A hozzáférés-korlátozott DVB CATV műsorterjesztés alapjai

WEIN TIBOR, műszaki menedzser

HFC Technics Kft.
t.wein@hfctechnics.hu

Kulcsszavak: interaktív fizető tévézés, titkosítási megoldások, kódolás

A többségben hozzáférés-korlátozott műsortartalmak terjesztése, és ennek elektronikai/informatikai infrastruktúrája csak a digitális műsorszórás rendszerébe integráltan valósítható meg. A digitális technika a műsorkínálat nagyságrendi felduzzadását, valamint az interaktív televíziózás műszaki lehetőségeit is magával hozta. Ez a járulékos információs szolgáltatások iránti igényt is felveti. A cikk a vezetékes DVB-be integrált fizető TV alapszolgáltatások rendszertechnikai megoldásait ismerteti.

1. Bevezető

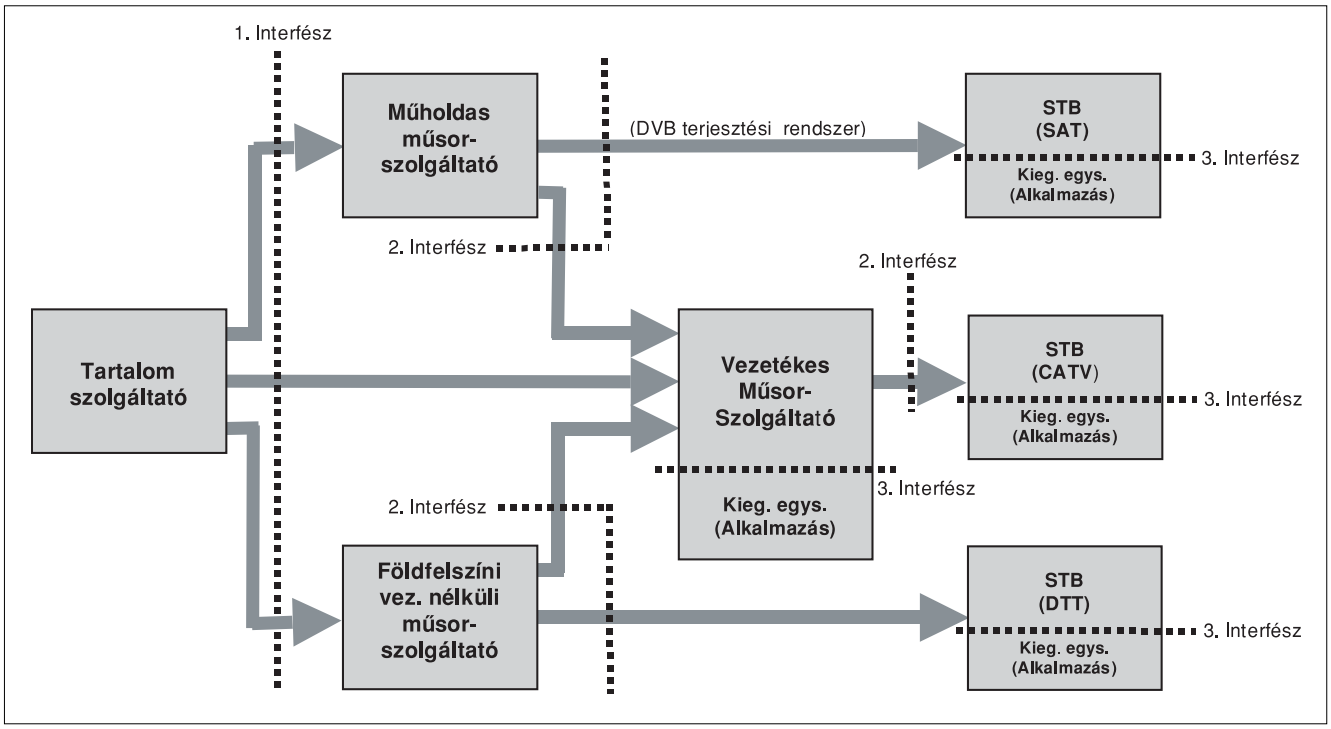
A műsorszórásban és -elosztásban alkalmazott hozzáférés-korlátozás a szerzői jog védelmét jelenti. A hozzáférés-korlátozás infrastruktúrájának megjelenése és elterjedése a felhasználói oldal szempontjából, jóllehet, népszerűtlen, ám elkerülhetetlen folyamat. A vállalkozási alapú műsortartalom előállítás és terjesztés költségeinek megtérülése és kezelése ma már csak hatékonyan működő üzleti modellekre épülhet. Az adminisztratív alapú, közvetett díjbeszedési rendszerek az információs társadalom korában túlhaladottak, a fizetési fegyelem fenntartásának eszközeként egyre hatástalanabbak. Az interaktív fizető tévézés, mint szolgáltatási üzletág kiépítése és működtetése természetesen megfelelő szabályzást igényel.

2. Az átviteli modell

Az *1. ábra* a digitális TV átviteli modelljét szemlélteti. Mint az ábrán látható, a digitális TV átvitel a tartalomszolgáltatók és -terjesztők, valamint a terjesztők és felhasználók közti hagyományos csatlakozási felületek (1. és 2. interfész) mellett egy továbbit (3. interfész) is definiál. Ennek rendeltetése a járulékos alkalmazásokkal kapcsolatos adatok leválasztása az átviteli rendszeren továbbított DVB jelfolyamról. Az átviteli lánc és az alkalmazás közé iktatott 3. interfész az API, a DVB vevőberendezés és a járulékos alkalmazásokat megvalósító kiegészítő egység(ek) csatlakozási pontja.

Az interaktív műsorterjesztés fejlődése folyamán a visszirányú átvitel igénye az 1. és 2. interfészeket is API funkciókkal ruházza fel. (Az ábrán látható átviteli modell

1. ábra A digitális TV átvitel modellje



Fogalmak, meghatározások

API	Applications Programing Interface	Szabványosítás alatt álló átjárás a DVB és az MHP alatt futó alkalmazások között
ASI	Asynchronous Serial Interface	Alapsávi DVB jelfolyamok szabványos csatlakozási felülete
CA(S)	Conditional Access (System)	Hozzáférés-korlátozás rendszer
CAM	Conditional Access Module	Kártyaolvasót tartalmazó PCMCIA/PC modul, melynek feladata az ECM/EMM üzenetek szűrése, konvertálása és továbbítása
CAT	Conditional Access Table	A hozzáférés-korlátozó rendszertől függő, a felhasználói adatokat és a CA leírókat tartalmazó táblázat
CI	Common Interface	Szabványos (EN50221) interfész a CAM és a DVB vevő között
CW	Control Word	Kódszó (kriptografikus kulcs)
CSA	Common Scrambling Algorythm	MPEG-2 kódolású DVB jelfolyam-titkosításhoz alkalmazott algoritmus
DTT	Digital Terrestrial Television	Az OFDM modulációt alkalmazó, DVB-T szabványú földfelszíni digitális televíziózás
ECM	Entitlement Control Message	Hozzáférési kritériumokat és kódszavakat tartalmazó titkosított üzenet (CA rendszertől függően általában 40 és 200 bájt közötti hosszúságú)
ECW	Even CW	Az ECM által szállított páros kódszó
EIT	Event Info Table	Kezdetek, végek és időtartamok időrendi esemény-táblázata
EMM	Entitlement Management Message	A kódkártyát meghatározott hozzáférési kritériumok alapján engedélyező titkosított üzenet, amely az aktuális jogosultsági adatokat tartalmazza
EPG	Electronic Program Guide	Elektronikus műsorkalauz vagy műsorfüzet
FEC	Forward Error Correction	Előre irányú hibakorrekciós eljárás
FTA	Free To Air	Titkosítás nélkül terjesztett programok
IRD	Integrated Receiver & Decoder	DVB-S/-T műholdjeleket videó/audió jelekké visszaalakító professzionális DVB vevőegység
MHP	Multimedia Home Platform	Általános interfész definíció az interaktív digitális alkalmazások és terminálok között
MPEG-2	Moving Pictures Expert Group	Digitális videó tömörített átviteli szabványait kidolgozó munkacsoport
Multicrypt	Multicrypt descrambling	Azon DVB vevő meghatározása, amely egynél több CAS-t kezel, így különböző hozzáférés-korlátozó rendszerek bármelyikével titkosított programok (PES-ek) helyreállítására képes
NIT	Network Information Table	A terjesztő hálózatokra vonatkozó információkat tartalmazó táblázat
NVOD	Near Video On Demand	„Majdnem” igény szerinti videó
OCW	Odd Control Word	Az ECM által szállított páratlan sorszámú kódszó
OFDM	Orthogonal Freq. Division Multiplexing	Ortogonális frekvenciaosztásos multiplexelés
PAT	Program Association Table	A programok azonosítása programszámuk alapján
PCMCIA	PC Module CI Access	A DVB CI és a CAM közötti csatlakozási pontra vonatkozó szabvány (hitelkártya méretű számítógépes kiegészítők csatlakozási felülete)
PCR	Programme Clock Reference	Videó kódolót vezérlő 27 MHz-es órajelből származtatott időzítő jel (90kHz)
PES	Packetised Elementary Stream	A program kódolt audio/video/adat jelfolyama
PID	Packet Identifier	A TS-ben továbbított különböző PES-ek azonosítója
PMT	Program Map Table	A programok elemi jelfolyamainak (PES) azonosító táblázata
PSI	Program Specific Information	A PES-eket és ezek PID-jeit egymáshoz rendelő táblázat, Segítségével a különböző programok elemi jelfolyamai (PES) követhetők nyomon az MPEG TS-ben, A PSI tartalmazza a PAT, PMT, NIT, CAT, ECM és EMM információkat
QPSK	Quadrature Phase Shift Keying	Több állapotú fázisbillentyűzés
RST	Running Status Table	A futó műsorok táblázata
SAS	Subscriber Authorisation Server	Az előfizetői jogosultságokat lefordító CA alrendszer
SCI	Smart Card Interface	A CAM modul szabványos kódkártya interfésze
SDT	Service Description Table	A műsorokat leíró táblázat
SMS	Subscriber Management Server	Az előfizetői adatokat és számla-egyenlegeket kezelő CA alrendszer
SI	Service Information	Szolgálati információk
STB	Set Top Box	Jelátalakító előfizetői vevőkészülék
Simulcrypt	Simulcrypt scrambling	A PES-ek titkosítási eljárása (többszörös CW-továbbítás)
Singlecrypt	Singlecrypt scrambling	A PES-ek titkosítási eljárása (egyenkénti CW-továbbítás)
TDT	Time & Date Table	A pontos időt és dátumot egyezményes formátumban szállító táblázat
TS	Transport Stream	Egy vagy több program PES-eiből multiplexelt összetett jelfolyam
VOD	Video On Demand	Igény szerinti videó

így kétirányúvá válik.) A visszirány ekkor a műsorszolgáltatástól részben független, de szintén hozzáférés-korlátozott „e-...” szolgáltatások (e-banking, e-gaming stb.) adatainak is hordozója lehet. A műsorterjesztés és ezen új szolgáltatások adatfolyamai hozzáférés-korlátozásának megvalósítása azonban közös platformon célszerű.

Jelen cikk a fent vázolt fejlődési folyamat első fázisával foglalkozik, azaz a DVB hozzáférés-korlátozó rendszerek szolgáltató – felhasználó irányú kommunikációjára épülő alapszolgáltatások elvi megoldásait ismerteti.

3. A hozzáférés-korlátozó rendszerek elemei

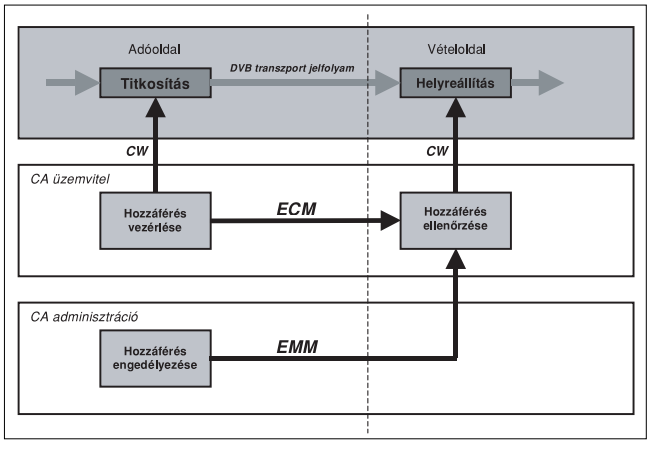
3.1. A hozzáférés-korlátozási alkalmazások kiegészítő egységei

A hozzáférés-korlátozás, mint alkalmazás elsődleges kiegészítő egységének rendszertechnikai elnevezése a **CAM,** amely egy PCMCIA szabványú dugaszolható csatlakozással ellátott modul. Funkciója a titkosított DVB jelek helyreállításának vezérlése a hozzáférési jogosultságok alapján. A PCMCIA felülettel a CAM a DVB vevő CI-jéhez csatlakozik. A CAM típusok többségének másik interfésze egy szabványos kódkártya olvasó interfész (SCI). A különböző CAS-ek CAM-jai ezért nem cserészabatosak. Léteznek azonban már univerzális hardverrel megvalósított CAM típusok is, melyekbe több CAS alkalmazásai letölthetők.

Az API interfész CAS specifikus megvalósítása a DVB vevőben a **CI,** amely lehetővé teszi az eltérő hozzáférés-korlátozó technológiák alkalmazását. A CI a DVB jelfolyamba ágyazott hozzáférési jogosultsági adatokat továbbítja a CAM számára. Egyes továbbterjesztői és végfelhasználói a DVB vevők CAM funkcióit költségtakarékossági céllal szoftver emuláltan (is) megvalósítják. Ezek az adott CAS-hez beépített kártyaolvasóval (is) ellátott típusok. A CI ebben az esetben virtuális.

A térítésköteles műsorkínálathoz való hozzáférési jogosultsági adatok tárolásának elterjedt megvalósítási formája a CAM-ba dugaszolható **kódkártya**. Az ellenőrzés kódkártyás megvalósítási formája különböző kriptografikus eljárások alkalmazásával a környezet manipulálhatatlanságát hivatott biztosítani. A vételoldali hozzáférés ellenőrzését a kódkártyába épített mikroprocesszor hajtja végre. A kódkártya adatait a gyártók az interfész specifikáció (ISO 7816) kivételével – érthető okból – gondosan titokban tartják.

2. ábra A hozzáférés-korlátozás jelzésrendszer-modellje



A műsorjel hozzáférés-korlátozásának lépései a DVB jel átvitel előtti titkosítása az adásoldalon, és a szelektív felhasználói helyreállítás vezérlése a vételoldalon. A **titkosító rendszert** általában a DVB multiplexer egység foglalja magában, melynek egy további szerepe a DVB TS szinkronizációja. A hozzáférés-korlátozás jelzésrendszerének modellje a *2. ábrán* látható.

3.2. Vezérlő rendszer

Szerepe a DVB jel titkosítása szabványos DVB titkosító algoritmussal (CSA) az adóoldalon, valamint – a hozzáférés jogának meghatározása és fennállása esetén – a helyreállítás vezérlése a vételoldalon. Mint az alábbiakban látni fogjuk, a DVB CA titkosítási rendszere hierarchikus, mivel az CSA-val titkosított DVB jelek vételoldali helyreállítását titkos adatokat (CW) szállító és ugyancsak titkosítást alkalmazó jelzésrendszer vezérli. E jelzésrendszer működése alábbi fejezetekben ismertetett információhordozó elemekre épül (v.ö. 2. ábra).

A titkosítás **kódszavak (CW)** segítségével történik. A DVB titkosító algoritmus (CSA) szimmetrikus, az adóoldalon használt kódszavakat ezért továbbítani kell a CAM felé. A CSA-al titkosított DVB jel helyreállításának vezérléséhez használt CW-t rendszerint 10-30 másodpercenként változtatják. A kódkártya ellátása a számára szükséges további információkkal valamint a CAM ellátása a kódszavakkal (a kódkártya közreműködésével) az alábbi két üzenettípus segítségével történik.

Az **EMM** hordozza azon információkat, melyek feltöltik és frissítik a kódkártya memóriáját az igényelt szolgáltatásra vonatkozó jogosultságokkal, hozzáférési kezdet/vég dátumokkal, kriptografikus kulcsokkal stb. Funkcióját tekintve az EMM a tartalomhoz vezető ajtó zárjának „kulcslyuka”.

Az **ECM** a CAM számára küldött **jogosultság-ellenőrző üzenet,** amely a CW-ket titkosítva szállítja. Az ECM ezen kívül tartalmazza az adott programra vonatkozó szolgáltatói, program-hivatkozási és jogosultsági információkat (például program-azonosító, kriptografikus változók, aktuális dátum és idő). A kódkártya ezeket az információkat összeveti a memóriájában tárolt előfizetési adatokkal és dönt a hozzáférés jogosultságáról. Amennyiben a hozzáférés engedélyezett, a kódkártya a helyreállított CW-t kiadja a CAM számára. Az előbbi analógia szerint az ECM a tartalomhoz vezető ajtó zárjának a „kulcsa”.

3.3. Átviteli elemek

A DVB átvitelnél legelterjedtebben alkalmazott szabványos kódolási eljárás az MPEG-2. Az adóoldalon a

stúdióból, vagy videó/audió szerverből induló DVB szabványos kép és hang forrásanyag az alábbi utat járja be:

- MPEG-2 tömörítés/kódolás
- Az MPEG-2 jelfolyamok és a kísérő adatfolyamok multiplexelése TS-ekbe
- Az átviteli közegnek (műhold, kábel, földfelszíni, esetleg egyéb szélessávú) megfelelő moduláció és frekvencia konverzió

A terjesztési rendszerek útján átvitt DVB/MPEG 2 jel (v.ö. 1. ábra) beszerzési, illetve továbbterjesztési eszközei az alábbiak:

- analóg továbbterjesztés: IRD, QPSK-PAL konverterek,
- digitális továbbterjesztés: QPSK-QAM konverterek,
- végfelhasználó: STB (6. fejezet).

3.4. Adathordozó elemek

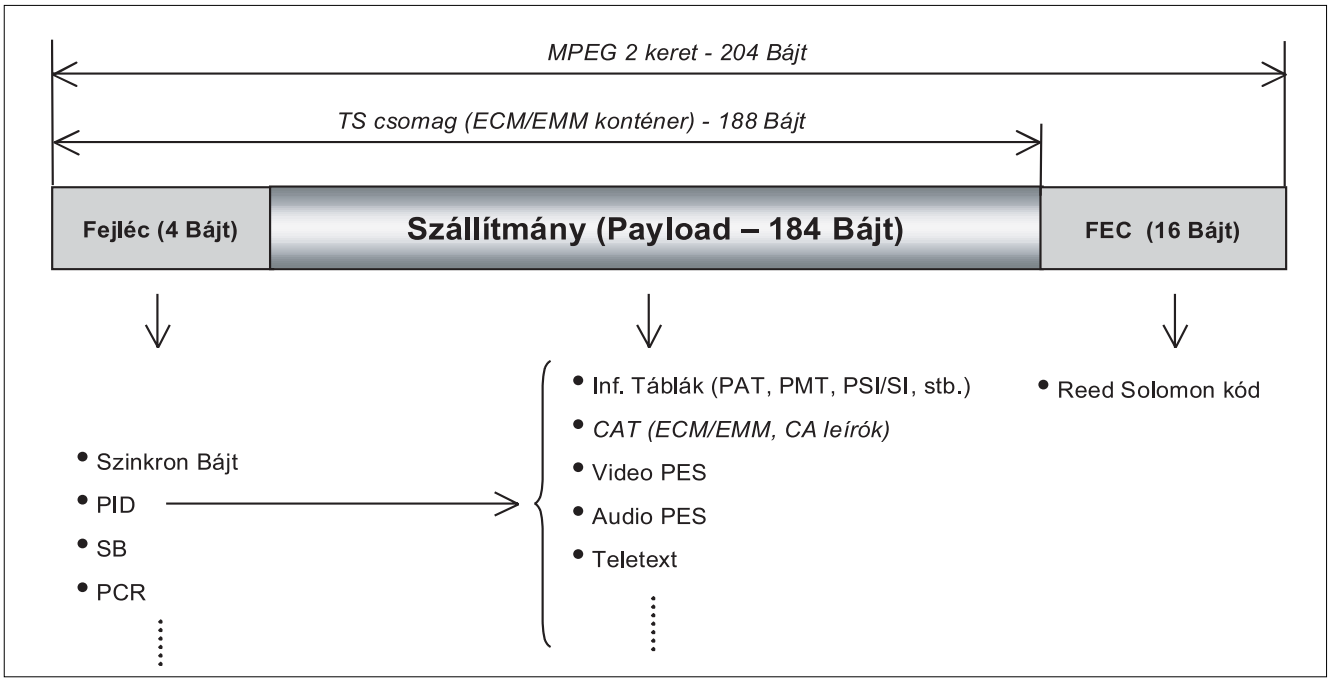
A DVB informatikai mechanizmusa rendkívül összetett, a szállított számtalan fajtájú és hatalmas bitmennyiségnek a hozzáférés-korlátozással kapcsolatos része szinte elenyésző. A DVB információhordozó struktúráját az ITU–T H.222.0 ajánlása határozza meg. Jelen cikk ezt csak olyan mélységben tárgyalja, amely a beleágyazott hozzáférés-korlátozással kapcsolatos üzeneteket (ECM, EMM) szállító adatcsomagok továbbítási mechanizmusának szemléltetéséhez szükséges. Az MPEG-2 kódolású TS-ek keretszervezési vázlata a *3. ábrán* látható. Az ábrán a fentieknek megfelelően csak az alapvető fontosságú, illetve a hozzáférés-korlátozással kapcsolatos információfajták vannak feltüntetve.

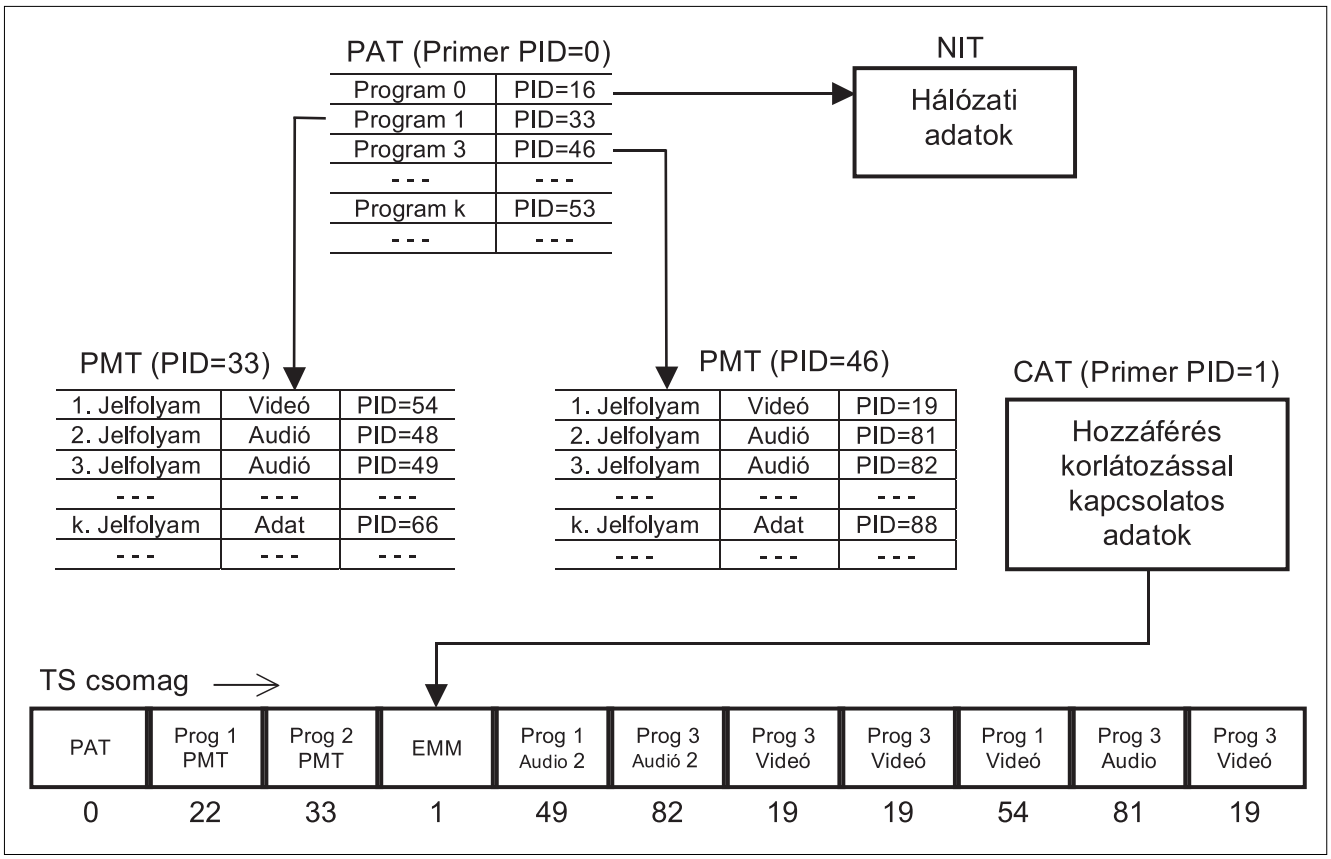
A TS csomagokat azonosító kódokat (PID) egy a fejlécben átvitt 13 bites mező hordozza. A DVB demultiplexer a különböző információfajtákat hordozó TS csomagokat ezek segítségével különbözteti meg. Egy adott TS-en belül minden PES-hez tartozó TS csomag PID-je azonos. A demultiplexer egy adott (például TV) program összetartozó adatfolyamait a hozzá tartozó (videó, audió, adat/felirat/teletext stb.) PES-ek PID-jeinek felhasználásával választja ki. Ha a TS hozzáférés-korlátozással kapcsolatos adatcsomagokat is továbbít, ugyanez érvényes ezek kiválasztására is. A csomagok helyes kiválasztásának feltétele, hogy a demultiplexer a TS csomagok és a PES-ek egymáshoz rendelését lássa. Ehhez a megfelelő PID-eket ismernie kell. Az egymáshoz rendeléseket a TS-ben kötelezően továbbított PAT (PID=0), illetve egy, vagy több PMT tartalmazza.

Mind a PAT-ot, mind a speciális rendszerinformációkat szállító további táblázatokat (CAT, NIT, SDT, EIT, TDT, RST stb.) egységes PID-del ellátott adat PES-ek szállítják. Ezek az úgynevezett rögzített értékű primer PID-ek, melyek a DVB szabvány szerint a speciális rendszer információkat tartalmazó táblázatokat hordozó csomagok (PSI, SI stb.) azonosítására szolgálnak. Ezek közé tartoznak hozzáférés-korlátozással kapcsolatos adatcsomagok (CAT) is. A speciális célú primer PID-ek értékeire a DVB szabvány a 0-31 mezőt tartja fenn. A 13 bites PID-ek értéke 0..2^13-1, azaz 0...8191 lehet. A változó értékű PID-ek mezeje ennek megfelelően a 32-es értékkel kezdődik. A kitöltő null-csomag PID azonosítója szintén foglalt, ennek értéke a 8191 (binárisan 111 1111 1111). A különböző videó, audió és adat PES-ek PID-jei ennek megfelelően 32 és 8190 közötti értékűek.

A demultiplexer a változó PID-ekhez a primer PID-ek által azonosított adat PES-ekben szállított táblázatokhoz való hozzáférés útján juthat. Ezen információkat a DVB szabvány szerint minden TS-nek periodikusan szállítania kell.

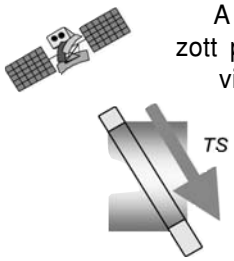
3. ábra MPEG-2 TS-ek keretszervezése





4. ábra A PID-es TS csomag azonosítás struktúrája (példa)

A hozzáférés-korlátozással kapcsolatos adatcsomagok azonosítói ebben a sorrendben a második helyen találhatók. Az ECM-eket és EMM-eket hordozó adatcsomagok PID-jeit a primer PID=1-el meghatározott hozzáférés-korlátozási adattáblázat, a CAT tartalmazza *(4. ábra)*.

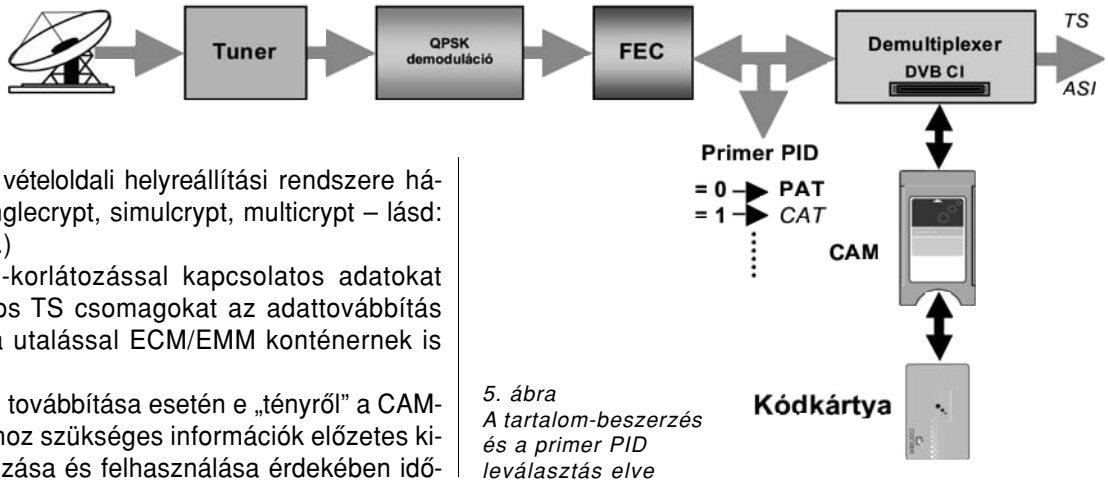


A CAT-ot csak hozzáférés-korlátozott programok jelfolyamaiban kell átvinni. A CA leírók a számukra fenntartott adatmezőkben szállított, csak a kódkártyák számára érthető titkos adatok. Ha a CAT egy CA leírót tartalmaz, az alkalmazott hozzáférés-korlátozás single-crypt, ha többet, simulcrypt rendszerű. (Ezek vételoldali helyreállítási rendszere háromféle lehet: singlecrypt, simulcrypt, multicrypt – lásd: meghatározások.)

A hozzáférés-korlátozással kapcsolatos adatokat szállító 188 bájtos TS csomagokat az adattovábbítás mechanizmusára utalással ECM/EMM konténernek is nevezik.

Tikosított PES továbbítása esetén e „tényről" a CAM-ot a helyreállításhoz szükséges információk előzetes kinyerése, feldolgozása és felhasználása érdekében időben „értesíteni" kell. A feladatot a fejlécben átvitt kétbites helyreállítás vezérlő jel, az SB látja el, melynek azonban ez nem az egyetlen szerepe.

A CSA-al titkosított DVB jel helyes helyreállításához mindig az aktuális CW-re van szükség, amelynek változásait nem lehet szinkronban tartani a CW-t tartalmazó ECM üzenetek, illetve a kódkártya által helyreállított CW megérkezésével. Az ECM-ben ezért általában egyszerre 2 CW-t továbbítanak, amelyből az egyik az aktuálisan használt CW, míg a másik a CW következő értékét adja. A SB másik feladata a CW változásainak pontos (csomagszintű) jelzése a titkosítás helyreállításakor.



5. ábra
A tartalom-beszerzés és a primer PID leválasztás elve

4. A továbbterjesztett tartalom titkosítási megoldásai

Az előfizetői jogosultságot rendszerint a műsorszolgáltató adja ki, a vezetékes műsorszolgáltató hatáskörén kívül. Előfizetőinek hozzáférési jogosultságát ezért utóbbinak is ellenőrzése alá kell vonnia. Jelen fejezet ennek lehetőségeit ismerteti.

4.1. Tartalom beszerzés

A műholdas tartalom beszerzés lépései, melyek a transzmodulációs megoldás kivételével bármely funkciót ellátó DVB vevő esetében azonosak, az *5. ábrán* láthatóak (az előző oldalon). A kivételként említett QPSK-QAM transzmoduláció esetén a műholdas TS eredeti titkosítását nem állítják helyre, így az ábrán feltűntetett CAM-nak és kódkártyának ebben az esetben nincs szerepe. A tartalombeszerzési eljárás egyes lépéseire a zajos távközlési közeg miatt van szükség. A megfelelő minőségű műholdas DVB átvitel alapvető feltétele, a szinkronizáció és hibajavítás biztosítása, amely nélkül a hozzáférés-korlátozás hibátlan működése sem biztosítható.

A DVB kétféle szinkronizációs elemet továbbít. Egyik az MPEG 2 keret szinkron bájtja, a másik a PCR, mint önálló PID-del továbbított PES. A kétféle szinkronizáció nincs kényszerkapcsolatban. A DVB keret szinkronizmusát a fejlécben átvitt szinkron bájt biztosítja, míg a videó/audió jeleket visszaállító MPEG dekódolás szinkronizmusának alapja a PCR.

Fentieknek megfelelően, első lépésben a tunert kell a TS-t szállító transzponder SAT frekvenciájára hangolni. A következő lépések a TS szimbólum sebesség szinkronizálója, majd a redundáns hibajavító információk feldolgozása, melynek eredményeként az MPEG 2 keretekből előállnak a TS csomagok (v. ö. 3. ábra). Az így kézben tartott minőségű MPEG 2 keret fejlécében elhelyezett primer PID-ek szoftveres elérése, illetve a további jelfeldolgozás e lépések után lehetséges.

Az eredeti TV formátum (PAL) visszaalakítása a DVB jel **analóg továbbterjesztése esetén** az előbbi lépéseket követően a továbbterjesztőnél történik. Ekkor a TV jelet le kell bontani alapsávra. Az analóg titkosítás rendszertechnikája bármely megoldás esetén független a beszerzett digitális tartalom titkosítási eljárásaitól. E megoldások túlhaladottak.

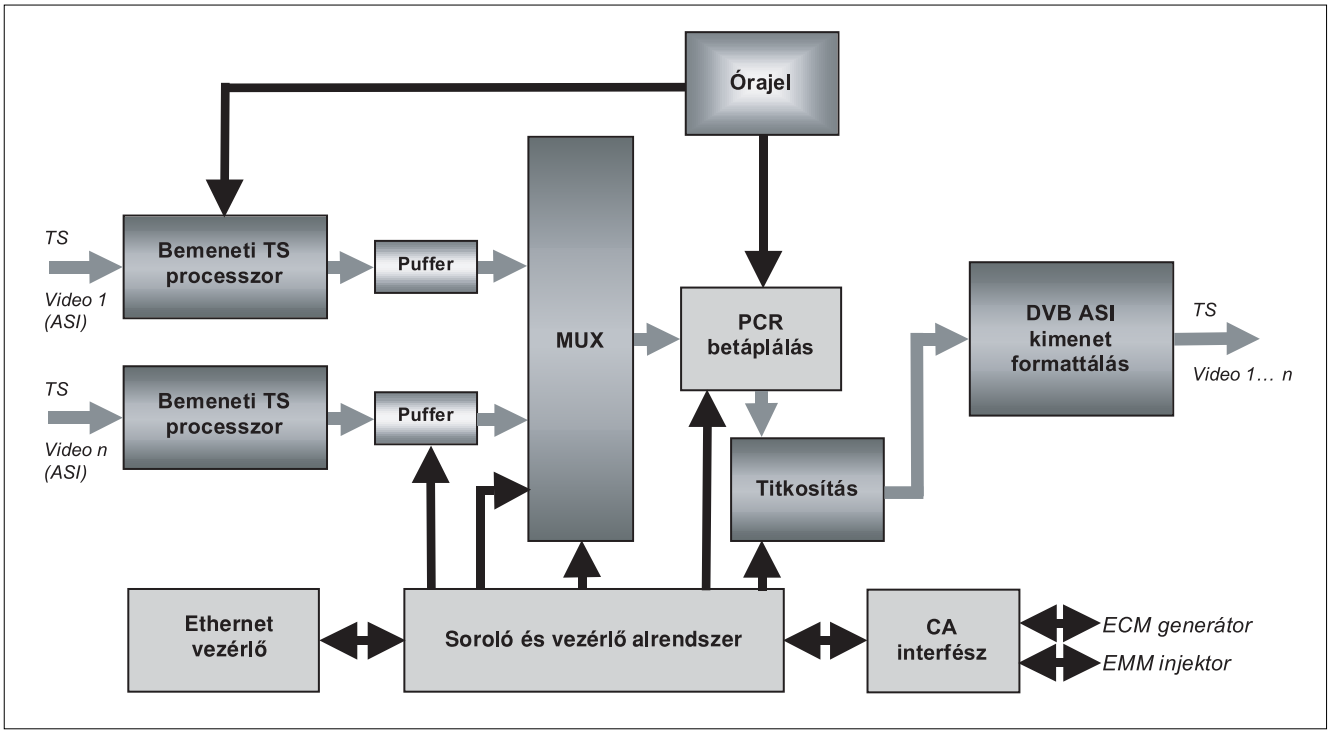
Az érdekeiket időben felismerő vezetékes tartalomtovábbterjesztők hosszú távú célja az analóg megoldás kiváltása. Az analóg titkosítású programok műholdas sugárzása gyakorlatilag már megszűnt.

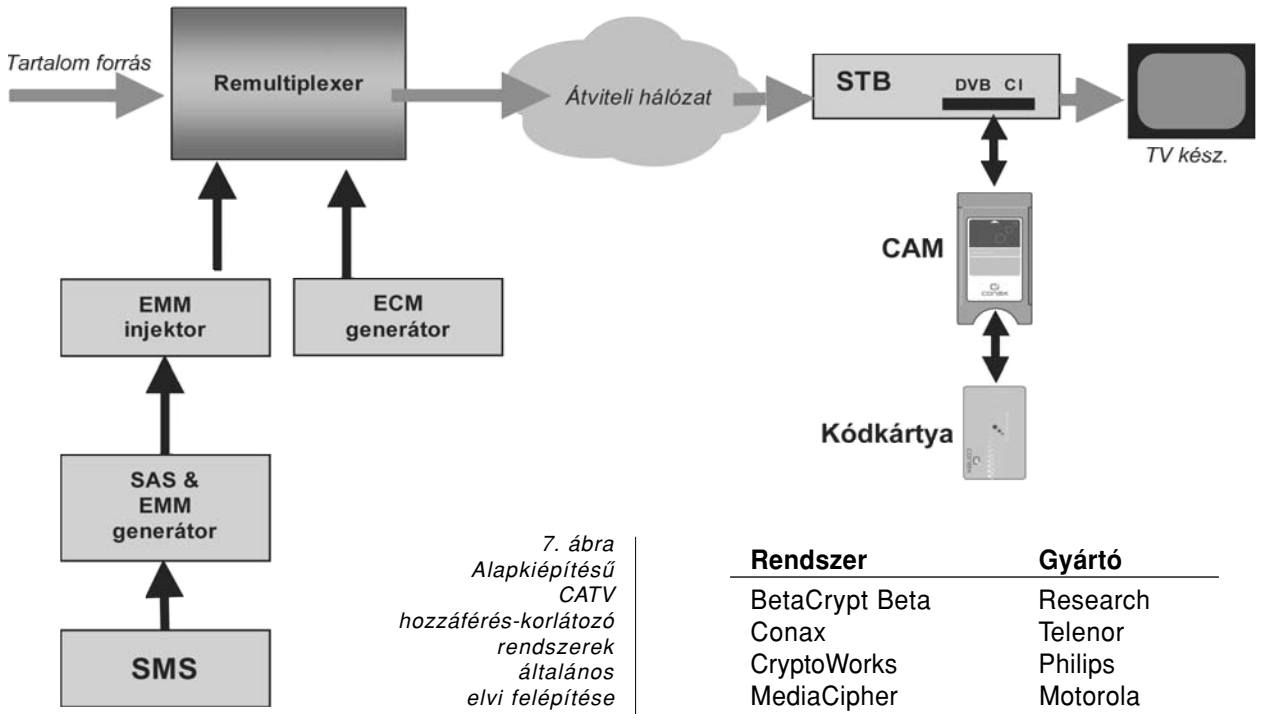
4.2. Továbbterjesztés

A műsortartalom DVB formátumú, hozzáférés-korlátozott, vezetékes továbbterjesztése esetén a szolgáltatói bevételszerzés műszaki megoldása az eredeti jogosultsági és szolgáltatásra vonatkozó adatok felülírása, vagy újragenerálása.

Ha a vezetékes szolgáltató a továbbítandó műholdas TS-ek összeállítását nem kívánja változtatni, akkor ezek közvetlen QPSK-QAM transzmodulációja a megfelelő megoldás. A továbbterjesztői hozzáférés-korlátozás itt egy, a kábeles szolgáltatóhoz rendelt azonosító, az Operator ID, melyet a műholdas szolgáltató bocsát a továbbterjesztő (CATV) szolgáltató rendelkezésére, az együtt járó kódkártyákkal. A transzmoduláció a műholdas TS titkosításának helyreállítása nélkül történik, az

6. ábra MPEG-2 TS-ek remultiplexelési folyamata





7. ábra Alapkiépítésű CATV hozzáférés-korlátozó rendszerek általános elvi felépítése

eredeti hozzáférés-korlátozás e továbbterjesztési megoldás során nem változik. Nagyobb vezetékes műsorszolgáltatók a saját műszaki/üzleti szempontjaik alapján kiválasztott titkosított tartalmakat saját CAS titkosításával terjesztik tovább. A továbbterjesztés így nem történhet változatlan szervezéssel.

A remultiplexer és a hozzáférés-korlátozó rendszer közti együttműködés elvét a *6. ábra* szemlélteti.

A demultiplexelés és remultiplexelés közötti átjárás hagyományos megvalósítása az ASI interfész. E megoldás hátránya, hogy a programok, vagy -csomagok jelfolyamának egymástól független kezelését nem teszi lehetővé. Digitális trönkökkel összekötött CATV hálózatok korszerű közös tartalom forrása az ATM alapú programbank (Híradástechnika 2003/8. sz.). Az ATM alapú demultiplexelést és remultiplexelést megvalósító processzor egységek működésének leírása és elvi felépítésének szemléltetése itt található.

5. Az alapszolgáltatású DVB CATV hozzáférés-korlátozó rendszerek felépítése

5.1. Az európai rendszerek

Az Európában alkalmazott digitális hozzáférés-korlátozó rendszerek működése a közös DVB titkosítási algoritmus (CSA) alkalmazásán alapul, így rendszerelemeik és működési mechanizmusaik egyezőek. A rendszerek közti különbség a jogosultságokkal kapcsolatos adatokat tároló előfizetői egységekben alkalmazott titkosítási eljárásokban rejlik. Az Európában alkalmazott CATV DVB hozzáférés-korlátozó rendszerek a következők:

Rendszer	Gyártó
BetaCrypt Beta	Research
Conax	Telenor
CryptoWorks	Philips
MediaCipher	Motorola
Mediaguard	Seca
Nagravision	Nagra-Kudelski
Viaccess	France Télecom
Videoguard	NDS

A további rendszerek védjegyzett működési elvei az előbbiektől eltérőek és biztonságuk érdekében szigorúan titkosak. Az egyes gyártók még különböző megoldásaik együttműködésének kizárására is törekszenek annak érdekében, hogy eladott rendszereik biztonsága bármelyik feltörése esetén a lehető legkisebb mértékben váljon veszélyeztetetté.

5.2. Rendszerelemek

A vezetékes műsorszolgáltatói hozzáférés-korlátozó rendszerek egyszerű fizető TV szolgáltatást támogató alapkonfigurációja a fenti, *7. ábrán* látható. A rendszerelemek funkciói az alábbiak:

Adóoldal

• *SMS adatbázis:* az előfizetői adat állomány nyilvántartása, az előfizetők számla egyenlegeinek követése (interfész a banki számítógépes nyilvántartás felé) és az EMM-ek kiadásának kérése a SAS tól.

• *SAS alrendszer:* a jogosultságok kiosztásának felügyelete, a kódkártya állomány állapot-fenntartása, hozzáférést biztosító jogosultsági adatok szolgáltatása a kódkártya számára.

• *EMM generátor:* a titkosított EMM-ek előállítása a SAS-tól kapott információk alapján, ezek betáplálása a DVB multiplexerbe.

• *EMM injektor:* a SAS felől érkező EMM-ek vételezése, az EMM kiadások sorolásának felügyelete és az EMM-ek betáplálása a DVB multiplexerbe.

• *ECM generátor:* a jogosultságok ellenőrzéséhez szükséges információ csomagok (dátum, programcsomag, CW) képzése és titkosítása.

Vevőoldal

• *CAM:* az ECM/EMM-ek szűrése, konvertálása és továbbítása a kódkártya felé, a CSA-al titkosított DVB jelek helyreállítása a CW felhasználásával.

• *Kódkártya:* a program-hivatkozási és jogosultsági információk tárolása, az ECM-ek és EMM-ek titkosításának helyreállítása és értelmezése a hozzáférési jogosultságok meghatározásához.

A leírt alapkonfiguráció az előfizetőnek egy, vagy több hozzáférés-korlátozott programhoz (TV csatornákhoz, vagy csatorna csoportokhoz) biztosítanak hozzáférést egy meghatározott (például hónapos, vagy éves) időtartamra. A hozzáférés, illetve a rákövetkező előfizetési időtartamra szóló újraengedélyezés kritériuma a számla kiegyenlítése.

5.3. Működési mechanizmus

Jelen fejezet a *8. ábrának* megfelelő elvi felépítésű, alapkiépítésű hozzáférés-korlátozó rendszerek működési mechanizmusát ismerteti.

Adóoldali adatgenerálás, vételoldali feldolgozás

Adóoldalon

– a DVB multiplexer előállítja a kódszót (CW) és az ECM generátort annak egy ECM-be történő beágyazására kéri.

– Az ECM generátor előkészíti az ECM tartalmát, a titkosított kódszavakat (CW) és a hozzáférési paramétereket, továbbá a szolgáltató-azonosítókat, a program-hivatkozást és az együtt járó jogosultsági információkat, kriptografikus változókat, valamint a digitális aláírást.

Vevőoldalon

– telepítésekor a kódkártya bizonyos információk megadásával (pl. CAS típusa, kártya sorozatszáma, a kártyán lévő szolgáltatók azonosítói stb.) regisztrálja magát a CAM-ba, amely ezután ezeket az információkat a kódkártyának szóló üzenetek kinyerésére használja. A kódkártya ettől kezdve rendre helyreállítja az érkező ECM-et, majd összehasonlítja a pillanatnyi dátumot és időt, a szolgáltató azonosítót, valamint a program-hivatkozási és jogosultsági információkat a saját memóriájában tároltakkal. Amennyiben az adott programhoz való hozzáféréshez jogosult, a kódkártya kiadja a CW-t a CAM számára a DVB TS helyreállításához.

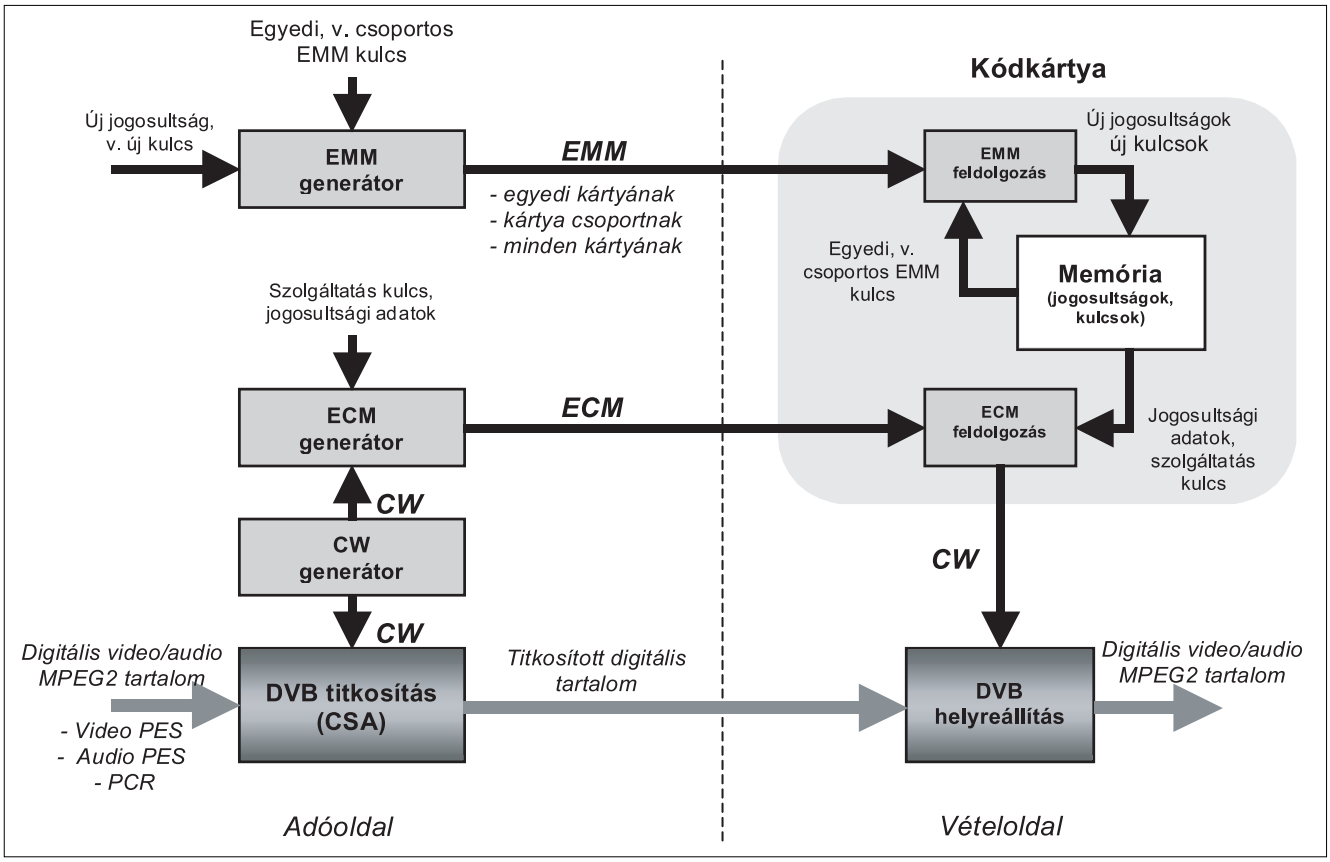
– A CAM a kapott kódszavak felhasználásával végrehajtja a PES-ek helyreállítását.

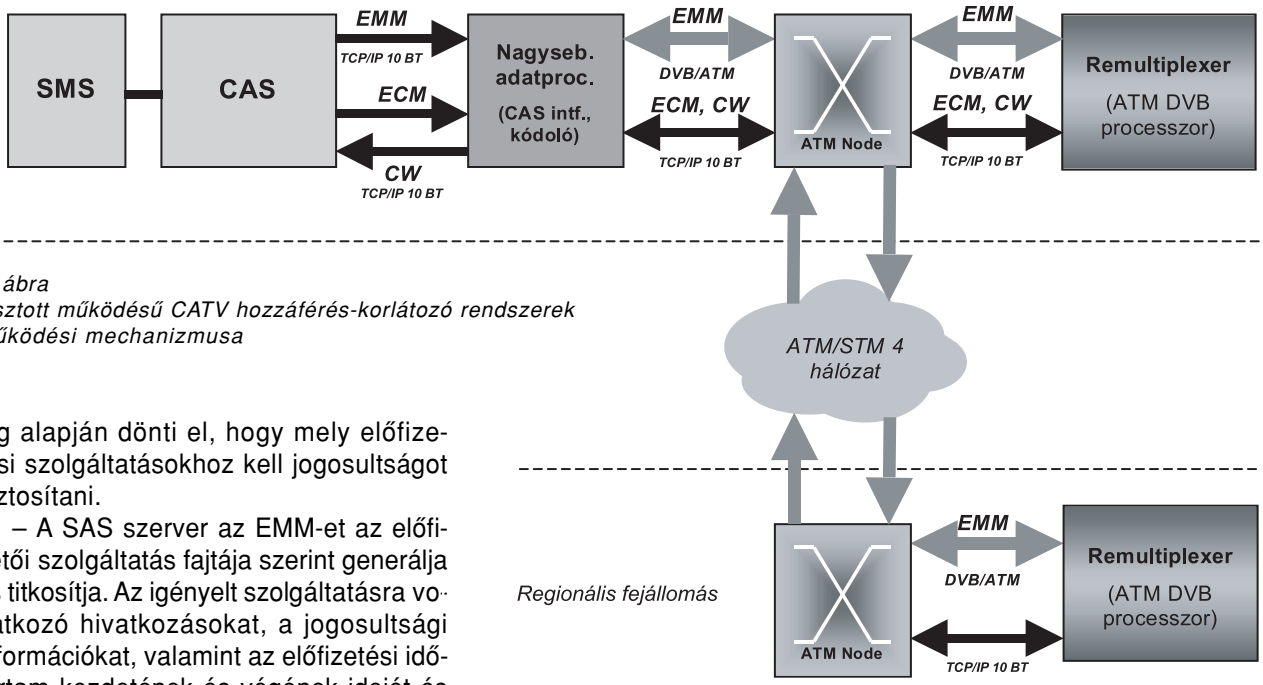
A jogosultságok kiosztása és frissítése

Adóoldalon

– az előfizetői menedzsment rendszer (SMS) nyilvántartja valamennyi felhasználót és kódkártyát. Az SMS a SAS szervertől az EMM-ek előállítását kéri. Az SMS az előfizető által igényelt szolgáltatás és a fizetési egyen-

8. ábra Alapkiépítésű DVB CATV hozzáférés-korlátozó rendszer működési mechanizmusa





9. ábra
Osztott működésű CATV hozzáférés-korlátozó rendszerek működési mechanizmusa

leg alapján dönti el, hogy mely előfizetési szolgáltatásokhoz kell jogosultságot biztosítani.

– A SAS szerver az EMM-et az előfizetői szolgáltatás fajtája szerint generálja és titkosítja. Az igényelt szolgáltatásra vonatkozó hivatkozásokat, a jogosultsági információkat, valamint az előfizetési időtartam kezdetének és végének idejét és dátumát az EMM tartalmazza.

Vevőoldalon

– a CAM a beérkező EMM-eket a kódkártya felé továbbítja, amely helyreállítja azokat, majd frissíti memóriáját az érkezett információval, az igényelt szolgáltatásra vonatkozó hivatkozással, a jogosultságokkal, valamint az előfizetési időtartam adataival.

5.4. Architektúrák

A DVB alapú CATV hozzáférés-korlátozó rendszerek fő gazdasági előnye az igények szerinti konfigurálhatóság. E rendszerek az osztott üzemet is lehetővé teszik, azaz egy közös hozzáférés-korlátozó rendszert több CATV szolgáltató is üzemeltethet. Ehhez azonban szükséges a szabványos kommunikációs mechanizmusra épülő SMS–SAS interfész, amely az együttműködést más típusú SMS-ek számára is lehetővé teszi. Az SMS ugyanis nem feltétlenül a hozzáférés-korlátozó rendszer gyártójának terméke. Előfizetői adat és számlanyilvántartással minden szolgáltató, minden körülmények között rendelkezik. A DVB alapú hozzáférés-korlátozó rendszer beruházásánál azt kell tehát mérlegelnie, hogy áttér-e egyúttal a hozzáférés-korlátozó rendszer gyártója által ajánlott SMS alkalmazására, vagy megoldja meglévő SMS rendszere és a hozzáférés-korlátozó rendszer közötti együttműködés esetleges problémáit.

A rendszer osztott távműködésének feltétele a SAS és ECM generátorok, valamint az EMM injektorok azonos helyű telepítése a szolgáltatási területet behatárolja. A szabványos kommunikációs mechanizmusra épülő SMS–SAS interfész e feltétel kielégítése mellett több SMS egyidejű csatlakoztatását is lehetővé teszi. Az osztott távműködés további feltételei:

– rugalmasan konfigurálható EMM kiadási rendszer, meghatározott prioritásokkal,

– az EMM-ek irányíthatósága valamennyi, vagy kiválasztott multiplexer telephelyre,

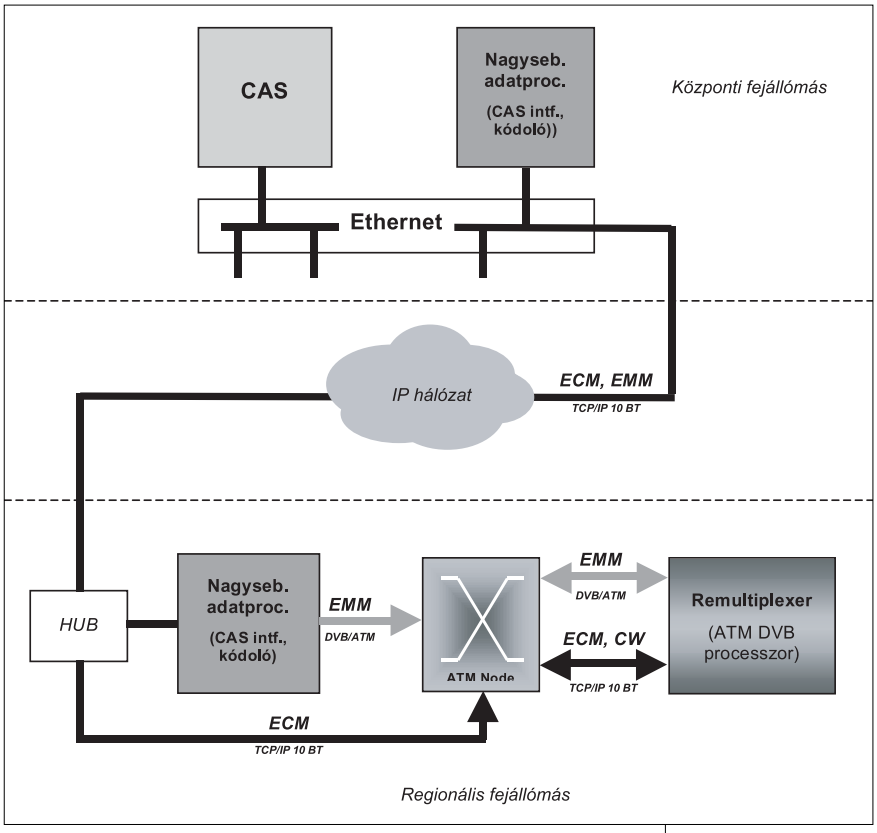
– a jogosultságok hozzárendelhetősége egy-egy alap-jelfolyamhoz, programhoz, vagy csoporthoz.

Az osztott működésű hozzáférés-korlátozó rendszerek legkönnyebben az ATM alapú programbankok hálózati architektúrájába integrálva alkalmazhatók *(9. ábra),* melyet a már hivatkozott ATMux™ rendszer leírása ismertet.

Az ATM program bank és a hozzáférés-korlátozó rendszer közötti ATM-DVB konverziót és az adatkommunikációt itt egy nagyteljesítményű adatprocesszor biztosítja. Az egység feladata a kapcsolatok felépítése és fenntartása az ECM generátorokkal, illetve EMM injektorokkal, az ECM és EMM jelfolyamok kezelése, valamint az ECM-ek és kódszavak szinkronizációja az ATM DVB processzorok beépített titkosító egységei számára.

Osztott működésű hozzáférés-korlátozó rendszermegoldás közös átviteli hálózatba nem kötött, de együttműködni szándékozó szolgáltatók számára is rendelkezésre áll. Ezt a megoldást mutatja be a következő oldalon a *10. ábra,* ahol a központi adatprocesszor a hozzáférés-korlátozó rendszerrel Ethernet hálózat segítségével tartja a kapcsolatot, és a hozzáférés-korlátozáshoz az ECM és EMM adatfolyamokat IP formátumban állítja elő.

A távoli fejállomás(ok)on az EMM adatfolyamokat az ott elhelyezett adatprocesszor konvertálja és ágyazza a DVB/ATM jelfolyamba. Az ECM-eket az adathálózati csomópontból (HUB) közvetlenül az ATM node 10 BT interfésze felé irányítják, ahonnan útja már azonos a 9. ábrán láthatóval.



10. ábra IP alapú centralizált CATV hozzáférés-korlátozó rendszerek működési mechanizmusa

6. Előfizetői végberendezések (STB)

A tartalom szolgáltatók és továbbterjesztők távlati célja egyaránt az, hogy a szociális célúakon („must carry") kívül minden műsortartalom hozzáférés-korlátozással jusson az előfizetőhöz. A közvetlen díjbeszedési rendszer megvalósításának járható útja tehát a „kábeles" STB megjelenése minden CATV-hez csatlakozó háztartásban.

A STB-ok jelenlegi változatai jelfeldolgozás szempontjából terjesztési rendszer (SAT, CATV, DTT) specifikusak. A STB alapvető szerepe mindhárom rendszerben a DVB jelek PAL/RGB jelekké alakítása. A műszaki távlat azonban a mindhárom terjesztési rendszerhez alkalmas univerzális, az adatforgalom szempontjából, pedig interaktív STB-ok megjelenése és elterjedése. A STB-ok CATV-s (vagy CATV-hez is alkalmas univerzális) változatai az adott CATV hálózatban alkalmazott hozzáférés-korlátozás kiegészítő egységeit is értelemszerűen tartalmazzák. Az alapszolgáltatású CATV-s STB-ok felépítése a *11. ábrán* látható.

Az interaktív STB-ok felépítése kábelmodemmel egészül ki. A STB-ok a CATV hálózatok visszirányán, különböző szabványos adatátviteli formátumokban (DOCSIS, EuroDOCSIS/QPSK moduláció) így már az előfizetéssel, számlázással, szolgáltatáskérésekkel és jogosultságokkal kapcsolatos adatokat is képesek lesznek a szolgáltatók felé közvetíteni (beleértve a jövőben várható járulékos új szolgáltatások, mint a NVOD, VOD, PPV stb. időzítéseivel kapcsolatosakat is).

A STB lényegében egy speciális számítógép TV-s alkalmazásokhoz. Fő részei az alábbiak:

Számítógép alrendszer: az alapvető számítástechnikai funkciókat látja el. Magában foglalja a standard számítógépegységeket, mint a CPU, a memória, valamint (interaktív változatoknál) a kábelmodemet.

TV alrendszer: feladata a DVB formátumú TV jelek feldolgozása. Magában foglalja az DVB jelfeldolgozás egységeit, a TV/VCR és audió csatlakozásokat, valamint a remodulátor és RF összegző egységeket.

Hozzáférés-korlátozó alrendszer: A CATV-s változatok egy CI-t, vagy (egyes készülék típusok esetében) beépített kártyaolvasót tartalmaznak. (A SAT típusok egy, vagy két CI-t tartalmazhatnak. Utóbbi esetben csak az egyik beépített.)

A digitális moduláció típusától függő specifikus STB-k:

– közvetlen műholdas műsorszórás (SAT),
– vezetékes (tovább)terjesztés (CATV),
– földfelszíni műsorszórás (DTT).

A vezetékes műsorterjesztéshez a QAM demodulátorral (is) ellátott STB típusok használatosak.

A STB-okban alkalmazott szoftverek referencia modellje a MHP, elhatárolt rétegei az alábbiak:

Alapszoftver: részei az operációs rendszer, boot loader, TV-s alapalkalmazások, middleware és az átviteli modell tárgyalásánál tárgyalt CA alkalmazás

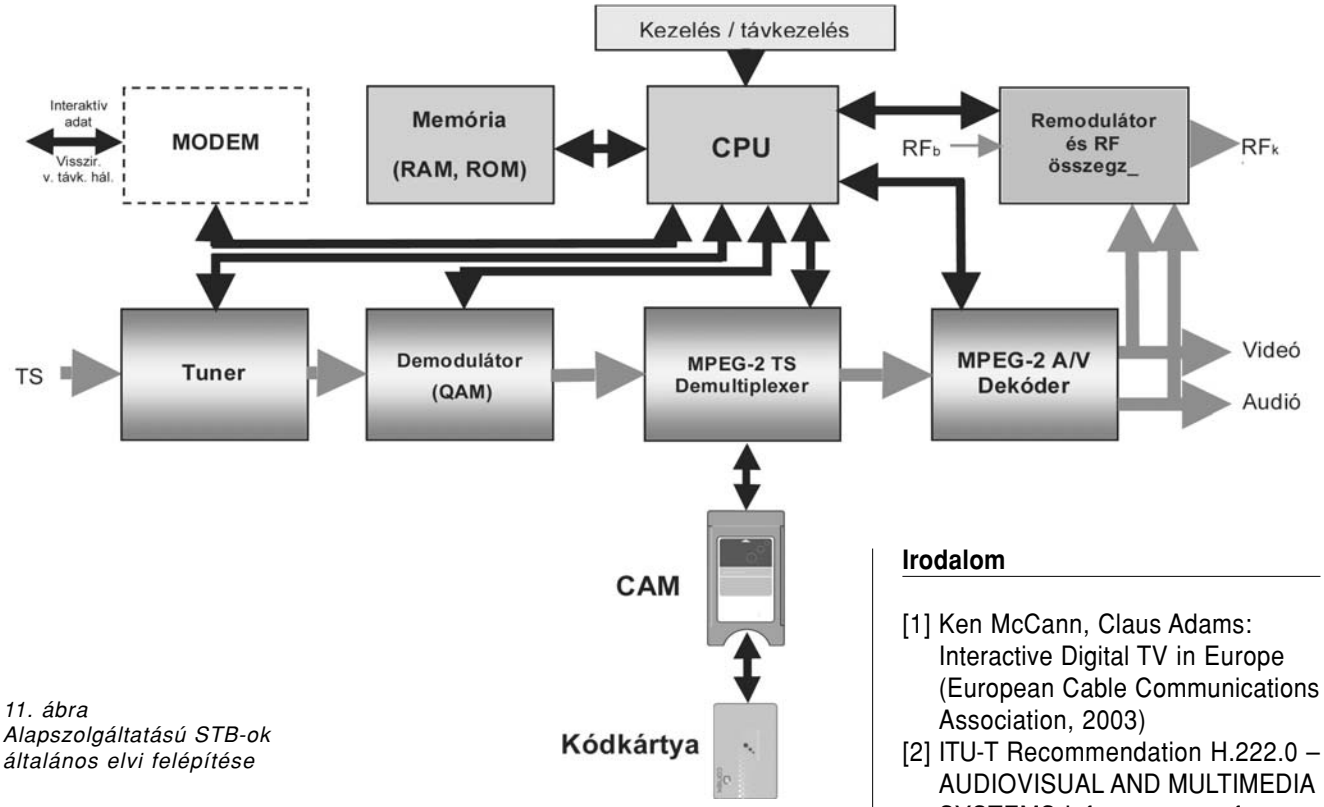
Hardver meghajtók: interfész a hardver és szoftver között. (A gyártók szállítják.)

Alkalmazások: a felhasználói igények szerinti funkciókat látják el, mint pl. EPG (a későbbiekben pedig az interaktív TV-s alkalmazások)

A helyreállított DVB TS-ből az MPEG demultiplexer kiválasztja és dekódolja (kitömöríti) a venni kívánt program videó és audió jelfolyamát. A PAL formátumú alapsávi videó, és audió tartalom visszaállítása az MPEG-A/V dekóder segítségével történik. A STB-ok adat- és információfeldolgozási mechanizmusa sem tartogat újat. Hozzáférés-korlátozott program esetén a CSA-al titkosított DVB TS helyreállítása a kódkártya által kiadott CW felhasználásával ezúttal is a CAM-ban történik.

7. A hozzáférés-korlátozott műsorterjesztés kockázatai

A hozzáférés-korlátozás, mint a bevezetőben is említett bevételforrás, a jogtalan haszonszerzést is jelentheti. Ez akkor valósul meg, ha a hozzáférést elősegítő eszközök kalóz terjesztése miatt a szolgáltató jelentős



11. ábra
Alapszolgáltatású STB-ok általános elvi felépítése

mértékű bevételtől esik el. A hozzáférés-korlátozás önmagából adódó második célja tehát ennek megelőzése, vagy visszaszorítása egy tűrhető mértékre.

A jogosultságokkal kapcsolatos adatok adótól vevőig történő átvitele a műsorterjesztés részét képezi. A cél e pont-multipont viszonylatú egyirányú információfolyam védelme. Bár a digitális televíziózás az interaktivitás felé halad, ahol a felhasználó oldali STB a szolgáltatók központi szervereivel a 6. fejezetben említettek szerint kommunikálhat, maga a tartalomkézbesítés továbbra is egy egyirányú kommunikáció marad.

Az adatok védelme a szolgáltató érdeke. Célkitűzése ezért lényegesen különbözik a kétirányú kommunikációnál érvényesektől, mint például a GSM esetében, vagy az on-line banki tranzakcióknál, ahol a biztonság sérthetetlensége a felhasználó érdeke. A kommunikáció biztonságában a jelen esetben nem érdekelt végfelhasználó, a tartalomhoz, mint termékhez, ha csak lehet, térítésmentesen szeretne hozzájutni. A jel-lopással kapcsolatos jogszabályoknak és betartatásuknak egyelőre számos törvényhozás kevés érvényt szerez, így a fizető TV magas bevételi lehetősége vonzza a jól felszerelt, képzett és szervezett kalózkodást. Ezért minden szolgáltató arra törekszik, hogy a felhasználónál telepített eszközök lehetőleg olcsók, de manipulálhatatlanok legyenek.

Irodalom

[1] Ken McCann, Claus Adams: Interactive Digital TV in Europe (European Cable Communications Association, 2003)

[2] ITU-T Recommendation H.222.0 – AUDIOVISUAL AND MULTIMEDIA SYSTEMS Infrastructure of audiovisual services – Transmission multiplexing and synchronization – Information technology (Generic coding of moving pictures and associated audio information systems)

[3] Guide to MPEG Fundamentals and Protocol Analysis (25W-11418-4 Tektronix, 2002)

[4] Georgieff Zsolt, Wein Tibor: ATMux™ – műsorterjesztés digitális transzporthálózaton, Híradástechnika, 2003/8.

[5] Conax CAS5 System Description (021115 Conax AS, 2002)

[6] Stefler Sándor: Hogyan tovább Set-Top-Box-ok? Híradástechnika, 2001/10.

[7] How to choose STBs (20020927 Conax AS, 2002)

Hírek

Az internetes hálózati berendezések legnagyobb gyártója, a **Cisco Systems** új termékeket mutatott be. A díjnyertes IP-alapú alközponti rendszer, a Cisco CallManager 4.0 lehetővé teszi a Cisco Video Telephony (VT) Advantage 1.0 megoldás alkalmazását, amellyel a felhasználók valós idejű személyes videokapcsolattal egészíthetik ki telefonbeszélgetéseiket. Szintén most mutatkozott be a Cisco MeetingPlace szerver, amelynek segítségével IP-telefonon, hagyományos telefonkészüléken vagy számítógépen keresztül vehetnek részt és szervezhetnek a felhasználók hang- videó- és webkonferenciákat. Az új megoldások fokozott biztonságot nyújtanak a vállalatok számára.