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**

DRM-Referenz-Modell

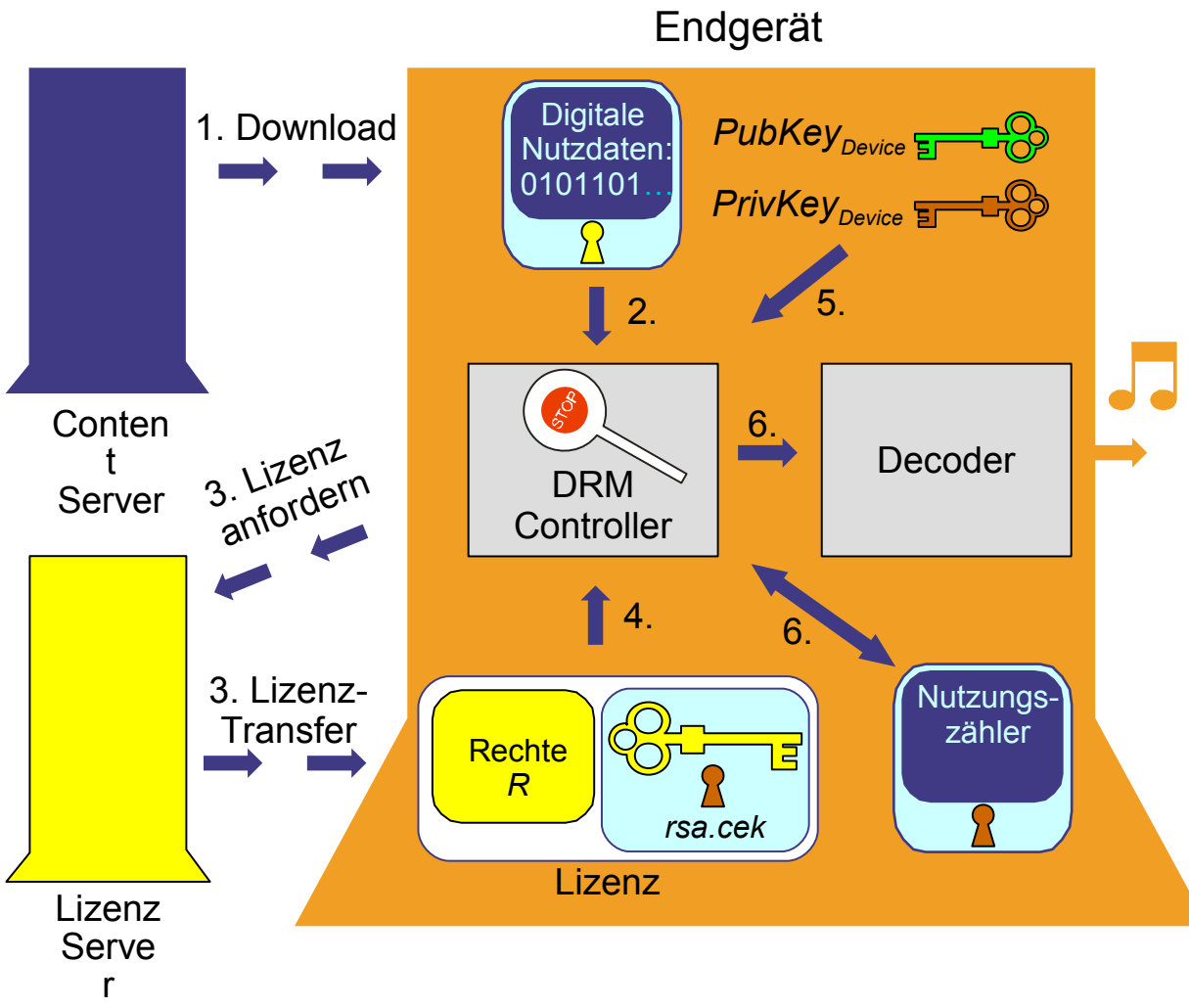
***Folien stellen ein zusätzliches Informationsangebot für die Teilnehmer der Vorlesung dar.
Die Vorlesung richtet sich an Studierende der Informatik,
der Ingenieurinformatik, Wirtschaftsinformatik, Medienwirtschaft,
Angewandten Medienwissenschaft und Medientechnik.***

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

Überblick

- **Aufbau des Referenz-Modells**
- **Zusammenfassung**
- **Neue Geschäftsmodelle**
- **Sicherheit der Implementierung**

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

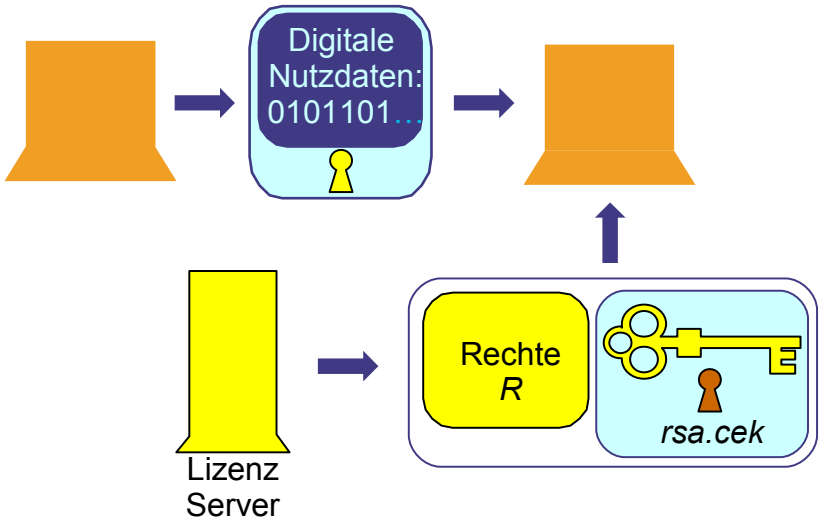
Zusammenfassung

- **Nutzdaten sind symmetrisch verschlüsselt**
  - *Nutzdaten sind ohne Schlüssel (CEK) wertlos*
  - *Im unverschlüsselten Teil steht die Adresse des Lizenz-Servers*
- **Schlüssel wird in der Lizenz transportiert**
  - *Lizenz enthält Rechtebeschreibung*
  - *Rechte werden im DRM-Controller ausgewertet*
- **Asymmetrische Kryptographie**
  - *Nachrichten (z.B. Rechtebeschreibungen) werden von beiden Seiten signiert*
  - *Zertifikate werden eingesetzt*
  - *Schlüssel (CEK) in der Lizenz wird vom Server mit dem öffentlichen Schlüssel des Endgerätes verschlüsselt*
  - *Der private Endgeräteschlüssel ist der Sicherheitsanker*

Neue Geschäftsmodelle

Superdistribution

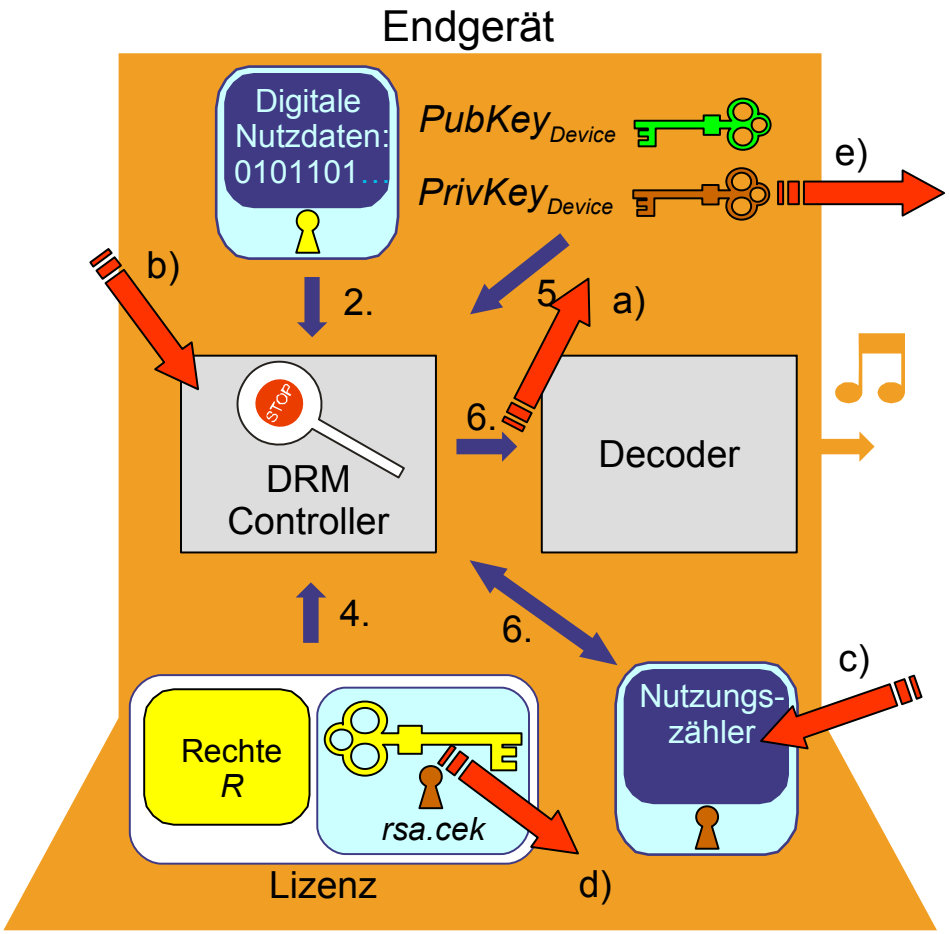
- *Legales P2P-File-Sharing*
- *Verschlüsselte Nutzdaten werden von den Kunden weitergegeben*
- *Lizenz wird vom Lizenz-Server nachgeliefert*



Musik-Abonnement

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

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

Weitere Informationen

- *Jürgen Nützel: Die informatorischen Aspekte virtueller Güter und Waren, Oktober 2006 im Universitätsverlag 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*
- *Rosenblatt, B.; Trippe, B.; Mooney, S.: Digital Rights Management, Business and Technology, M&T Books, New York, 2002*
- *Eilam, Eldad: Reversing: Secrets of Reverse Engineering, Wiley Publishing Inc., Indianapolis, USA, 2005*