Digitális tartalmakhoz kapcsolódó szerzői jogok védelmének technológiai megoldása
– az OMA szabványok áttekintése –

Pándi Zsolt (pandi@hit.bme.hu)
2004 október

A digitális formában elérhető tartalmak egyszerű, korlátlan és elhanyagolható költségekkel járó reprodukálhatóságából adódóan az ezekhez kapcsolódó szerzői jogok érvényesítése komoly problémát jelent. Az angol nyelvű szakirodalomban Digital Rights Management-nek (DRM) nevezett témakörben mindeddig nem született teljesen általános érvényű és hatékony megoldás, aminek következményeit súlyosbítja, hogy az Internet-lefedettség gyors ütemű növekedésével a szerzői jogokkal védett tartalmakhoz való hozzáférésért fizetni hajlandó és képes kereslet egyre nagyobb részének van lehetősége illegális úton hozzáférni védett tartalmakhoz. A jogok tulajdonosai mindezidáig inkább csak jogi úton tudtak érvényt szerezni követeléseiknek, aminek talán legelső nemzetközi példája a Napster fájlcserélő hálózat fejlesztői és fenntartói elleni közelmúltbeli per volt.
Nyilvánvaló, hogy működőképes megoldást csak valamilyen speciálisan erre a célra kidolgozott technológiai megoldással lehet nyújtani. A mobilkészülékek piacának jelentősebb résztvevőt tömörítő Open Mobile Alliance (OMA) 2002-es létrejötte óta foglalkozik a mobil számítástechnika eszközeihez kapcsolódó ajánlások kidolgozásával. A szervezet viszonya a mobiltechnológiai piachoz az Internet Engineering Task Force (IETF) és az Internet viszonyához hasonlítható. Az OMA a DRM-et kiemelten kezeli és külön munkacsoportja foglalkozik az ezzel kapcsolatos ajánlások kidolgozásával. A szervezet 2004-re elkészült a DRM ajánlások második, átdolgozott verziójával, amelyet a későbbiekben mutatunk be.

Előfeltételek

A digitális tartalmak kézbentartható felhasználásának előfeltétele, hogy ezen tartalmak a felhasználáshoz szükséges eszközökre, a bemutatandó ajánlások esetében a mobilkészülékekre a felhasználó által irányított, de lépéseiben közvetlenül nem befolyásolható folyamat eredményeképpen jussanak el. Az ún. *media object*ek (média tartalmak) mobilkészülékekre való letöltésének technikai hátterét összefoglaló néven Over-The-Air provisioningnak (OTA) nevezik és [1] külön fejezetet szentel neki. A media object értelmezése teljesen általános: lehet csengőhang, háttérkép, MIDlet (J2ME alkalmazás), digitális formájú zene, digitalizált könyv(részlet), stb.
A hasonló célokra az Interneten legelterjedtebben használt Hypertext Transfer Protocol (HTTP) alkalmazása mobilkészülékek esetében számos problémát vet fel. Például a felhasználó nem ellenőrizheti, hogy a letöltendő fájl formátumát egyáltalán képes-e kezelni a készüléke, van-e elég memória a letöltéshez mielőtt a tényleges letöltés megtörténne. A HTTP 1.1 verziója mindezek ellenére olyan hasznos funkcióhalmazt biztosít, amelyet fel lehet használni egy, az említett hiányosságokat kiküszöbölő letöltési folyamat megvalósításához.
Az [1]-ben definiált letöltési folyamat a következő lépéseket definiálja:

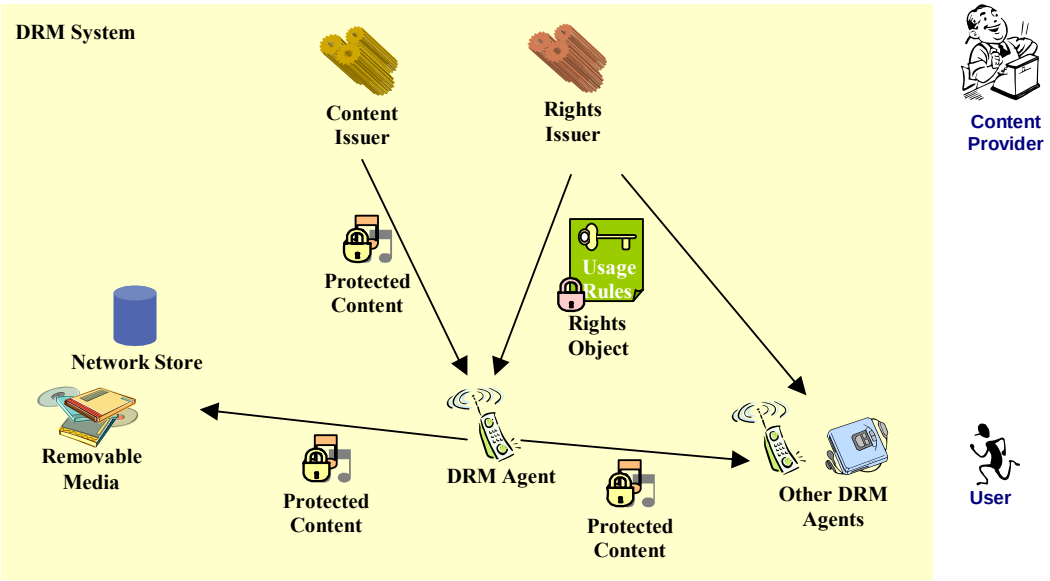
1. A hozzáférhető Application Descriptorok (media objectek tulajdonságait leíró adatcsoportok) böngészése a mobilkészülékkel, és a kívánt media object kiválasztása.
2. Download User Agent (a letöltési folyamatot levezénylő, a felhasználó készülékén futó program) elindítása.
3. Szükséges előzetes ellenőrző lépések elvégzése az Application Descriptor tartalma alapján a media object felesleges letöltését elkerülendő.
4. Megerősítés kérése a felhasználótól a letöltés megkezdéséhez.
5. Media object letöltése.
6. Medi object telepítése a felhasználó készülékére.
7. A media object szolgáltatójának értesítése a telepítés sikerességéről.
8. A felhasználó értesítése a telepítés sikerességéről.

A fentebb részletezett folyamatba a felhasználó csupán az 1. és 4. lépéseknél tud beavatkozni, a többi lépést a Download User Agent végzi automatikusan. A vázolt módszer a következő előnyökkel bír:

- A szolgáltató visszajelzést kap a media object telepítéséről, amely felhasználható például a számlázáshoz.
- A media objectek elérhetővé tétele és letöltése a hálózat oldalán elválasztható egymástól, mert az Application Descriptorban megadható a media object közvetlen hozzáférési helye, amely eltérhet az Application Descriptor hozzáférési helyétől.
- A haszontalan letöltési (és halózati erőforrás foglalási) kísérletek száma jelentősen csökken.
- A folyamat teljes egészében hálózatfüggetlen, azaz a fenti működéshez szükséges funkcionalitást biztosító tetszőleges hálózati környezetben működtethető.

DRM ajánlások

Az imént ismertetett letöltési folyamat nem ad módot a tartalmak felhasználásának szabályozására, csupán a hozzáférés technológiai részleteivel foglalkozik. A felhasználás szabályozásához kiegészítő információk és további technológiai megoldások szükségesek, amelyekkel az OMA DRM ajánlásai foglalkoznak [2-5].
A DRM szabványok célja a digitális tartalmak kontrollált terjesztésének és felhasználásának lehetővé tétele. A DRM alapgondolata szerint a digitális tartalmakat hozzájuk kapcsolódó, a tartalmak tulajdonosai által definiált használati jogok szerint használják fel és terjesztik azonosított készülékek segítségével. A DRM ajánlások ehhez tartalomformátumokat (Content Format, CF) [4], protokollokat (Rights Object Acquisition Protocol, ROAP) [5] és jogleíró nyelveket (Rights Expression Language, REL) [3] határoznak meg.
Az ajánlások által leírt architektúrát a következő ábra mutatja be.



A rendszer résztvevői a tartalomszolgáltatók (Content Issuer, CI), a jogszolgáltatók (Rights Issuer, RI), a DRM Agentek, a védett tartalmak (Protected Content), és a felhasználási jogok (Rights Object, RO).
A DRM Agent szerepe, hogy a védett tartalmakhoz biztosítson hozzáférést a felhasználóknak. Alapvető kérdés továbbá, hogy csak rajta keresztül lehessen ezekhez a tartalmakhoz hosszáférni. A DRM Agent a felhasználó készülékén futó program (tényleges implementációja azonban valószínűleg hardvertámogatást is feltételez), amely a rendszerben ún. trusted entity, azaz a felhasználó által nem manipulálható, mindig helyesen működőnek feltételezett szereplő. A tartalomszolgáltatónál hozzáférhető tartalmak csak a megfelelő felhasználási jogok birtokában használhatók fel, amelyeket a jogszolgáltatótól lehet beszerezni. A védett tartalmak a jogokkal együtt és azoktól függetlenül is továbbíthatók.
A rendszer a következő alapvető terjesztési eseteket különbözteti meg [2]:

- Basic pull: A felhasználó a tartalomszolgáltatótól letölti a védett tartalmat, majd a jogszolgáltatótól megszerzi a felhasználáshoz szükséges jogokat.
- Push: két alapesete lehetséges:
  - Content push: A tartalom- és jogszolgáltatónak szerződése van a felhasználóval, és információval rendelkezik a felhasználó készülékének képességeiről, így meghatározott időnként rendszeresen küld a felhasználó készülékére védett tartalmakat a szerződésben szabályozott jogokkal együtt.
  - Push initiated pull: A tartalomszolgáltatónak szerződése van a felhasználóval, de nem rendelkezik információval a felhasználó készülékének képességeiről.
- Streaming: Ha felhasználó folyamszerűen továbbított tartalmat szeretne felhasználni (például valós idejű tévéközvetítés), akkor a továbbítás formátumával kapcsolatos speciális kérdések merülnek fel, mivel a védett tartalom nem kezelhető egyetlen kompakt csomagként. Ezek lehetséges megoldására külön kitér az ajánlás.

- Domains: Ha nem egyetlen felhasználónak, hanem felhasználók egy csoportjának szeretnénk azonos jogokat biztosítani (például munkahelyi környezetben), akkor szükség van a *domain* fogalmának bevezetésére, amely tulajdonképpen az azonos jogokkal rendelkező felhasználói csoport. Az ajánlás a domainek kezelésével is foglalkozik.
- Backup: Mivel a digitális tartalmak általában jelentős mennyiségű memóriát igényelnek, célszerű lehet különböző háttértárakra archiválni őket. Ezt a rendszer lehetővé teszi, hiszen a tartalmak önmagukban nem használhatók. Az egyes RO-k ugyanúgy tárolhatók háttértáron, amennyiben állapotmentes korlátozásokat tartalmaznak csak (például adott számú megtekintés típusú jog nem).
- Super distribution: A védett tartalmakhoz való hozzájutás lehetséges közvetlenül egy másik DRM Agent-től is, akár alternatív csatornákon keresztül is (a felhasználáshoz azonban külön kell kérni jogokat). Így a hálózatot és a tartalomszolgáltatót terhelő letöltések száma némileg csökkenthető.
- Export: A szabvány kitér a nem az OMA ajánlások alapján működő DRM rendszerekkel való együttműködés kérdéseire, és specifikálja a külső rendszerrel szemben támasztott kritériumokat.
- Unconnected Device Support: A hálózathoz nem kapcsolódó eszközöknek lehetőségük van arra, hogy védett tartalmakhoz jogokat kérjenek a jogszolgáltatótól egy olyan DRM Agent közreműködésével, amely a hálózathoz kapcsolódik. Ekkor tulajdonképpen a közvetítő DRM Agent nem a saját, hanem megbízója számára kér jogokat egy adott védett tartalom felhasználásához.

Felhasználói jogok

A rendszerben definiált jogleíró nyelv (REL) célja kettős: a tartalmakhoz kapcsolódó felhasználási módokat, és az azokhoz kapcsolódó korlátozásokat rögzíti [3], de csak a felhasználásra korlátozódik a hatásköre, a menedzsmenthez kapcsolódó jogokkal (például hol és hány példány tárolható a védett tartalomból) nem foglalkozik. Az alapvető jogok a play (lejátszás), display (megtekintés), execute (futtatás) és print (nyomtatás). Ezekhez időtartambeli és az egyes, felhasználást jelentő események számát korlátozó szabályok kapcsolhatók.

A bizalmi modell

A rendszer működése a Public Key Infrastructure-ra (PKI, nyilvános kulcsú titkosítás) épül. Minden DRM Agent-nek van saját nyilvános/titkos kulcspárja, amelyek segítségével biztosítható, hogy a kommunikációhoz szükséges üzenetek tartalma csak a feladó és a címzett számára legyen ismert.
A védett tartalmakat szimmetrikus kulccsal titkosítják (Content Encryption Key, CEK), és ilyen formában csomagolják. A kulcs ismerete nélkül a védett tartalmat nem lehet felhasználni. A DRM Agent-ek azonosítása a PKI megfelelő kulcsainak alkalmazásával történik, továbbá a DRM Agentet futtató hardver- és szoftverkörnyezetre vonatkozó információk továbbítását is magában foglalja. Az XML-ben leírt Rights Object adja meg a megadott védett tartalomhoz való jogokat, továbbá a CEK-t. A Rights Object-et a

jogszolgáltató kriptografikusan a jogokat kérő DRM Agenthez közti annak nyilvános kulcsa segítségével, továbbá az üzenetet alá is írja.
A rendszer így szerkezetileg biztonságos, mert egy adott védett tartalmat felhasználni egy adott DRM Agent segítségével csak akkor lehet, ha:

1. a felhasználó rendelkezik az adott védett tartalommal,
2. a felhasználó rendelkezik az adott védett tartalom szándékolt felhasználásához megfelelő jogokat biztosító RO-val, és
3. a jogokat a felhasználást biztosító DRM Agent számára állították ki.

Ha ezen feltételek közül bármalyik nem teljesül, akkor a védett tartalmakhoz való hozzáférés elvileg lehetetlen (gyakorlatilag a rejtjelezett tartalom visszafejtésével meg lehet próbálkozni).
Fontos kérdés továbbá, hogy a DRM Agent-ek által érzékelt idő hiteles forrásból származzon, azaz a felhasználóknak semmilyen módjuk ne legyen arra, hogy befolyásolják.

Értékelés

A bemutatott OMA ajánlás egy lehetséges megoldást kínál a digitális tartalmakhoz kapcsolódó szerzői jogok védelmének technológiai kérdéseire.
Az ajánlás legkritikusabb része a DRM Agent, amelynek implementációs részleteire az ajánlás nem tér ki. Alapvető kérdés ezzel kapcsolatban, hogy a DRM Agent-et implementáló piaci szereplő és a védett tartalmak tulajdonosai között jól működő, bizalmi viszony alakuljon ki, amelynek elengedhetetlen feltétele valamilyen törvényi szabályozás és a megfelelő szerződések megléte. Ha ugyanis a DRM Agent (vagy annak működése) manipulálható, akkor lehetőség nyílik a védett tartalmak felhasználásával való visszaélésre.
További fontos kérdés a valós felhasználók és a DRM Agent-ek összerendelésének meghatározása, amelyre szintén nem tér ki az ajánlás. Ha a felhasználó egy adott készülékén futó DRM Agent bizonyos jogokkal rendelkezik, de például hardverhiba miatt a felhasználó kénytelen a DRM Agentet egy másik berendezésen futtatni, akkor a korábbi DRM Agent számára kiállított RO az új környezetben értéktelenné válik. GSM alapú mobil telefonhálózatban az előfizetőket azonosító kártya (Subscriber Identity Module, SIM) megfelelő lehet a DRM Agent identitásának alátámasztására, de ennek pontos tisztázása alapos vizsgálatot igényel.
Lényeges továbbá, hogy a védett digitális tartalmak rejtjelezéséhez használt CEK-et úgy kell megválasztani, hogy a kitalálásához szükséges idő hosszabb legyen, mint amennyi időre védettséget kell biztosítani az adott tartalomnak, ez azonban minden további nélkül megtehető.

Irodalom

[1] JSR 118, Mobile Information Device Profile for Java 2 Micro Edition, Version 2.0, 2002. november
[2] OMA-DRM-ARCH-V2_0-20040820-C, DRM Architecture, Draft Version 2.0, 2004. augusztus

[3] OMA-DRM-REL-V2_0-20040716-C, DRM Rights Expression Language V2.0, Candidate Version 2.0, 2004. július
[4] OMA-DRM-DCF-V2_0-200400716-C, DRM Content Format V2.0, Candidate Version 2.0, 2004. július
[5] OMA-DRM-DRM-V2_0-20040617-D, DRM Specification V2.0, Draft Version 2.0, 2004 június