Multimédia védelem

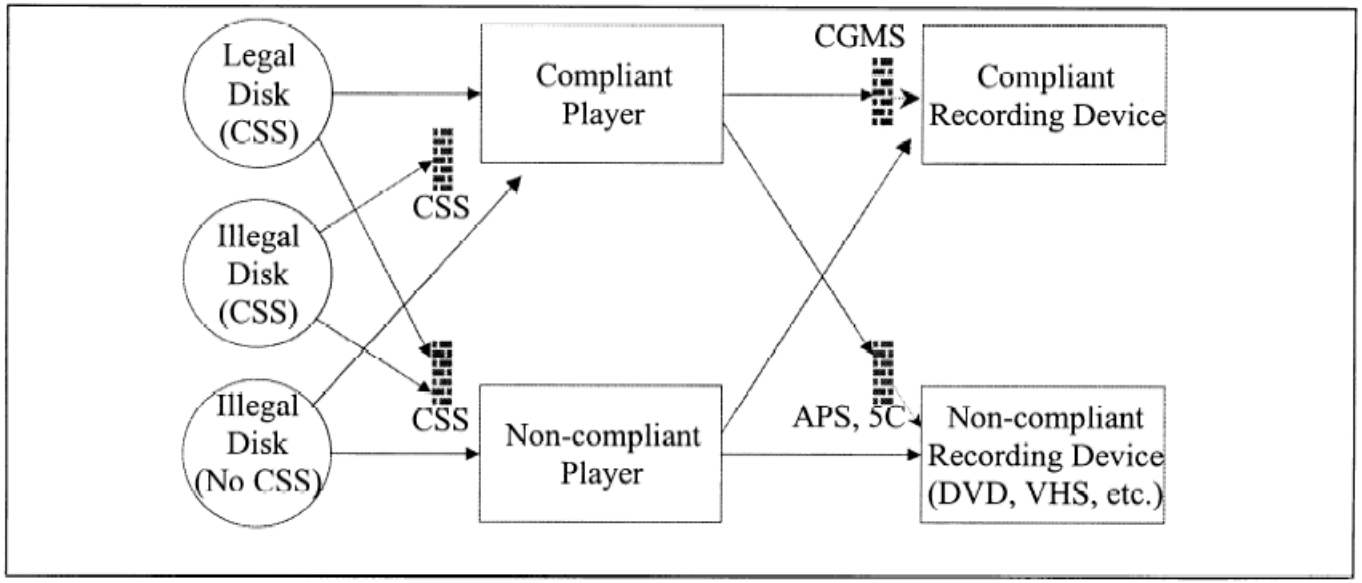
BME - TMIT
Médiabiztonság
feher.gabor@tmit.bme.hu

Tárolás védelme

DVD másolásvédelem

- Hagyományos megoldás elemei
  - CSS (Content Scrambling System)
    - Kulcsok a filmhez és a diszkhez, amit csak a megfelelő (azaz legitim) szerkezet olvas
    - Aki legitim lejátszót gyárt, annak a többi másolásvédelmi funkciót is implementálnia kell
  - APS (Analog Protection System)
    - Analóg videofelvételek készítésének megakadályozása
    - Információ az MPEG fejrészben
  - CGMS (Copy Generation Management System)
    - Másolatok számának szabályozása (0, 1, akárhány)
    - Információ az MPEG fejrészben:
      - 0,0: Copy free
      - 0,1: Undefined („No more copies”)
      - 1,0: Copy once
      - 1,1: Never copy
  - Five Company (5C) (Hitachi, Intel, Matsushita, Sony, Toshiba)
    - Titkosított információk az adatbuszon
    - Pl. Digitális TV és a lejátszó között
    - Ma már sok médiumon jelen van: USB, IP, WiFi, Bluetooth, FireWire, …

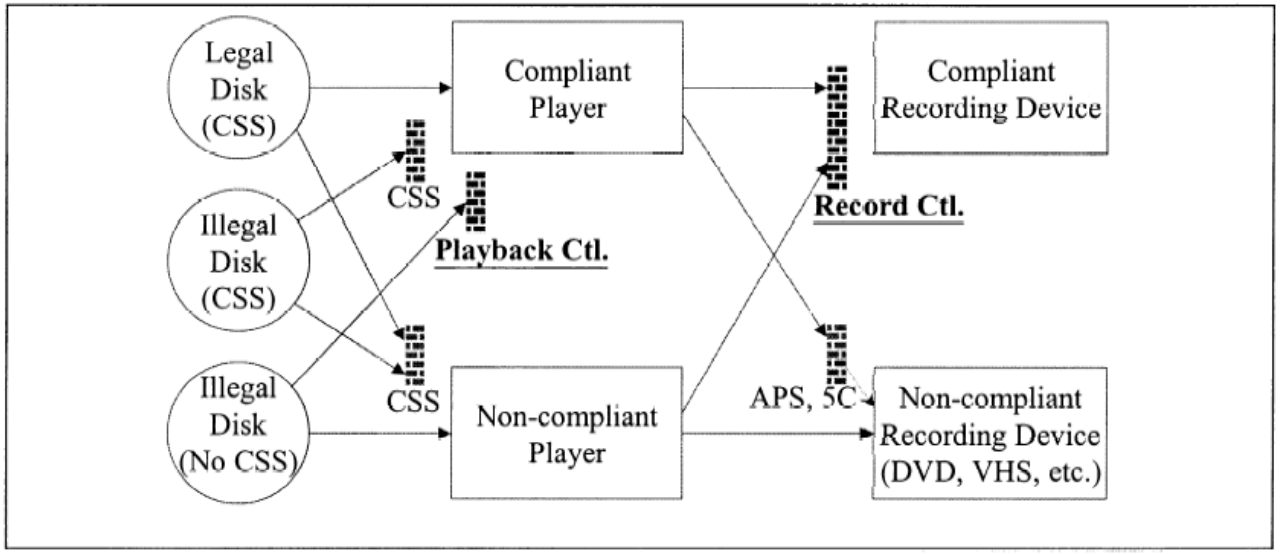
DVD másolásvédelem 2.



- Gondok
  - A legitim eszköz lejátssza az illegális másolatokat
    - Nem tudja, hogy illegális
  - A legitim eszköz újabb másolatot készíthet illegális másolatokból
    - A másolatok számára már nincs megkötés

DVD másolásvédelem 3.

- Nyilvános kulcsú vízjel használata
  - A vízjelet nem tudja törölni az illegális másolat
  - A vízjelet felismerik a legitim eszközök
    - Lejátszás, felvétel megakadályozása
  - Még nem létezik?, de tervezik
- Cél, hogy a becsületes emberek becsületesek maradjanak!



DVD védelem

- CSS – Content Scramble System (1997)
  - Valójában hozzáférés-vezérlés (jogilag lényeges!)
    - Lejátszás csak a megfelelő kulcsok segítségével
    - Kulcsok a filmstúdiók kezében
    - A DVD lejátszó feljogosítva a lejátszásra
      - Nem összeegyeztethető a nyílt forrással
- DeCSS
  - 1999 Jon Johansen (16 évesen)
    - Lejátszás Linuxon, ahol nincs feljogosított lejátszó
  - MPAA – Motion Picture Association of America
    - DeCSS üldözés (algoritmus, futó kód, leírások, linkek, …)
  - Nincs illegális másolás! (Vagy mégis?)

DVD kulcsok a lemezen

- DVD lemez
  - Régió kód – A Föld régiókra osztva, filmek külön régiónként
  - Lemez (Disc) kulcs
    - Kulcs az adott lemezhez (filmhez)
    - A kulcsok az elfogadott (409) lejátszókulccsal titkosítva
    - Ellenőrzés a lemezkulccsal titkosított lemezkulcs
  - Cím (Title) kulcs
    - A lemez tartalmának titkosítása
    - A kulcs a lemezkulccsal titkosítva
  - Szektor kulcs
    - A lemez tartalmának titkosítása
    - Kulcs a szektorok elején
    - 40 bit !!!

- A lemez és cím kulcsokat nem lehet 1:1 lemásolni, ugyanis ez a terület nem írható
  - De egy arra alkalmas író, akár írhatja is egy speciális lemezre!

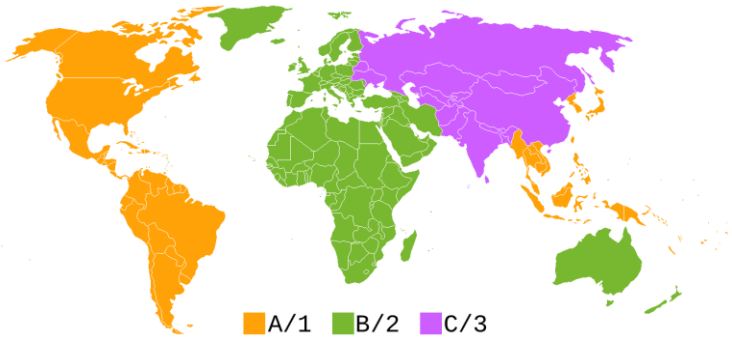
DVD kulcsok a lejátszón

- DVD játékos
  - Régió kód
    - A lejátszó régiója
  - Lejátszó kulcs
    - A lejátszó DVD lejátszásra jogosított
- PC
  - Régió kód (a DVD olvasóban)
  - Kapcsolat kulcs
    - adatátvitel a DVD olvasó és a SW között
  - Lejátszó kulcs
    - A lejátszó SW DVD lejátszásra jogosított

DVD régiókód

- 6 régiókód
  - 1 - USA, Canada
  - 2 - Japan, Europe, South Africa, Middle East, Greenland
  - 3 - S.Korea, Taiwan, Hong Kong, Parts of South East Asia
  - 4 - Australia, New Zealand, Latin America + Mexico
  - 5 - Eastern Europe, Russia, India, Africa
  - 6 - China
  - 0 or REGION ALL
- Első bemutatás meghatározása
- Megbukott? - Világpremier

- Blu-ray régiók



- ~70% a mai lemezeknek régió független

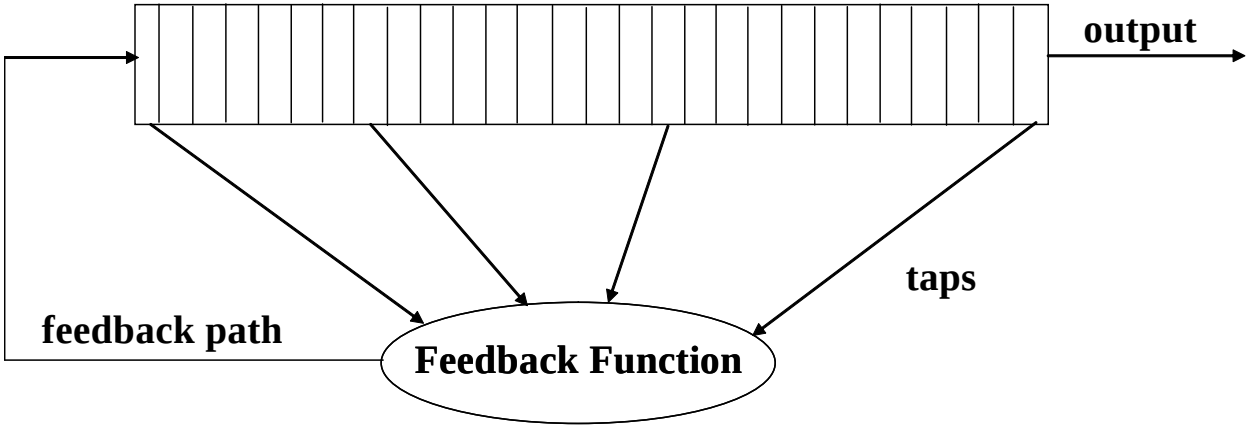
DVD egyeztetés

1. Kölcsönös azonosítás (PC)
   - Kihívás alapú azonosítás
   - Megegyezés a viszonykulcsban
   - További adatforgalom titkosítása a viszonykulccsal
2. Lemezkulcs megtalálása
   - A lejátszó kulcs(ok) próbája
3. Lemezkulcs, és a címkulcs begyűjtése
4. Adatátvitel szektoronként
   - A szektorok kikódolásához szükséges a címkulcs és a szektorkulcs

Álvéletlen sorozat

- Egyszerű kezelés
  - Adat XOR álvéletlen -> titkosított
  - Titkosított XOR álvéletlen -> Adat
- Egyszerű megvalósítása: LFSR
  - Linear Feedback Shift Register
    - Inicializálás után álvéletlen sorozat léptetéssel

LFSR

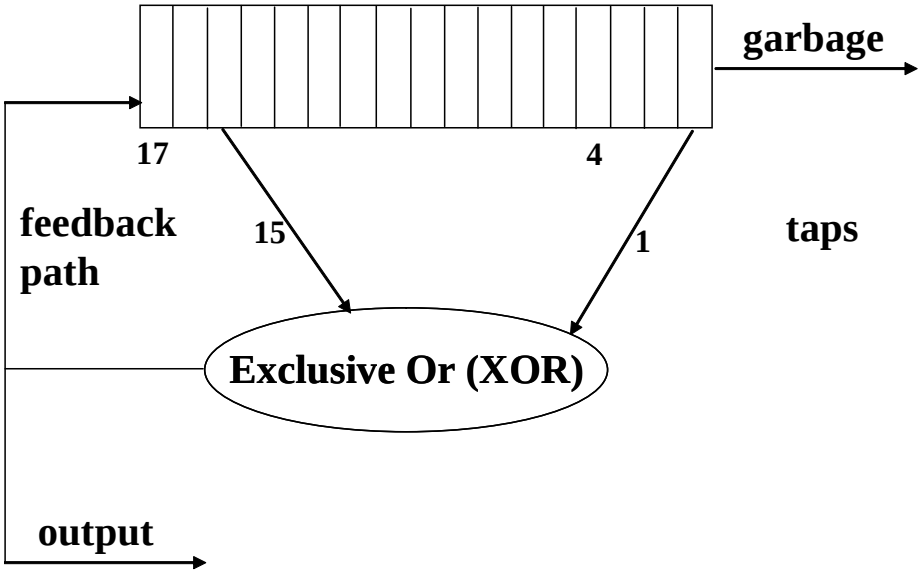


- Inicializálás
- Pár helyérték visszacsatolása

- Csak álvéletlen, sőt periodikus!
- A periódus függ a helyértékek számától és a konfigurációtól
- Gyakran kombinálják más elemekkel (összeadás, szorzás, …)

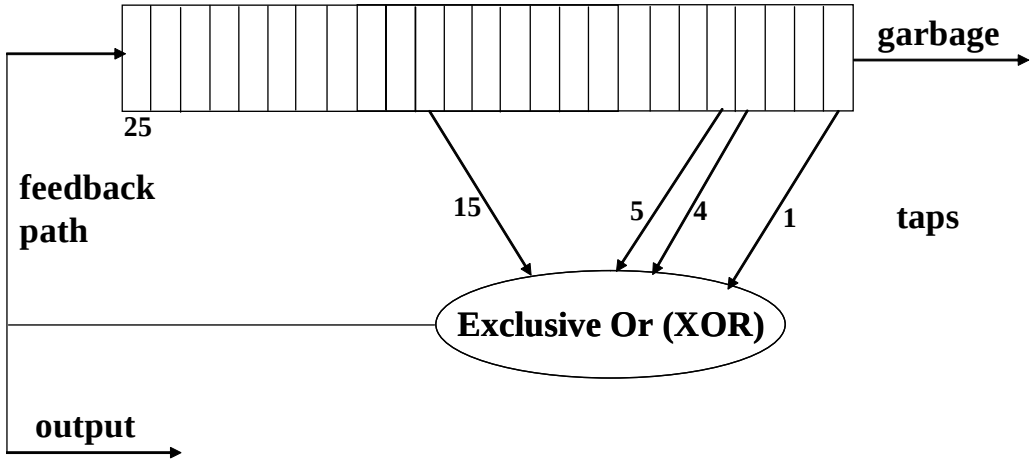
A CSS LFSR 1.

- LFSR-17
  - 2 bájt a kulcsból
  - A 4. helyértékre 1 (Ne lehessen csak 0)
  - Visszacsatolás:
    - XOR
    - 1 és 15 helyérték
  - Kimenet a visszacsatoláson

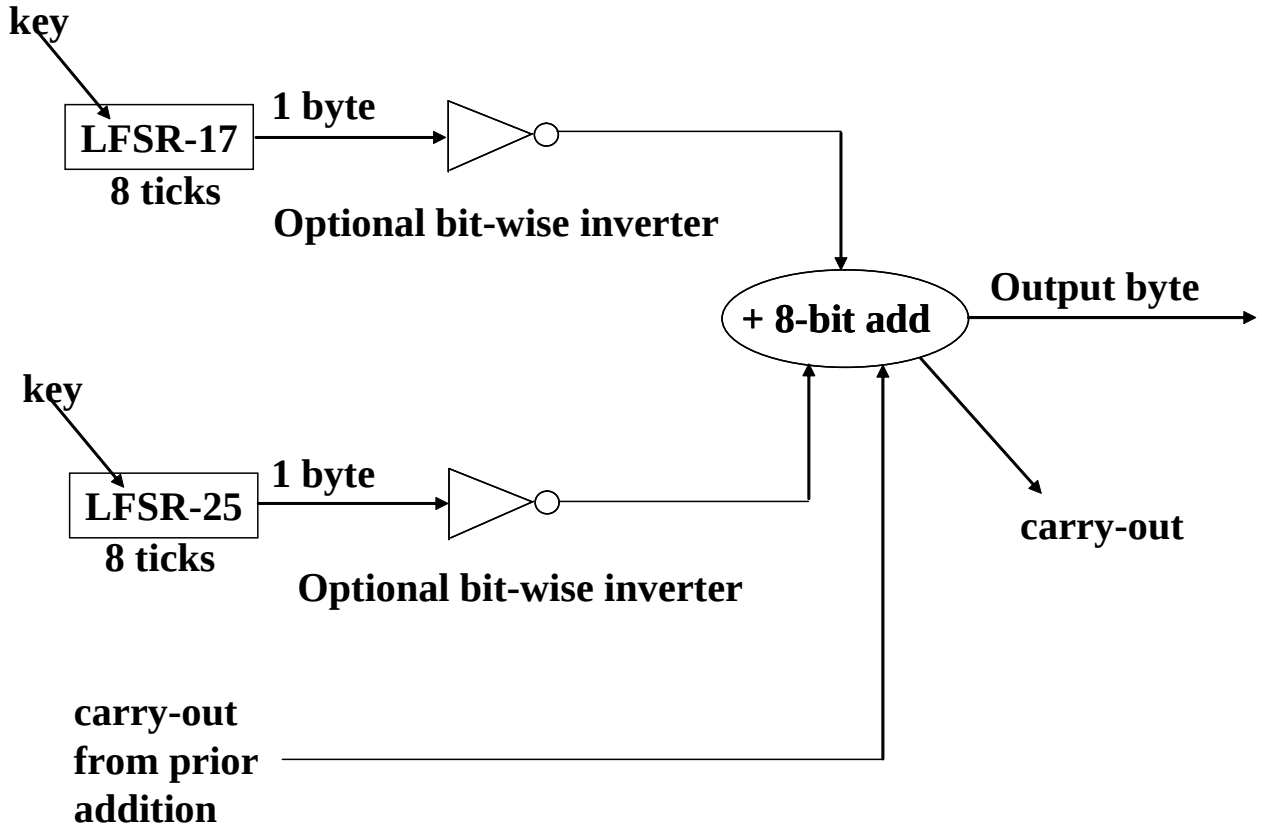


CSS LFSR 2.

- LFSR-25
  - 3 bájt a kulcsból
  - A 4. helyértékre 1
  - Visszacsatolás:
    - XOR
    - 1, 4, 5 és 15 helyértékek
  - Kimenet a visszacsatoláson

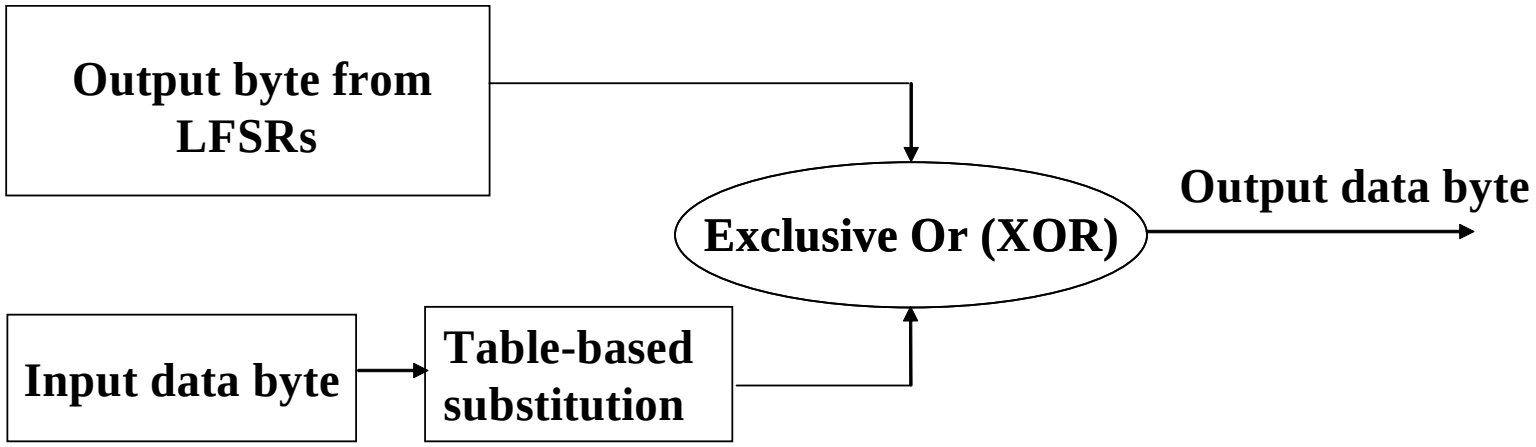


CSS extrák



- Bitek invertálása változik a kulcs típusától függően
  - Szektorkulcs esetén csak LFSR-17 esetén

Szektor dekódolása



- Kulcsok:
  - LFSR-17: Címkulcs 0,1 és a szektor 80,81 bájt
  - LFSR-25: Címkulcs 2,3,4 és szektor 82,83,84 bájt

CSS problémák

- Kulcsméret
  - A 2^{40} ma már nem túl nagy szám
  - Muszáj a kicsi méret (export tilalom)
- Törések
  - Különböző megközelítések
    - 2^{16} ,2^{25} ,2^{8} ha ismert a kódolatlan adat is
  - Mindenki nézze meg maga ☺

DVD és vízjelek

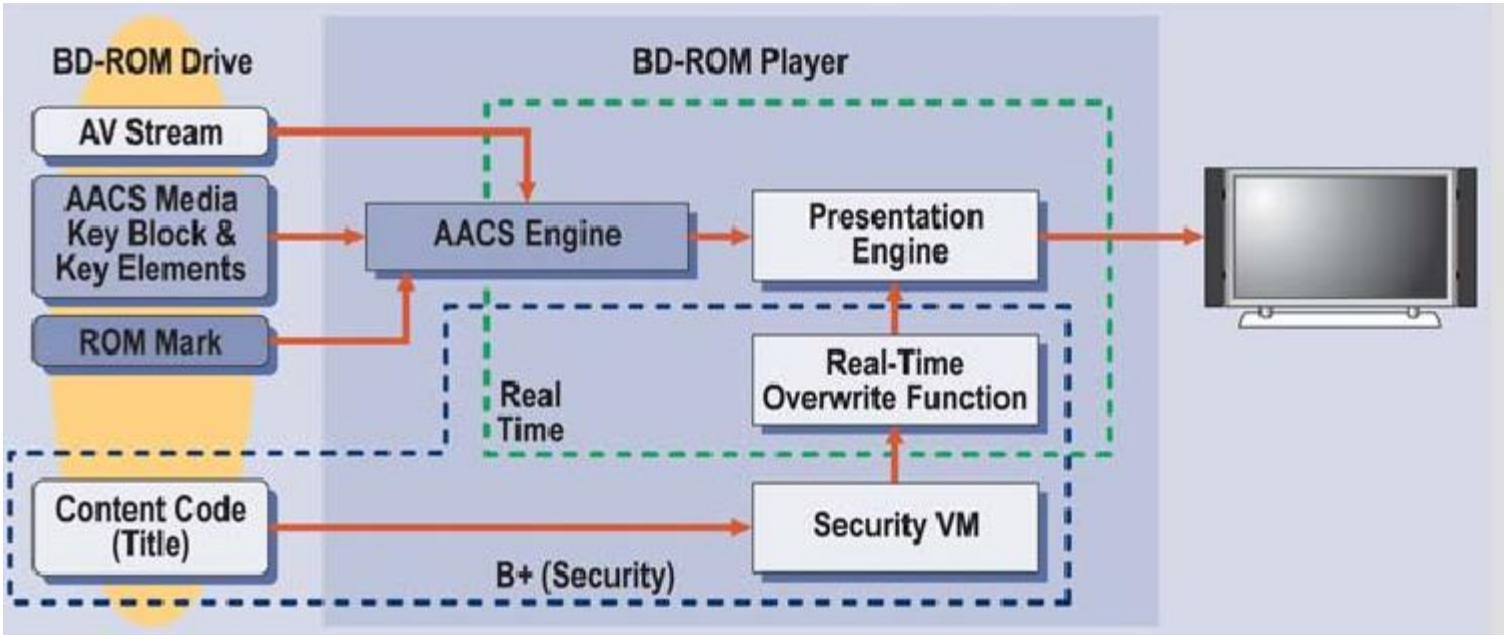
- Két csoport (1999-)
  - Millennium: DigiMarc, Macrovision és Philips
    - Robusztus
    - Biztonságos
  - Galaxy: IBM, NEC, Hitachi, Pioneer és SONY
    - Robosztus
      - DA, MPEG2 konverziót túléli
      - Különböző transzformációk
    - Biztonságos
      - 10s alatt 10^{-12} –nél kisebb hibás detektálás
- Nincs használatban!

Blu-ray and HD-DVD tartalom védelme

- 2005: AACS (Advanced Access Content System) (http://www.aacsla.com)
  - Lejátszásban résztvevő eszközök hitelesítése
  - Tartalom titkosítás
  - AACS LA (lincenszelés): Disney, Warner, Microsoft, Panasonic, IBM, Toshiba, Sony
- ROM Mark
  - Fizikai védelem titkos adatoknak
- BD+ (ez újdonság a DVD védelemhez képest)
  - Kód futtatás, biztonsági alkalmazások frissítése, felülírása

Blu-ray and HD-DVD tartalom védelme

- AACS + ROM Mark + BD+



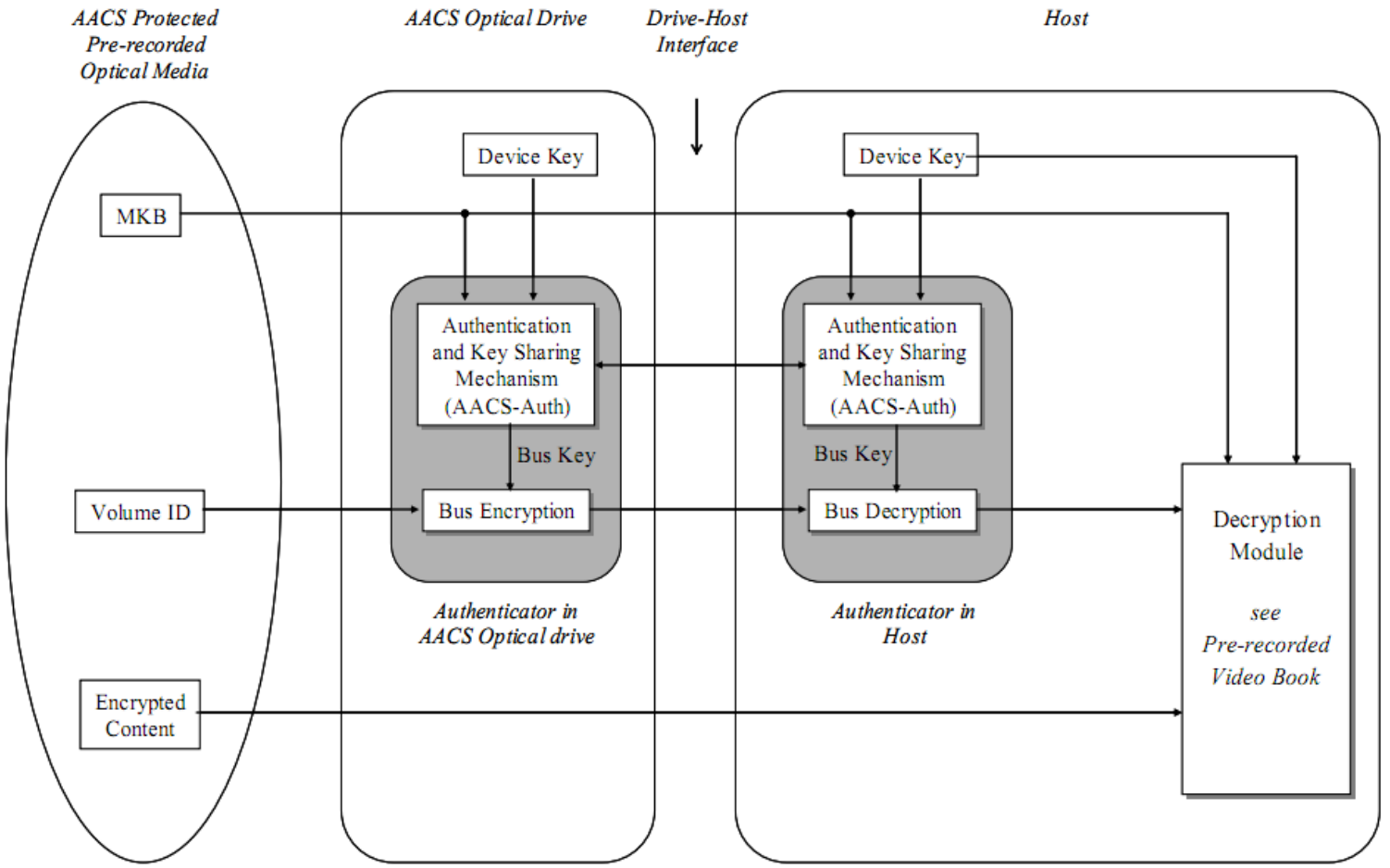
AACS - tartalom

- Tartalom titkosítás
  - AES 128 bites kulcsok, AES-CBC
  - A kulcsok a Media Key Block (MKB) –ból származnak + ROM Mark
    - Hierarchikusan tartalmazza a kulcsait a létező lejátszóknak (márka és modell)
    - Ha egy lejátszó kompromittálódik, akkor az letiltható, egy újabb MKB esetén már le lesz tiltva
    - Sikeres kikódolás esetén megkapjuk a cím kulcsot (Title key)
  - A tartalomból több féle kulcs szerinti verzió is lehet egy lemezen
    - A különböző verziók különböző vízjeleket tartalmazhatnak. Ennek segítségével lenyomozható a kiszivárgott kulcs

AACS - adatbusz

- PC esetén a BD-ROM és a szoftver közötti út (SATA, PATA, USB)
  - Készülékek, szoftverek azonosítása. Kölcsönös kihívás-válasz módszer
  - Lista a letiltott elemekről. A lista frissülhet az újabb lemezekkel

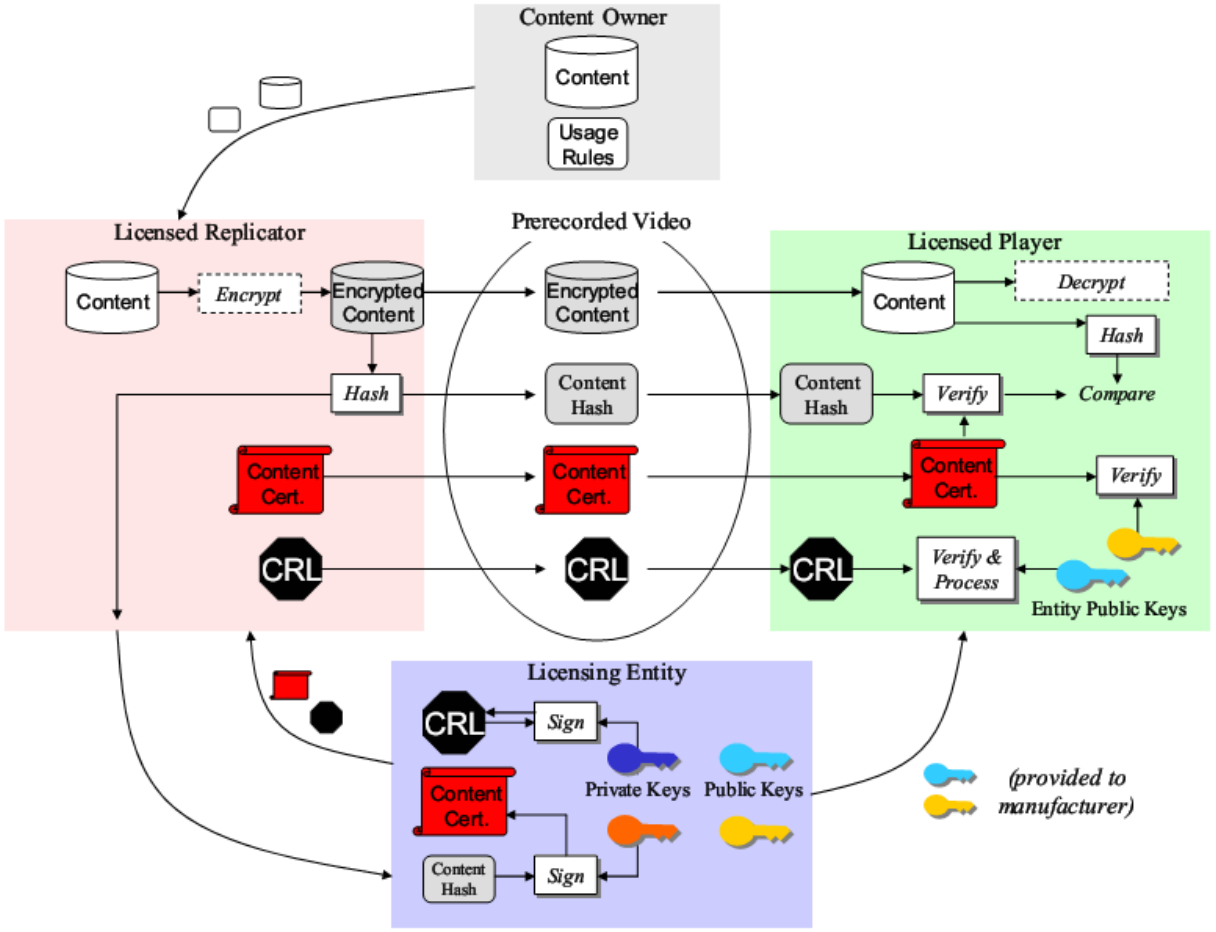
AACS – adatbusz 2.



AACS – Analóg kimenet védelme

- Hang vízjelezése
  - Cinavia - Verance algoritmus (2009)
  - „Mozi” és „házi” vízjelek. Ha a lejátszó mozi vízjelet hall vagy nem hall vízjelet, akkor megáll a lejátszás/elnémul
- Analóg formátum vége (analog sunset)
  - 2011.01.01 –től csak SD formátumhoz mehet analóg videó interfész
  - 2014.01.01 –től nincs analóg formátum! (nem árusítható)
- Felbontás visszafogása (Image Constraint Token)
  - A stúdió dönthet, hogy milyen képfelbontást enged meg, dönthet csak SD felbontásban analóg interfész esetén
- Csak digitális interfész (Digital-Only Token)
  - A stúdió dönthet úgy, hogy nem engedélyezi az analóg kimenetet

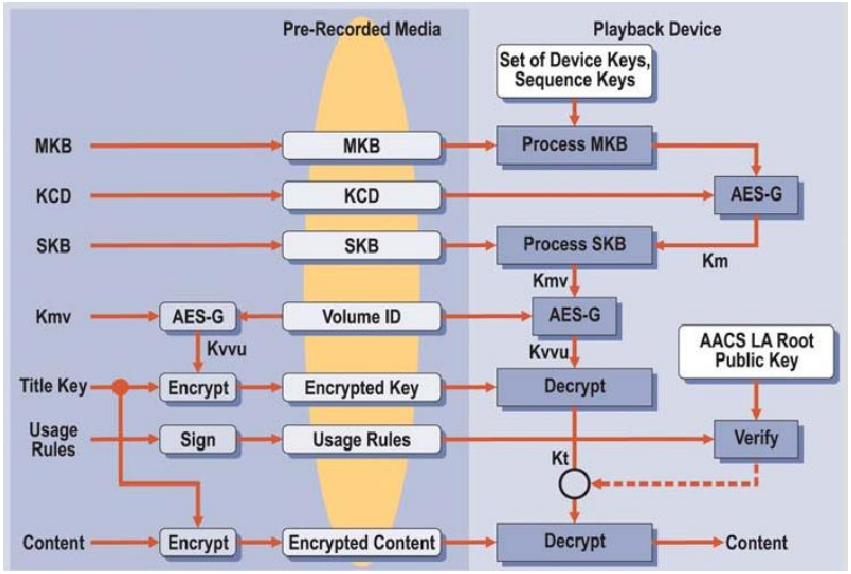
AACS – Tartalom ellenőrzés



ROM Mark

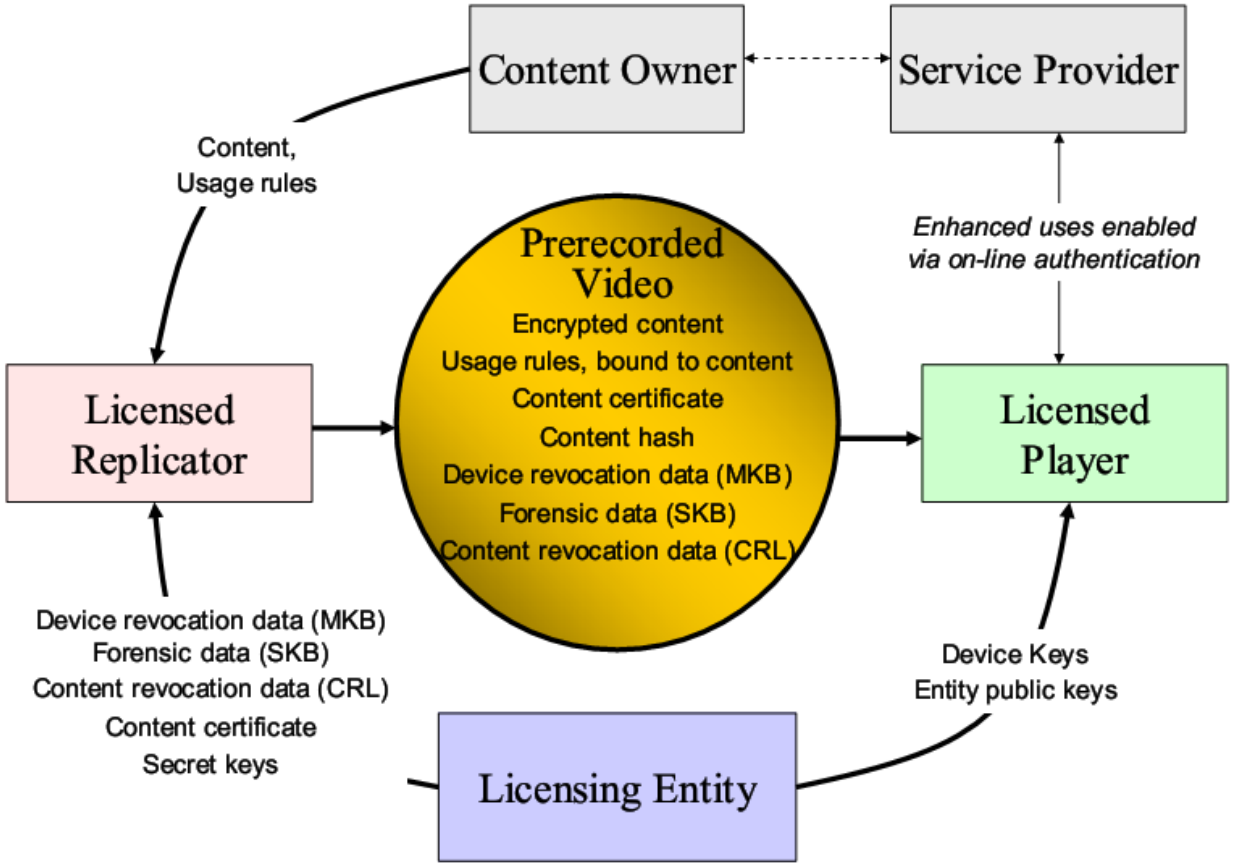
- Adatok a lemezek írhatatlan részén
  - Volume ID
  - Másolással nem lehet átvinni a másik lemezre
  - 128 bites kulcs
- A kiolvasást nem kezdeményezheti más szoftver
  - Az olvasáshoz AACS LA által aláírt tanúsítvány szükséges

AACS és ROM Mark



- MKB – Media Key Block
- KCD – Key Conversation Data (KCD Mark)
- SKB – Sequence Key Block – Lejátszó azonosítása (opcionális)
- Volume ID – Kötet azonosító (ROM Mark)
- Km – Media Key
- Kmv – Media Key Variant
- Kvvu – Volume Variant Unique Key
- Kt – Title Key

AACS rendszer

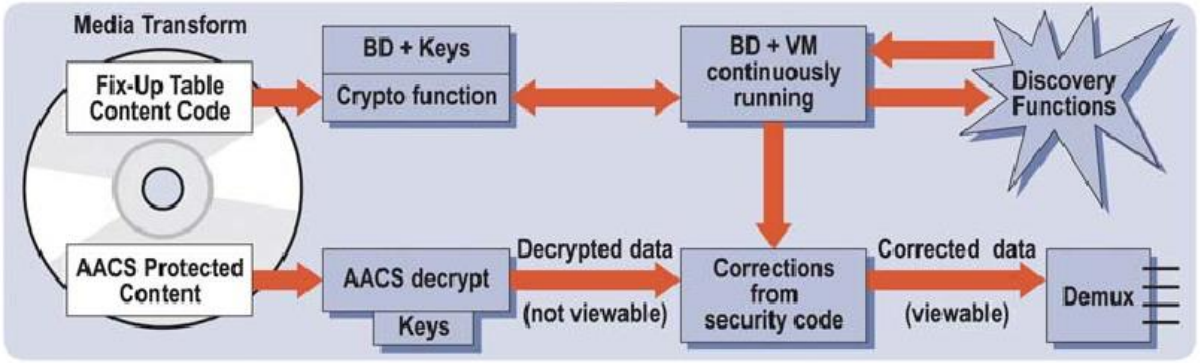


Managed copy

- A felhasználó legális másolása
  - Másolat példány, hordozható lejátszó, házimozi szerver
- Nem került bele az „előzetes” AACS szabványba, így a lejátszók többsége nem ismeri
  - 2009-től része a szabványnak

BD+

- AACS és ROM Mark független
  - Plusz biztonság
- Virtuális gép
  - Lejátszó környezet biztonsági ellenőrzése
    - A gyártó elküldi a lejátszó memória lenyomatát
  - Tartalom specifikus kód a lemezről (Phase 1)
    - Javítások a kikódolt részben: Media Transform
    - Hitelesített kód
    - A kód nem permanens



BD+ Phase 2 &3

- Phase 2
  - Ha ismert, hogy a lejátszó fel van törve, akkor olyan tartalom specifikus kód is lehet, ami megszünteti a sebezhetőséget (lejátszó specifikus tartalom specifikus kód)
- Phase 3
  - VM kód helyett natív kód a fenyegetettség eltávolítására

- Mindkét esetben cél, hogy a lejátszót ne kelljen kivonni a forgalomból a törések miatt!

High-Bandwidth Digital Content Protection

- HDCP (High-Bandwidth Digital Content Protection) 2.0 (Intel - http://www.digital-cp.com/)
  - Lejátszó azonosítása HDCP licenc alapján
  - A tartalom védelme a forrástól a kijelzőig
    - DVI (Digital Visual Interface) vagy HDMI (High-Definition Multimedia Interface) interfészek
    - + DisplayPort, GVIF, DLI, UDI, IP, WHDI, TCP/IP, USB
  - Forrás (source), átjátszó (repeater), kijelző (sink)
    - Pl.: BR lejátszó, Videó felevevő, HDTV
    - Fa struktúra (max. 4 szint és 32 eszköz)
  - A lejátszó hitelesítése és tartalom titkosítása

Hitelesítés, lejátszás titkosítás

- HDCP 2.0
  - Egyedi 1024 bit RSA kulcsos tanúsítványok a lejátszó egységeknek. 40 bites lejátszó azonosító. Tanúsító a DCP ICC
  - 3072 bites RSA kulcs a CA-nak (DCP LLC)
  - 128 bites AES-CTR védelem a média tartalomnak (tömörített vagy tömörítetlen)
    - Jól párhuzamosítható és előre számolható
  - Készülék párosítás
    - A lejátszó tanúsítványának ellenőrzése. Lokalitás ellenőrzés. Kulcs küldése a lejátszónak. Ha a párosított készülék átjátszó, akkor a fa mélységének és számosságának ellenőrzése is megtörténik
    - A lejátszók egyedi azonosítója alapján a készülékek letilthatóak
  - Lokalitás ellenőrzés
    - A küldött üzenetekre kapott válaszoknak egy adott időn belül vissza kell érkeznie (RTT ellenőrzés)

Audio CD védelme

Audio CD védelme

- Kompatibilitás!
  - CD lejátszót nagyon rég gyártanak
    - DVD Audio esetén már van beépített másolás védelem
  - Philips: Ami nem szabványos, az nem CD!
- Megveszem a zenét
  - MP3 lejátszók támogatása?
- Másolásvédelem hatásai
  - Gyorsabb öregedés?
  - Tönkrement hi-fi rendszer?

SafeAudio

- Macrovision
- Hang CD-k védelme
  - Másolásvédelem! (ripping)
  - A lejátszás hibátlan (PCn is)
- Technológia
  - Az adatok hibásan vannak a lemezen tárolva (mintha karcolások lennének)
  - A hibákat egy lejátszó könnyen kijavítja
  - Másolásnál a hibákat mindenáron jól olvassák, eredménye kattanások, ugrások a zenében

Cactus Data Shield

- Macrovision (Midbar)
- 3 különböző fajta
  - CDS100 – Csak CD lejátszón
  - CDS200 – CD lejátszó, PC
  - CDS300 – CD lejátszó, PC + vízjelek?
- Technológia
  - A 2. session tárolja a tömörített adatokat a PC lejátszáshoz + lejátszó SW
  - Egyben összezavarja az első session adatait is…
  - Esetlegesen további védelem:
    - Hibák a lemezen
    - Hibás az eredeti TOC is

Software CD védelme

SafeDisc

- Macrovision (C-Dilla)
- Technológia
  - Hármas védelem
    - Azonosító ujjlenyomat
    - Titkosítás
    - Anti-hacking szoftver
  - Hibás fájlok (~10000 hiba)
- Sebezhetőség
  - Bizonyos írók képesek másolni (Philips)

LaserLock

- Technológia
  - LASERLOK rejtett könyvtár hibás fájlokkal (10-20 MB)
    - A hibák akár szemmel is láthatóak 3-5 mm
    - A hibás fájlokat lehetetlen másolni
    - Ezeket a fájlokat az alkalmazás ellenőrizheti
    - „Az alkalmazást nem lehet feltörni”
- Sebezhetőség
  - Mégis lehet másolni..
  - Mégis fel lehet törni..

SecuROM

- SONY
- Technológia
  - Bizonyos fájlokat a lemez nem másolható területeire helyeznek el
  - Az alkalmazás futtatásakor a másolhatatlan fájlok tartalmát/pozícióját visszaellenőrzik

További CD védelmek

- Túlméretezett CDk
  - Több adatot írnak fel, mint amennyit másolni lehet
  - Ma már nem hatásos
- Hamis TOC bejegyzés
  - Nem valódiak a fájlbejegyzések (dummy fájlok)
  - Nem hatásos, felül lehet bírálni 1:1 másolás
- Fájlelérés mérések az eredeti CDn (CD-Cops)
  - Az elérési idő egy access kód, ami azonosítja a CDt
- Speciális ujjlenyomat, amit CD íróval nem lehet írni

CD védelem sebezhetőség

- CD másolása
  - Több író képes megbirkózni a hibákkal is
    - Nagyon hosszú másolási idő
- Alkalmazás módosítása
  - A védelmek jól ismertek, visszafejthetőek
    - A legtöbb alkalmazásban visszafejtés elleni védelem
    - Általános patch -ek
    - Védelem emuláció (DAEMON Tools)

CloneCD – Házi CD másolat

- SafeDisc old
- SafeDisc v2.0
- SecuROM old
- SecuROM *new*
- CD-Cops
- Discguard
- LaserLok
- Psx/Lybcrypt
- Cactus Data Shield (Audio CDs)
- Lock Blocks
- CD Check
- ProtectetCD-VOB
- CD-Extra
- Bad read errors
- Dummyfiles
- Illegal TOC
- overlength of CDs
- Tracks < 4sec.

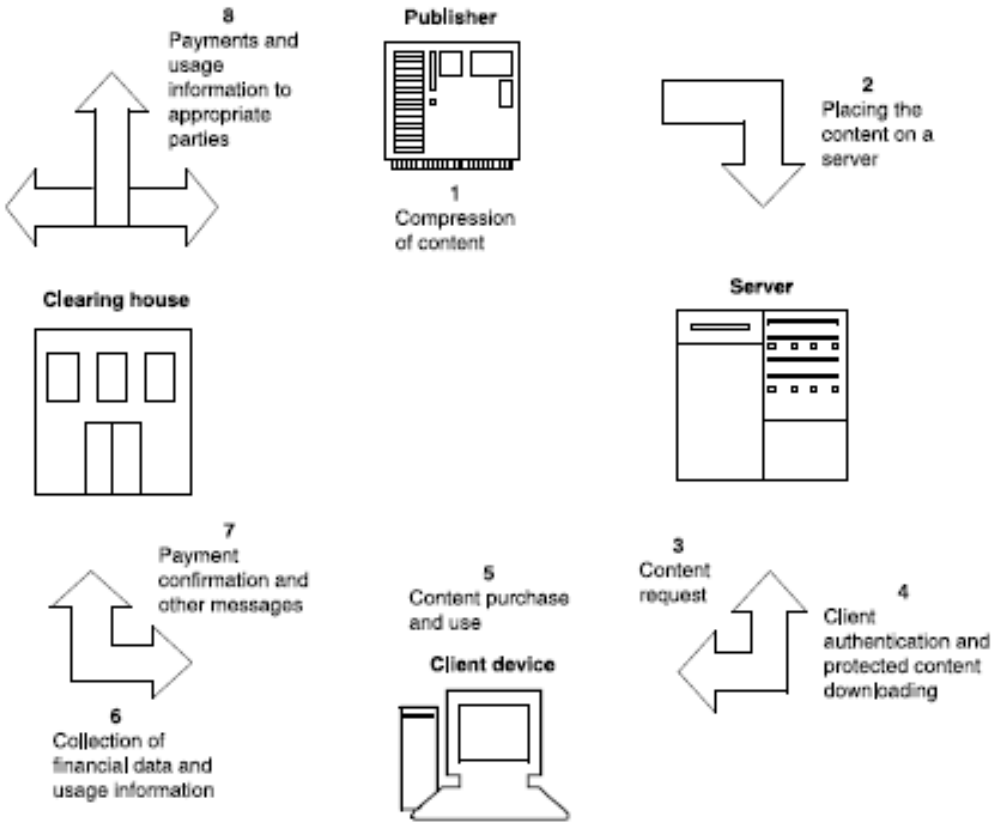
SW védelem - Dongle

- Nem médiához kötött
- HW kulcs
  - USB / soros port / párhuzamos port
  - Egyedi azonosító
    - Előre fel kell programozni (lehet tartományt is)
  - Nehéz feltörni az algoritmust
  - Sokszor változtatható adatokkal

DRM

Digital Rights Management DRM

- 1. A kiadó titkosítja a tartalmat
- 2. A tartalmat egy web szerverre helyezik
- 3. A felhasználó kéri a tartalmat
- 4. A felhasználó letölti a tartalmat és megszerzi a kulcsot hozzá
- 5. A felhasználó a szabályoknak megfelelően használja a tartalmat
- 6. Időnként kiszámlázzák a tartalmat
- 7. A felhasználó számlát kap
- 8. A felhasználók által fizetett összeg szétosztásra kerül



DRM

- Titkosítás
  - Titkos kulcs
- Digitális vízjelezés
  - Az elrejtett információ lehet a tartalom tulajdonosának valamilyen azonosítója, vagy a tartalmat letöltő felhasználó azonosítója.
- Jogleíró nyelv
  - A felhasználó számára biztosított jogokat és megkötéseket
  - ODRL (Open Digital Rights Language).
- Kommunikációs protokollok

- Eszközök, amik betartatják a szabályokat

OMA DRM

- Open Mobile Alliance (2002)
  - Mobil eszköz és rendszergyártók
    - Ericsson, Thomson, Siemens, Nokia, Philips, Motorola, Texas Instruments, ...
  - Mobil szolgáltatók
    - Vodafone, T-Mobile, Orange, Telefónica, ...
  - Szoftverforgalmazók
    - Microsoft, IBM, Oracle, ...
  - Tartalomszolgáltatók
    - Time Warner, Yahoo, ...

OMA DRM 1.0

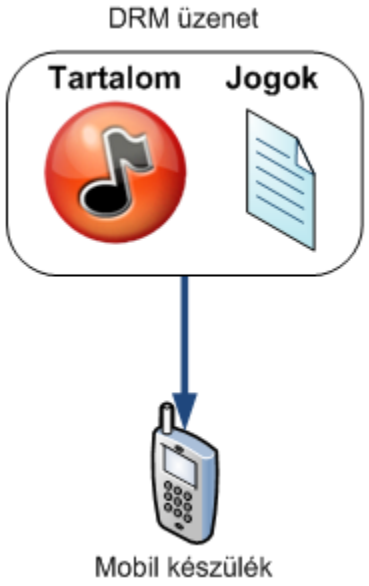
- OMA DRM 1.0 (2004)
  - Jogosultság leírás XML fájlban
  - DRM agent – a készüléken futó ügynök
  - DRM message – Digitális tartalom
    - Leginkább csengőhang, logo, háttérkép, játék

Forward Lock / Tiltott továbbítás

- A felhasználó letölt a készülékére egy média objektumot 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 ő gondoskodik arról, hogy csak olyan alkalmazás érje el a tartalmat, amely megbízható

Combined Delivery / Kombinált letöltés

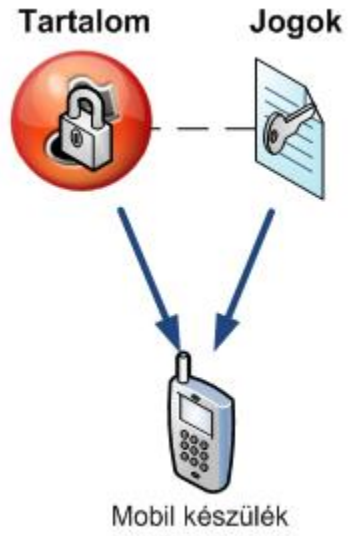
- A letöltött DRM üzenet: média + jogosultság objektumok
- A jogosultság határozza meg, hogy a felhasználó miként használhatja a média objektumot
  - Pl: preview funkció
- A jogosultság leírása a Right Expression Language (REL) segítségével történik
  - Egyszerű, eljárások és kényszerek minimális halmazát tartalmazza
  - Funkciók: Lejátszás, megjelenítés, végrehajtás és nyomtatás
  - Kényszerek a funkciókat limitálják, tehetik ezt darabszámra, meghatározott időpontok között vagy meghatározott időintervallumra.
- A tartalom továbbítására nincs lehetőség



Separate Delivery / Szétválasztott letöltés

- A média objektum és a jogosultság objektum külön akár különböző csatornán, különböző időben, különböző szerverről érkezik
- A média objektum egészen addig nem használható, amíg a hozzá tartozó jogosultság objektum nem áll rendelkezésre

- Lehetővé teszi a tartalmak továbbítását más készülékekre. A média objektum továbbítása után a céleszköznek is be kell szereznie a tartalomhoz tartozó jogosultságokat, különben a DRM ügynöke nem fogja engedélyezni a tartalom használatát



Streaming

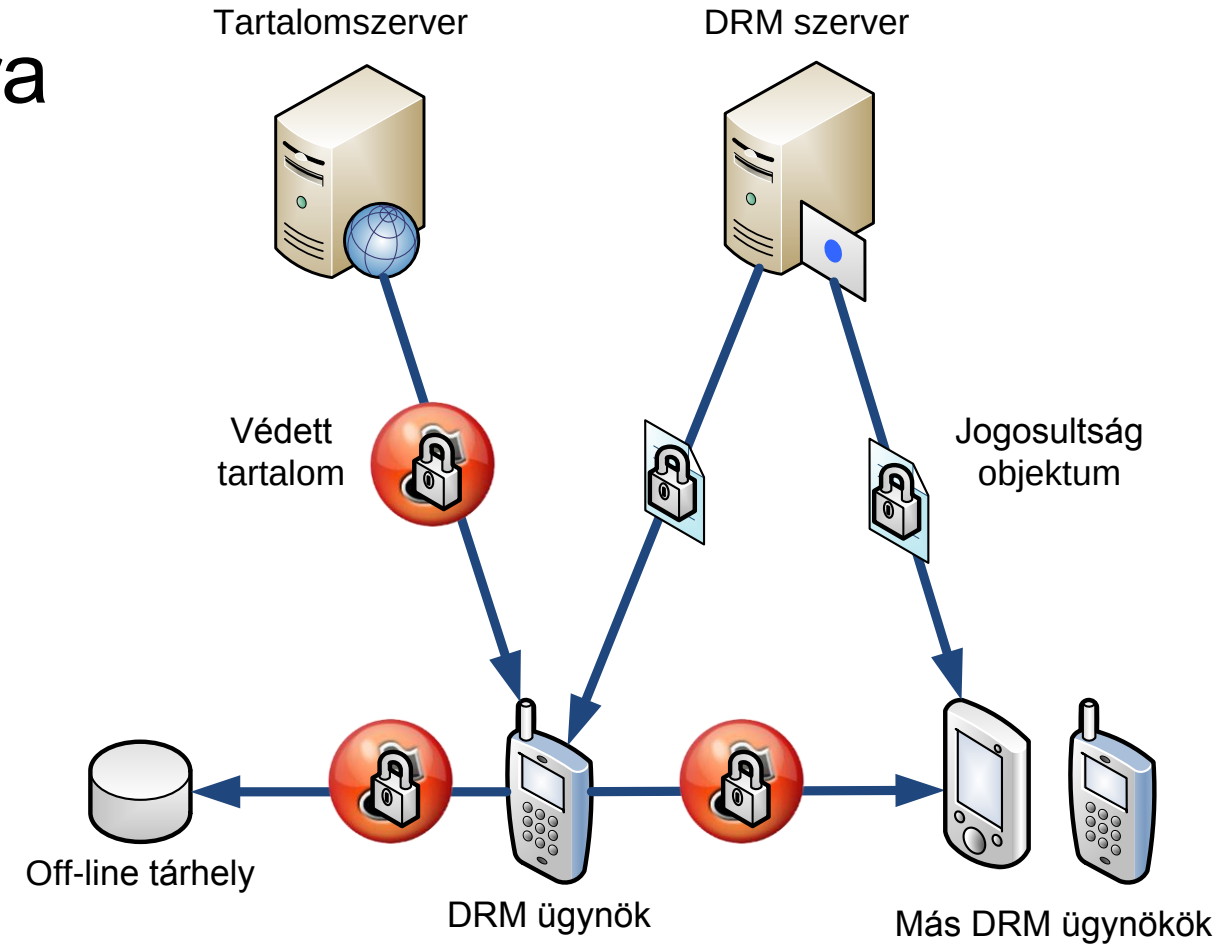
- OMA DRM 1.0 –ban nincs kifejezetten streaming lehetőség
  - A DRM üzenet tartalmazhatja az SDP-t, illetve a stream-re mutató URL-t
    - Az SDP titkosító kulcsot is tartalmazhat
  - A lejátszó nem mentheti el a tartalmat

OMA DRM 2.0

- OMA DRM 2.0 (2006) / 2.0.1 (2008)
  - Az új verzióban kizárólag a szétválasztott letöltés használható, mégis több funkcionalitás
    - 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

OMA DRM 2.0

- Architektúra



OMA DRM biztonság

- Tartalom csomagolása
  - A tartalomszolgáltató egy biztonságos konténerbe (DRM Content Format - DCF) csomagolja a média objektumot
  - A DRM tartalmat egy szimmetrikus tartalomtikosító kulcs (Content Encryption Key - CEK) segítségével rejtjelezi
  - A CEK-t a jogosultág objektum tartlamazza

- DRM ügynök hitelesítése
  - Minden DRM ügynök rendelkezik egy publikus / privát kulcspárral és egy tanúsítvánnyal. A tanúsítvány kiegészítő információkat tartalmaz, mint a gyártó, a készülék típusa stb.
  - A kulcsok a tartalom- és a jogosultság szolgáltató képes hitelesíteni az ügynököt
  - A jogosultság titkosítása a DRM ügynök publikus kulcsával

OMA DRM 2.1

- Új funkciók
  - Mérések támogatása
    - A jogosultság kibocsátójának szüksége lehet információra a különböző tartalmak felhasználásairól
  - Jogosultság feltöltése
    - Lehetőség van a jogosultság objektumot a DRM szolgáltatóhoz feltölteni. Erre akkor lehet szükség, ha a felhasználó át akarja mozgatni a jogosultság objektumot egyik készülékről a másikra
  - Megerősítés a jogosultság objektum telepítéséről
    - A DRM ügynök megerősítő üzenetet küld a DRM szervernek a jogosultság objektum telepítése után.

„Más” DRM megoldások

- Microsoft Windows Media DRM
- RealNetworks - Media Commerce Suite
- Marlin DRM
  - Intertrust, Panasonic, Philips, Samsung, Sony
- Apple FairPlay
- SUN DReaM (DRM/everywhere available)

- … vagy DRM nélkül…