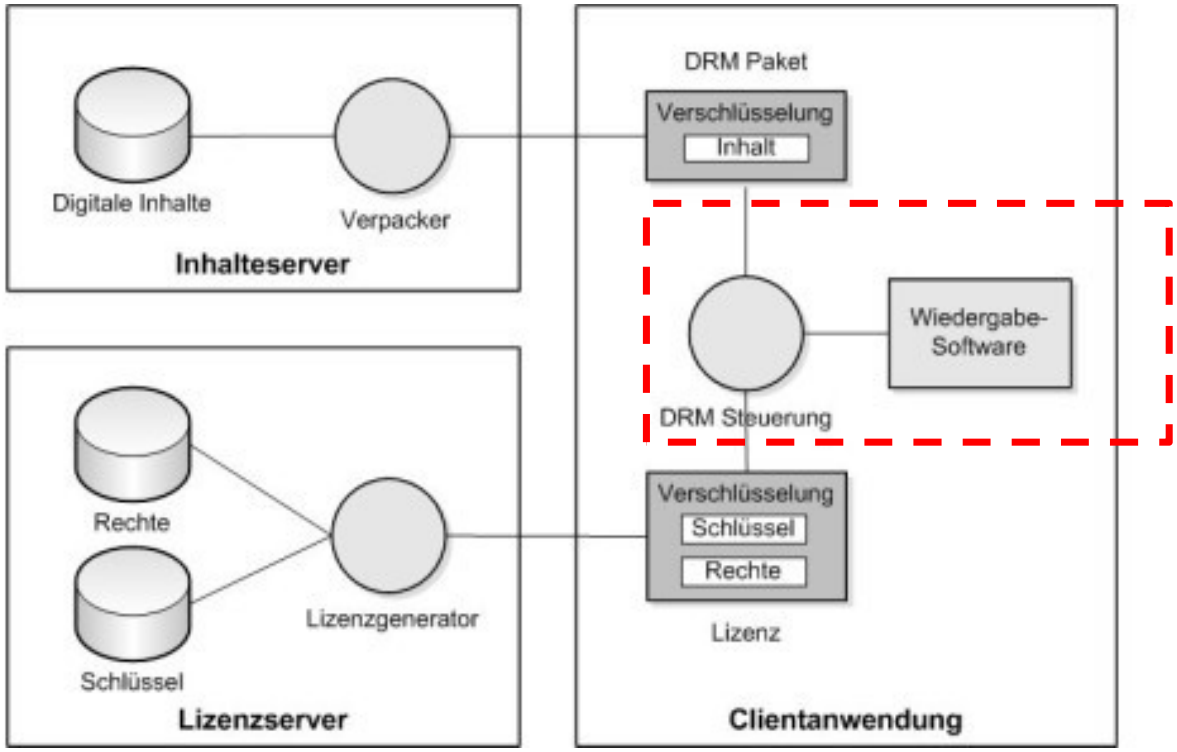
DRM

Digital Rights Management

- Kritiker: Digital *Restriction* Management
- Schutz von Urheber- und Vermarktungsrechten an geistigem Eigentum
  - vor allem an Film- und Tonaufnahmen
  - aber auch an Software oder elektronischen Bücher
- Abrechnungsmöglichkeiten für Lizenzen und Rechte
- Kernproblem: beliebige Kopierbarkeit von digitalen Inhalten
  - ohne jeden Qualitätsverlust
  - ohne nennenswerten Aufwand ("Mausklick genügt")
- DRM könnte Zwangsabgaben z.B. auf Leerkassetten und Fotokopierer an GEMA und VG Wort überflüssig machen
- Aber:
  - Datenschutzproblemen
  - erhebliche Einschränkungen bei der Benutzerfreundlichkeit von Computer-Dateien .

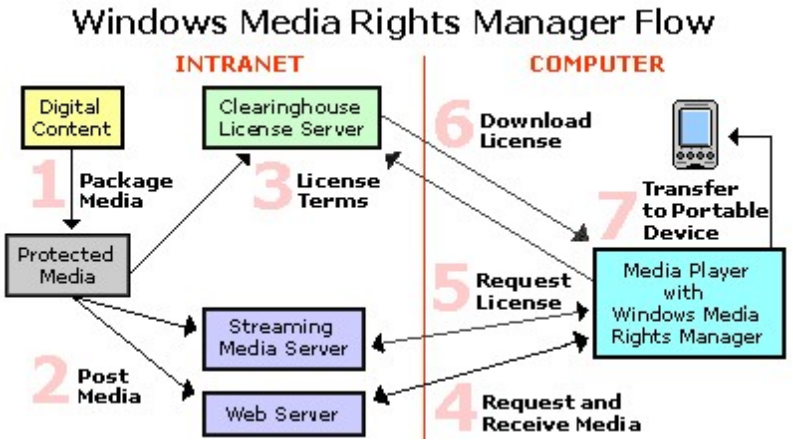
http://de.wikipedia.org/wiki/Digital_Rights_Management

DRM - Schema

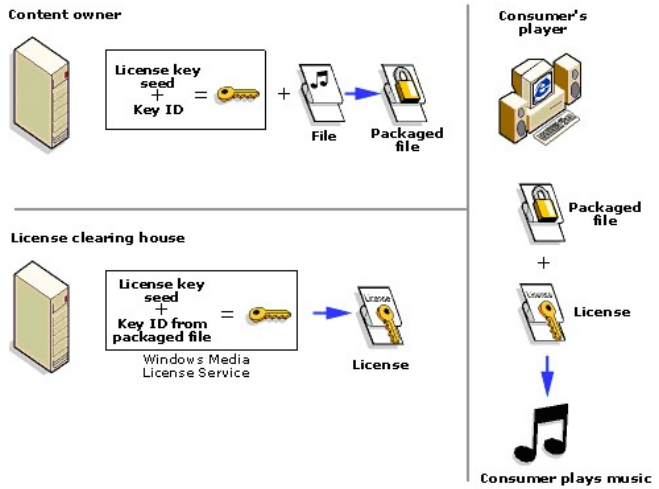


Wikipedia/Prussio, CC-by-sa 2.0/de

- Beispiel für ein weit verbreitetes DRM System
- Ablauf:
  - Packaging
    - Verschlüsseln der Mediendatei
    - Resultat
      - Verschlüsselte Mediendatei inklusive URL von der Lizenzquelle
      - Lizenzdatei mit Schlüssel
  - Distribution der verschlüsselten Mediendatei
  - Zugriff auf einen Lizenz-Server
    - Authentisieren des Käufers wird vorgenommen
  - Kauf einer Lizenz
    - Kann z.B. auch automatisch beim Zugriff auf eine verschlüsselte Datei durchgeführt werden
    - „Stille“ Lizenzierung ist möglich
  - Abspielen der verschlüsselten Mediendatei
    - Unter Beachtung der in der Lizenzdatei festgelegten Rechte

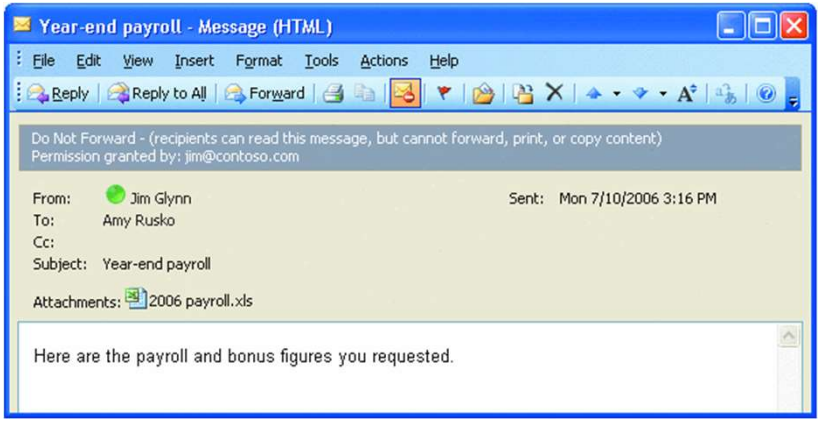


http://www.microsoft.com/windows/windowsmedia/howto/articles/drmarchitecture.aspx



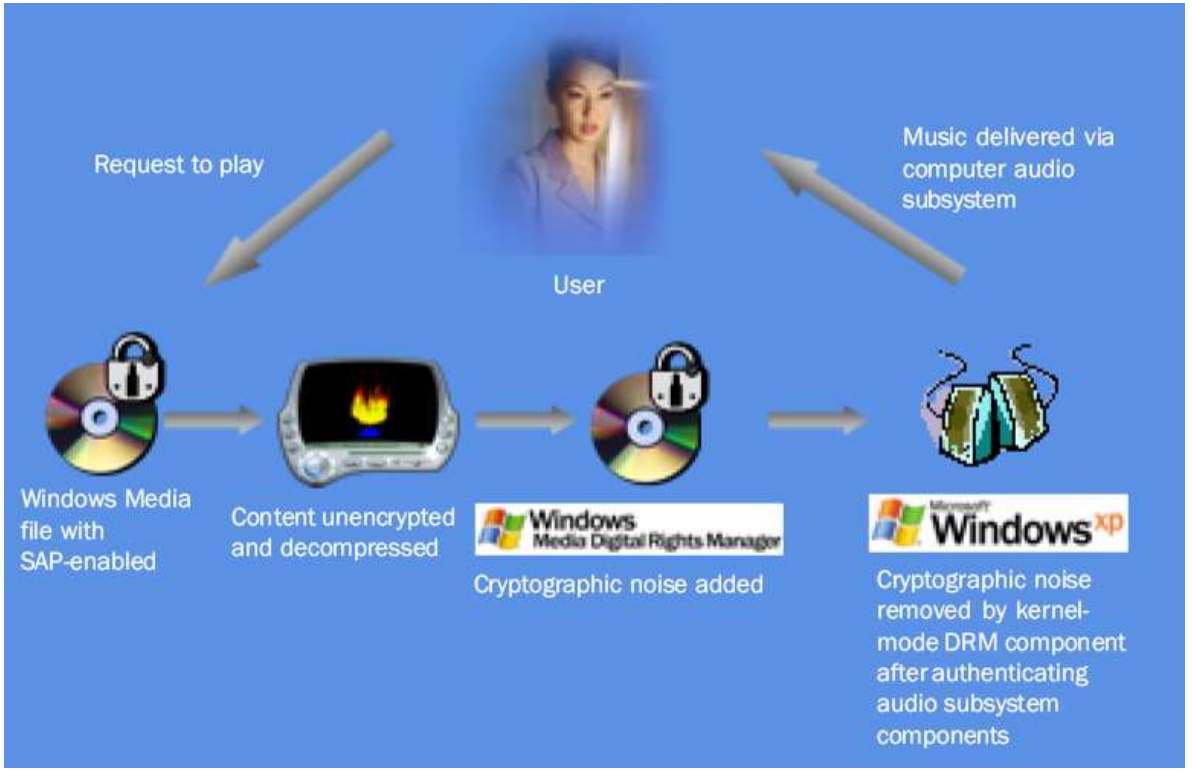
- In Windows System integriert
- Besteht aus
  - Server
  - Client
  - Anwendung
- Schutz durch PKI
  - PKI wird von Server organisiert
- Rechte in REL definiert
  - Rights Expression Language
  - XRML
- Erlaubt beispielsweise Erstellen von geschützten Office Dokumenten

https://technet.microsoft.com/de-de/magazine/2006.10.howitworks(en-us).aspx



DRM / Microsoft DRM Secure audio path

- Beliebte Angriffsstrategie auf DRM: Virtuelle Treiber, die Medien direkt aufzeichnen
- Gegenmaßnahme bei Microsoft DRM: Secure Audio Path



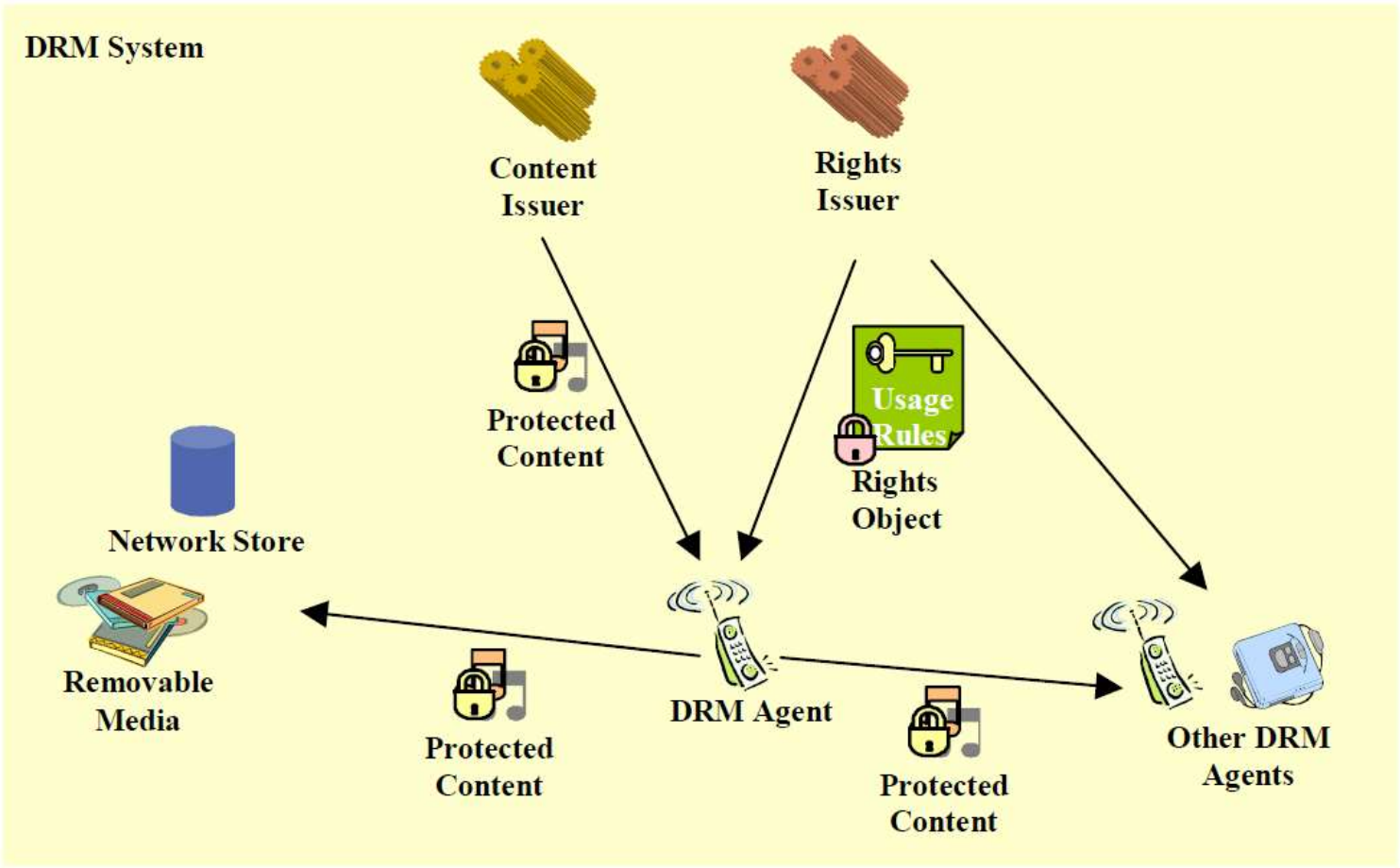
http://download.microsoft.com/download/a/1/a/a1a66a2c-f5f1-450a-979b-ddf790756f1d/WMRMsap_bro.pdf

MPEG-21

- Auch "Multimedia Framework“ genannt
- Aktiv seit 6/2000
- Aufgeteilt in 14 unabhängige Teile, inklusive
  - Rights Expression Language (Part 5)
  - Rights Data Dictionary (Part 6)
  - Beide Teile sind DRM-relevant
- Grundkonzept von MPEG-21: Das “Digital Item”
  - Entspricht einem Paket mit einem freien Inhalt, mit dem der Anwender interagieren kann
  - Beispielsweise Mediendaten, Metadaten oder Referenzen

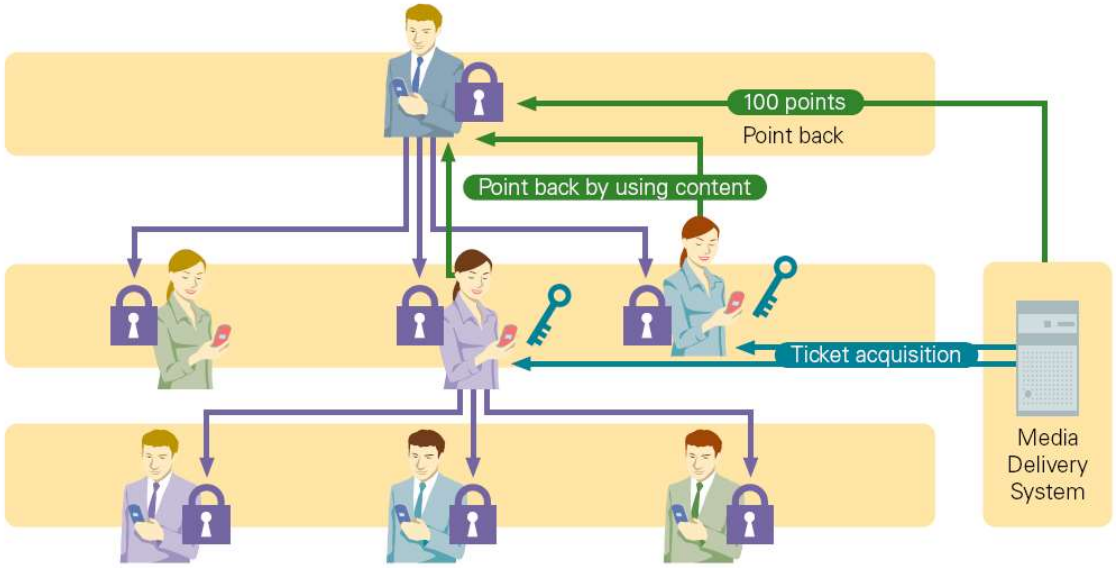
Open Mobile Alliance (OMA)

- Aktiv seit 6/ 2002
- Ca. 200 Unternehmen, unter anderem die wichtigsten Mobilfunkanbieter, Hardwareentwickler und Netzbetreiber
- OMA DRM 1.0: DRM für Klingeltöne und Hintergrundbilder, gedacht für Geräte mit minimalen Fähigkeiten
  - Verschlüsseln von Inhalten
  - Schlüsseltransfer ungeschützt über XML
- OMA DRM 2.0: Lösung für komplexere Geräte, unter anderem inklusive
  - Public Key Verschlüsslung
  - Integritätsschutz für Objekte
  - Rights Expression Language
    - Basierend auf ODRL
  - Unterstützung Offline Geräte
- Spezifikationen unter http://openmobilealliance.org/release/DRM/



http://www.openmobilealliance.org/Technical/release_program/docs/DRM/V2_0_2-20080723-A/OMA-AD-DRM-V2_0_1-20080226-A.pdf

- Super distribution: Nutzen von DRM Architekturen zu Marketing-Zwecken
- Kunden dürfen DRM-geschützten Inhalt frei verteilen
- Empfänger kann Inhalt in Preview-Qualität konsumieren
- Volle Qualität nach Kauf von Lizenzen
- Vorteil für Rechtinhaber: Entlastung der Distributionswege



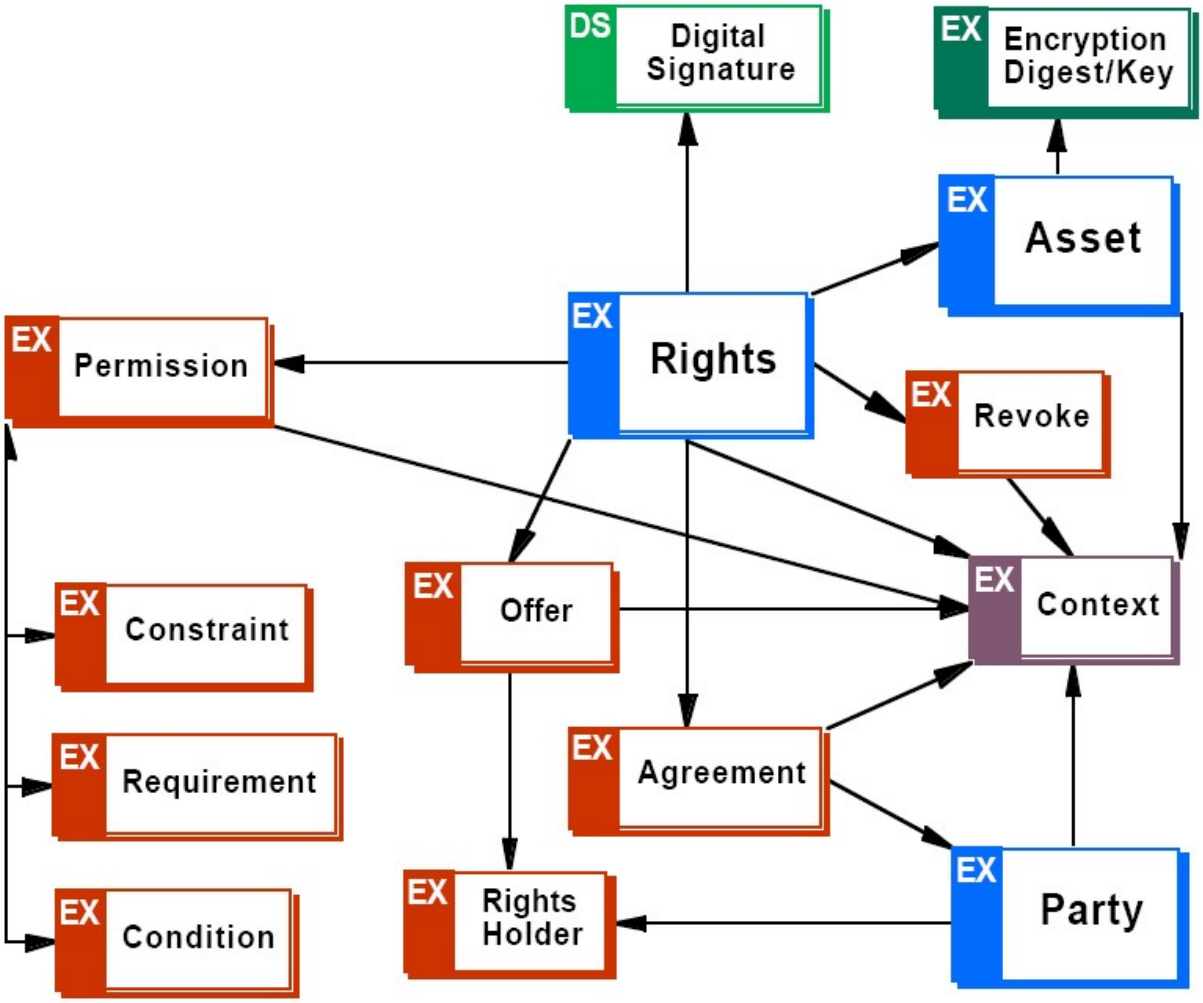
http://www.nec-mobilesolutions.com/application/pdf/oma_drm.pdf

DRM / Open Digital Rights Language (ODRL)

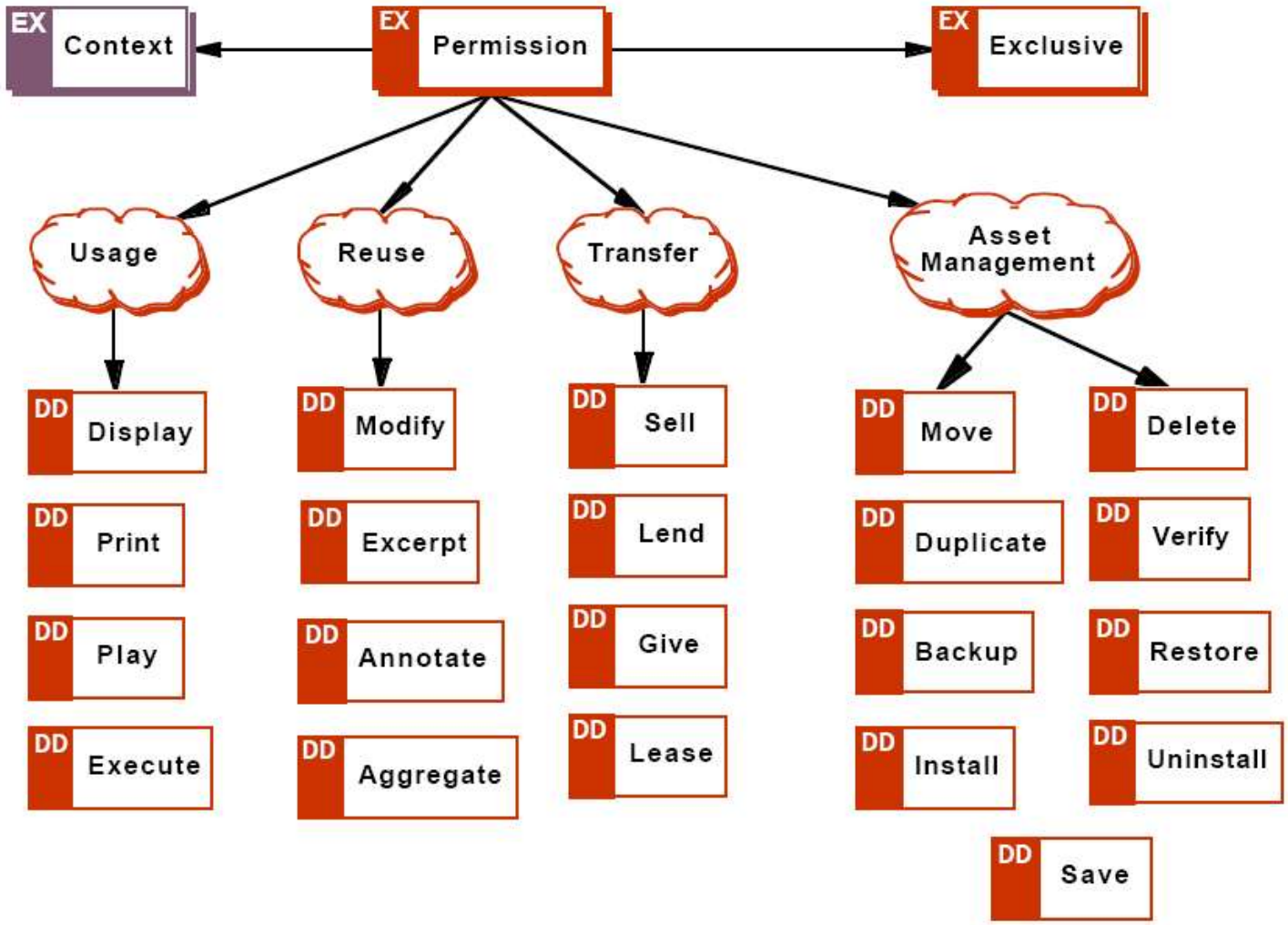
- Ziele
  - Standardisierte DRM Sprache schaffen
    - Alle notwendigen Sprachelemente beinhalten, die zur Formulierungen von DRM-Vorgängen notwendig sind
    - flexibel und erweiterbar
  - Unterstütze Objekte
    - Bilder, Audio, Video, Software, ...
- Wird heute z.B. genutzt, um Rechte an Nachrichten zu handhaben
- Grundlage für OMA RDL

- Expression Language
  - XML basierte Definition von Modellen und Funktionen eines DRM Systems

Open Digital Rights Language (ODRL)
Version: 1.1
Date: 2002-08-08
Available at: <http://odrl.net/1.1/ODRL-11.pdf>



- Expression Language
  - Permission Model

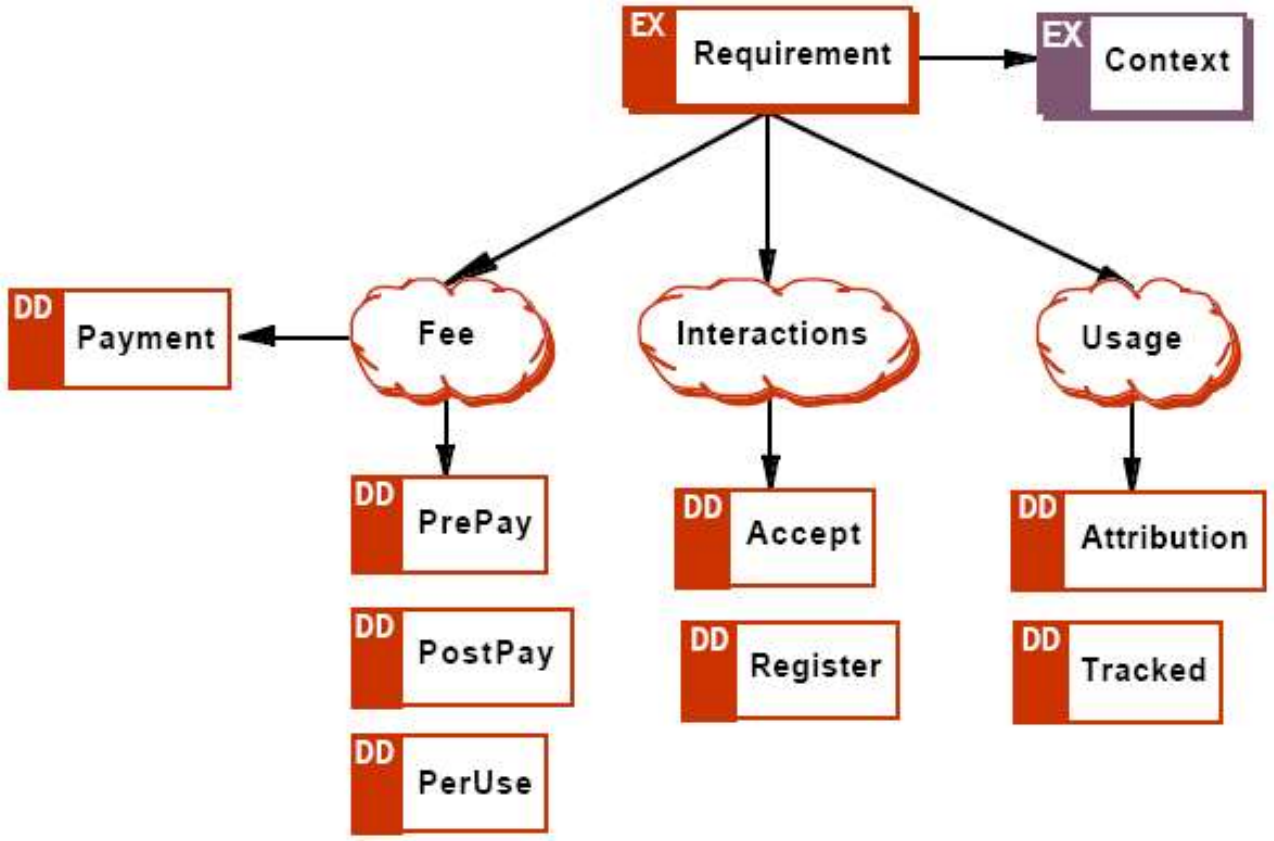


Open Digital Rights Language (ODRL)
Version: 1.1
Date: 2002-08-08
Available at: <http://odrl.net/1.1/ODRL-11.pdf>

- Beispiel für Permission
  - erlaubt Anzeigen
  - Drucken (5-maliges)
  - Annotieren

```
<permission>
    <display/>
    <print>
        <constraint>
            <count>5</count>
        </constraint>
    </print>
    <annotate/>
</permission>
```

- Expression Language
  - Requirements Model



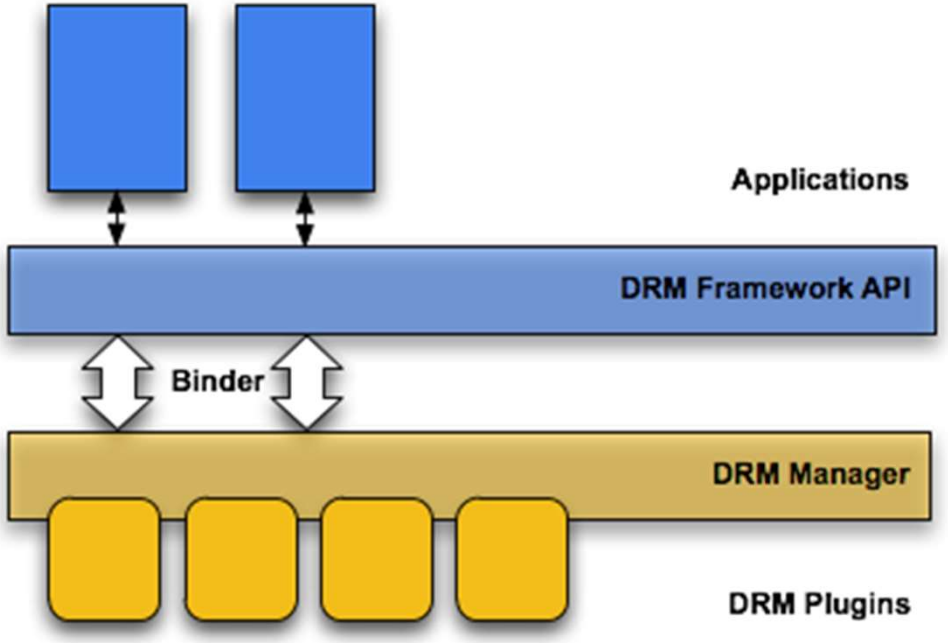
Open Digital Rights Language (ODRL)
Version: 1.1
Date: 2002-08-08
Available at: <http://odrl.net/1.1/ODRL-11.pdf>

DRM / Open Digital Rights Language (ODRL)

- Letztendlich werden hier Nutzungsrechte auf Objekte allgemein definiert
  - Möglichst eindeutig
  - Vergleichsweise intuitiv verständlich
  - Umfassend
- DRM Systeme sollen diese Beschreibung dann in technische Regeln übersetzen
- Vorteil:
  - Allgemeine Beschreibung über Systemgrenzen hinweg
  - Teilung von Rechtedefinition und Rechteumsetzung

Android DRM

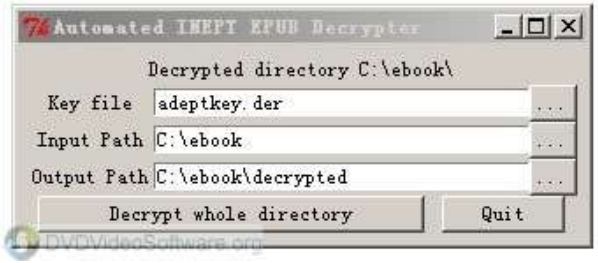
- DRM als Service/ Framework



http://developer.android.com/

Adobe ADEPT

- Gebrochen durch Werkzeug, welches
  - Schlüssel ausliest
  - Verschlüsselte Datei entschlüsselt



http://www.dvdvideosoftware.org/guide/remove-drm-from-adobe-adept.html

http://www.pc-magazin.de/

Schutz auf der Blu-ray Disk:

- Advanced Access Content System (AACS)
  - Verwendet 128 Bit AES
  - Jeder Player hat eine Menge von Schlüsseln, mit denen er Content entschlüsseln kann
    - Wird ein Schlüssel korrumpiert, sollen zukünftige Medien diesen nicht mehr unterstützen
  - Erlaubt das Verfolgen von Kopien durch das Konzept „*Sequence keys*“
    - Anhängig vom Schlüssel werden unterschiedliche Teile der Disk entschlüsselt
    - Wird eine entschlüsselte Kopie, z.B. als DivX weitergegeben, kann anhand der Bestandteile auf den verwendeten Schlüssel geschossen werden
  - Managed Copy Konzept
    - Ermöglicht Erstellen von Kopien nach Kontakt zu Server
    - Gedacht für Umgebungen, in denen Kopien ein Recht des Nutzers sind

Spezifikation unter http://www.aacsla.com/specifications/

Schutz auf der Blu-ray Disk:

- Advanced Access Content System (AACS)
  - Erfolgreiche Angriffe auf verschiedene Schlüssel
    - Sowohl für einzelne Filme als auch für alle Filme, die zu diesem Zeitpunkt verfügbar waren
  - Ausspähen der Schlüssel von Software-Playern aus dem Speicher
    - WinDVD
    - PowerDVD
  - Revocation der Schlüssel durch Software-Updates
    - Neue Schlüssel bereits eine Woche vor Verkaufsstart der neuen Softwareversionen verfügbar

Schutz auf der Blu-ray Disk:

- BD+
  - Basiert auf Self-Protecting Digital Content (SPDC)
  - Virtuelle Maschine auf dem Player, die
    - Softwareupdates durchführen kann
    - Integrität von Playern prüfen kann
      - Schlüssel
      - Firmware
    - Inhalte entschlüsseln kann
  - Spezifikationen sind nicht öffentlich
  - Potential: Hersteller können Sicherheitslücken durch Patches nachträglich schließen

Schutz auf der Blue-ray Disk:

- BD+

  AnyDVD HD now with BD+ support

  Film studios that have switched to Blu-ray may have crowed a little too early because the much-praised BD+ copy protection is an ad absurdum affair now, too. With today's release of version 6.4.0.0 of AnyDVD HD it is now also possible to make backup security copies of Blu-ray discs protected with BD+.

  Richard Doherty of the Envisioneering Group will have to revise his statement from July, 2007 regarding BD+: "**BD+, unlike AACS which suffered a partial hack last year, won't likely be breached for 10 years**". It is worth mentioning that since he made that statement only eight months have gone by.

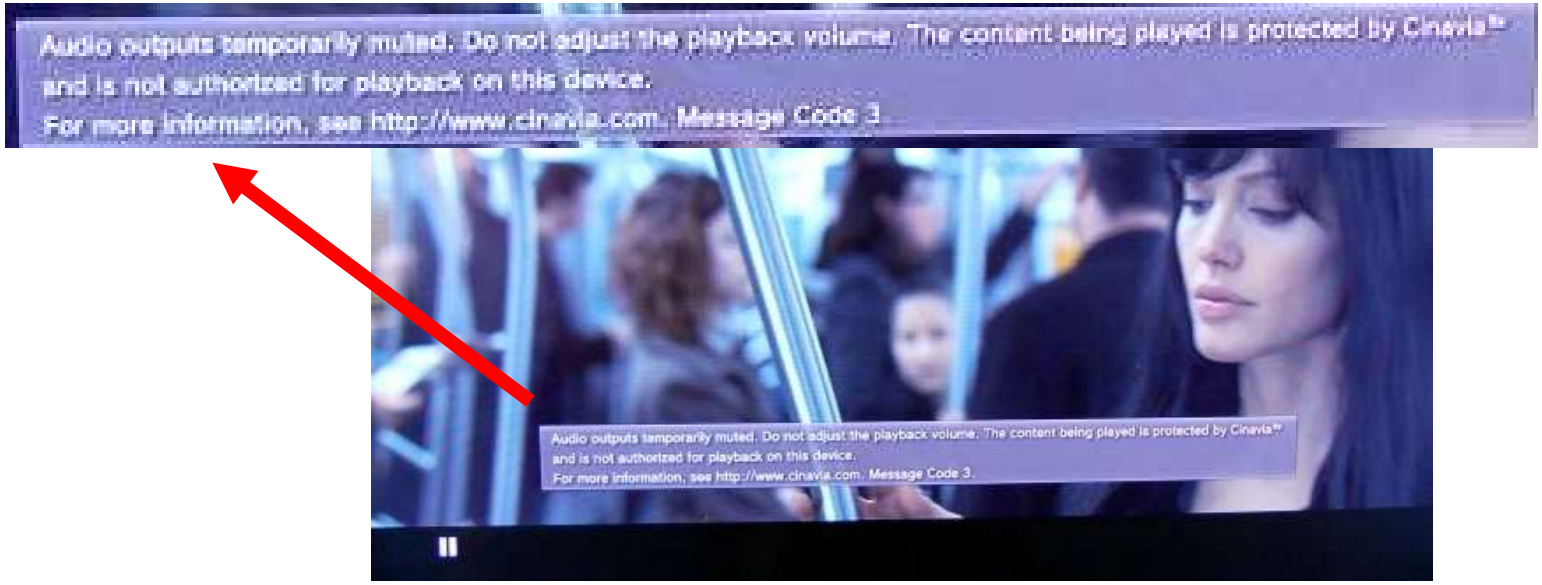
  http://forum.slysoft.com/showthread.php?t=14786

- Slysoft war in Antigua beheimatet
  - 2016 aufgelöst
  - Angeblich auf Druck der US Regierung auf Antigua über Banken

Schutz auf der Blue-ray Disk:

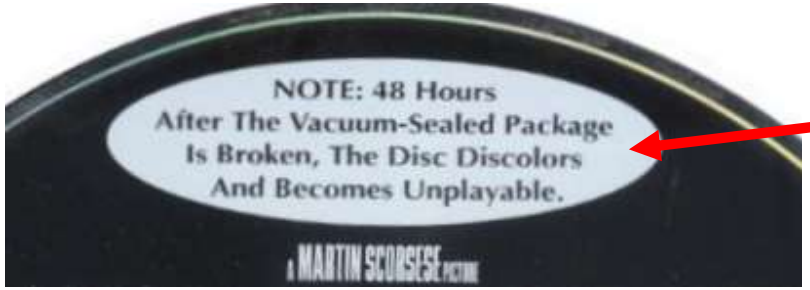
- Audiowasserzeichen Cinavia
  - Einbetten von Wasserzeichen in Kinovorführungen und in Tonspuren
  - Wird ein Wasserzeichen aber kein Kopierschutz gefunden, geht man von einer illegalen Kopie aus
    - Stummschalten nach 20 Minuten
  - Alle Geräte, die seit 2012 verkauft wurden, müssen Wasserzeichendetektor unterstützen

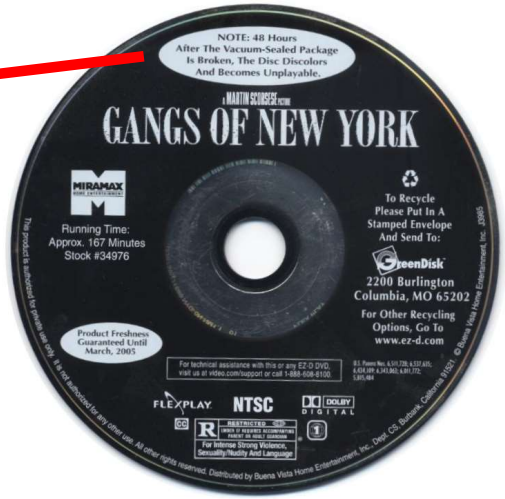
https://tarnkappe.info/blu-ray-kopierschutz-cinavia-geknackt/



DRM / Blu-ray

- Angriffe auf Cinavia
  - Entfernen des Wasserzeichens
    - Verursacht oft starken Verlust der Klangqualität
      - Von Disk zu Disk individuelle Anpassung nötig
      - Erfordert Disk-Datenbank
    - Hacken der Abspielsoftware
      - Cinavia Abfrage oder Meldung wird deaktiviert
  - Seit April 2015 angeblich erfolgreiches Entfernen durch SlySoft
    - Immerhin hat sich der Schutz selbst dann mehrere Jahre gehalten

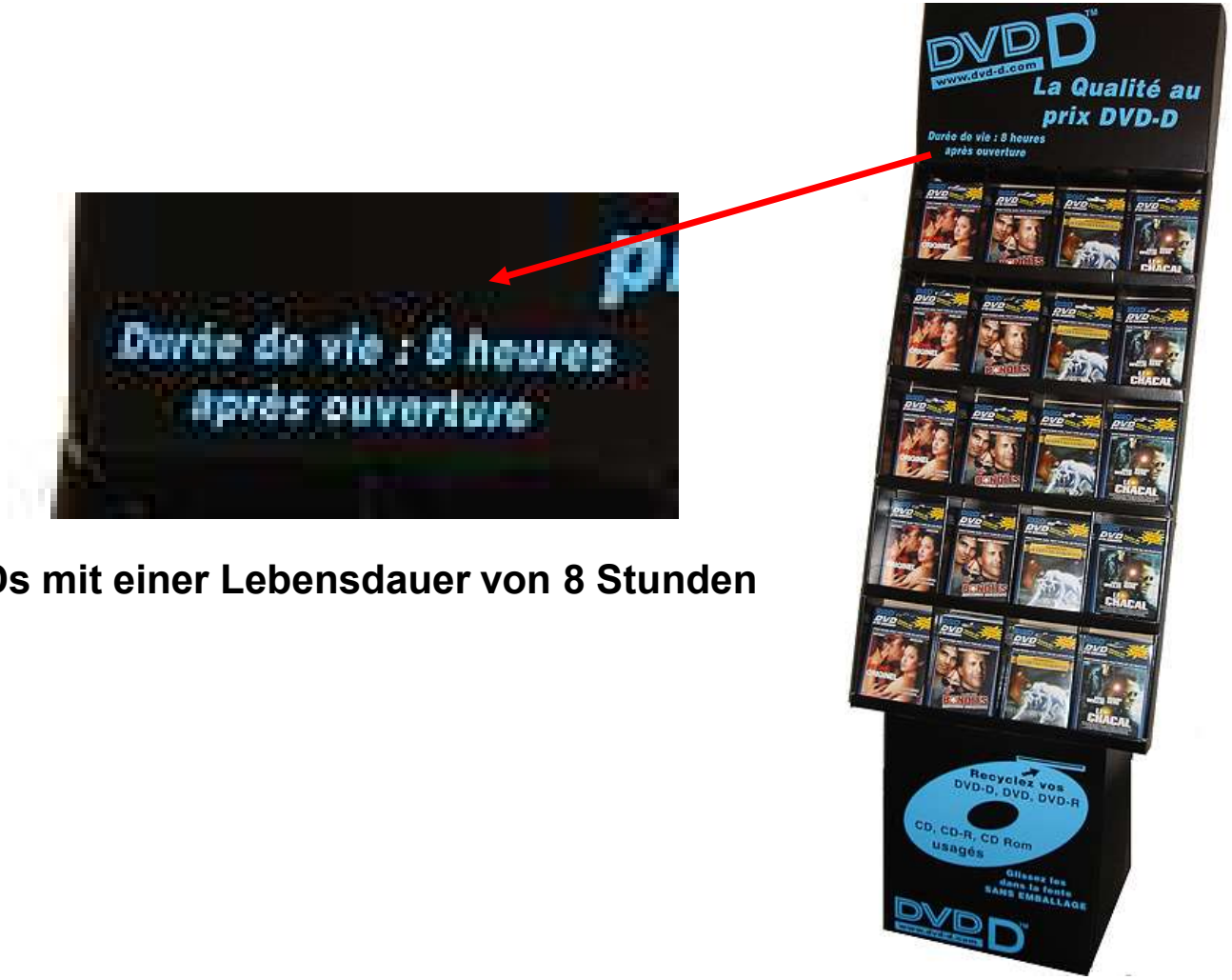




- „Disposable CD“
- DVD wird in Vakuum-Verpackung geliefert
- Nach Öffnen zerstört ein chemischer Prozess die DVD innerhalb von 48 Stunden
- Spezieller Farbstoff, der mit Sauerstoff reagiert
- Alternativ auch von „SpectraDisc”angeboten
- Kein kommerzieller Erfolg
- Ablehnung wegen Umweltbelastung

http://en.wikipedia.org/wiki/Flexplay

- http://www.dvd-d.com



DVDs mit einer Lebensdauer von 8 Stunden

DRM / Resümee

- DRM benötigt
- Verschlüsslung von Inhalten
- Authentifizierung von Nutzern oder Geräten
- Manipulationsschutz
- Sichere Wiedergabekanäle

- Realisiert wird DRM meist durch enge Integration in Betriebssystem
  - MS DRM
  - Fairplay
  - OMA DRM
- Bindung von Inhalten an Geräte
  - Public Key (OMA)
  - System-ID (MS)

DRM / Resümee

- DRM wird üblicher Weise gebrochen durch
- Ausspähen von Schlüsseln
- Abgreifen von entschlüsselten Inhalten
- NICHT MEHR durch Brechen der Kryptographie
  - Üblicher Weise wird hier Standard-Krypto verwendet
  - Früher kamen auch Caesar-Codes zum Einsatz…

DRM / Resümee

- DRM & Akzeptanz
- Akzeptiert bei Verleihlösungen
  - Hier nehmen Nutzer für geringe Kosten Restriktionen in Kauf
- Bei gekauften Inhalten viel Kritik
  - Revocation durch DRM (Amazon und Orwel Rücknahmen)
  - Beschränkung von Wiedergabegeräten
    - Was geschieht bei Wechsel vom Hersteller?
  - Bedenken hinsichtlich Bestandsunterstützung
    - Kann ich in 10 Jahren noch mein DRM-geschütztes Ebook lesen?