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**

Open Mobile Alliance DRM 2.0

***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

- **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***
  - ***Abo-Modelle***

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*
- *2002 aus dem WAP-Forum hervorgegangen*

Was ist OMA DRM?

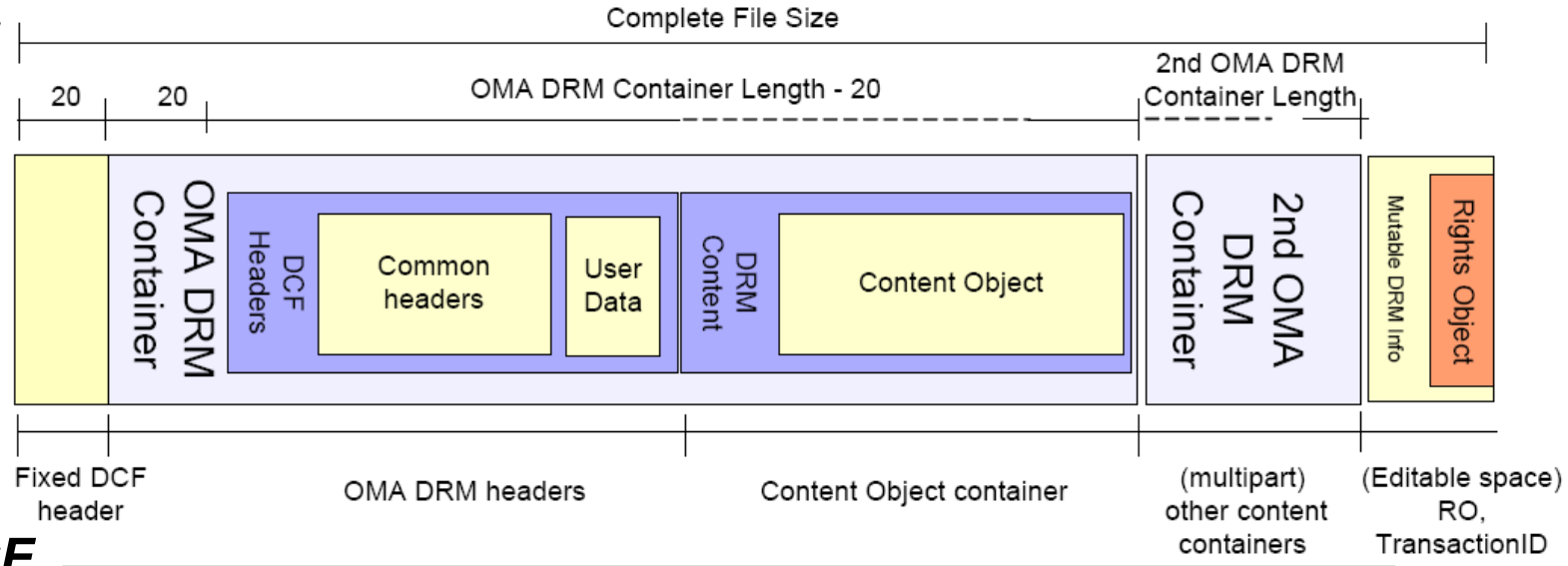
- *In der Version 1.0 ein sehr einfacher formatunabhängiger Standard für mobile Endgeräte. Einfache Sicherheitsanforderungen wurden berücksichtigt.*
- *Version 2.0 ist ein umfassender Standard, der auch komplexe Sicherheitsanforderungen (nicht nur für mobile Endgeräte) umsetzt. Final seit März 2006.*
- *Die Version 2.0 bietet unter anderem das Domain-Konzept*

OMA DRM Content Format

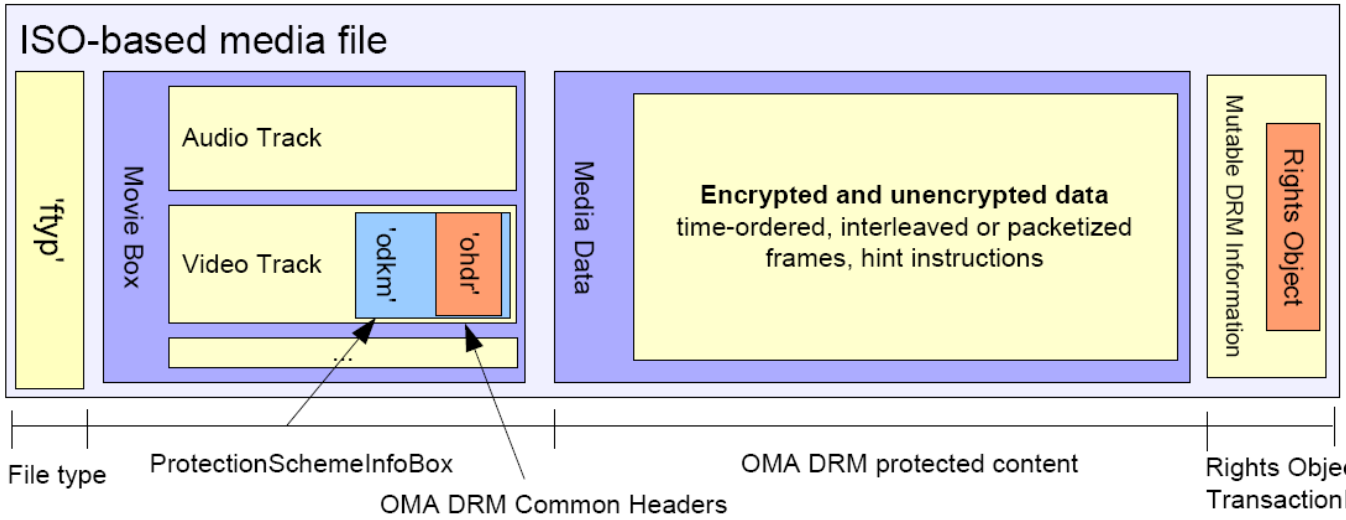
- **OMA DRM ist formatunabhängig**
  - ***Das DCF (Discrete Media Profile) ist ein Container-Format für AES-verschlüsselte Inhalte, die als Einheit betrachtet werden. DCF ist an das ISO-Fileformat angelehnt. (Endung: .odf)***
  - ***PDCF (Packetized DCF) ist für kontinuierliche Formate (Audio und Video). Verschlüsselung (mit AES) erfolgt hier paketweise.***
  - ***DCF und PDCF enthalten keinen Hinweis auf einen Schlüssel***
  - ***Schlüssel (CEK) wird durch getrennte Rechteobjekte (RO) bereitgestellt***

DCF und PDCF

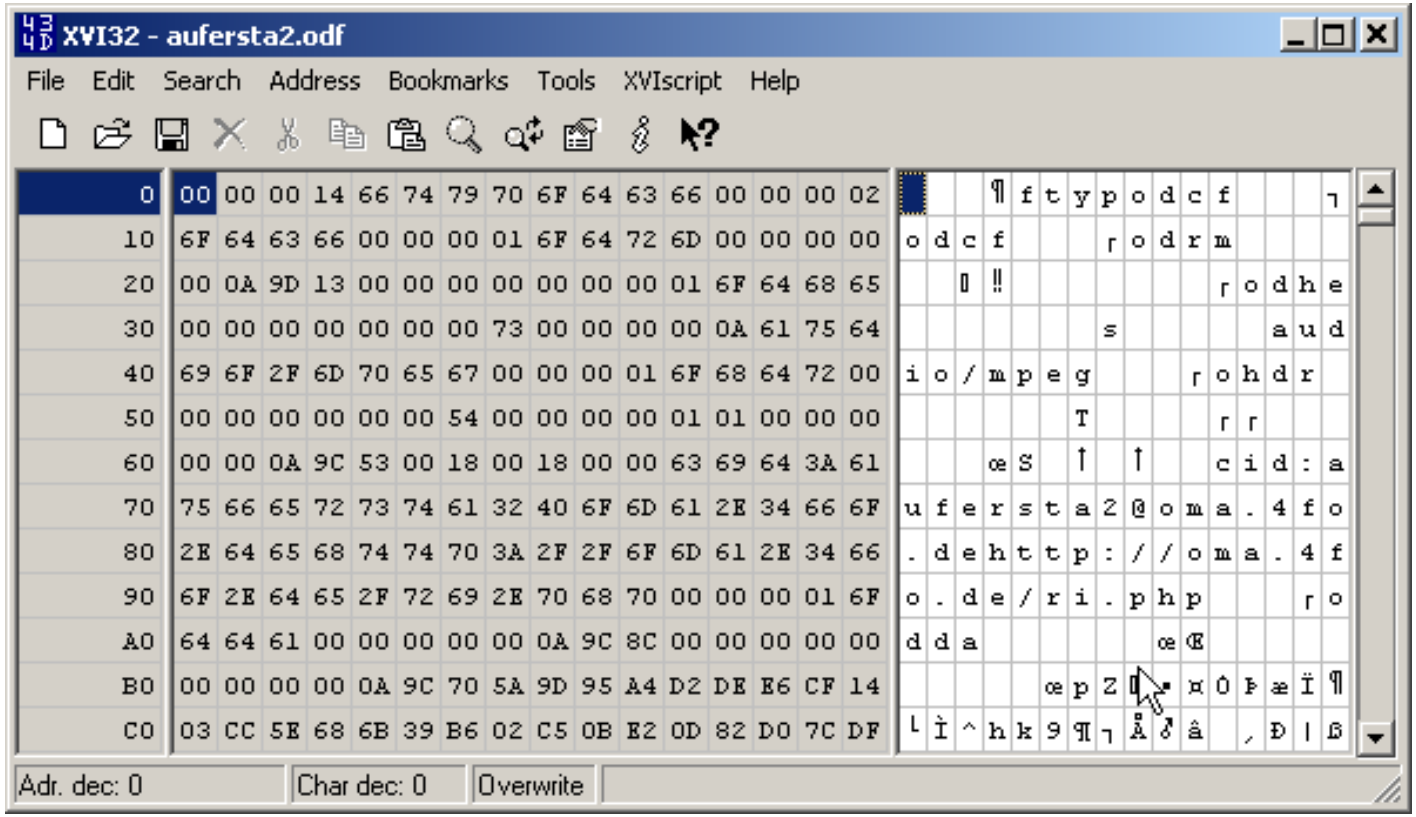
- **DCF**



- **PDCF**

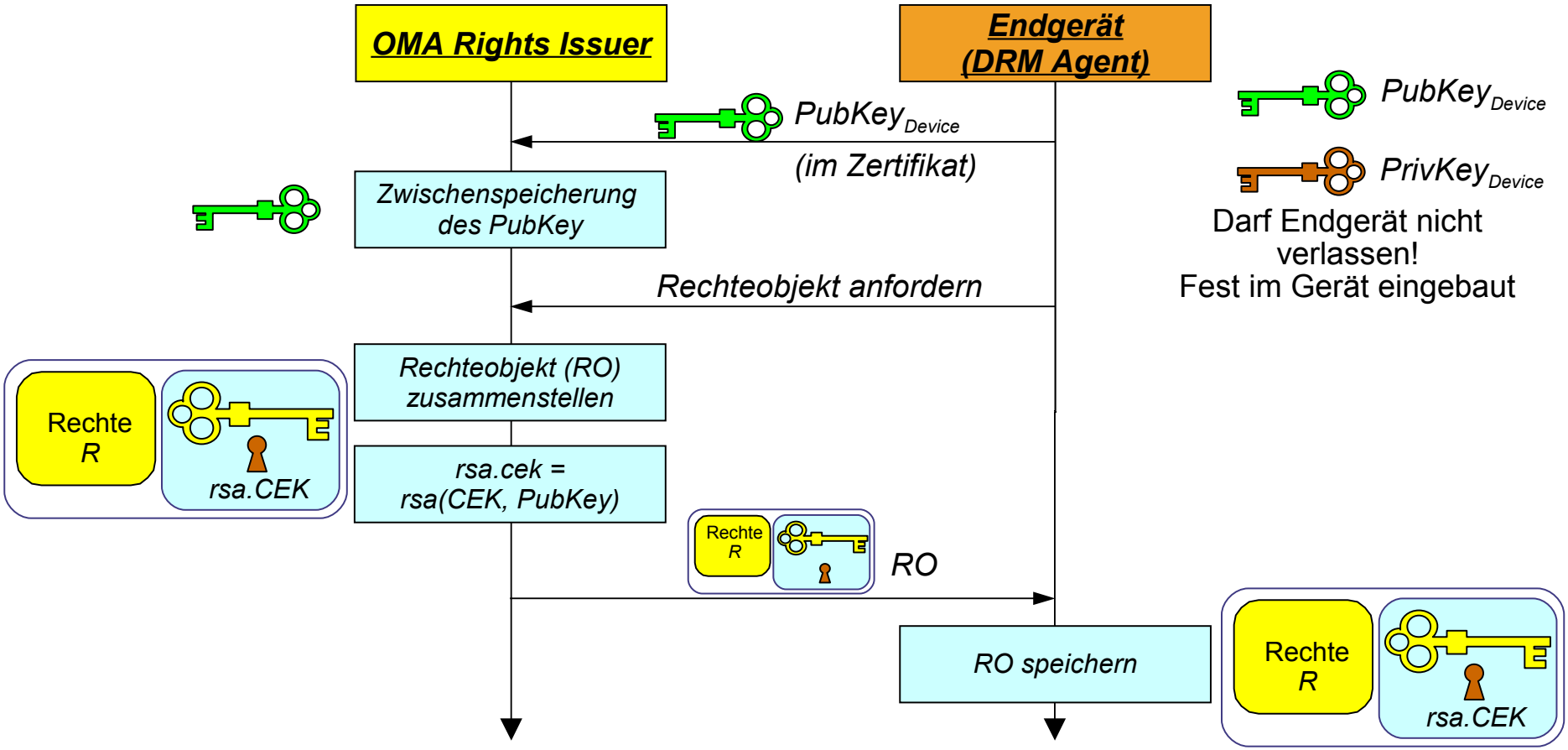


Ein Beispiel-File (.odf)



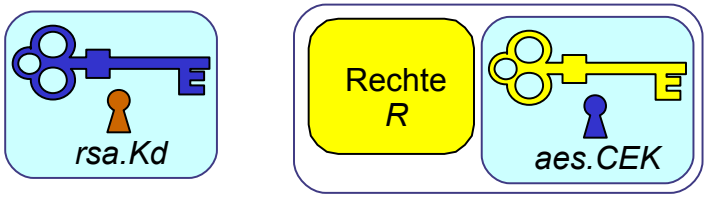
Rechte anfordern

- **ROAP (Rights Object Acquisition Protocol)**
  - ***Stark vereinfacht (Registrierung & RO Bezug)***



Das Domain-Konzept

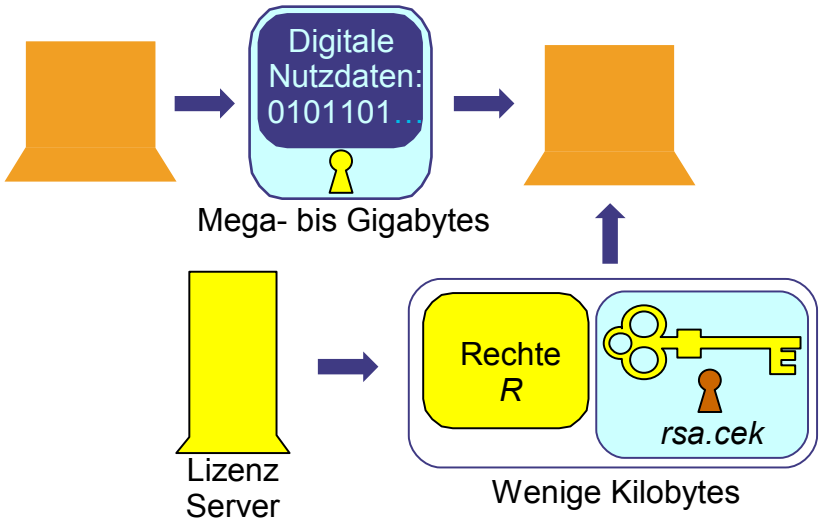
- **Ziel**
  - ***Einfaches Kopieren von Content- und Lizenz-Dateien zwischen mehreren Geräten eines Nutzers oder Nutzergruppe***
- **Umsetzung**
  - ***Endgeräte einer Domain erhalten vom Lizenz-Server einen gemeinsamen Domain-Key (Kd), der mit dem öffentlichen Schlüssel des jeweiligen Gerätes verschlüsselt ist***
  - ***Die Content-Keys (CEK) in den Lizenzen (Rechte-objekten) werden mit dem symmetrischen Domain-Key (AES) verschlüsselt***



Neue Geschäftsmodelle

Superdistribution

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

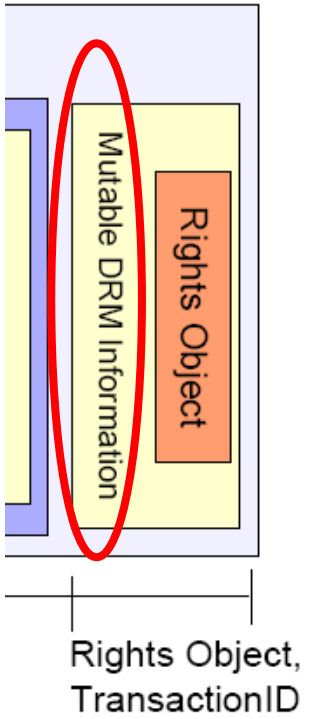


Musik im Abo/Miete

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

Transaction Tracking bei OMA DRM 2.0 für die belohnte Superdistribution

- **DRM Agent ließt und schreibt die TransactionID**
  - *Jedes mal wenn ein Rechteobjekt angefordert wird, wird die TransactionID (Transaktionsnummer - TAN) aus der DRM Datei ausgelesen*
  - *Die TAN wird an der Rights Issuer (RI) gesendet*
  - *Der Rights Issuer liefert das Rechteobjekt (RO) und eine neue TAN*
  - *Der DRM Agent ersetzt die TAN in der DRM Datei (in der Mutable DRM Info)*
  - *Ginny gibt die DRM Datei weiter (Superdistribution)*
  - *Empfänger (z.B. Harry) fordert ebenfalls ein RO an*
  - *An der TAN erkennt der Anbieter, vom wem Harry die DRM Datei erhalten hat*
  - *Ginny kann vom Anbieter/Betreiber belohnt werden*



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*
- *www.openmobilealliance.org*