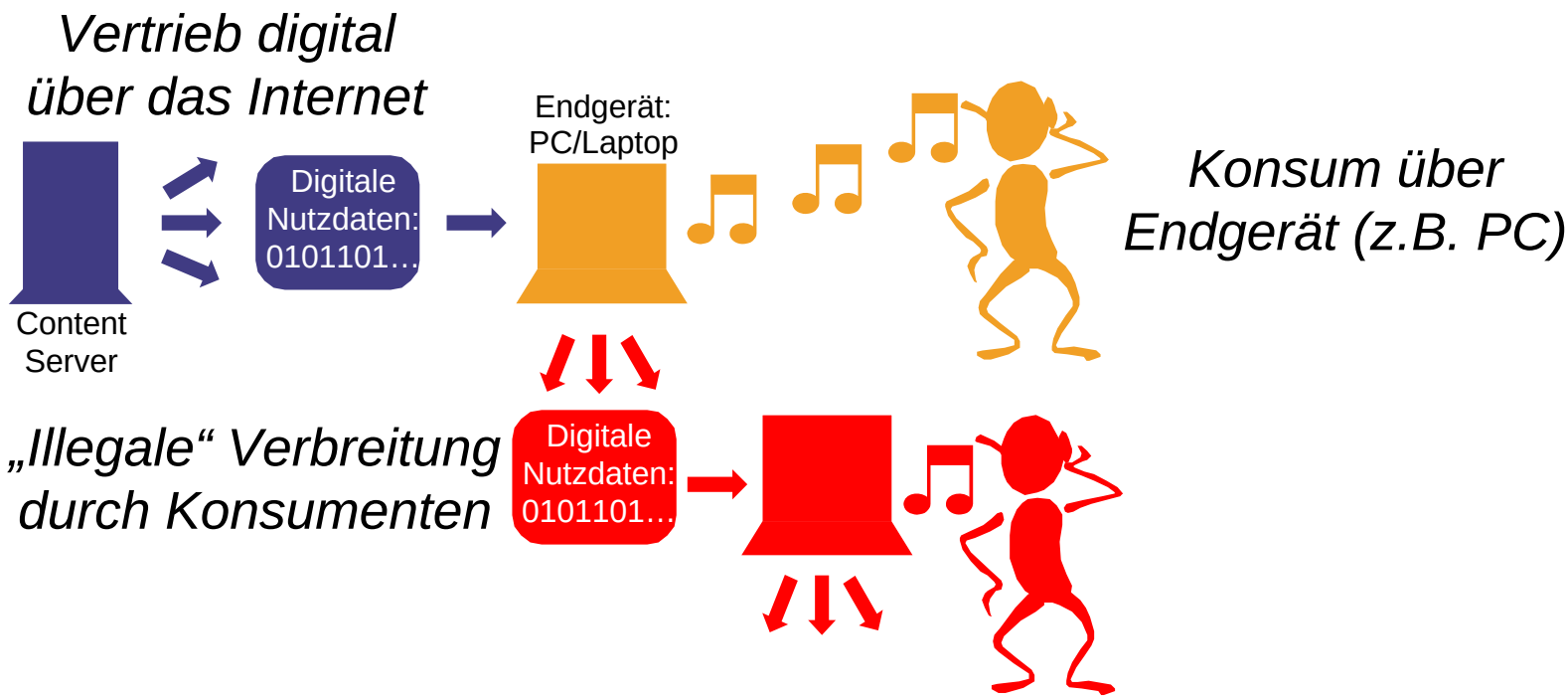
Übungsaufgaben: www.juergen-nuetzel.de/drm.html

Überblick

- Ausgangslage: Virtuelle Waren
- Unterschiedliche Sichten auf DRM
- Technische Grundprinzipien von DRM
- Rechte und Rechtebeschreibung
- Public-Key-Kryptographie
- Referenz-Modell eines DRM-Systems
- Neue Geschäftsmodelle mit DRM
- DRM der Open Mobile Alliance (OMA)
- Sicherheit der Implementierung
- Am Schluss bleiben viele Fragen

Ausgangslage: Virtuelle Waren

Beispiel: Musik-Download



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

Viele Fragen stellen sich

- ***Kopieren allen erlauben?***
  - *Wer bezahlt dann noch?*
  - *Urheber über Steuern entlohnen?*
- ***Raubkopierer bestrafen?***
  - *Wer will das machen?*
  - *Wie findet man die Raubkopierer?*
  - *Wird dadurch mehr verkauft?*
- ***Illegale Kopien zurückverfolgen?***
  - *Wie findet man die Verursacher?*
  - *Angst bei den legalen Nutzern?*
- ***Nutzung kontrollieren?***
  - *Was ist eine legale Kopie/Nutzung?*
  - *Gibt es dann noch ein Kopieren?*

Virtuelle Waren und DRM

Die eigene Sichtweise:

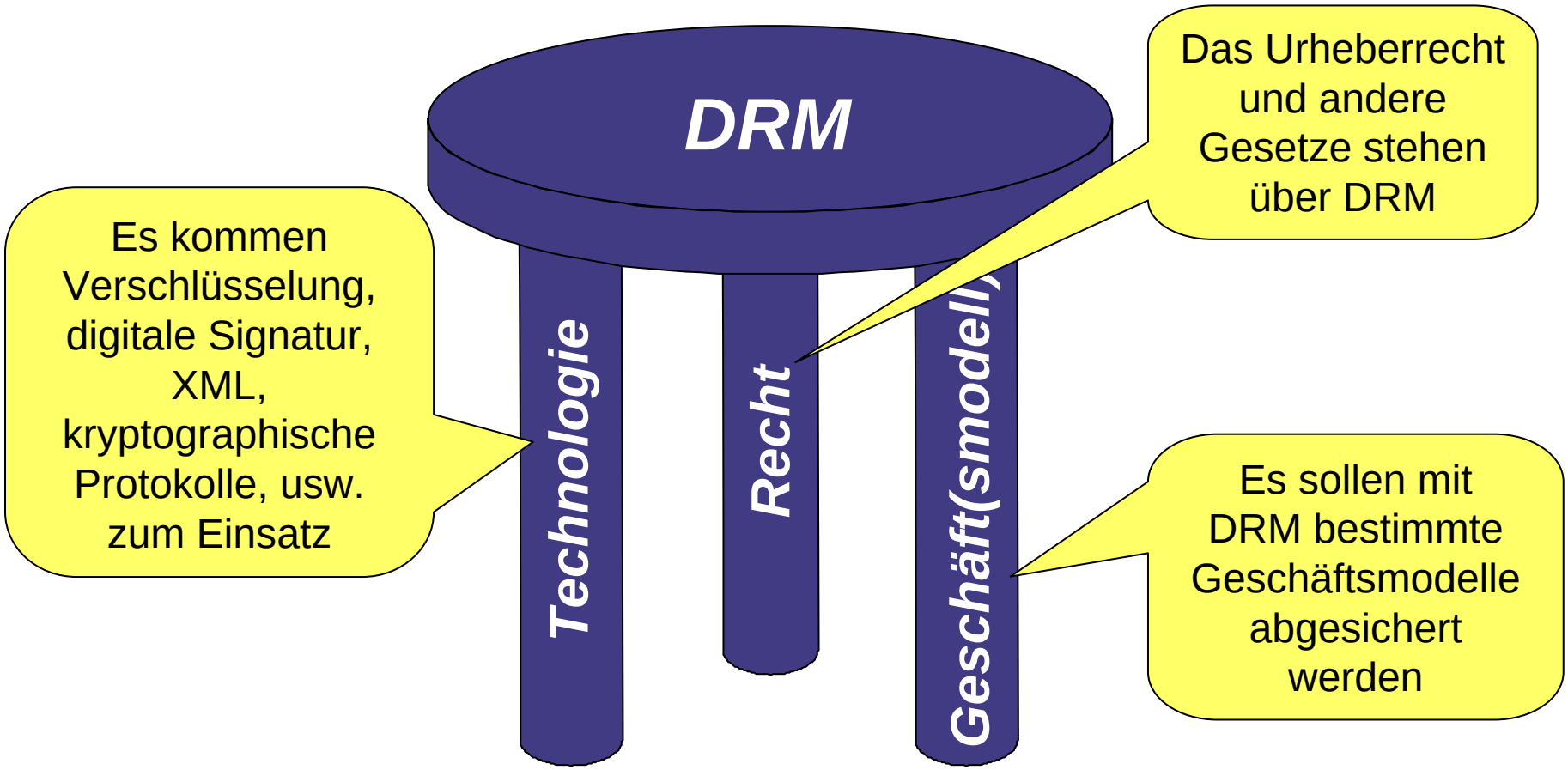
- ***Virtuelle Waren wie bspw. Musik …***
  - *… können ohne Qualitätsverlust **digitalisiert** werden und sind somit nicht mehr an ein physikalisches Trägermedium gebunden*
- ***Digitalisierte virtuelle Waren können daher von allen …***
  - *… sehr leicht **transferiert** werden (z.B. über das Internet)*
  - *… fast ohne Kosten **kopiert** werden*
  - *… beliebig oft **konsumiert** werden*
- ***DRM ermöglicht den Anbietern virtueller Waren …***
  - *… diese Eigenschaften der Digitalisierung dem Konsumenten wieder zu nehmen, um sie ihm daraufhin als getrennt erwerbbare **Nutzungsrechte** wiederzugeben*
  - *… (**mindestens**) die von den realen Waren her **gewohnten Geschäftsmodelle** auf die virtuellen Waren auszudehnen, ohne dabei die spezifischen Eigenschaften von diesen beachten zu müssen.*

Verschiedene Sichten auf DRM

Andere Definitionen für DRM:

- ***Eine kritische Sichtweise***
  - *„Verfahren, die helfen Rechte an **digitalen Waren so zu schützen**, **wie wir das** von den an physische Medien gebundenen intellektuellen Erzeugnissen her **gewöhnt sind**. Kopie und Weitergabe sollen an die Regeln des Rechteinhabers, also der Warenanbieter (Content Provider) gebunden sein.“ (Grimm 2004)*
- ***Eine optimistische Sichtweise***
  - *„… DRM covers the description, identification, trading, protection, monitoring and tracking of all forms of rights usages over both tangible and intangible assets including management of rights holders relationships. Additionally, it is important to note that DRM is the "**digital management of rights**" and not the "management of digital rights". That is, DRM manages all rights, not only the rights applicable to permissions over digital content.“ (Iannella 2001)*

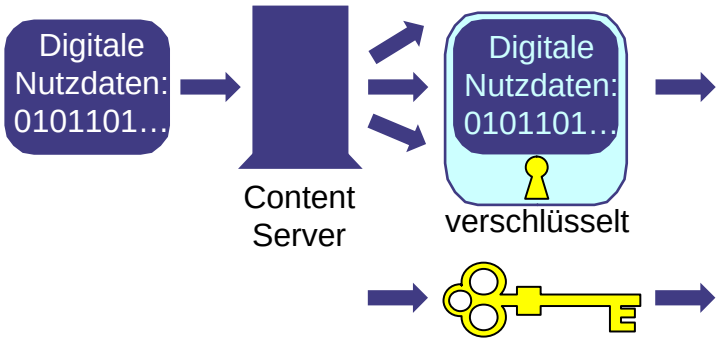
DRM ist nicht nur Technik



DRM ist ein dreibeiniger Hocker (Nils Rump 2004)

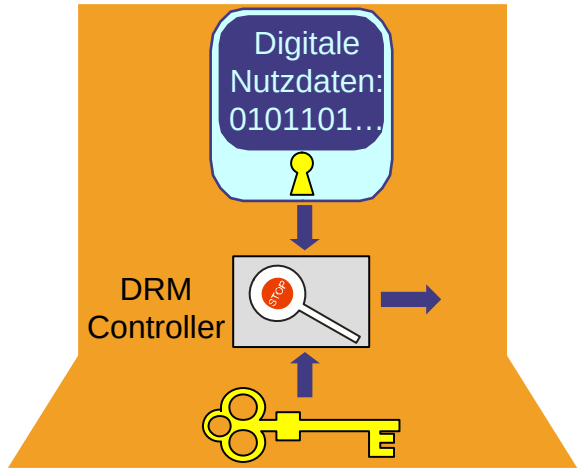
Technische Grundprinzipien [1]

Verschlüsselung der Nutzdaten



- ***Anbieter verteilt nur verschlüsselte Nutzdaten***
- ***Verschlüsselung und Entschlüsselung mit dem gleichen Schlüssel (z.B. AES)***
- ***Schlüssel muss getrennt übermittelt werden***

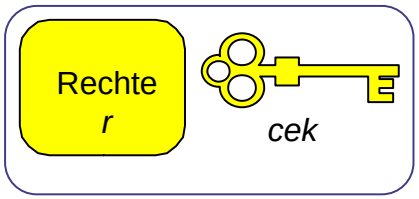
Kontrolle des Schlüssels auf dem Endgerät



- ***Der DRM-Controller kontrolliert die Verwendung des Schlüssels***

Technische Grundprinzipien [2]

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



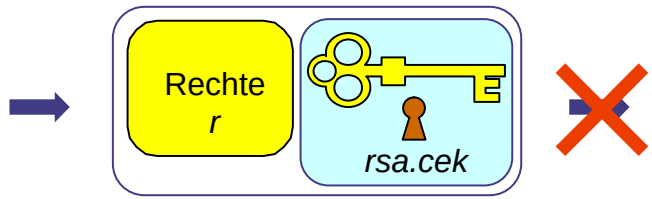
Lizenz

  - ***Verschlüsselte Nutzdaten sind ohne Lizenz wertlos***
  - ***Rechtebeschreibung legt die zulässige Nutzungsart und Nutzungsdauer fest.***

- **Sichere Speicherung der Lizenzen auf dem Endgerät**

  - ***Verschlüsselte Nutzdaten können kopiert werden***

  - ***Schlüssel in Lizenzen können nicht weitergegeben werden***



Schlüssel in der Lizenz ist zusätzlich verschlüsselt

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.*
- *Meist sind Rechte in einer speziellen Sprache (Rights Expression Language, REL) in XML notiert.*
- *Unterschiedliche REL Standards: ODRL, XrML, MPEG-21 …*
- *Der DRM-Controller interpretiert und exekutiert die Rechte.*

Mögliche Nutzungsrechte

- *Abspielen (Anzahl, Zeitraum …)*
- *Auf Audio-CD brennen*
- *Auf Portable übertragen*
- *Drucken (Texte, Bilder)*

Rechte und Rechtebeschreibung [2]

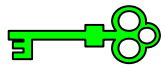
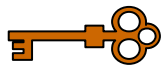
- ***XML-Rechtebeschreibung (ODRL Beispiel):***

```
<o-ex:rights
  xmlns:o-ex="http://odrl.net/1.1/ODRL-EX"
  xmlns:o-dd="http://odrl.net/1.1/ODRL-DD"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#/">
  <o-ex:context>
   <o-dd:version>1.0</o-dd:version>
  </o-ex:context>
  <o-ex:agreement>
   <o-ex:asset>
    <o-ex:context>
      <o-dd:uid>cid:20141-9729@http://contentpro.com</o-dd:uid>
    </o-ex:context>
    <ds:KeyInfo>
      <ds:KeyValue>PkerZ9f5g0a37UC2u/G+QA==</ds:KeyValue>
    </ds:KeyInfo>
  </o-ex:asset>
  <o-ex:permission>
   <o-dd:display>
    <o-ex:constraint>
     <o-dd:count>3</o-dd:count>
    </o-ex:constraint>
   </o-dd:display>
  </o-ex:permission>
 </o-ex:agreement>
</o-ex:rights>
```

Die Erlaubnis etwas 3 mal anzusehen

Public-Key-Kryptographie [1]

Grundprinzip

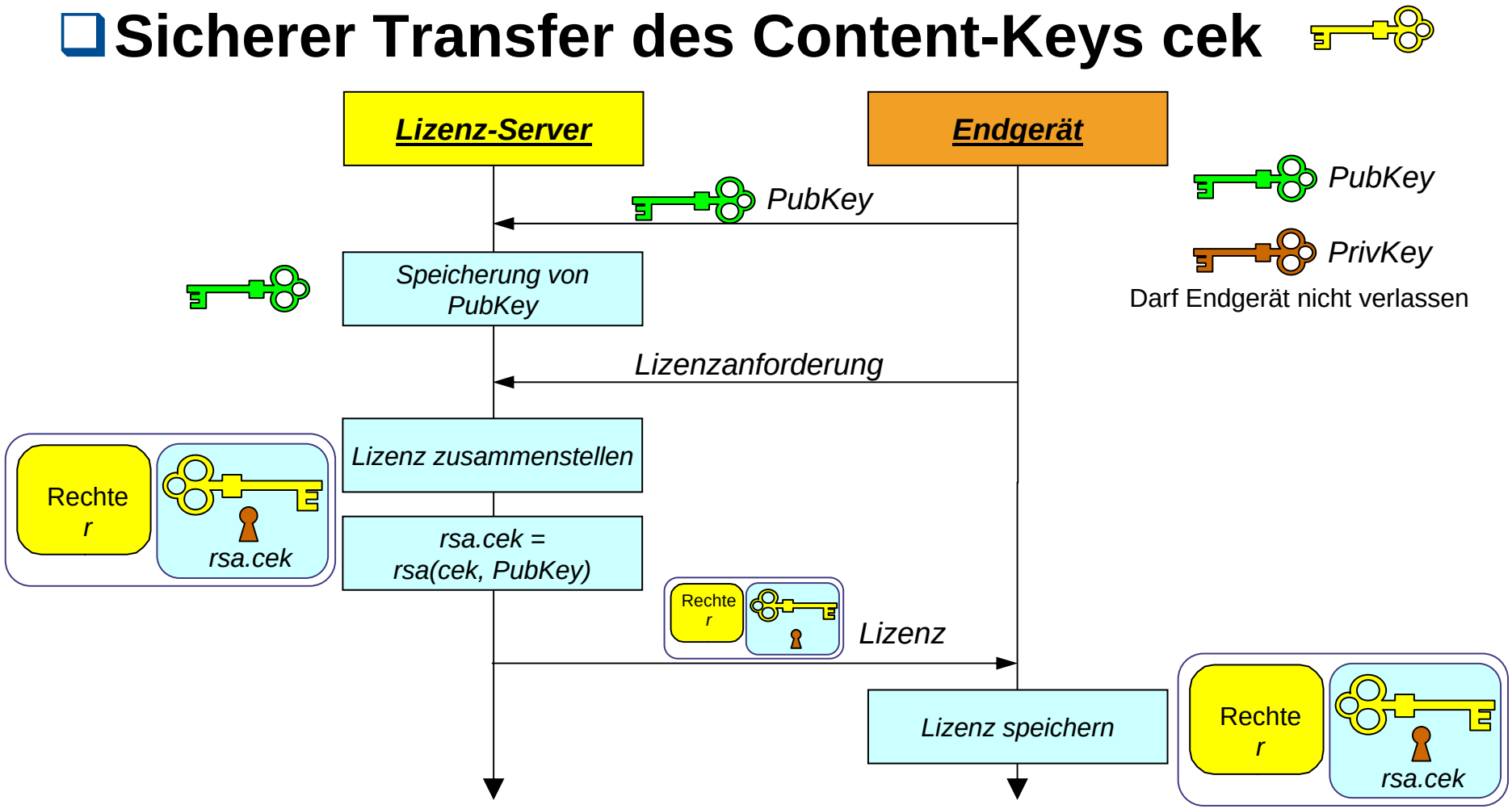
- ***Es gibt zwei Schlüssel (=Schlüsselpaar)***
- ***Was mit dem einen verschlüsselt wird kann nur mit dem anderen entschlüsselt werden***
- ***Der eine Schlüssel heißt öffentlich: Public Key*** 
- ***Der andere Schlüssel heißt privat: Private Key*** 

Anwendungen bei DRM

- ***Sicherer Schlüsselaustausch:***
  - *Sender einer geheimen Nachricht (Nutzdaten) verschlüsselt diese mit dem öffentlichen Schlüssel des Empfängers (Endgerät)*
- ***Digitale Signatur:***
  - *Der Sender verschlüsselt eine Prüfsumme (Hash-Wert) über ein Dokument mit seinem privaten Schlüssel*

Public-Key-Kryptographie [2]

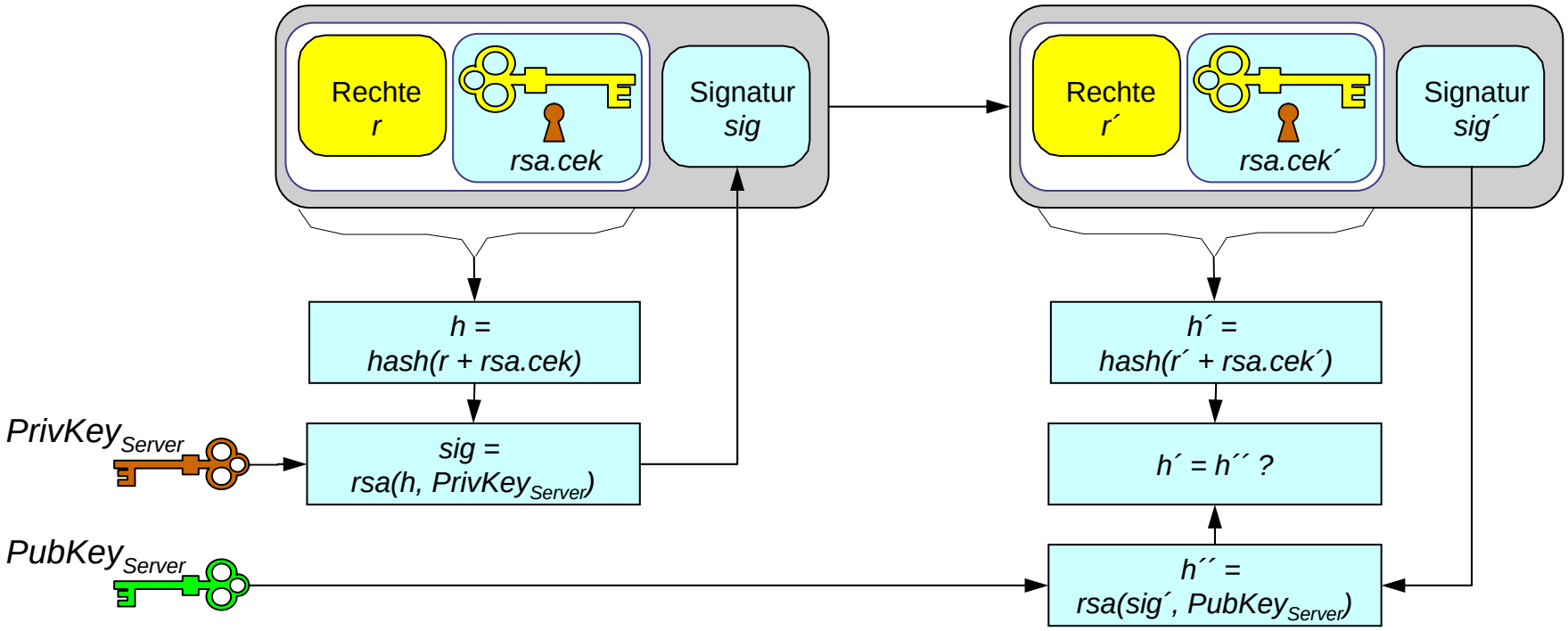
Sicherer Transfer des Content-Keys cek



Public-Key-Kryptographie [3]

Digitale Signatur …

- *zur Sicherung der Integrität und Authentizität der Lizenz*
- *Mit dem Private Key des Lizenz-Servers wird ein über die Rechte errechneter Hash-Wert verschlüsselt*



Public-Key-Kryptographie [4]

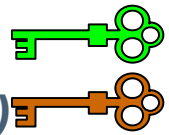
- RSA (Rivest, Shamir, Adleman)
- Idee: Multiplikation ist einfach. Die Umkehrung, die Faktorisierung, ist schwierig
- Nehme zwei etwa gleich lange Primzahlen: p und q
  (Beispiel: p=11, q=13)
- Berechne $n = p*q$ ($n = 143$)
- Berechne $\varphi(n) = (p-1)*(q-1)$ ($=120$)
- Wähle e (23) mit $ggT(e,\varphi(n)) = 1$
- Berechne d so, dass

  $e * d \equiv 1 \bmod \varphi(n)$ gilt,

  $e * d = k * \varphi(n) + 1$

  ($d = 47$ mit $k = 9$)

- Public Key: (n,e) (143, 23)
- Private Key: (n,d) (143, 47)



- Verschlüsselung mit Public Key:

  $C \equiv K^e \bmod n$

  $2 \equiv 7^{23} \bmod 143$

- Entschlüsselung mit Private Key:

  $K \equiv C^d \bmod n$

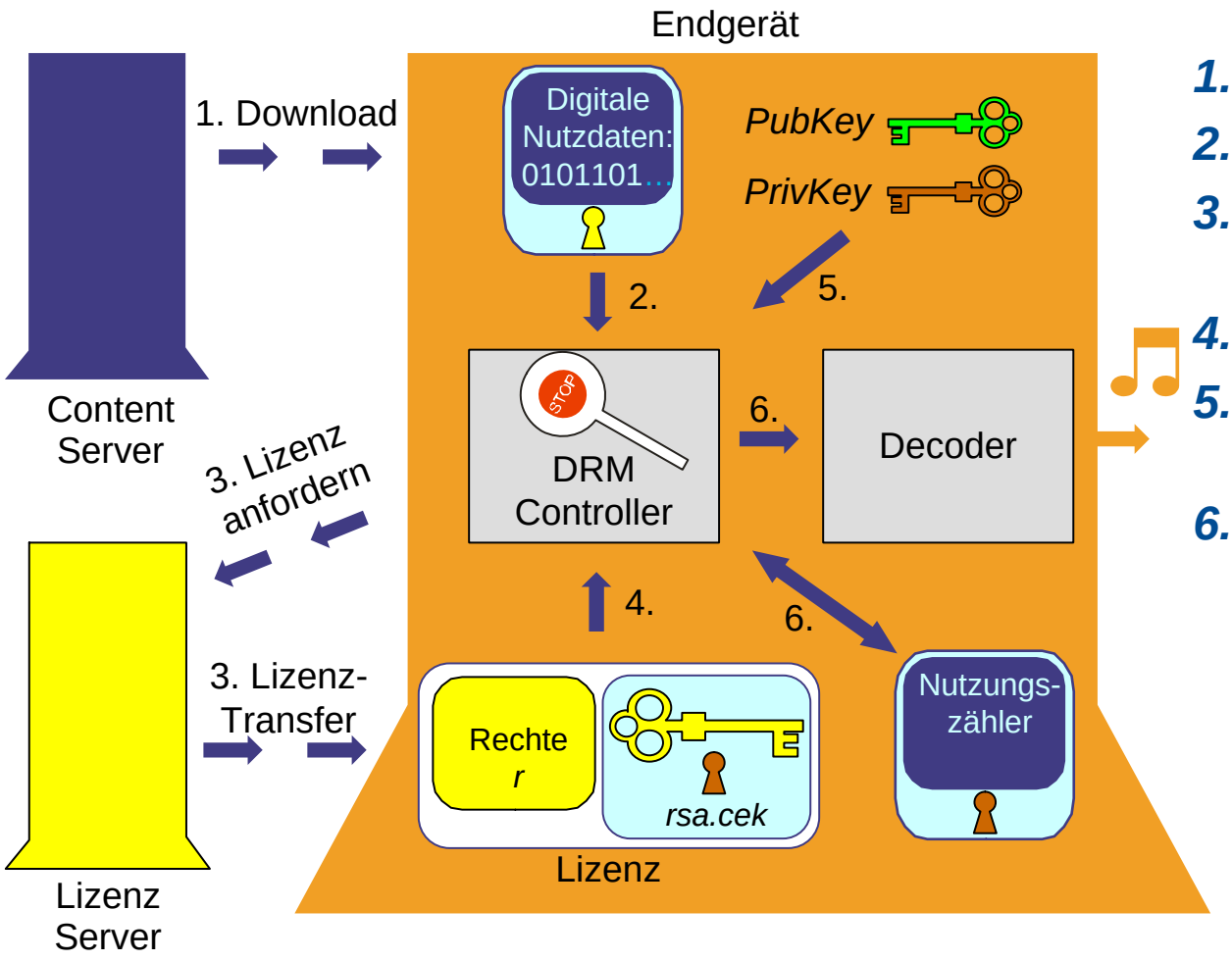
  $7 \equiv 2^{47} \bmod 143$

- Damit n im praktischen Anwendungsfall nicht in p und q faktorisiert werden kann, muss n aktuell eine 1024 bis 2048 bit lange Zahl sein !!

Public-Key-Kryptographie [5]

- **Ein 1024 bit RSA-Schlüsselpaar**
  - *n=151117088560515543543583509112099097962003663556607044995537346278481881284114992437661794727300361132467861422736444261887801298612841233509930473048074186874048225374579833810514168500718834144275902347213750223932752522075922296123467024433402797906496071473309891192170853187418104035346071158728163015279*
  - *e=65537 (fast immer gleich, damit öffentlich)*
  - *d=2843778404896223810249195748782394945092682275117314930390408611398930439106138824989979575463929312978510055276574403896825081123322964024715767465861877478265358316264940054666690151307499107403870146364067664383999167594213162163415356043745514827295718821577348779430091933159737486190654802667109123565 7*

Referenz-Modell für DRM-Systeme

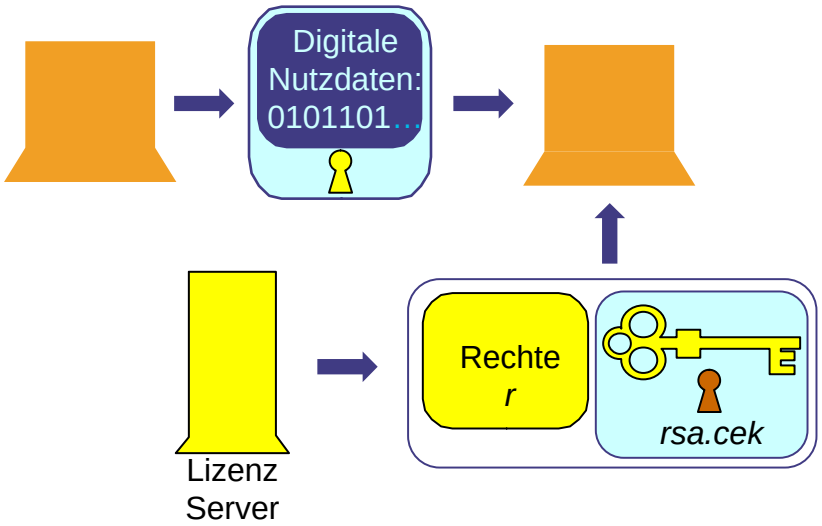


1. ***Download des Contents***
2. ***Content wird geöffnet***
3. ***DRM-Controller fordert eine Lizenz an***
4. ***Lizenz wird geöffnet***
5. ***Der private Geräte-schlüssel wird benötigt***
6. ***Nutzungszähler werden geprüft und angepasst. Entschlüsselter Content wird decodiert***

Neue Geschäftsmodelle

Superdistribution

- *Legales P2P-File-Sharing*
- *Verschlüsselte Nutzdaten werden von den Kunden weitergegeben*
- *Lizenz wird vom Lizenz-Server nachgeliefert*



Musik im Abo

- *Lizenzen sind zeitlich begrenzt (z.B. einen Monat)*
- *Endgerät muss zyklisch neue Lizenzen beziehen*
- *Zahlt der Kunde die Miete nicht mehr, erhält er im nächsten Monat keine neuen Lizenzen*

Open Mobile Alliance DRM V2.0

Was ist OMA?

- *„OMA is the leading industry forum for developing market driven, interoperable mobile service enablers“*
- *OMA setzt sich für die Interoperabilität mobiler Dienste ein*
- *www.openmobilealliance.org*

Was ist OMA DRM?

- *In der Version 1 ein sehr einfacher formatunabhängiger Standard für mobile Endgeräte. Einfache Sicherheitsanforderungen wurden berücksichtigt.*
- *Version 2 ist ein umfassender Standard, der auch komplexe Sicherheitsanforderungen (nicht nur für mobile Endgeräte) umsetzt*
- *Die Version 2 bietet unter anderem das Domain-Konzept …*

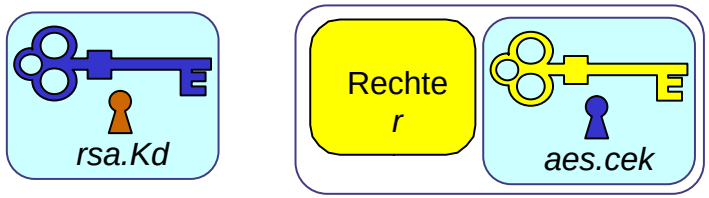
Das Domain-Konzept

Ziel

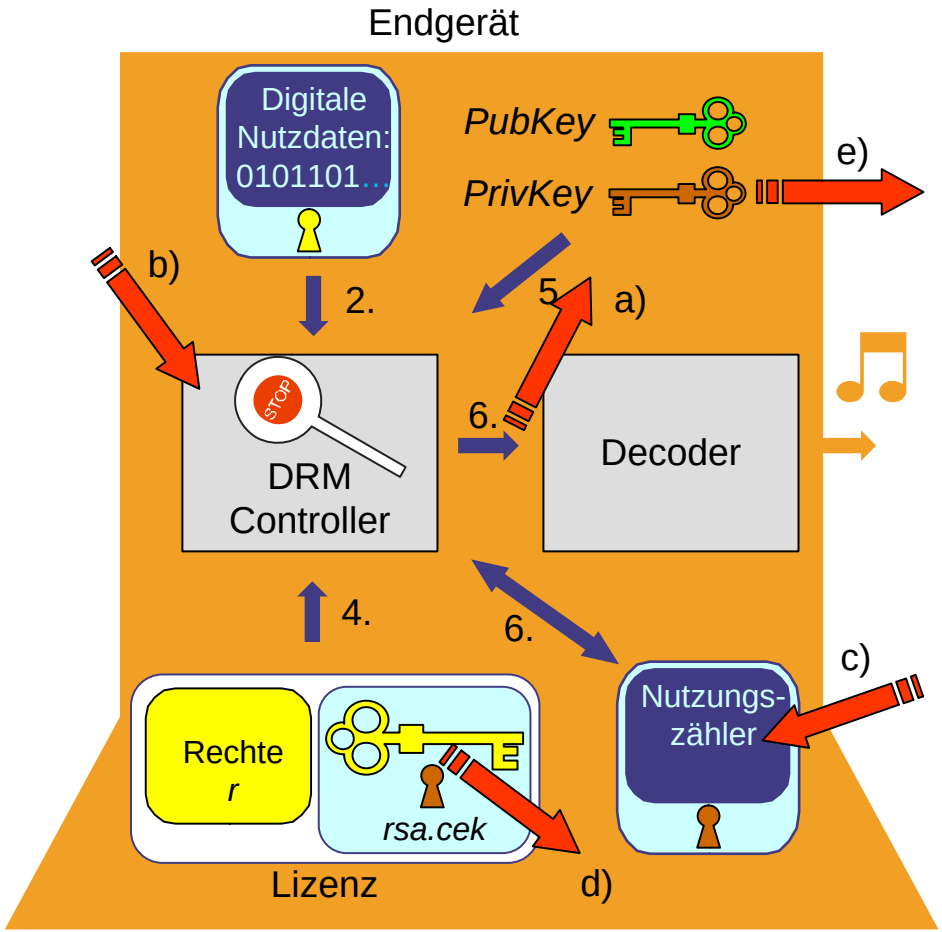
- *Einfaches Kopieren von Content- und Lizenz-Dateien zwischen mehreren Geräten eines Nutzers oder Nutzergruppe*

Umsetzung

- *Endgeräte einer Domain erhalten vom Lizenz-Server einen gemeinsamen Domain-Key (Kd)*, *der mit dem öffentlichen Schlüssel des jeweiligen Gerätes verschlüsselt ist*
- *Die Content-Keys (cek) in den Lizenzen (Rechte-objekten) werden mit dem symmetrischen Domain-Key (AES) verschlüsselt*



Sicherheit der Implementierung



a) ***Zugriff auf unverschlüsselte Daten***

b) ***Modifikation des DRM-Controllers***

c) ***Manipulation der Zähler***

d) ***Auslesen eines Content-Keys***

e) ***Der schlimmste Fall: Auslesen des privaten Geräteschlüssels***

Obfuscation-Techniken (Anti-Debugging, …) können die Sicherheit der Implementierung erhöhen

Am Schluss bleiben viele Fragen

- Wird DRM sich überhaupt durchsetzen?
- Welches DRM wird sich durchsetzen?
- Welche Geschäftsmodelle werden sich durchsetzen?
- Wie sicher muss DRM sein?
- Welche Einfluss hat DRM auf das Urheberrecht?
- Welchen Einfluss hat DRM auf die Privatheit?
- Wem nützt DRM wirklich?
- Welchen Einfluss hat DRM auf die PC-Branche?
- Wird es noch legale Angebote ohne DRM geben?
- Werden körperliche Datenträger verschwinden?

Vielen Dank

Probevorlesung
Dr.-Ing. Jürgen Nützel,
Juergen.Nuetzel@tu-ilmenau.de
Technische Universität Ilmenau

TECHNISCHE UNIVERSITÄT ILMENAU

Diese Folien zeigen einen Ausschnitt und eine Zusammenfassung einer Vorlesungsreihe, die ab dem Sommersemester 2006 vom Autor für Studierende der Informatik, Wirtschaftsinformatik, Medientechnik und Medienwirtschaft angeboten wird.

Übungsaufgaben: www.juergen-nuetzel.de/drm.html