# DRM technológiák

FEHÉR GÁBOR, POLYÁK TAMÁS, OLÁH ISTVÁN

*Budapesti Műszaki és Gazdaságtudományi Egyetem, Távközlési és Médiainformatikai Tanszék*
*{feher, polyak, olah}@tmit.bme.hu*

***Kulcsszavak: szerzői jogok védelme, tartalomszolgáltatók, DRM***

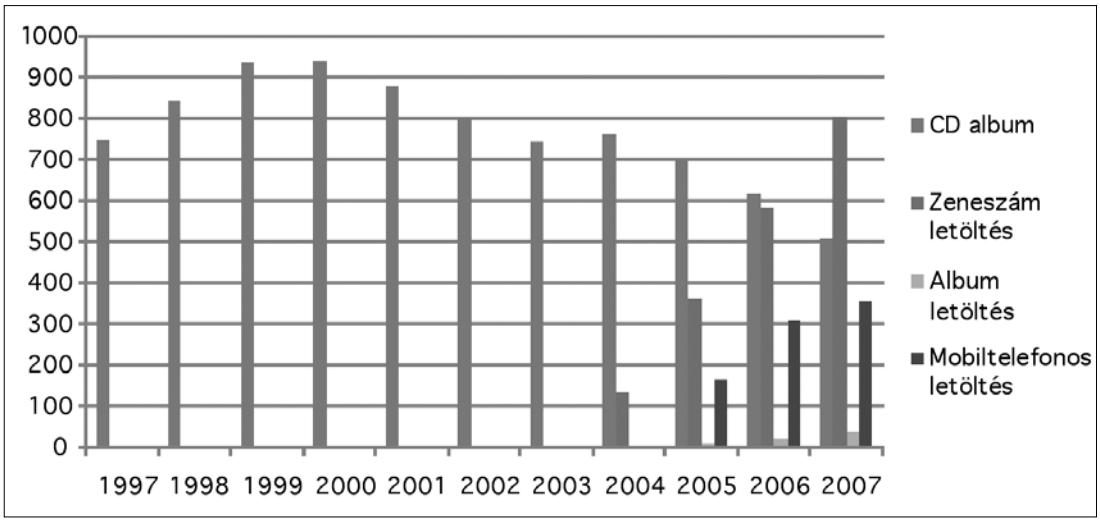
*A szerzői jogok védelme örök probléma a társadalomban: biztosítani kell, hogy akik értékes tartalmat állítanak elő, megkaphassák érte a jussukat. Az analóg világban a problémát egyszerűen lehetett kezelni, mivel a másolás közben a mű minősége romlott, így aki igazi minőségre vágyott, annak muszáj volt fizetnie a tartalomért. A digitális világban azonban már más a helyzet, a digitális másolat minősége egy az egyben megegyezik az eredeti mű minőségével. Szükségszerű tehát, hogy a tartalmat védjük, a tartalomhoz köthető jogokat pedig kezeljük. Ez a védelem és jogkezelés a DRM (Digital Rights Management). A cikk célja, hogy az olvasót megismertesse a DRM technológia alapjaival és a felhasználásával.*

## 1. Bevezetés

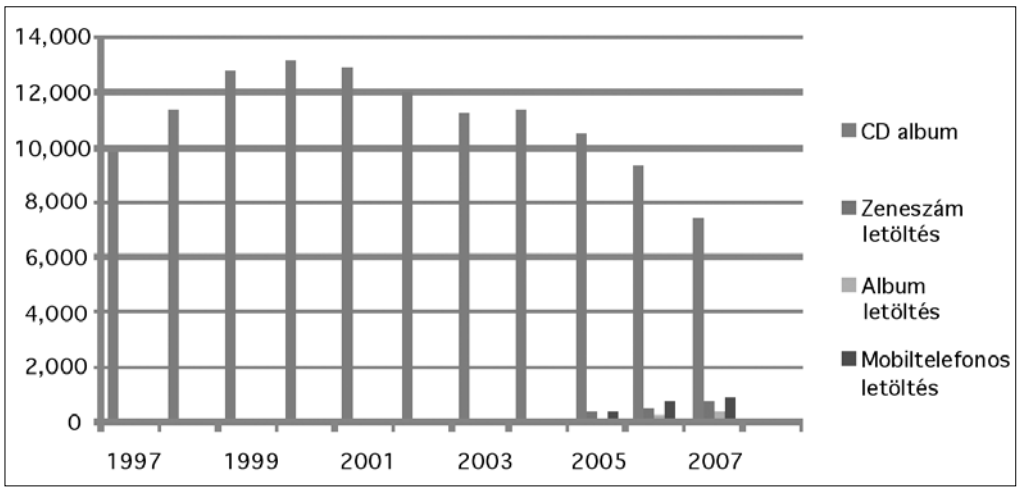
A digitális technika és az internet megjelenése és elterjedése számos jelentős és visszafordíthatatlan változást okozott több piacon is. Az egyik ilyen jelentősen érintett piac a szerzői jog oltalma alá eső tartalmak terjesztésével és kereskedelmével foglalkozó piac volt. A hagyományos zenei kazetták, CD-k, videokazetták és DVD-lemezek kiadói számos új, eddig ismeretlen kihívással kellett (és kell ma is) szembenézzenek. A hagyományos analóg adathordozókhoz képest (hangkazetták és videokazetták) a CD és DVD lemezek sokkal jobb minőségben és digitálisan tárolták a tartalmakat. Mivel ezek az adathordozók lehetővé tették, hogy otthoni körülmények között minőségveszteség nélkül lehessen másolatot készíteni róluk, megjelenésük potenciális veszélyt jelentett a kiadók számára. A felhasználók ugyanis ugyanazt a vizuális- és hangélményt kapták a másolt tartalomtól, mint amilyet a bolti változattól kaphattak.

A digitális tartalomtovábbítás elterjedését egy másik tény is elősegítette: megjelentek olyan tömörítési algoritmusok, amelyek akár tizedére, századrészére, vagy – videók esetében – akár ennél is jobban képesek voltak tömöríteni a tartalmakat. Ilyen úttörő volt a hanganyagok MPEG 1 Layer 3 (MP3) tömörítése és a videótartalmak tömörítésére szolgáló különböző MPEG 1-2-4 videó tömörítési eljárások, melyek a kis méret ellenére jó minőséget nyújtottak.

Az internet megjelenésével lehetővé vált, hogy ezeket a tömörített, kicsi és viszonylag jó minőségű digitális tartalmakat a felhasználók egymás között másolgassák. Ezt a folyamatot csak fokozta az egyre nagyobb sebességet kínáló szélessávú internetelérés. Kialakultak különböző fájlcserélő hálózatok, ahol a felhasználók különösebb bonyodalom nélkül juthattak hozzá illegálisan a tartalmakhoz. A kiadók szövetségeinek véleménye szerint ez a gyakorlat vonta maga után azt, hogy csökkenni kezdtek a lemezeladások, más csoportok szerint azonban máshol kell keresni a népszerűségvesztés okát. Tény azonban. hogy a hagyományos CD és DVD eladási modell mellett új módokat kellett keresni a tartalmak értékesítéséhez. Az *1. és 2. ábra* az amerikai lemezkiadók szövetségének (RIAA, Recording Industry Association of America) eladási adatait mutatja be.




*1. ábra*
*RIAA szövetség által eladott médiapéldányok (millió db)*
*Forrás: Recording Industry Association of America*




*2. ábra*
*RIAA szövetség által eladott médiapéldányok bevétele (nettó millió USD), Forrás: Recording Industry Association of America*

Az ábrákon jól látszik, hogy a legálisan forgalmazott médiapéldányok tekintetében a CD egyre kevésbé preferált, míg a digitális letöltések száma rohamosan nő. A 2. ábrán viszont az is látható, hogy a letöltött tartalmak után a kiadóknak nincsen akkora nyereségük, mint a hagyományos médiahordozók esetén. Összességében tehát még a legális digitális letöltések térnyerése is jelentős bevételtől fosztja meg a kiadókat.

## 2. A kiadók válasza: DRM

A kiadók látva a terjedő illegális fájlcsere-hálózatok népszerűségét, szerették volna elejét venni a tartalmak további illegális cseréjének. Mindezt úgy próbálták elérni, hogy megpróbálták megakadályozni, hogy a szerzői jogi védelem alatt álló tartalmak bekerülhessenek a fájlcserélő hálózatokba, valamint megpróbálták megakadályozni, hogy az ilyen hálózatokból letöltött tartalmak bekerülhessenek a legális tartalmak közé, vagyis lejátssza őket egy általános otthoni lejátszó eszköz. Ennek a problémának a kezelésére jöttek létre a különböző digitális jogkezelő rendszerek (DRM, Digital Rights Management).

A DRM rendszerek lehetővé teszik a kiadók és terjesztők számára, hogy menedzseljék a rendszerükben található tartalmakat. Legtöbbször a tartalmakhoz különböző jogokat és korlátozásokat lehet csatolni, amik segítségével megszabható, hogy a felhasználó hogyan használhatja fel a tartalmat. Meg lehet szabni, hogy ki játszhatja le a rendszerben megvásárolt filmet, milyen lejátszón lehet lejátszani, lehet-e róla másolatot készíteni stb. Az, hogy egy tartalomszolgáltató vagy kiadó milyen jogokat és korlátozásokat enged meg, az adott cég üzleti modelljétől függ. Ezen kívül persze fontos része egy DRM rendszernek, hogy milyen titkosítást használ, hogyan használja azt, valamint, hogy milyen egyéb védelmi elemeket definiál.

Egy DRM rendszer legtöbbször többféle technológiai elemből épül fel:

**Titkosítás:** Segítségével titkosítani lehet a tartalmakat, hogy azokhoz csak az férjen hozzá, aki jogosult rá. Ezt egy titkos kulccsal oldják meg, úgy hogy a kulcsot csak az (vagy annak a lejátszója) ismeri, aki megvásárolta a tartalmat.

**Digitális vízjelezés:** Vízjelezés segítségével úgy lehet információt elrejteni a tartalomban, hogy az észrevétlen marad az egyszerű felhasználó számára. Az elrejtett információ lehet a tartalom tulajdonosának valamilyen azonosítója, vagy a tartalmat letöltő felhasználó azonosítója. Jelenleg azonban nincs még olyan vízjelező algoritmus, amit ne lehetne eltávolítani az algoritmus ismeretében. Egyelőre egy lehetséges védelem az eltávolítással szemben az algoritmus titokban tartása, ami persze meggátolja az együttműködést más rendszerekkel, ugyanakkor nem garantálható, hogy az algoritmus nem kiismerhető és feltörhető.

**Jogleíró nyelv:** A felhasználó számára biztosított jogokat és megkötéseket valamilyen módon le kell írni, hogy az érthető legyen a különböző eszközök számára. Fontos tulajdonsága egy leíró nyelvnek, hogy milyen a kifejezőképessége. Ilyen nyílt jogleíró nyelv szabvány például az ODRL (Open Digital Rights Language).

**Eszközök, amik betartatják a szabályokat:** A jogleírásban meghatározott szabályokat tartatják be a felhasználóval. Például a lejátszó nem engedi lejátszani a fájlt, ha elfogyott a megvásárolt lejátszások száma.

**Kommunikációs protokollok:** Azoknak a kommunikációs protokolloknak az összessége, amik segítségével a különböző eszközök kommunikálnak egymással.

### 2.1. Az érintett iparágak és szereplőik

A DRM rendszereknek több érintettje is van. Sok érintett az itt felsorolt szerepek közül akár többet is betölthet.

**Tartalom-előállítók:** Ide sorolhatóak a művészek és filmstúdiók, akik a tartalmakat előállítják. Az ő érdekük, hogy minél többet értékesítsenek a jogvédett tartalomból és hogy minél ismertebbek legyenek. Van azonban példa már arra is, hogy az előállítók (általában maguk az előadók) hajlandóak lemondani az értékesítésből származó közvetlen bevételről a növekvő népszerűségből fakadó bevétel javára.

**Tartalomszolgáltatók:** Ők juttatják el az online tartalmakat a felhasználókhoz. Ezek lehetnek a kiadók tulajdonában, vagy függetlenek, mint például az Ama-

zon. Érdekük, hogy minél olcsóbb legyen a továbbítás, vagyis ne kelljen licenszdíjat fizetniük egy DRM rendszerért, de ugyanakkor biztonságos legyen a rendszerük, hogy a kiadók megbízzanak bennük, így minél több kiadóval tudjanak szerződni.

**Hardvergyártók:** Ők gyártják a tartalomlejátszó eszközöket, mint amilyenek a DVD lejátszók és a hordozható mp3 lejátszók. Céljuk, hogy minél olcsóbb legyen az eszközük, ezért nem akarnak olyan technológiát a gépeikbe építeni, amit a felhasználó nem fizet ki. Kénytelenek ugyanakkor DRM-et integrálni az eszközökbe, különben a védett tartalmakat nem fogja tudni lejátszani az eszköz.

**DRM rendszerek szállítói:** DRM rendszereket állítanak elő, és értékesítenek a piacon a tartalomszolgáltatóknak és a hardvergyártóknak. Céljuk, hogy az ő rendszerük legyen a legelterjedtebb.

**Tartalomfogyasztók:** A felhasználók, akik egyszerűen tartalmat akarnak fogyasztani, zenét hallgatni és videókat nézni, és nem akarnak olyan dolgokkal foglalkozni, mint a DRM. Egyesek fizetni se akarnak a tartalomért, mások nem akarják, hogy a DRM megmondja nekik, hogy melyik eszközökön lehet lejátszani a tartalmakat.

### 2.2. A DRM rendszerek gyenge pontjai

Sokan kritizálják a DRM rendszereket és nem alaptalanul. A fő kritikusok két táborból kerülnek ki: a felhasználók közül, valamint a tartalomszolgáltatók közül.

A felhasználó szempontjából a legnagyobb problémát az jelenti, hogy sokszor nehézkes ezeknek a rendszereknek a használata és sok olyan korlátozást kényszerítenek rá a felhasználóra, amivel nem nagyon akar együtt élni.

A legfontosabb ezek közül, hogy a tartalomszolgáltatók legtöbbször készüléktípushoz és készülékpéldányokhoz kötik a tartalmak lejátszását, ezért azt nem lehet egy másik lejátszón meghallgatni, vagy például az autónkban lévő lejátszóra átmásolni, még akkor sem, ha esetleg azon is van valamilyen DRM rendszer, csak éppen nem az a fajta, mint amilyenben a tartalmat megvásároltuk.

A kiadók szempontjából a legnagyobb probléma ezekkel a rendszerekkel, hogy még mindig nem teljesen tökéletesek, azaz gyakran feltörik a rendszereket. Egyre inkább elterjedt az a nézet, hogy egy rendszernek nem kell feltörésbiztosnak lennie, azonban ezt olyan nehéz legyen a felhasználónak megtenni, hogy inkább a zenék megvásárlását választja.

Szintén nagy probléma, hogy nincs átjárás a különböző DRM szabványok között, azaz nem lehet lejátszani például a mobiltelefon-rendszerben vásárolt tartalmat egy PCs DRM rendszerben. Léteznek azonban törekvések arra, hogy kialakuljon valamiféle szabvány az átjárásra.

## 3. Mai DRM technológiák

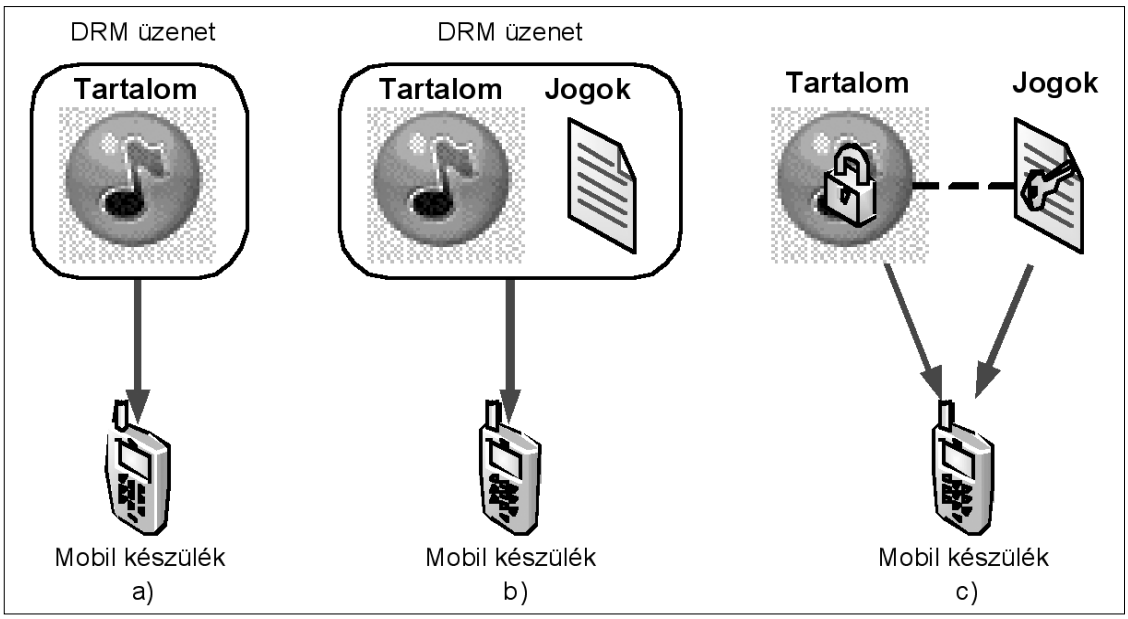
Aki ma DRM-védett tartalmat szeretne kínálni, sokféle DRM technológia közül választhat. A választásban döntő lehet, hogy a védett tartalmat milyen lejátszó platformon kívánja elérhetővé tenni. Mint írtuk, gondot jelent azonban az, hogy az egyes technológiák között az átjárás nehézkes vagy nem megoldható.

A mobiltelefonon elérhető technológiák esetében létezik egy DRM megoldás, amely igen széles körben támogatott. Ez az OMA DRM. Más platformok, mint például a PC-k esetén azonban nem létezik ennyire széles körű támogatása egyetlen technológiának sem.

### 3.1. Open Mobile Alliance – OMA DRM

Az Open Mobile Alliance 2002 júniusában jött létre, jelenleg több mint 350 nemzetközi cég alkotja. Az OMA tagjai az egész mobil szolgáltatási értékláncot lefedik:

– *Mobileszköz- és rendszergyártók:*
Ericsson, Thomson, Siemens, Nokia, Philips, Motorola, Texas Instruments stb.




*3. ábra*
*OMA DRM 1.0 által támogatott metódusok:*
*a) Forward lock,*
*b) Combined delivery ,*
*c) Separate delivery*

– *Mobilszolgáltatók:*
  Vodafone, T-Mobile, Orange, Telefónica stb.
– *Szoftverforgalmazók:*
  Microsoft, Sun, Microsystems, IBM, Oracle, Symbian stb.
– *Tartalomszolgáltatók:*
  Time Warner, Yahoo stb.

A testület a mobil távközlési ipar számára készít nyílt specifikációkat, elősegítve ezzel az eszköztől, hálózattól, szolgáltatótól független mobil szolgáltatások fejlesztését.

Az OMA által kidolgozott szabványok többek között digitális médiaobjektumok jogvédelmét megvalósító rendszerek specifikációit is tartalmazza (OMA DRM).

*3.1.1. OMA DRM 1.0*

A szervezet 2004 júniusában fogadta el a szabvány 1.0-ás verzióját, amit jelenleg több mint 550 mobiltelefon típus támogat.

A szabvány lényege, hogy a megvásárolt médiaobjektum használata meghatározott jogosultságokhoz kötött. Ugyanahhoz a tartalomhoz többféle jogosultság is tartozhat (pl. egy film esetén a felhasználó választhat korlátozott és korlátlan számú megtekintés között). A jogok leírása egy, a szabványban meghatározott XML formátumú fájl segítségével történik. A jogok érvényesítését a készülékeken található DRM ügynök *(DRM agent)* végzi.

A digitális tartalom egy DRM üzenetben *(DRM Message)* kerül terjesztésre. A tartalom sokféle lehet, kezdetekben azonban ez inkább csak csengőhangokra, háttérképekre, operátor logókra, játékokra korlátozódott. A DRM üzenet tulajdonképpen a bináris tartalom illetve az esetlegesen hozzá kapcsolódó leíró fájlok MIME csomagolása. A DRM üzenetben a tartalom lehet akár titkosítva is.

Az OMA DRM 1.0 a tartalom terjesztésben három fő metódust támogat *(lásd az előző oldali 3. ábrán)*.

*Tiltott továbbítás (Forward lock)*

A felhasználó letölt a készülékére egy médiaobjektumot a szerverről. A tartalom egy DRM üzenetben érkezik, a letöltéshez szükség van a tartalom URL-jére. Letöltés után a tartalom szabadon megtekinthető, ahányszor csak a felhasználó kívánja, azonban nem továbbítható más készülékekre. A továbbítás tiltását a készülék DRM ügynöke felügyeli, illetve szintén az gondoskodik arról, hogy csak olyan alkalmazás érje el a tartalmat, amely megbízható.

*Kombinált letöltés (Combined delivery)*

Ebben az esetben a letöltött DRM üzenet a választott médiaobjektumon kívül egy jogosultságobjektumot is fog tartalmazni. Ez az objektum határozza meg, hogy a felhasználó miként használhatja a médiaobjektumot. A jogosultságobjektumon keresztül lehetőség van például arra, hogy a felhasználó beletekinthessen a megvásárolandó tartalomba.

A jogosultság leírása a *Right Expression Language (REL)* segítségével történik. A nyelv kialakításánál az egyszerűségre törekedtek, így csak az eljárások és kényszerek minimális halmazát tartalmazza. Az engedélyhez köthető funkciók a következőek: lejátszás, megjelenítés, végrehajtás és nyomtatás. A kényszerek a funkciókat limitálják, tehetik ezt darabszámra, meghatározott időpontok között vagy meghatározott időintervallumra. A tartalom továbbítására itt sincs lehetőség.

*Szétválasztott letöltés (Separate delivery)*

Szétválasztott letöltésről beszélünk, ha a médiaobjektum és a jogosultságobjektum külön (akár különböző csatornán, különböző időben, különböző szerverről stb.) érkezik meg a készülékre. A médiaobjektum egészen addig nem használható, amíg a hozzá tartozó jogosultsági objektum nem áll rendelkezésre.

Ez a metódus lehetővé teszi a tartalmak továbbítását más készülékekre. A médiaobjektum továbbítása után a céleszköznek is be kell szereznie a tartalomhoz tartozó jogosultságokat, különben a DRM ügynöke nem fogja engedélyezni a tartalom használatát.

*Streaming OMA DRM 1.0 rendszerben*

Bár az OMA DRM 1.0 szabványt nem úgy fejlesztették, hogy kimondottan alkalmas legyen stream-elt tartalom lejátszására, mégis kisebb kerülő úton lehetőségünk van erre is. Az ajánlás szerint, ilyenkor a videófolyam specifikációja van a DRM üzenetben. A specifikáció leggyakrabban egy SDP (Session Description Protocol) üzenet és tartalmazza a videófolyam eléréséhez szükséges URL-t. A lejátszás során ügyelni kell arra, hogy amennyiben a tartalom csak egyszer nézhető meg, olyan lejátszót válasszunk, amely nem képes a kapott tartalmat elmenteni. A biztonság fokozására a folyamot titkosítani is szokták, ekkor a dekódoláshoz szükséges kulcs is a védett SDP üzenetben található.

*3.1.2. OMA DRM 2.0*

Az Open Mobile Alliance 2006 júniusában fogadta el szabvány második verzióját, ami tulajdonképpen az első verzió „Szétválasztott letöltés” metódusának kiterjesztése. Később, 2008 elején a 2.0 szabványt módosították, így lett belőle 2.0.1. Ebben a verzióban csak a szétválasztott letöltés modell használható, azonban az nagyobb funkcionalitást és biztonságot kínál, mint az 1.0 verzióban. A legfőbb újítások:

– A tartalom és jogok mozgatása különböző eszközök között
– Tartalom exportálása offline eszközökre (pl. mp3 lejátszó)
– Szabad tartalommegosztás felhasználó csoportok között (domain)
– PKI alapú kölcsönös azonosítás a felhasználó eszköze és a jogkezelő között
– Bővülő leírás a jogokhoz
– P2P szuperdisztribúció támogatás

Az OMA 2-es szabvány ugyanakkor még koránt sem annyira elterjedt, mint előző verziója, így aki mobiltelefonos DRM platformban gondolkozik, annak még mindig egy megfontolandó lehetőség az OMA DRM 1.0.

*Az architektúra résztvevői és elemei*

A DRM architektúra részeit a *4. ábra* mutatja.

**DRM ügynök:** Hasonlóan az előző verzióhoz, egy megbízható entitás a felhasználó készülékén, ő felelős azért, hogy egy tartalmat csak a hozzá tartozó jogosultságobjektumban meghatározott módon lehessen felhasználni.

**Tartalomszolgáltató:** Elérhetővé teszi a DRM tartalmat. A szabvány pontosan definiálja a DRM tartalom formátumát. A tartalom DRM ügynökhöz juttatása különféle átviteli módszerekkel (HTTP, WAP, MMS stb.) történhet.

**Jogosultságszolgáltató:** Engedélyeket és megkötéseket rendel a DRM tartalomhoz, majd létrehozza az ezeket tartalmazó jogosultságobjektumot. A DRM tartalom nem használható a jogosultságobjektum nélkül, és csak annak megfelelően használható.

**Felhasználó:** DRM tartalmat igényel, ezekhez csak a DRM ügynökön keresztül fér hozzá

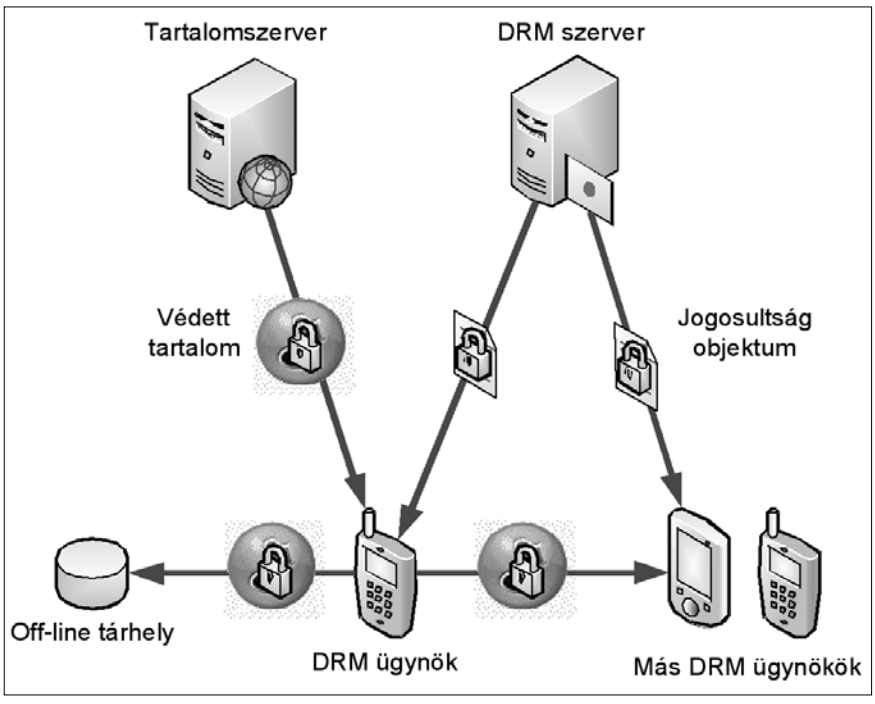
**Készüléken kívüli tárhely:** Az OMA DRM 2.0 szerinti DRM tartalom biztonsága nem sérül, ha azt a felhasználó a készüléken kívül (is) eltárolja. Ennek oka lehet biztonsági másolat, tárhely felszabadítása a készüléken stb. a jogosultságobjektumok közül csak azok tárolhatók készüléken kívül, amelyek nem tartalmaznak állapotinformációt (például fennmaradó lejátszások száma).

*Biztonság*

Az OMA DRM 2.0 nagy erőssége az első verzióval szemben a biztonság. A szabvány biztosítja, hogy a tartalomhoz csak az férhessen hozzá, aki arra jogosult, valamint a jogosultságobjektumot csak a megfelelő készülék (vagy csoport) tudja értelmezni.

A biztonságos DRM tartalom létrehozása és küldése a következő lépésekből áll:

*4. ábra OMA DRM 2.0 architektúra*




**1. Tartalom csomagolása:**

A tartalomszolgáltató egy biztonságos konténerbe (DCF, DRM Content Format) csomagolja a média objektumot. A DRM tartalmat egy szimmetrikus tartalomtikosító kulcs (CEK, Content Encryption Key) segítségével rejtjelezi.

**2. DRM ügynök hitelesítése:**

Minden DRM ügynök rendelkezik egy publikus/privát kulcspárral és egy tanúsítvánnyal. A tanúsítvány kiegészítő információkat tartalmaz, mint a gyártó vagy a készülék típusa. Ennek segítségével a tartalom- és a jogosultságszolgáltató képes hitelesíteni az ügynököt.

**3. A jogosultságobjektum generálása:**

Elkészül a jogosultságobjektum XML fájlja. Ez tartalmazza a CEK-et is. Ez biztosítja, hogy a tartalmat ne lehessen használni a jogosultság objektum nélkül.

**4. A jogosultságobjektum védelme:**

A jogosultságobjektum küldése előtt annak érzékeny részei (pl. a CEK) titkosításra kerülnek. Ez a titkosítás a DRM ügynök publikus kulcsával történik. Ez biztosítja, hogy csak a megfelelő DRM ügynök férjen hozzá a DRM tartalomhoz. A DRM szerver ezen kívül digitálisan aláírja a jogosultság objektumot.

**5. Szállítás:**

A DRM- és a jogosultságobjektum készen állnak arra, hogy eljuttassák őket a DRM ügynökhöz. Mivel mindkettő biztonságos, tetszőleges szállítási protokoll (HTTP, Wap Push, MMS stb.) használható.

*3.1.3. OMA DRM 2.1*

A második verzió kiadása után az újabb piaci igényekre reagálva az OMA elkészítette a DRM szabvány 2.1-es verzióját. Ennek architektúrája megegyezik a 2.0-val, azonban beleépítettek néhány új felhasználási lehetőséget:

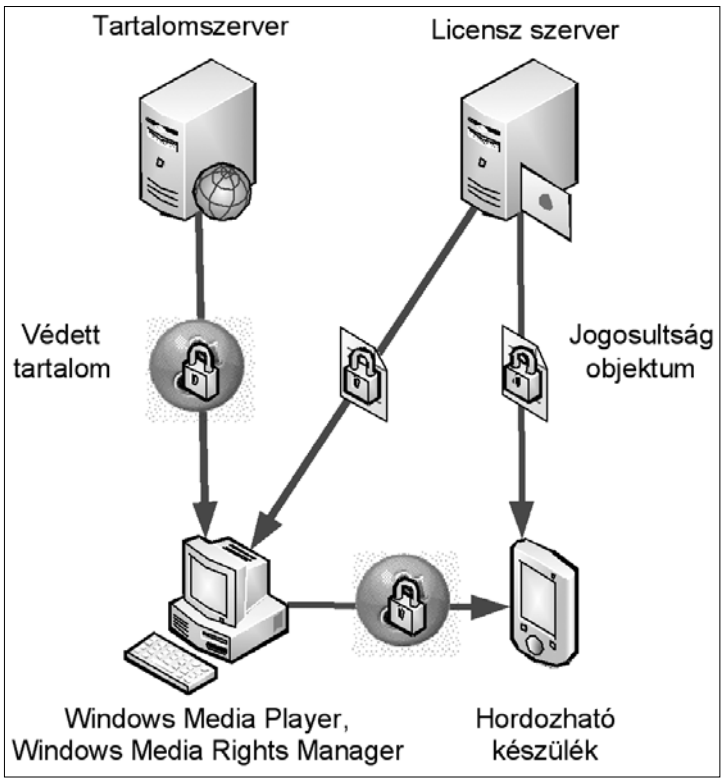
– *Mérések támogatása:* A jogosultság kibocsátójának szüksége lehet információra a különböző tartalmak felhasználásairól.

– *Jogosultság feltöltése:* Lehetőség van a jogosultságobjektumot a DRM szolgáltatóhoz feltölteni. Erre akkor lehet szükség, ha a felhasználó át akarja mozgatni a jogosultságobjektumot egyik készülékről a másikra.

– *Megerősítés a jogosultságobjektum telepítéséről:* A DRM ügynök megerősítő üzenetet küld a DRM szervernek a jogosultságobjektum telepítése után.

### 3.2. Microsoft Windows Media DRM

A Microsoft Windows Media DRM a Microsoft saját jogvédelmi megoldása, ami végponttól-végpontig tartó biztonságot garantál. A rendszer aktuális verziója a 2004-ben kiadott Microsoft Windows Media DRM 10.




*5. ábra*
*A Windows Media Rights Manager architektúrája*

A *5. ábra* mutatja a rendszer architektúráját. Látható, hogy a rendszer felépítése nagyrészt egyezik az OMA DRM 2.0 felépítésével. A felhasználó csak akkor férhet hozzá a becsomagolt tartalomhoz, ha rendelkezik a szükséges jogosultsággal.

A Windows Media Rights Manager által szolgáltatott biztonságos tartalom létrehozása és küldése a következő lépésekből áll:

**1. Csomagolás:** A Windows Media Rights Manager egy kulcs segítségével titkosítja a médiafájlt. Ezt a kulcsot a rejtjelezett licenszobjektum fogja tartalmazni. A csomagolt médiafájlba egyéb információk is kerülnek, például a cím, ahonnan a licensz megszerezhető. A rendszer a Microsoft saját médiaformátumait használja (*.wma illetve *.wmv fájlok).

**2. Elosztás:** A csomagolt fájl elérhetővé tételére több lehetőség van: feltölthető egy webszerverre, terjeszthető CD-n, e-mail-en küldhető stb. A rendszer a tartalmak másolását, továbbküldését is engedélyezi.

**3. Licensz-szerver:** A tartalomszolgáltató választ egy licensz szolgáltatót, aki a tartalmakra vonatkozó specifikus jogokat és szabályokat fogja tárolni. A licensz-szerver feladata a felhasználó licensz igényének elbírálása.

**4. Licenszkérelem:** Védett tartalom lejátszásához a felhasználónak rendelkeznie kell a titkosítás feloldásához szükséges kulccsal. Az ezt tartalmazó licenszet a licensz-szervertől kérvényezi. A licenszkérelem automatikusan megtörténik, amikor a felhasználó első alkalommal tekinti meg a tartalmat. A rendszer ilyenkor vagy egy regisztráció oldalra irányítja a felhasználót, vagy a háttérben kéri le a licenszet.

**5. Médiafájl lejátszása:** A tartalom lejátszásához Windows Media Rights Manager-t támogató lejátszóprogramra van szükség. A felhasználó a licenszben meghatározott feltételek szerint tekintheti meg a tartalmat. Ez különböző jogosultságokat tartalmazhat: kezdeti időpontot és időtartamot, lejátszások számát stb. Lehetőség van egy licenszen belül több készülék számára is jogokat biztosítani.

### 3.3. RealNetworks – Media Commerce Suite

A RealSystem által kifejlesztett DRM rendszer szintén az on-line terjesztett tartalmak védelmét hivatott ellátni. Számos üzleti modellt támogat, mint feliratkozás (subscription), Video on Demand (VOD) stb. Létező RealSystem rendszerek is kiegészíthetők vele.

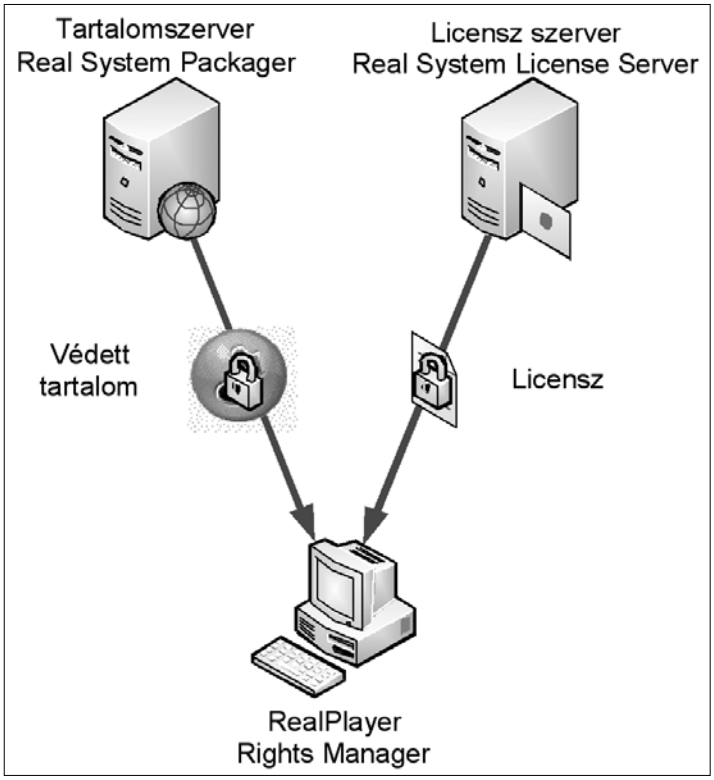
A RealSystem Media Commerce Suite négy komponenst nyújt a médiatartalmak védelmére, terjesztésére és a jogosultságok érvényesítésére:

- **RealSystem Packager**
  Tartalomszolgáltatók részére nyújtott szoftver, segítségével a médiafájlok biztonságos formátumba csomagolhatók.
- **RealSystem License Server**
  HTTP szerver, ami licensz kérelmeket fogad, és licenszeket generál, amik lehetővé teszik a védett médiafájlokhoz való hozzáférést.
- **Media Commerce kiegészítés a RealPlayer-hez**
  Egy megbízható kliens, ami képes biztonságos RealMedia fájlokat (*.rms) értelmezni.
  Ez a fájlformátum speciálisan erre a célra, RealMedia tartalom biztonságos tárolására lett létrehozva.
  A kiegészítés biztosítja, hogy a tartalom megbízható környezetben, a rendelkezésre álló jogosultságoknak megfelelően lesz felhasználva.
- **RealSystem biztonságos fájlformátum beépülő modul**
  RealSystem szerver számára teszi lehetővé a védett tartalom terjesztését (streaming).

### 3.4. Marlin DRM

A Marlint 2005 januárjában alapította öt vállalat: az Intertrust, a Panasonic, a Philips, a Samsung és a Sony. Céljuk egy DRM-en alapuló tartalom megosztási platform létrehozása volt. 2005 októberében az alapító vállalatok bejelentették a Marlin Developer Community (MDC) megalakítását. A közösség tagjai számára nyilvános a Marlin specifikációja, eszközei, SDK-ja stb. A tagok így részt vehetnek a rendszer fejlesztésében, tesztelésében, a forráskód felülvizsgálatában. Az MDC ezen kívül tréningeket és más eseményeket is szervez.

Az alapítók által létrehozott másik szervezeti egység, a Marlin Trust Management Organization (MTMO) felügyeli az MDC munkáját. Ez a szervezet végzi a Marlin termékek számára a kulcsok és licenszek kezelését, valamint a közösség által fejlesztett Marlin termékeket kötelezi a meghatározott szabályok, feltételek betartására.




*6. ábra*
*RealSystem Media Commerce Suite Architektúrája*

A Marlin DRM architektúra is ugyanazokból a szereplőkből áll, mint az OMA DRM: tartalomszolgáltató, jogosultságszolgáltató és felhasználó. A tartalom- és jogosultságobjektumok használata is az OMA DRM-ben leírtakhoz hasonlóan történik: a tartalomszolgáltató egy szimmetrikus kulcs segítségével titkosítja a tartalom objektumot. A jogosultságobjektum pedig tartalmazza a tartalom felhasználási szabályait, valamint a tartalom titkosításának feloldásához szükséges kulcsot. A két rendszer közti fő különbség a jogosultság értelmezésében van.

*3.4.1. Csomópont- és kapcsolatobjektumok*

A Marlin csomópont (*node*) és kapcsolat (*link*) objektumokat használ a résztvevők (felhasználók, tartalomszolgáltatók és jogosultságszolgáltatók) közötti reláció kifejezéséhez. A tradicionális DRM rendszerekben a jogosultság közvetlenül az azt lekérő készülékhez van kötve. A Marlinban a jogosultság felhasználóhoz van kötve és a felhasználók és készülékek, vagy felhasználók és előfizetések közötti kapcsolatok csomópontok és kapcsolatok rendszereként vannak tárolva. A csomópontok szerinti szétválasztás nagyon rugalmassá teszi a rendszert.

A csomópontok a rendszer logikai entitásait reprezentálják: készülékek, felhasználók, feliratkozások stb. A kapcsolatok a csomópontokat kötik össze, egy irányított gráfot hozva létre.

Erre mutat példát az *7. ábra*.

*7. ábra*
*Csomópontokból és kapcsolatokból álló irányított gráf*

Egy csomópont akkor használhatja egy másik tartalmat, ha az irányított gráfban vezet hozzá út. A 7. ábra példájában „Készülék A” használhatja a tartalomszolgáltató által küldött tartalmat, míg „Készülék C” nem.

### 3.5. Apple FairPlay

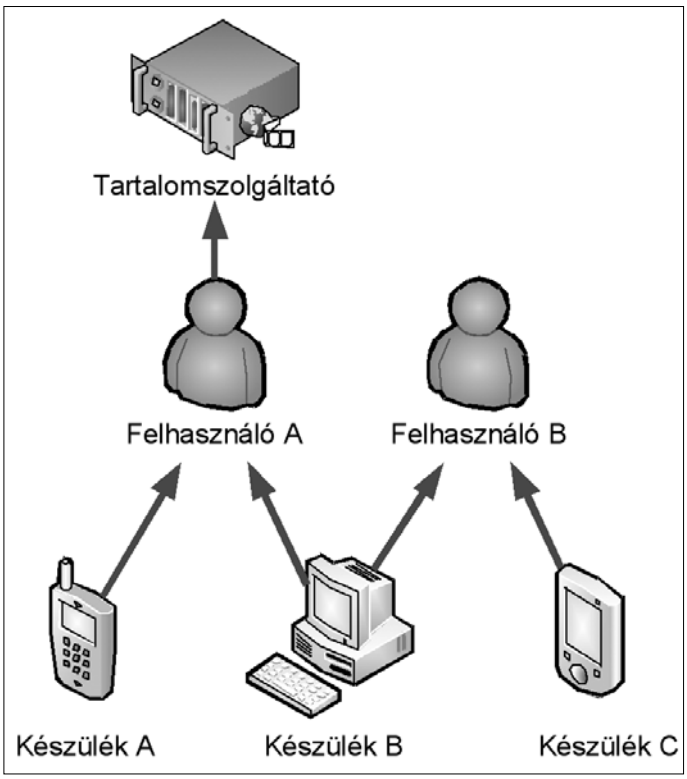
A FairPlay az Apple Inc. által létrehozott és alkalmazott DRM technológia. Ismertségét az iTunes on-line zeneboltnak köszönheti, az innen vásárolt zeneszámokat a FairPlay technológia védi. Az AAC fájlok titkosított formátumban érkeznek, a felhasználó a következő megkötésekkel használhatja őket:

– egy zeneszám tetszőleges iPod készülékre másolható;
– egy zeneszám maximum 5 különböző, az iTunes Store oldalán regisztrált számítógépen játszható le;
– a zeneszám akárhányszor másolható audio CD-re, azonban ugyanaz az összeállítás maximum hétszer írható fel.

A jelenleg támogatott készülékek: Apple iPod, Apple iPhone, Motorola ROKR E1, Motorola SLVR, Motorola RAZR V3i.

### 3.6. SUN DReaM (DRM/everywhere available)

A Sun Microsystems nem gyárt szórakoztatóelektronikai eszközöket, 2005 szeptemberében mégis beszállt a DRM üzletbe, mivel a DRM piac egyre növekszik és az elérhető DRM megoldások csak a nagy gyártók, vagy konzorciumok saját megoldásai körül csoportosulnak. A Sun ezzel szemben egy licenszdíjmentes változatot ígér nyílt forrással, ahol magának a gyártónak azért van némi kontrollja az elkészült szabványon.



A Sun DRM architektúrájának az alapja az DRM-OPERA. Ez a megoldás egy korábbi EU által támogatott projektből származik, ahol a hangsúly az együttműködésen volt. Előnye, hogy a tartalom csak a hitelesített felhasználóhoz kötődik, és nem függ attól az eszköztől, amit a felhasználó éppen használ.

A SUN DReaM megoldás legnagyobb előnye az OPERA projektből átvett együttműködésben van, valamint abban, hogy a megoldás használata nem lesz licenszköteles.

#### 3.7. A DRM elterjedése

A DRM esetében is nagyon fontos tényező az elterjedtség. Az OMA DRM 1.0-t a legtöbb mobiltelefon támogatja, azonban a biztonság és felhasználhatóság szempontjából kedvezőbb 2.0 (vagy 2.1) szabványt már kevesebben. A többi szabvány, amelyek mögött egy vagy több, de összességében kevés számú cég áll, várhatóan csak a saját platformján tudja elterjeszteni saját megoldását. Ennek a technikai okok mellet szabadalmi okai is vannak. Ilyen esetben például várható, hogy a Windows alapú rendszereken mindig is Windows DRM fut majd, az Apple készülékein a FairPlay, míg a Panasonic, Philips, Samsung, valamint a Sony készülékeken a Marlin DRM.

Az elterjedtséggel szorosan összefügg a szabadalmak kérdése. A legtöbb DRM szabvány mögött álló cég licenszdíjat kér technológiájuk felhasználásáért. Ezért is van az, hogy az egyik DRM szabványban érdekelt cég nem fogja a konkurens technológiát alkalmazni. Vannak azonban olyan megoldások is, ahol nincs licenszdíj. Elterjedtség szempontjából a DRM technológiák közötti átjárhatóság egy nagyon fontos kérdés, és – bár a felhasználók örülnének ilyen megoldásoknak –, úgy tűnik, hogy a gyártók nem látják érdekeltségüket ezen a területen.

## 4. Élet DRM nélkül

A DRM-et teljesen elutasítók legfőképpen azt hozzák fel a DRM rendszerek ellen, hogy az csak egy olyan torzszülött, ami azért jött létre, hogy a kiadók (jobb híján) fenn tudják tartani a régi rendszert, vagyis hogy fizetünk a tartalmakért. Ezzel szemben sokkal jobb volna, ha olyan új üzleti modelleket dolgoznának ki, ami jobban illeszkedik ahhoz, hogy a tartalmakat teljesen szabadon másolgatják a felhasználók. A kiadók azonban nagyon erősek, így nehéz velük szembeszállni. Azt például, hogy milyen online zeneboltokban árulják a tartalmakat, a kiadók döntik el, legtöbbször az alapján, hogy a bolt milyen DRM rendszerrel van felszerelve.

#### 4.1. DRM-mentes üzleti modellek

Sok üzleti modell azonban már most szakít a DRM-mel és helyette DRM mentesen vagy akár ingyenesen teszi elérhetővé a tartalmat. A DRM-védelem nélküli tartalmak letöltés után akár szabadon másolhatóvá válnak.

Az egyik legfontosabb dolog ezzel az elvvel kapcsolatban, hogy a kiadók döntik el, hogy odaadják-e a számaikat azoknak a kereskedőknek, akik nem használnak semmilyen DRM rendszert. A fő visszatartó erő, hogy eddig még nem sikerült bizonyítani, hogy jobban megéri DRM mentes tartalmat eladni a felhasználóknak, mint DRM-védettet.

A DRM-mentesség értéket jelent a felhasználónak, ezért a jelenleg üzemelő zeneboltok egy része DRM-védett, és DRM-mentes tartalmakat is kínál, utóbbiakat valamivel drágábban, mint a védett tartalmakat, hiszen az árban így kompenzálja a kieső eladása utáni veszteséget. A felhasználók többnyire azért veszik meg a DRM-mentes tartalmakat, mert esetleg több lejátszón is le akarják játszani azt.

Azok a tartalomszolgáltatók, akik teljesen védelemmentes tartalmat is kínálnak, többféle üzleti modellel dolgoznak. Van olyan, akiknél számonként kell fizetni, mint a legnépszerűbb eMusic, Amazon MP3 vagy Aime Street. Léteznek olyan szolgáltatók, akik csak online hallgatásra kínálják a számokat, mint amilyen például a radio.blog.club.

Újfajta kezdeményezések is napvilágot láttak. 2007 szeptemberében a Radiohead együttes saját kiadóját megkerülve, a honlapjáról ingyen letölthetővé tette legújabb albumát. A rajongóknak annyit kellett fizetnie érte, amennyit akartak, de akár ingyen is letölthették. Egy hónappal az indulás után minden harmadik letöltő fizetett valamennyit a számokért, átlagban 6 dollárt. Ennek nyomán a Radiohead körülbelül 2,4 millió dollár bevételt eszközölt ebből az akcióból (amit már nem kell megosztania a kiadóval).

Hasonlóan nagy lépés volt a kiadók átformálásában, hogy a popénekesnő Madonna 2007 októberében szerződést bontott 20 éves kiadójával és az új szerződését a következő 3 albumára már egy koncertszervező céggel kötötte meg. Így Madonna, a tartalom tulajdonosa már egy csatolt terméken keresztül jut a pénzéhez, illetve az is előfordulhatna, hogy most már maga a zenei tartalom is csak csatolt termék.

Az említett zenei példák mellett olyan is akad, ahol a készülék árába tervezik beépíteni a tartalomletöltés előfizetését. Bár az ilyen jellegű üzleti modellek még nem elterjedtek, mégis számos kísérlettel találkozunk.

## 5. Összefoglalás és jövőkép

Cikkünkben ismertettük a DRM technológia mögött található motivációkat. Amennyiben a régi tartalom és annak elosztásának gyakorlatát tekintjük, elengedhetetlen, hogy a digitális médiával együtt megjelenjen a DRM, amely annak védelmével hivatott foglalkozni. A DRM térnyerésével a kiadók tovább folytathatják bevált üzleti modelljeiket. A jól működő DRM így orvosság a média tartalom kiadói számára a felhasználók illegális másolásai ellen.

Az egyszerűen kivitelezhető, bár illegális másolást megismerő felhasználóknak viszont ez a modell nem

tetszik. A másolást nem tartják nagy bűnnek, a kiadókat viszont, látva az elrettentő pereket, elítélik. Nagyjából itt tart ma a világ.

Ugyanakkor az illegális másolások és a kezdeti DRM rendszerek gyengesége azt is eredményezte, hogy a kiadók lassan kezdik belátni, hogy új értékesítési modellekre is szükség van a hagyományos eladások mellett vagy helyett. Jelenleg az online zeneboltok szaporodásának és a havidíjas tartalomfogyasztás elterjedésének is tanúi lehetünk. A DRM technológia itt is segít, és úgy látszik, az új modellek esetében a felhasználók befogadják már a DRM-et.

A közeljövőben várhatóan a tartalomkínálat még inkább a letöltéses eladások irányába fog mozdulni és egyre kevésbé lesz népszerű a tartalmak fizikai hordozókon, mint például CD lemezeken történő árusítása. Az egyre nagyobb számú fogyasztó már rákényszerítheti a DRM technológiák mögött álló cégeket, hogy dolgozzák ki a technológiák közötti átjárás megvalósítását. Így végül a DRM elhozza mindenki megelégedettségét, a szerzőknek és kiadóknak nem kell tartani a jelentős mértékű illegális másolásoktól, a felhasználók pedig reális áron jutnak a tartalomhoz, amit bármilyen DRM képes készülékkel le is hallgathatnak vagy meg is nézhetnek. Ez azonban sajnos még csak a jövő...

**Irodalom**


[1] Iannella, R.,
The Open Digital Rights Language:
XML for Digital Rights Management .
Information Security Technical Report,
Volume 9, Issue 3, July-September 2004, pp.47–55.

[2] OMA (2004).
Open Mobile Alliance DRM Specifications,
Version 1.0, Approved Enabler, 2004. június,
http://www.openmobilealliance.org/Technical/
release_program/drm_v1_0.aspx

[3] OMA (2008).
Open Mobile Alliance DRM Specifications,
Version 2.0.1, Approved Enabler, 2008. február,
http://www.openmobilealliance.org/Technical/
release_program/drm_v2_0.aspx

[4] OMA (2007).
Open Mobile Alliance DRM Specifications,
Version 2.1, Candidate Enabler, 2007. július,
http://www.openmobilealliance.org/Technical/
release_program/drm_v2_0.aspx


## Hírek

Vegyes vállalatot hozott létre az operatív irányítás terén szerzett tapasztalatáról ismert két cég, a Siemens AG és a Gores Group. Az elsősorban vállalatok bővítésével foglalkozó amerikai magántőkebefektető társaság, mely széles körű tapasztalatokkal rendelkezik a technológiai és a távközlési szektor vállalatainak irányításában, történetének eddigi legnagyobb volumenű felvásárlásával a **Siemens Enterprise Communications** vállalat üzletrészének 51 százalékát vásárolta meg. Az egységes vállalati kommunikáció területén a világ egyik vezető cégeként működő, 13 ezer alkalmazottat foglalkoztató vállalat 2007-ben 3,1 Milliárd eurós forgalmat produkált. Amint azt a Siemens magyarországi leányvállalatának sajtótájékoztatóján Jürgen Liss ügyvezető igazgató elmondta, hogy a tranzakció kapcsán 350 millió eurót fektetnek a vegyes vállalatba – a kutatásra és fejlesztésre amúgy is betervezett összegeken és a normál üzletmenet keretén belül felmerülő kiadásokon felül. A beruházások és a további párhuzamos akvizíciók nyomán létrejött SEN Group célja a Siemens Enterprise Communications értékesítési szervezetének lehető legnagyobb mértékű hasznosítása, a további terjeszkedés elősegítése, valamint a vállalat átalakításának ösztönzése hardverszállítóból szoftvereket és szolgáltatásokat kínáló társasággá.

•

A **Sun Microsystems**, Inc. megjelentette a Solaris operációs rendszer legújabb, 10 10/08 számú verzióját. Az új verzió a Solaris 10 operációs rendszer alapvető erősségeire építve segít az ügyfeleknek maximalizálni az erőforrások kihasználását és a rendszerteljesítményt, kezelni az összetett adatközpontokat, illetve fenntartani az üzletvitel folytonosságát és csökkenteni a költségeket. A Solaris 10 10/08 verzió számos termékfrissítést és fejlesztést tartalmaz, amelyek közül több az OpenSolaris közösség munkájának köszönhető.

•

A HP újgenerációs adattárolói virtualizációs megoldása a **HP StorageWorks** SAN Virtualizációs Szolgáltatási Platform (SVSP) néven kerül forgalomba mely, tovább növeli az adattárolók hatékonyságát és egyszerűsíti a különböző adattároló rendszerek menedzsmentjét. A HP SVSP egy új, hálózat-alapú adattároló platform, amely egyesíti a HP és akár más gyártótól származó tárolórendszerek erőforrásait. Az új platform együttműködik a HP Storage Works Modular Smart Array-jel (MSA) és az Enterprise Virtual Array-jel (EVA), valamint számos más gyártó megoldásával, így központosítja a virtuális SAN környezet menedzsmentjét.