

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

Digitális tartalmak kezelése

Pándi Zsolt, Híradástechnikai Tanszék alapján

Jakab Tivadar

Híradástechnikai tanszék

2010



Áttekintés

- Törvényi keretek
- Technológiai részletek
 - Tartalmak eljuttatása a (mobil)készülékekre
 - Tartalmak felhasználása



DRM

- Digitális tartalmak kezelésének a *technológiai* kérdéseit igyekeznek megválaszolni
- A tartalom alatt *elsősorban nem szoftver* típusú tartalmat ért
- *Nem csak mobilkészülékekre* vonatkozik



DRM

- Meghatározó szereplők:
 - OMA DRM
 - Microsoft WMDRM
 - Real Networks Helix
 - Apple FairPlay
 - Sun OpenGM
 - ...

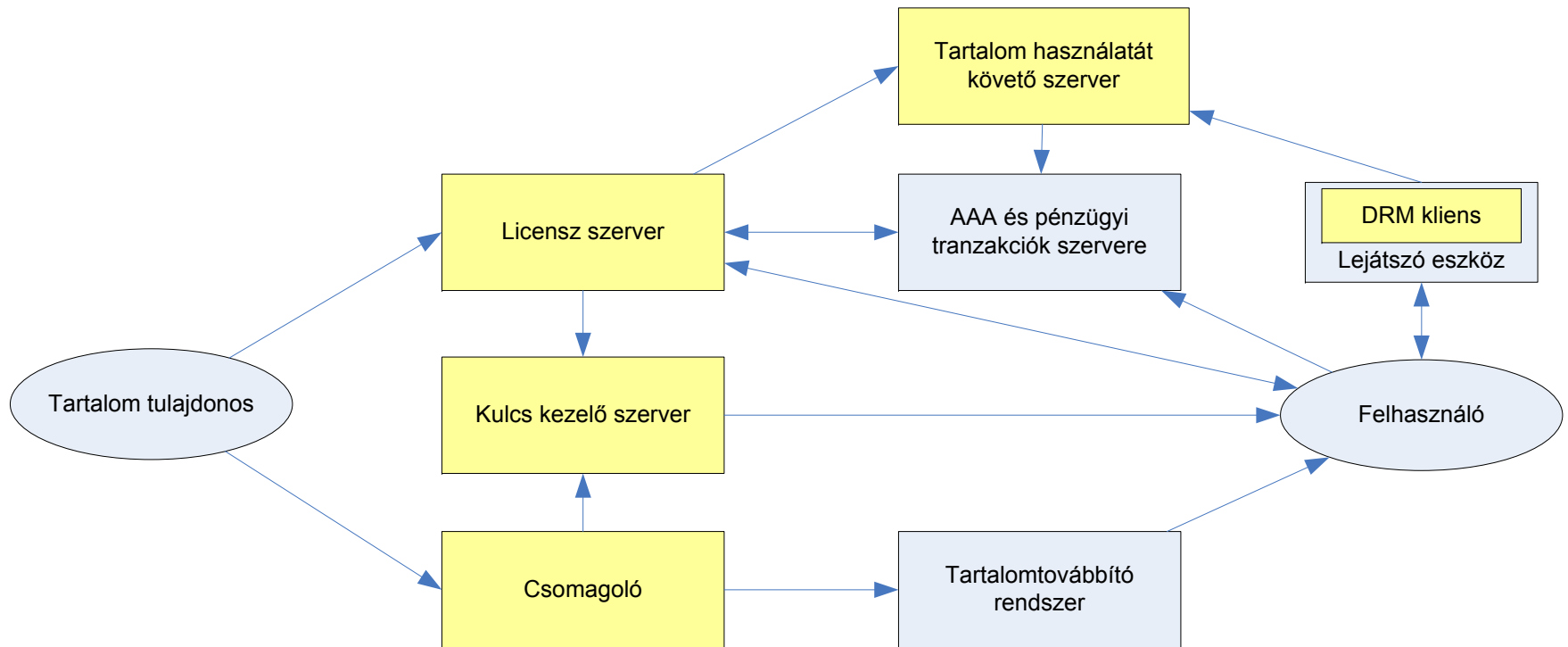


DRM (OMA)

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

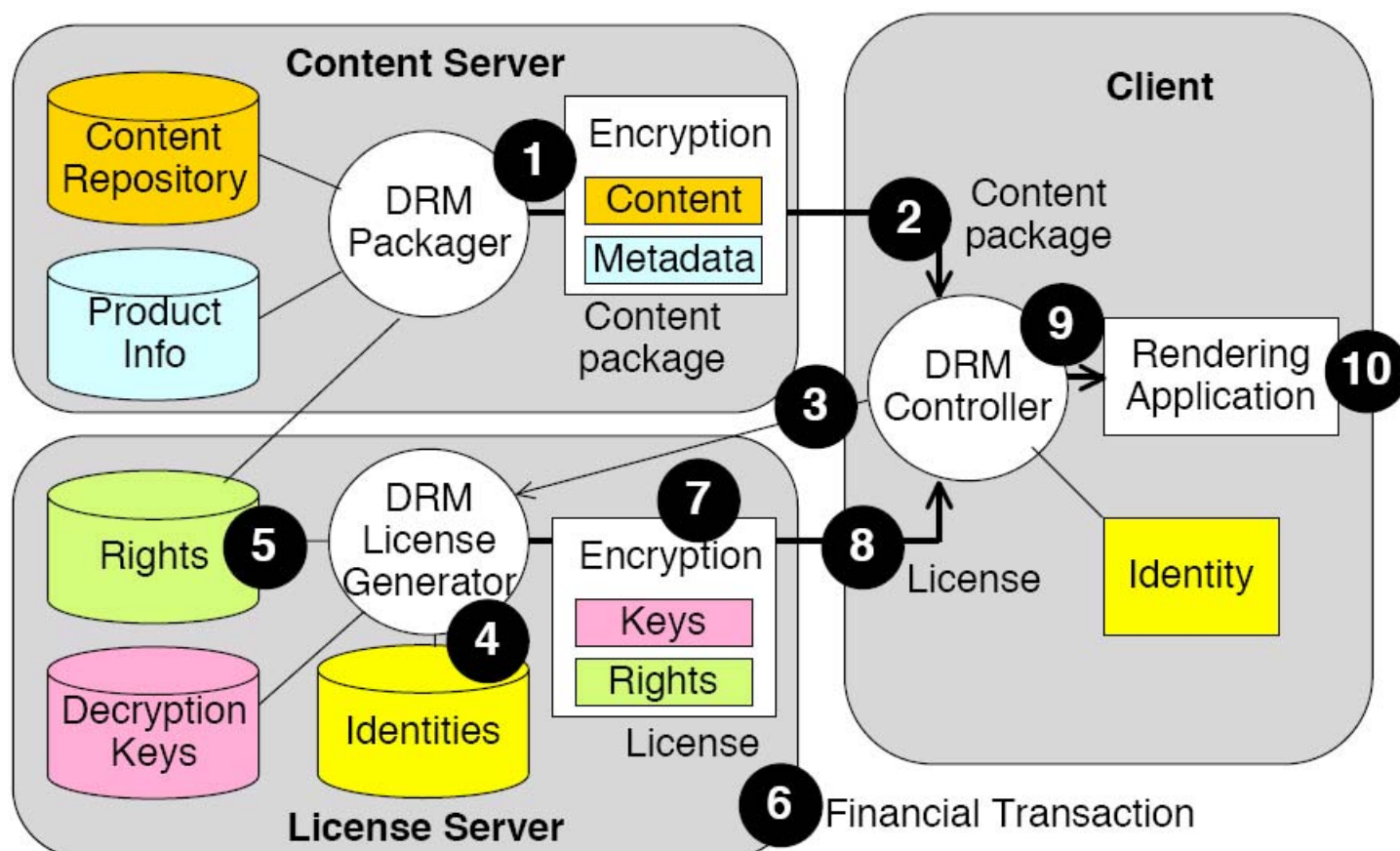


Fontosabb fogalmak

- Meta-adatok: az adott tartalomhoz kapcsolódó információk (azononsítás)
- Jogok: a felhasználás módjai (jogleíró módszerek) – licence 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: ???



Védett tartalom felhasználása

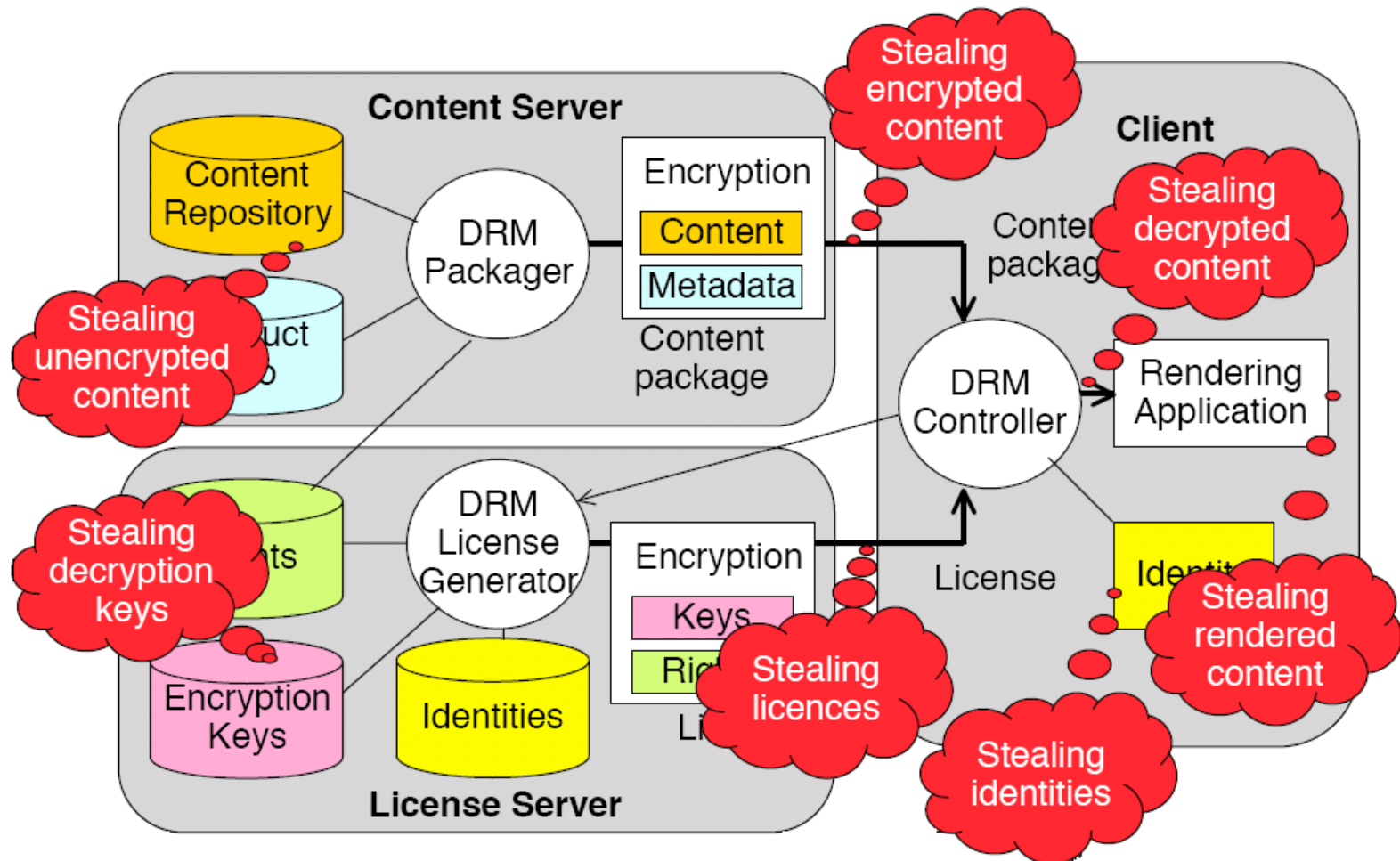


Védett tartalom felhasználása

- (1) User obtains a content package, e.g. by download
- (2) User makes request to exercise rights, e.g. to play or store the content
 - Rendering software activates the DRM controller
- (3) DRM controller determines identity of user and content and contacts license server
 - May require user interaction, e.g. filling a registration form
- (4) License server authenticates user against identities database
- (5) License server looks up rights specification for the requested content
- (6) If necessary, a financial transaction is started
 - Financial transaction may happen also at another point in the process
- (7) License generator combines rights information, client identity and decryption keys and seals them (packaged by encryption again)
- (8) License is sent to the client
- (9) DRM controller decrypts the content and hands it over to the rendering application
- (10) Content is rendered for the user



Lehetséges támadások a DRM ellen

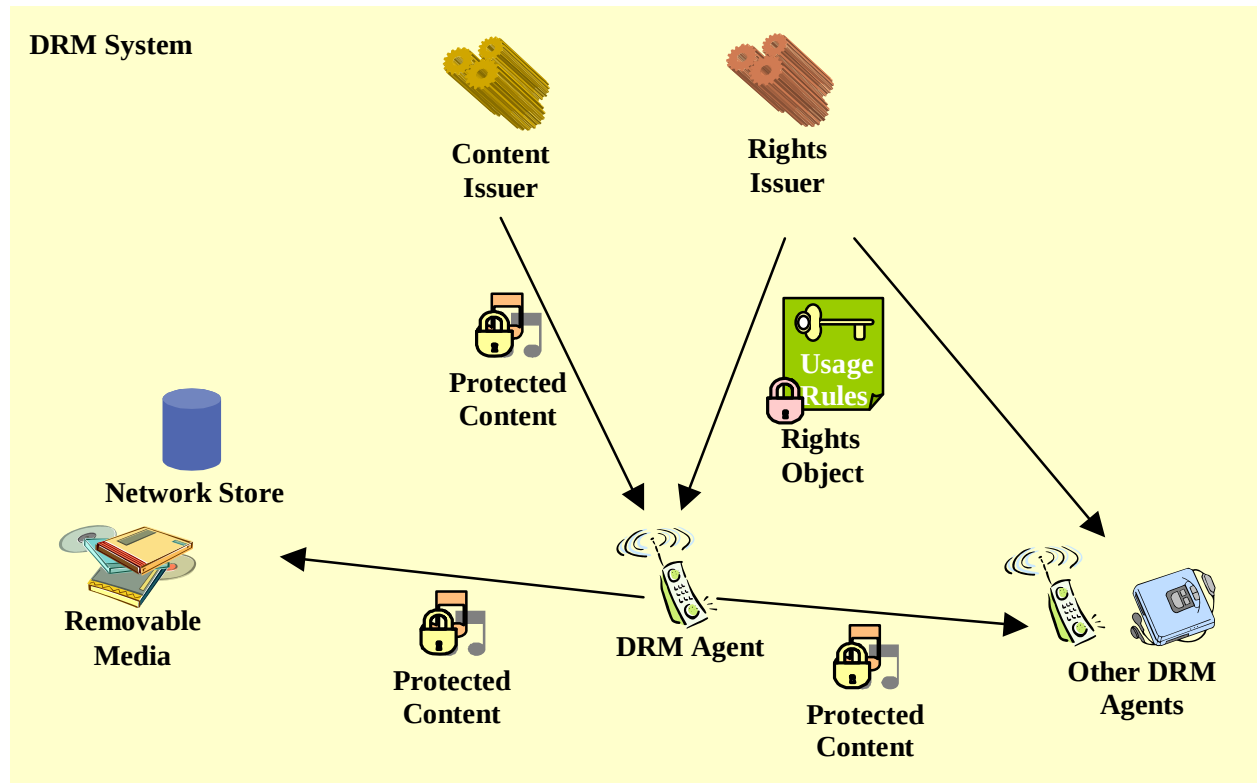


DRM

- media objectek felhasználása
- különböző jogok különböző 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 modellek)
 - 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



DRM (OMA)



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



DRM (OMA)

- Fő hangsúly a védett tartalomk és kapcsolódó jogok terjesztésén
- Védett tartalom és jogok terjesztése elválík 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 teljesítése
- 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 jogkéréselyét is)
 - Push-initiated pull (csak reklám, pl. URL)
 - Streaming (védett stream, ehhez is külön kell a jog)
- Domainek:
 - DRM ügynökök csoportja: egy felhasználó lejátszója (pl. off-line eszköz is), felhasználók csoportja (pl. csoportos jogszerzés – vállalat)
- Backup:
 - csak titkosított biztonsági másolat (jogokról is, de ezt külön kelle 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)



DRM (Microsoft)

- Alapvető összetevők
 - A digitális tartalom létrehozásának és terjesztésének erős támogatása
 - Csomagolás
 - Windows Media formátum
 - csak DMO (Direct Mode Operation) kodekeket támogat (ACM-et nem – Association for Computing Machinery)
 - Kulcs Key ID-dől és Key seed-ből
 - Titkosítás adategységenként (adatvesztésre hibatűrő)
 - A fájlhoz, fejlécként hozzá lehet fűzni a tartalomszolgáltatótól származó kiegészítő információkat, mint pl. key ID, content ID, licencigénylési URL, egyedi azonosítás verziószáma, stb.
 - Terjesztés (gyakorlatilag szabad)



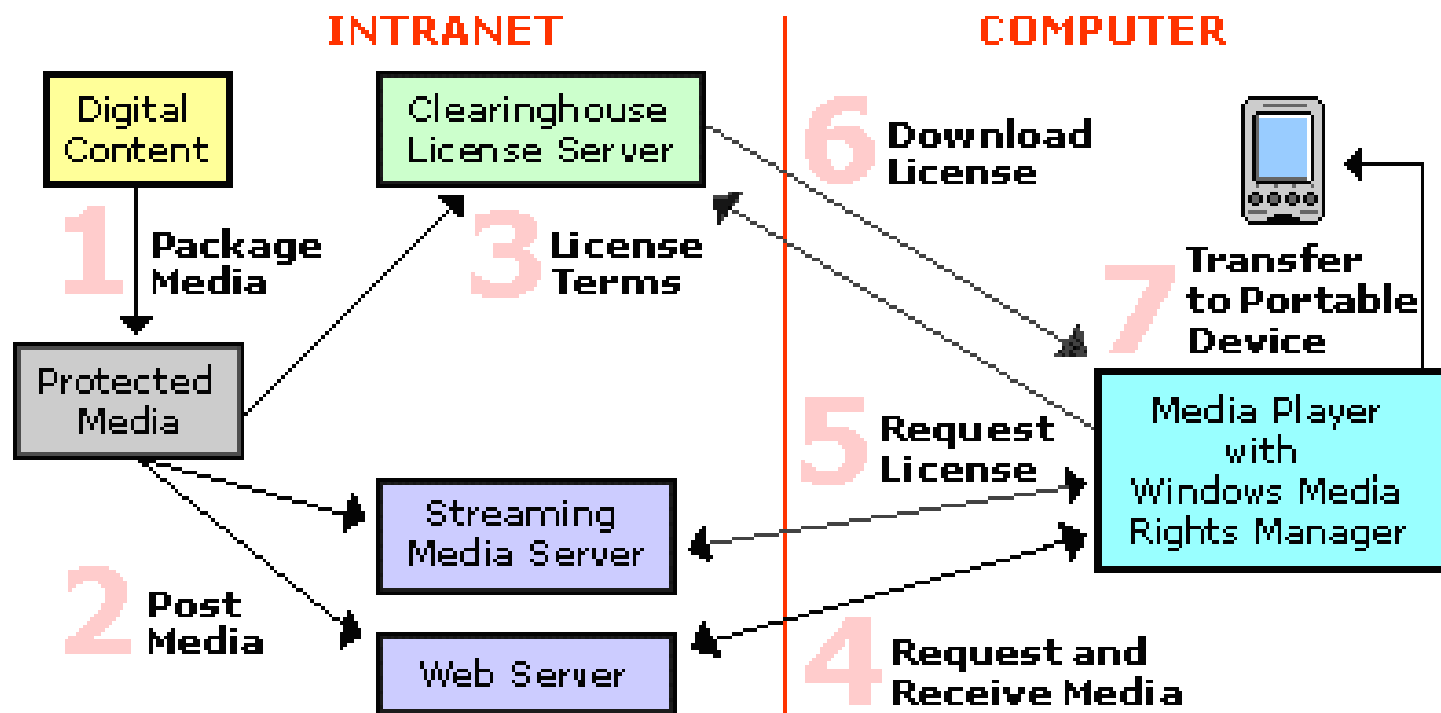
DRM (Microsoft)

- Alapvető összetevők
 - Licenzek
 - pl.: AllowBurnToCD, AllowPlayOnPC, BeginDate, DeleteOnClockRollback, DisableOnClockRollback, ExpirationDate, PlayCount, TransferCount, stb.
 - License server
 - Jogok és szabályok tárolása
 - Felhasználói kérések hitelesítése
 - License beszerzés
 - Számítógépez kötött
 - Lejátszás

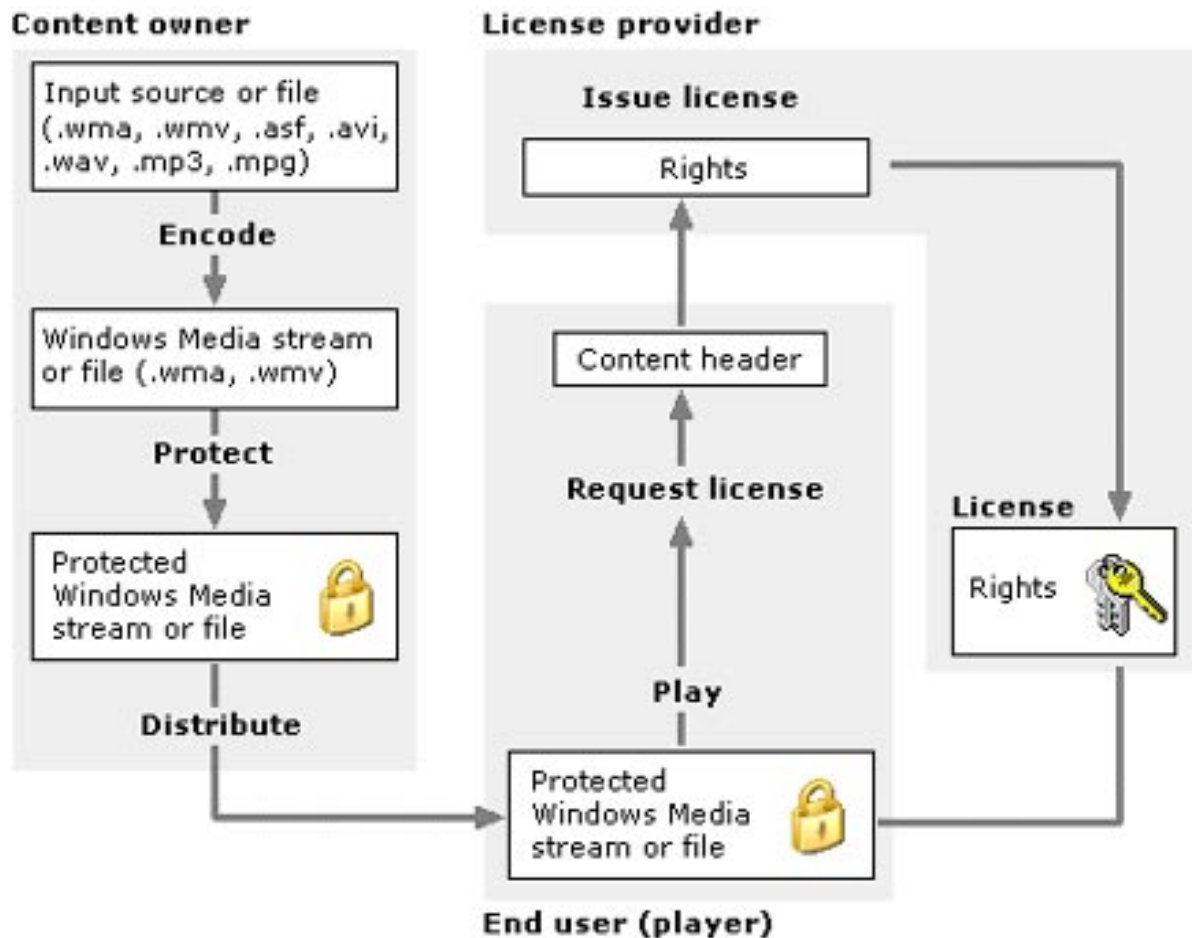


DRM (Microsoft)

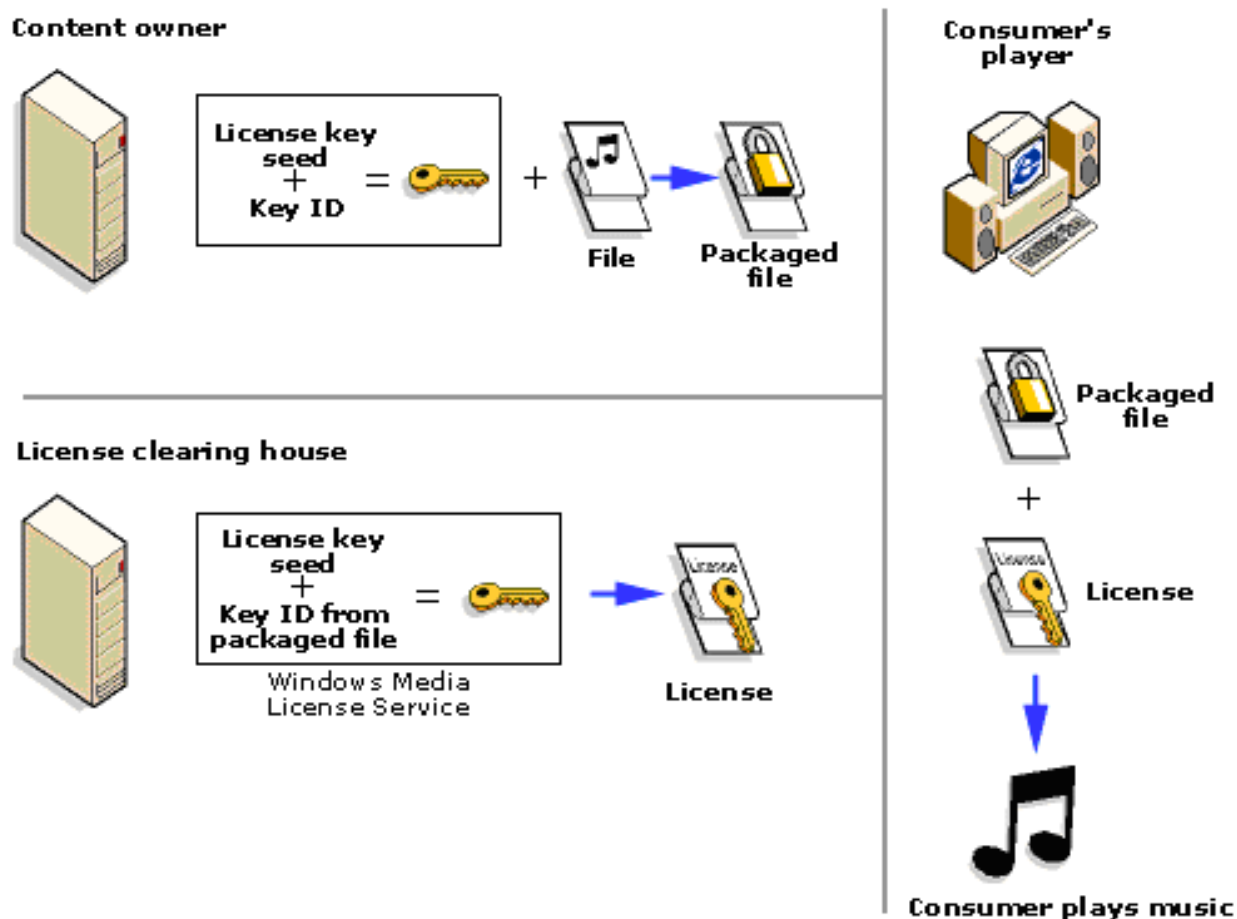
Windows Media Rights Manager Flow



DRM (Microsoft)



DRM (Microsoft)

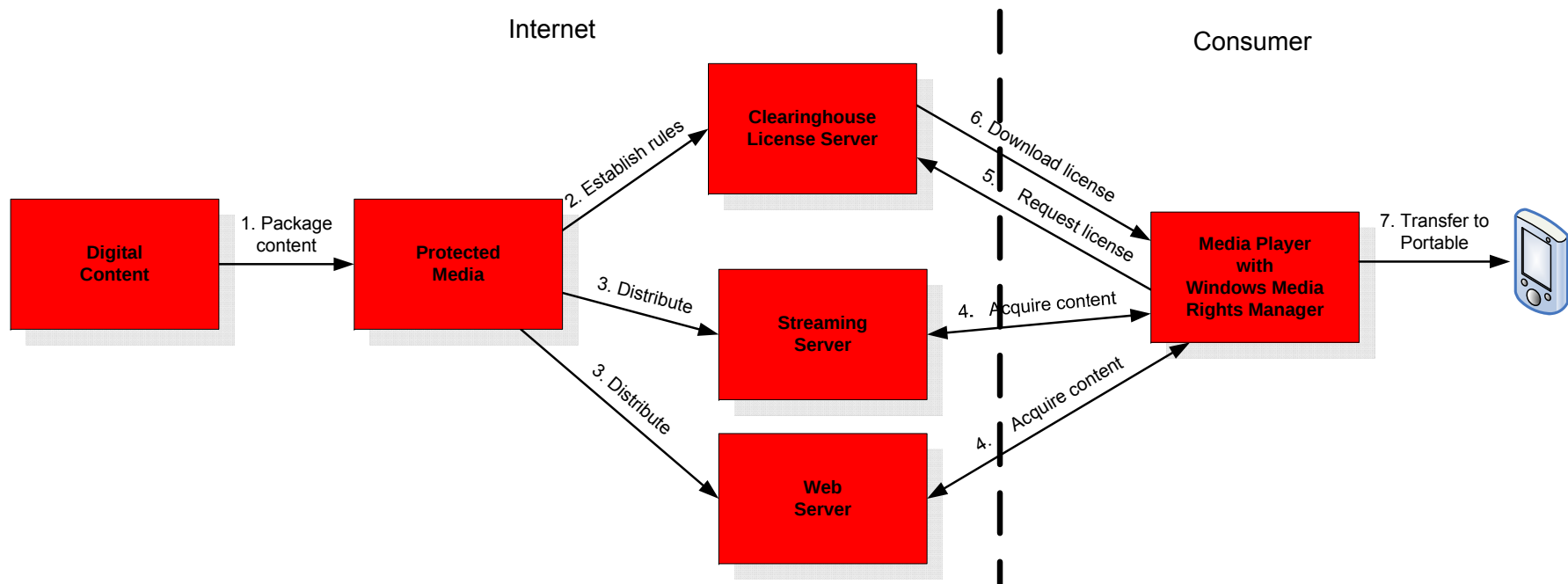


DRM (Microsoft)

- License tartalma
 - hányszori lejátszásra érvényes
 - milyen készülékeken
 - mikortól meddig
 - CD íróra küldhető-e
 - license archiválható-e



DRM (Microsoft)

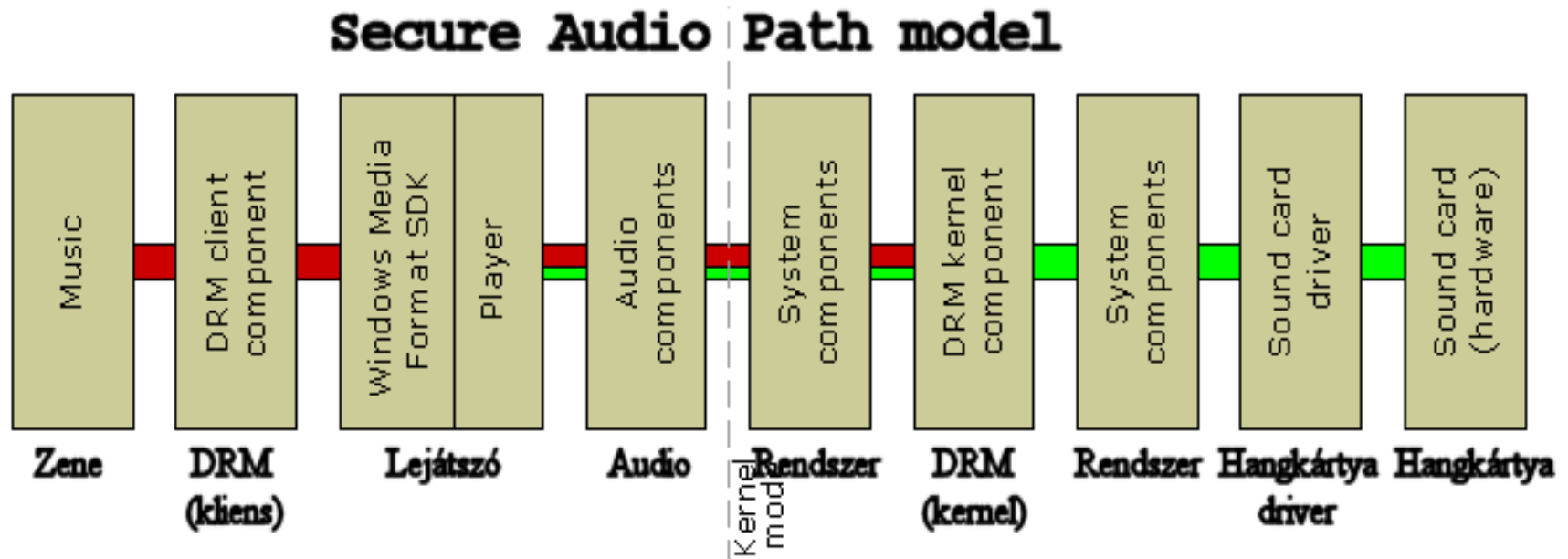


Medialejátszó

- **Egyedi azonosítás:** (individualization) A Windows Media DRM az egyes médialejátszókat egyedivé teszi és az adott számítógéphez köti. Installáláskor a lejátszó szoftver kérést küld a Microsoft Individualization Service-hez, amire válaszként, egy generált, egyedi, digitálisan aláírt DLL-fájlt, ami összeköti a lejátszót a kliens gép hardver ID-jával. Ez lecsökkenti a globális licencfeltörés veszélyét, és így, egy feltört DRM kliens (visszavonással) kitiltható a további licencek megszerzéséből.
- **Megújíthatóság:** A biztonság fokozása érdekében a Microsoft különböző Windows Media DRM verziófrissítéseket ad ki, amely a felmerült biztonsági réseket „tömik be”. A tartalomtulajdonosok el is utasíthatják a szolgáltatáskéréseket a kevésbé biztonságos ügyfelektől, amíg az ügyfél bizonyos összetevőket nem frissít, vagy nem újít meg.
- **Secure Audio Path:** A SAP technológiával védve vannak az operációs rendszeren (Windows XP, ME) belül a médialejátszótól a hangkártya felé haladó adatok (4. ábra). Így csökken a hamis beépülő modulokon alapuló támadások esélye, mert csak ezek az összetevők férnek hozzá a titkosított adatokhoz.



Microsoft Secure Audio Path modell



Secure Audio Path: A SAP technológiával védve vannak az operációs rendszeren (Windows XP, ME) belül a médialejátszótól a hangkártya felé haladó adatok. Így csökken a hamis beépülő modulokon alapuló támadások esélye, mert csak ezek az összetevők férnek hozzá a titkosított adatokhoz.

Egy tanúsítvánnyal rendelkező Microsoft összetevő ellenőrzi, hogy tanúsítva legyen a folyamat következő fázisaiban részt vevő összes összetevő (beleértve a hangkártya illesztőprogramját is). Nem fejt vissza az adatfolyamot, ha illetéktelen vagy biztonsági szempontból sérült összetevőket talál a végrehajtás folyamatában. A hangminták csak a kernelben kerülnek kibontásra, addig titkosítva haladnak.

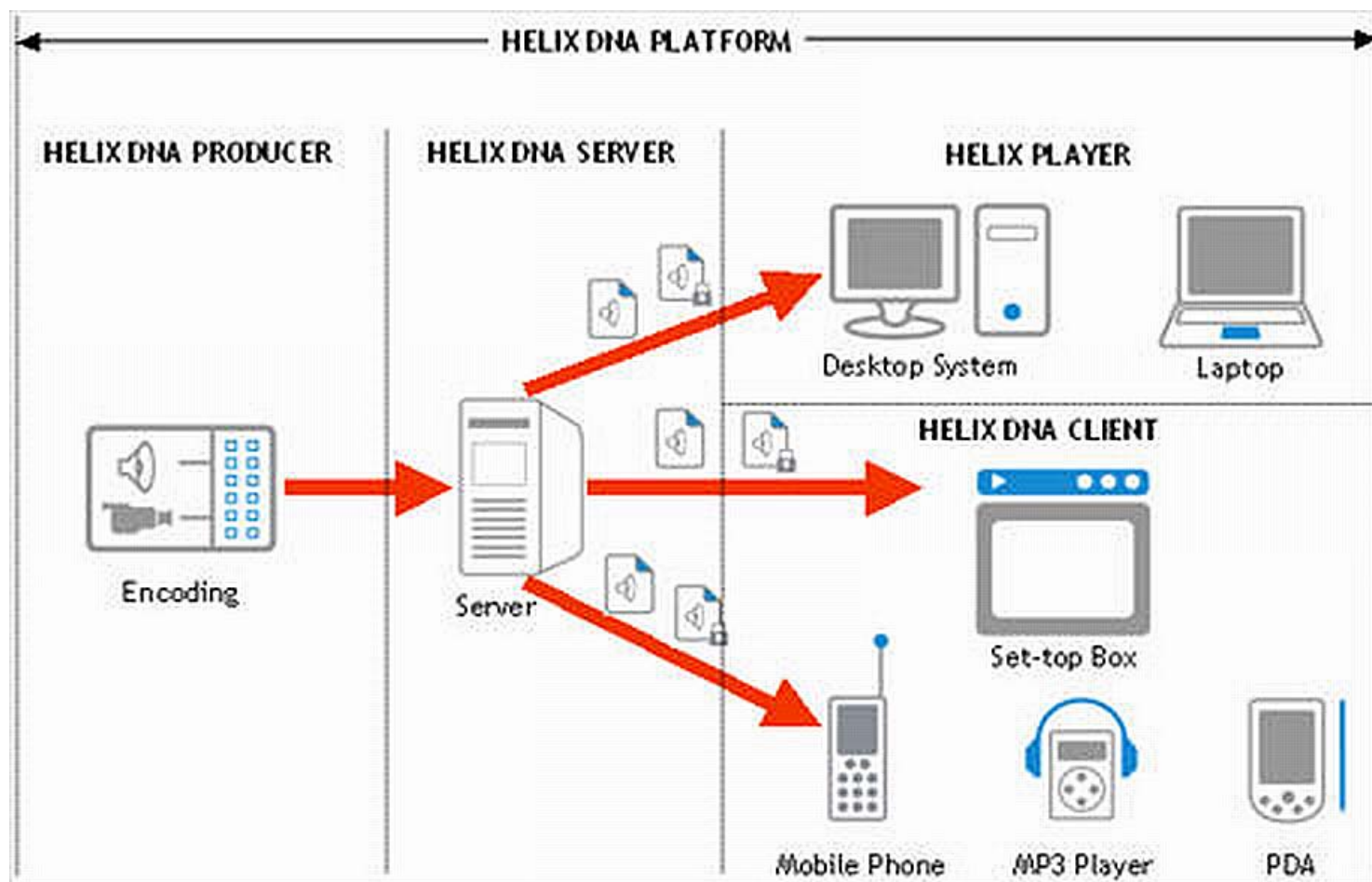


HELIX

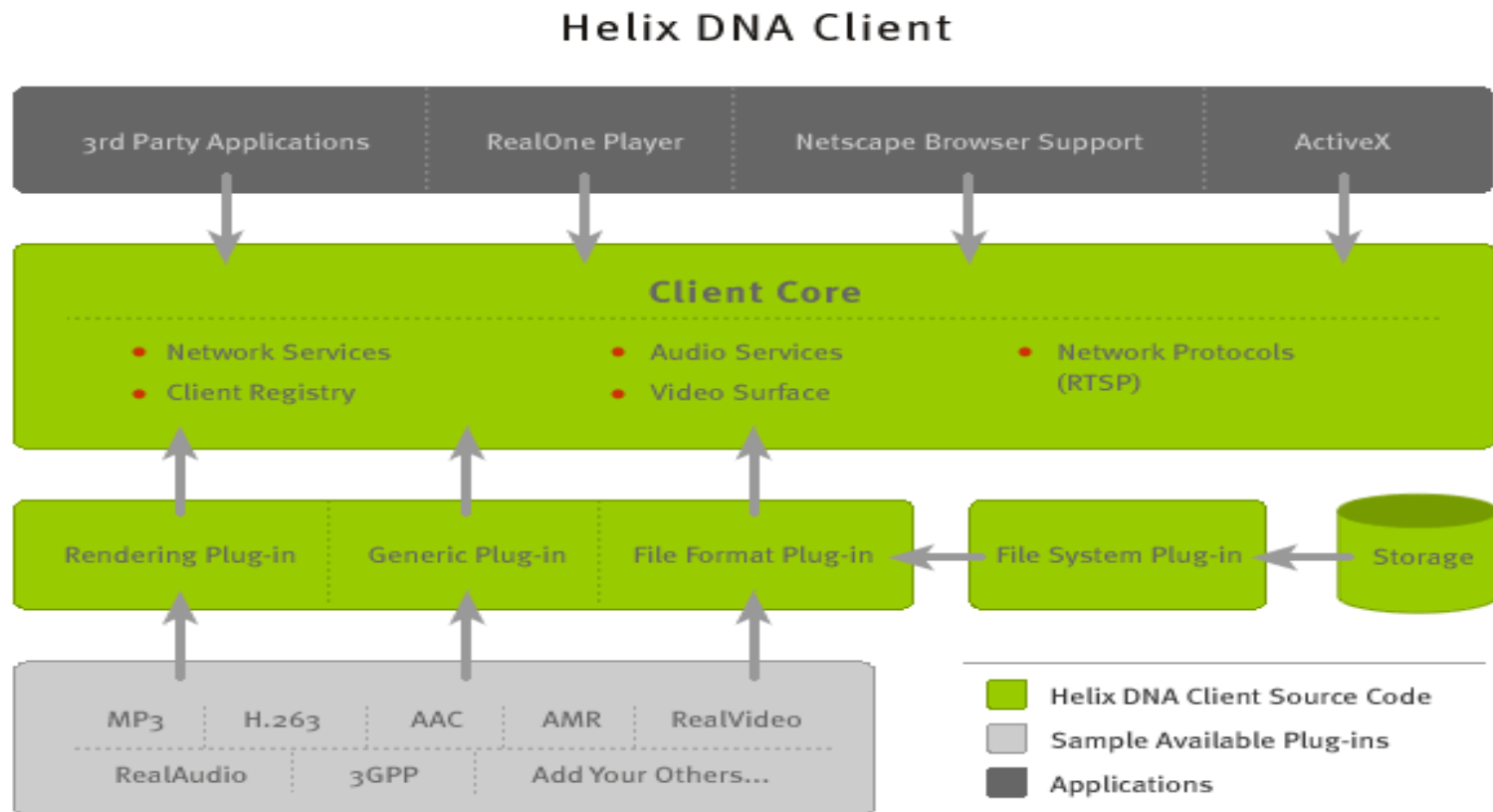
- A platform lehetővé teszi, hogy a cégek az igényiknek megfelelő rendszert fejlesszenek a tartalmak kezelésére. A platform hozzáférést nyújt sok API-hoz is, ami megkönnyíti a fejlesztést. A rendszer alapvetően három komponensből áll: a kliensből, ami hozzáfér a tartalmakhoz, a szerverből, ami a tartalmak szolgáltatásáért felel, és a producer-ből, a tartalmak kódolásáért és titkosításáért felel.



Helix DNA platform



Helix DNA kliens



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
 - HELIX
- Interoperabilitási kérdések

