Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar
Mérnök informatikus szak, mesterképzés – Hírközlő rendszerek biztonsága szakirány
Villamosmérnöki szak, mesterképzés - Újgenerációs hálózatok szakirány

BMEVIHIM134 Hálózati architektúrák

6a. Tartalmak digitális kezelése

Pándi Zsolt, Híradástechnikai Tanszék,
és Papp Dorottya 2014-ben készült előadásda alapján
Jakab Tivadar
Híradástechnikai tanszék
2015

Áttekintés

- Digital Right Management (DRM)
- Törvényi keretek
- Technológiai részletek
  - Tartalmak eljuttatása a (mobil)készülékekre
  - Tartalmak felhasználása

Szabályozás

- Anticircumvention – csalás elleni védelem: tegyünk lakatot a tartalomra és szabályozzuk azt
  - Tilos feltörni a lakatot
  - Tilos olyan eszközt készíteni, ami feltöri a lakatot
  - Tilos elmondani bárkinek, hogy hogyan kell ilyen eszközt készíteni
  - Tilos elmondani bárkinek, hogy hol lehet ilyen eszközt találni
- USA: Digital Millennium Copyright Act
- EU: Az Európai Parlament és a Tanács 2001/29/EK irányelve (2001. május 22.) az információs társadalomban a szerzői és szomszédos jogok egyes vonatkozásainak összehangolásáról

EU

II. FEJEZET

JOGOK ÉS KIVÉTELEK

2. cikk

A többszörözési jog

A tagállamok biztosítják a **közvetett vagy közvetlen, ideiglenes vagy tartós, bármely eszközzel vagy formában, egészben vagy részben történő többszörözés** engedélyezésének, illetve **megtiltásának kizárólagos jogát**:

a) a szerzők számára műveik tekintetében;

b) az előadóművészek számára előadásaik rögzítése tekintetében;

c) a hangfelvétel-előállítók számára hangfelvételeik tekintetében;

d) a filmek első rögzítése előállítói számára filmjeik eredeti és többszörözött példányai tekintetében;

e) a műsorsugárzó szervezetek számára műsoraik rögzítése tekintetében függetlenül attól, hogy a műsor közvetítése vezeték útján vagy vezeték nélkül történik, ideértve a kábelen keresztül vagy műhold útján történő közvetítést is.

Üzleti modellek

- DRM rendszerek nem átjárhatóak
  - Nincs közös formátum
  - Nincs kapcsolat a rendszerek között
  - Nincs egységes konfiguráció
- Hogyan használhatom?
  - Vö.: papír könyv vs. DVD region-code-dal
- Mit vettem meg? Hordozót vagy tartalmat?
  - Pl.: tönkremegy egy zenei CD
- Időkorlát videókon, szoftvereken
- Jogosultságok szerzése bónuszként

Mit kell biztosítania egy DRM rendszernek?

KÖVETELMÉNYEK

Résztvevők és követelményeik

Készítő	Terjesztő	Fogyasztó
Kívánt szerzői jogok specifikálása	Metaadatok származtatása	Milyen tartalmat akar?
	Terjesztő jogainak specifikálása	Hogyan akarja használja a tartalmat?
	Tartalomhasználat felügyelete	
	Fizetési információk követése	

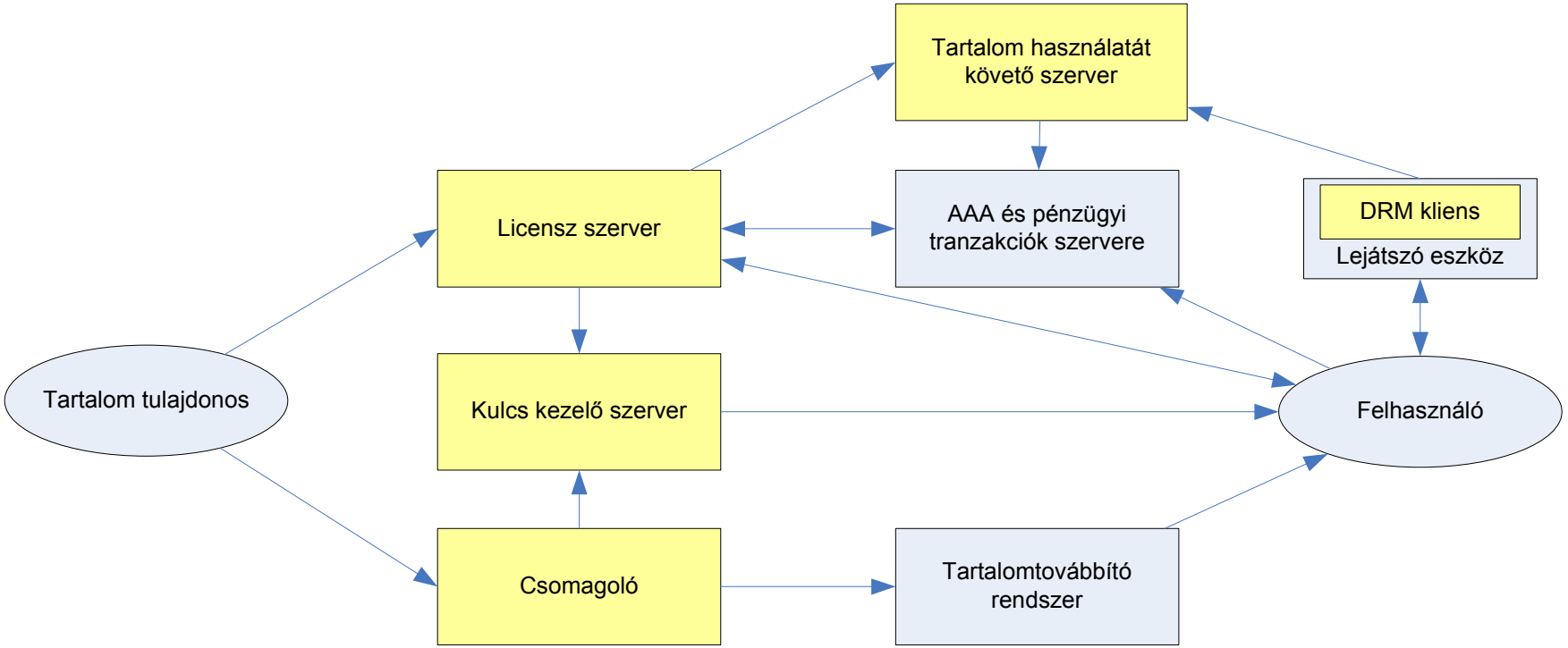
DRM

- DRM – Digital Right Management (jogok digitális kezelése)
- Digitális tartalmakhoz kapcsolódó jogok kezelésének a *technológiai* kérdéseit igyekszik megválaszolni

DRM (OMA)

The scope of OMA “Digital Rights Management” (DRM) is to enable the *distribution* and *consumption* of digital content in a controlled manner. The content is distributed and consumed on authenticated devices per the usage rights expressed by the content owners. OMA DRM work addresses the various technical aspects of this system by providing appropriate specifications for *content formats*, *protocols*, and *rights expression languages*.

Általános DRM architektúra



Fontosabb fogalmak

- Meta-adatok: az adott tartalomhoz kapcsolódó információk (azonosítás)
- Jogok: a felhasználás módjai (jogleíró módszerek) – lience file-ban
- Biztonság: illetéktelen hozzáféréstől, felhasználástól védve legyen a terjesztési út minden szakaszában
- Kulcskezelés: tartalom-hozzáférés, licence-file, vízjelek, kulcshoz jutás, kulcsszétosztás
- Együttműködés DRM rendszerek között: ???

Tartalom védelme

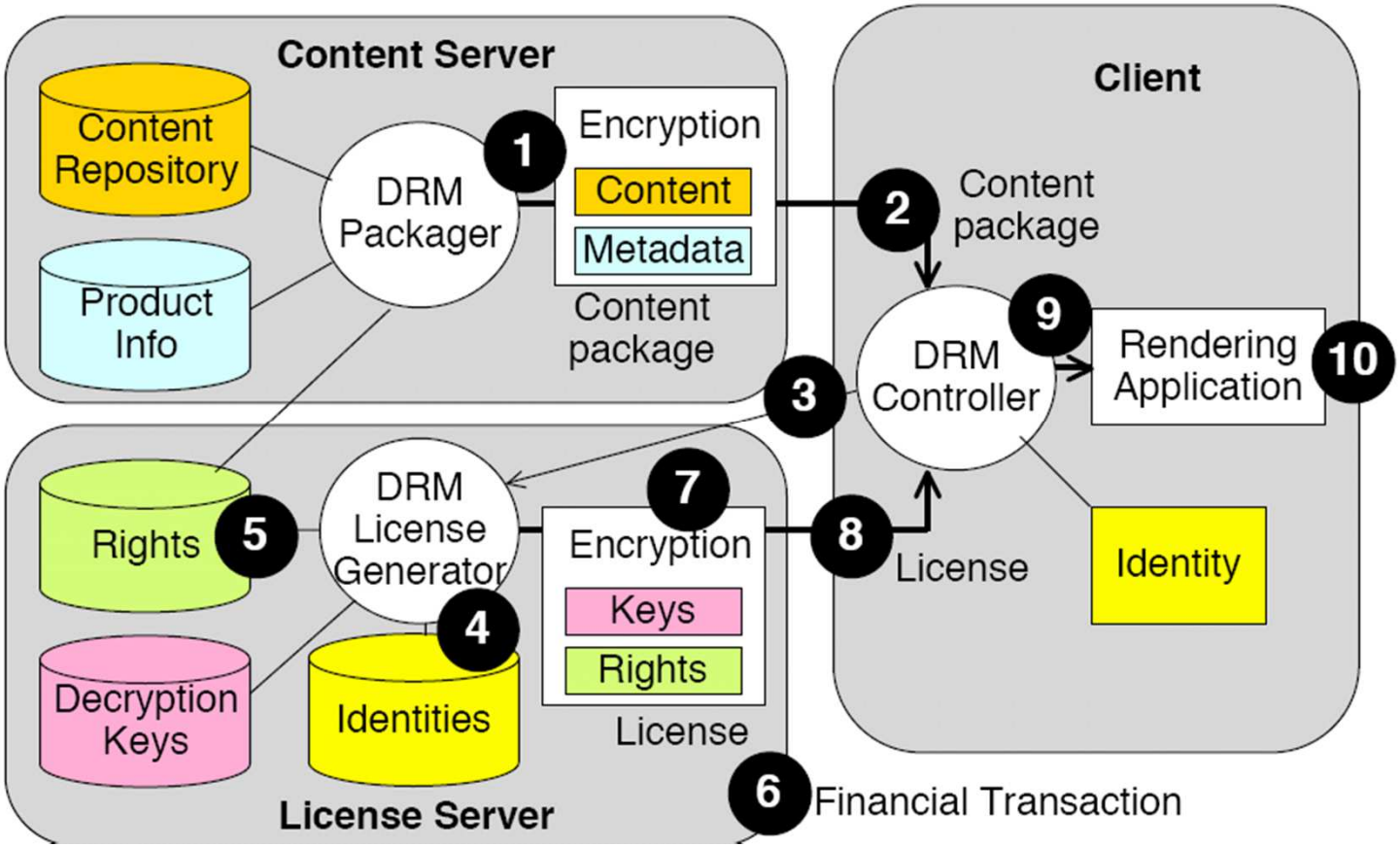
Titkosítatlan

- Szabadon továbbítható
- Jogosultsági objektumok garantálják a hozzáférést

Titkosított

- Tartalom titkosítása
  - Algoritmus
  - Dekódoló kulcs
- Digitális aláírás hitelesítéshez
- Digitális tanúsítványok érvényességhez
- Vízjelezés

Védett tartalom felhasználása

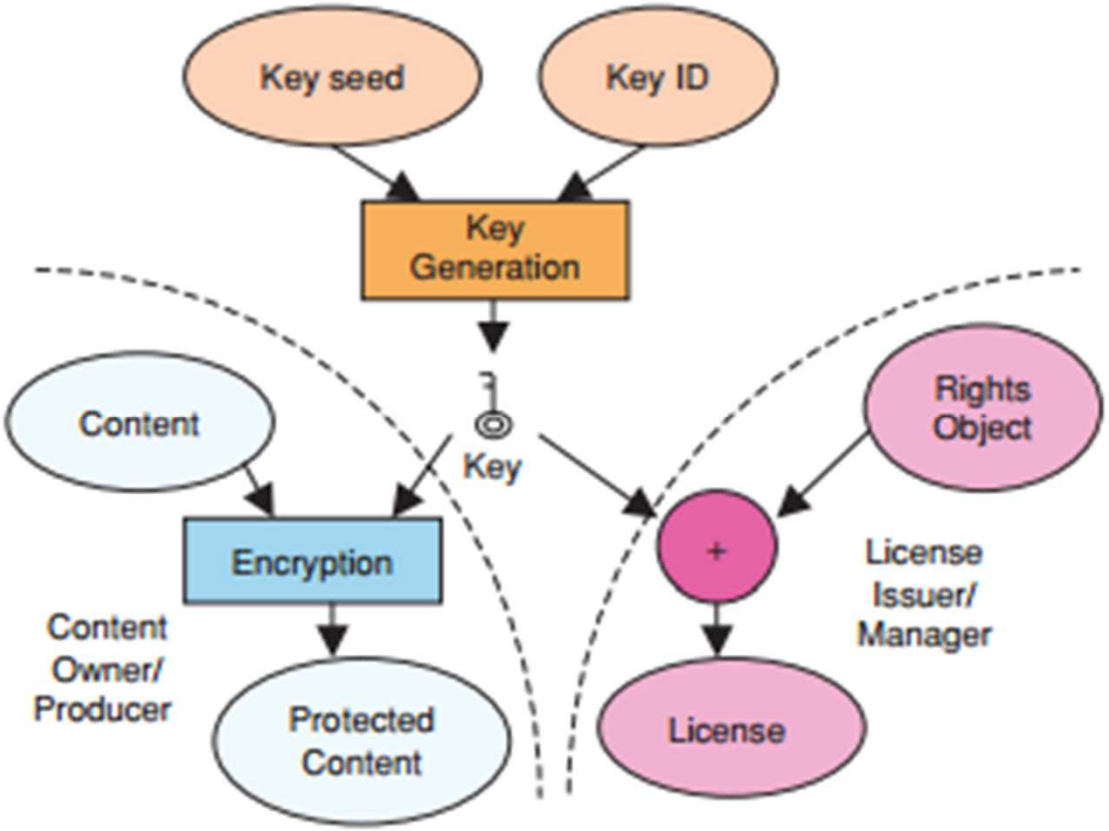


Védett tartalom felhasználása

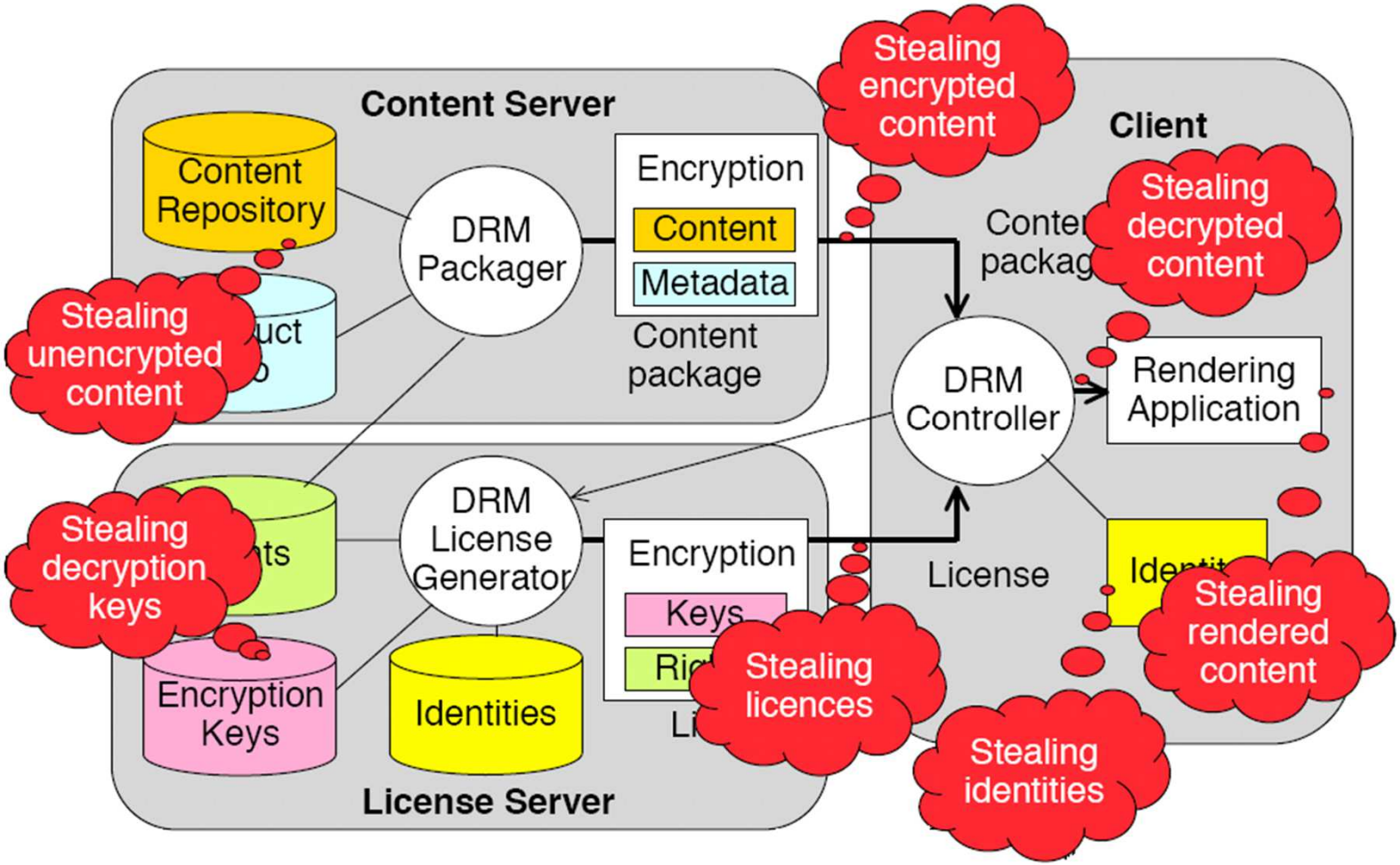
1) A felhasználó hozzájut egy tartalomcsomaghoz (pl. letöltéssel)
2) A felhasználó hozzáférési jogot kér
   - A *Rendering Application* aktiválja a DRM vezérlőt
3) A DRM vezérlő azonosítja a felhasználóz és a tartalmat és kapcsolatba lép a *Licence Server*rel
   - Felhasználói közreműködésre lehet szükség (pl. adatlap kitöltése)
4) A *Licence Server* azonosítja a felhasználót az azonosítási adatbázis alapján
5) A *Licence Server* kikeresi a tartalomhoz tartozó jogok specifikációját
6) Pénzügyi tranzakció indulhat – szükség szerint
7) A *Licence Generator* összeállítja a jogok, a felhasználói azonosító és szükséges kulcsok csomagját és lepecsételi (valamint titkosítja)
8) A licensz elküldése a felhasználónak
9) A DRM vezérlő feloldja a titkosítást és a tartalmat továbbítja a *Rendering Application*nek
10) A tartalom hozzáférhető a felhasználó számára

Licenszek

- Jogosultsági objektum
- Tartalom használatához szükséges kulcs
- Nem átruházható



Lehetséges támadások a DRM ellen



DRM

- media objectek felhasználása
- különböző jogok kölünböző áron
- nem a media objectek, hanem a jogok eladása
- jogok leírása XrML-ben (eXtensible Rights Expression Language) vagy ODRL (Open Digital Rights Language Initiative) alapján
- Fontos jellemző, hogy egy DRM megoldás a jogok milyen részletességű leírását támogatja (üzleti modelek)
  - jogok pl. végrehajtás,megtekeintés/lejátszás, másolás, formátum konverzió, ismétlések számának vagy időtartamának korlátozása, hordozhatóság (más eszközre), stb.
  - kapcsolódó fizetési konstrukciók (előre, utólag)
  - egyedi és csoportos jogok

OMA DRM funkciók

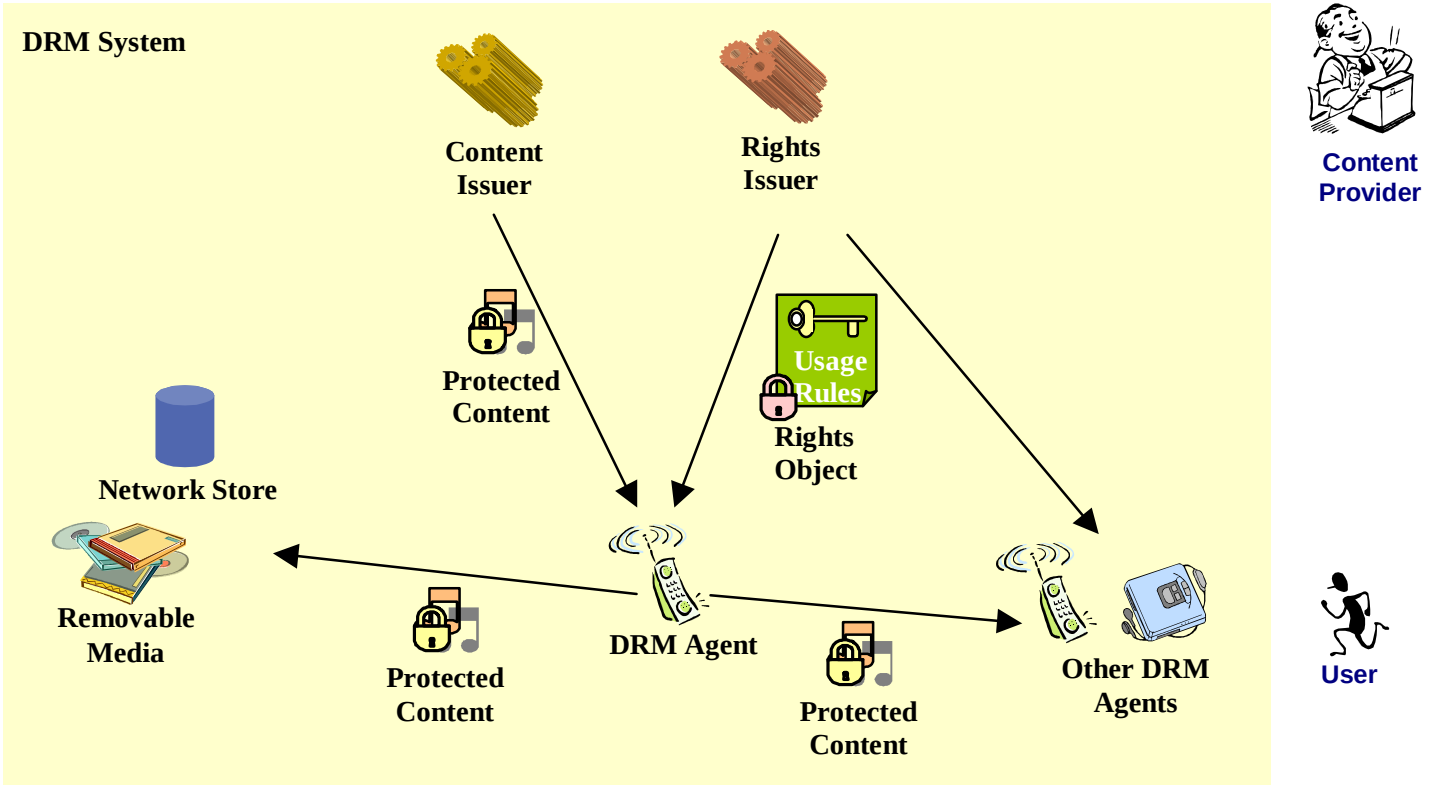
OMA DRM 1.0

- Forward lock: ne hagyhassa el a tartalom a eszközt
- Combined delivery: objektum és jogok együttes továbbítása
- Separate delivery
  - = szuper-elosztás

OMA DRM 2.0

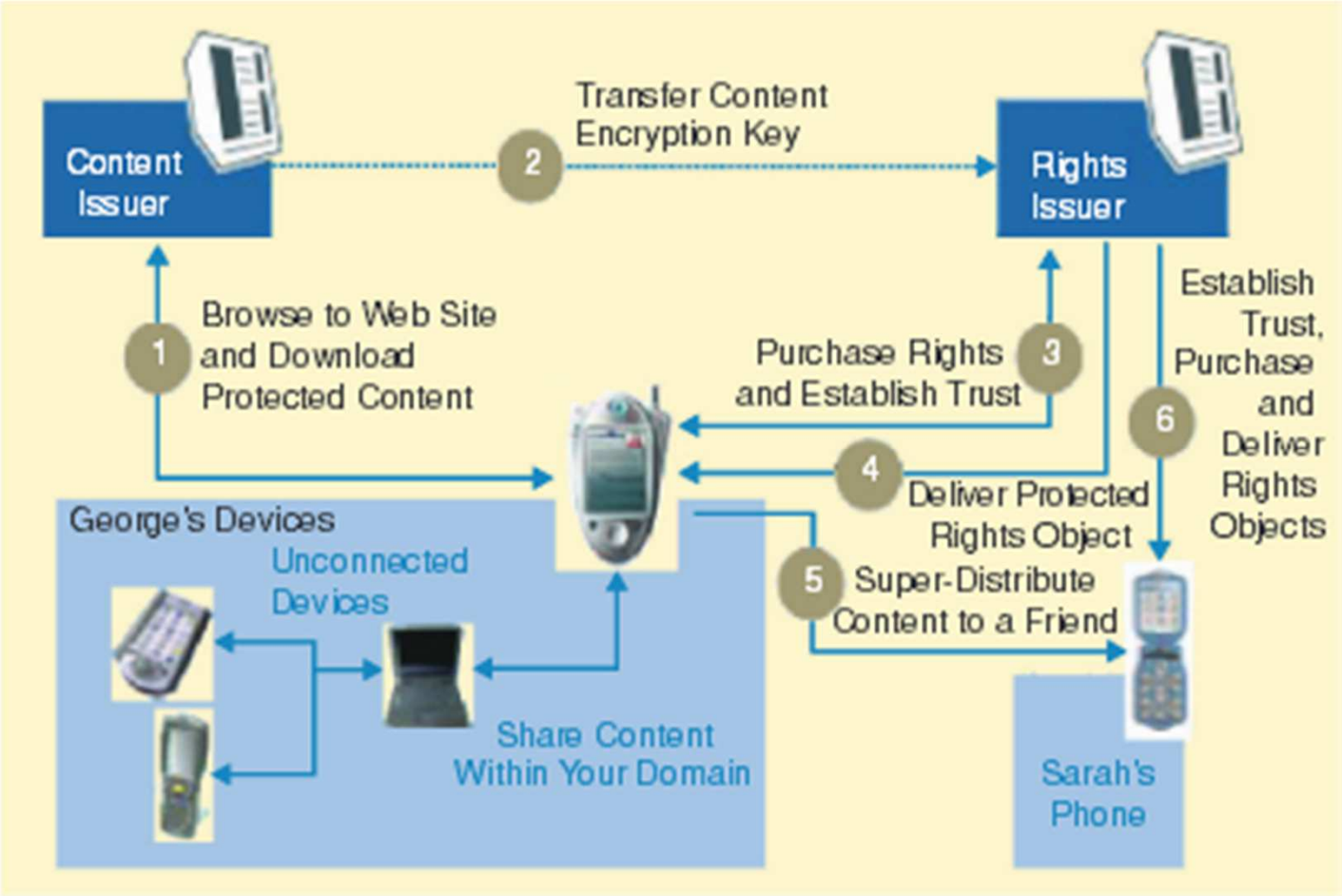
- Minden, ami az 1.0-ban megvolt
- Domain: otthonon belüli megosztás eszközök között

DRM (OMA)



Szereplők: felhasználó, DRM ügynök, tartalomszolgáltató, jogszolgáltató, védett tartalom, jogleíró állomány

Architektúra



DRM (OMA)

- Fő hangsúly a védett tartalmak és kapcsolódó jogok terjesztésén
- Védett tartalom és jogok terjesztése elválik egymástól
- Adott jogleírás DRM ügynökhöz kötött, de köthető több ügynökhöz is – domain

DRM (OMA) - komponensek

- Rights Expression Language (REL)
  - jogok és kényszerek megfogalmazása a media object felhasználásával kapcsolatban
- Content Format (DCF)
  - media objectek megadott kulcs és algoritmus segítségével történő titkosítása (ha nem szükséges, mehet plaintext-ben is)
- Protokollok (egyelőre ROAP)
  - Jogok tejesztése
- Értékelés:
  - Az alkalmazásszintű biztonság gyenge. A szállítási szinten (WTLS, TLS) biztosítható a media objectek biztonságos kezelése a mobilkészülék és a szerver között. A DRM-ben azonban ez önmagában nem elég.
  - A készülékgyártók és a tartalomszolgáltatók között komoly és kölcsönös bizalomnak kellene kialakulnia.

DRM (OMA)

- Hozzáférési modellek
  - Basic pull (felhasználó kéri)
  - Push
    - Content push (terjesztő leküldi + a jogkérés helyét is)
    - Push-initiated pull (csak reklám, pl. URL)
  - Streaming (védett stream, ehhez is külön kell a jog)
- Domainek:
  - DRM ügynökök csoportja: egy felhasználó lejátszói (pl. off-line eszköz is), felhaználók csoportja (pl. csoportos jogszerzés – vállalat)
- Backup:
  - csak titkosított biztonsági másolat (jogokról is, de ezt külön kell a DRM ügynöknek menedzselnie)
- Super distribution: titkosított tartalom nemcsak szolgáltatótól
- Export: más, megbízható DRM rendszerbe
- Unconnected DeviceSupport : domainekre alapozottan

DRM (OMA)

- Trust model komponensek
  - PKI
  - Content packaging (DCF)
    - Packaging: symmetric content encryption key (CEK)
  - DRM Agent authentication
    - Agent authentication: public/private key, info on hw and sw
  - RO generation (REL), RO protection (REL)
    - RO: XML, tartalmazza a CEK-et, a DRM Agent-hez köti kriptografikusan, Rights Issuer alá is írja
  - Delivery
    - Bármilyen transzport mechanizmus jó, mert szerkezetileg biztonságos
  - DRM Time:
    - A DRM Agent időmérése a felhasználótól függetlenül és biztonságosan kell, hogy történjen

DRM: REL (OMA)

- csak consumption és nem management jogokkal foglalkozik
- play, display, execute, print
- felhasználások száma, időkorlátok
- bizalmas tartalmak – titkosítás
- metaadatok

DRM: REL (OMA)

```
<o-ex:rights
(…)
 <o-ex:context>
  <o-dd:version>2.0</o-dd:version>
  <o-dd:uid>RightsObjectID</o-dd:uid>
 </o-ex:context>
 <o-ex:agreement>
  <o-ex:asset>
  (…)
  </o-ex:asset>
  <o-ex:permission>
   <o-dd:display>
    <o-ex:constraint>
     <o-dd:count>1</o-dd:count>
    </o-ex:constraint>
   </o-dd:display>
  </o-ex:permission>
 </o-ex:agreement>
</o-ex:rights>
```

DRM: DCF (OMA)

- Media Object kódolása és csomagolása
- Rights Object-től elkülönül
- Metadata
  - tartalom
  - Object ID
  - rejtjelezési info
  - honnan lehet jogokat szerezni
  - egyéb

DRM: DCF (OMA)

- DCF Media Profiles:
  - Discrete Media (DCF)
  - Continuous Media (PDCF)

- ISO Base Media file format alapú mindkettő
- DRM Content Format: boríték
- Packetized DCF (a content tartalmi szerkezetét ismerni kell a használatához)

Interoperabilitási kérdések

- A különböző szereplők érdekei eltérőek
- Példák
  - RealNetworks – Apple harc
  - Nokia – Microsoft megállapodás
- Megoldandó problémák:
  - Infrastruktúrák összehangolása
  - Üzleti modellek és felhasználási szabályok szinkronizálása

Összefoglalás

- Digitális tartalmak kezelése
  - törvényi keretek
  - technológiai megoldások
    - OTA
    - DRM
- DRM ajánlások
  - OMA
  - Microsoft
  - Apple
  - …
- Interoperabilitási kérdések