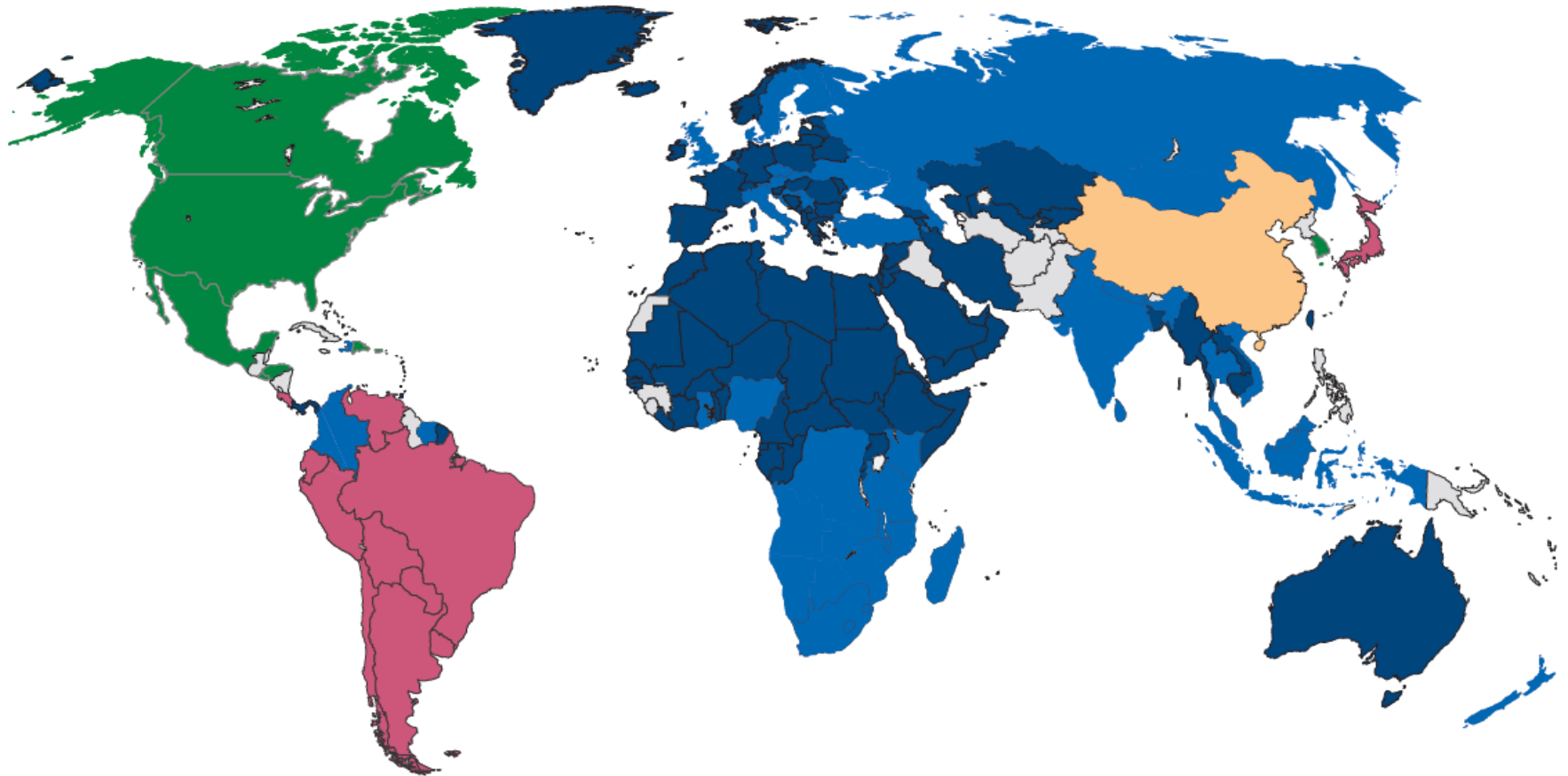


DVB Conditional Access

PPKE, ITK

Csapodi Márton

DVB – Digital Video Broadcasting



DVB-T

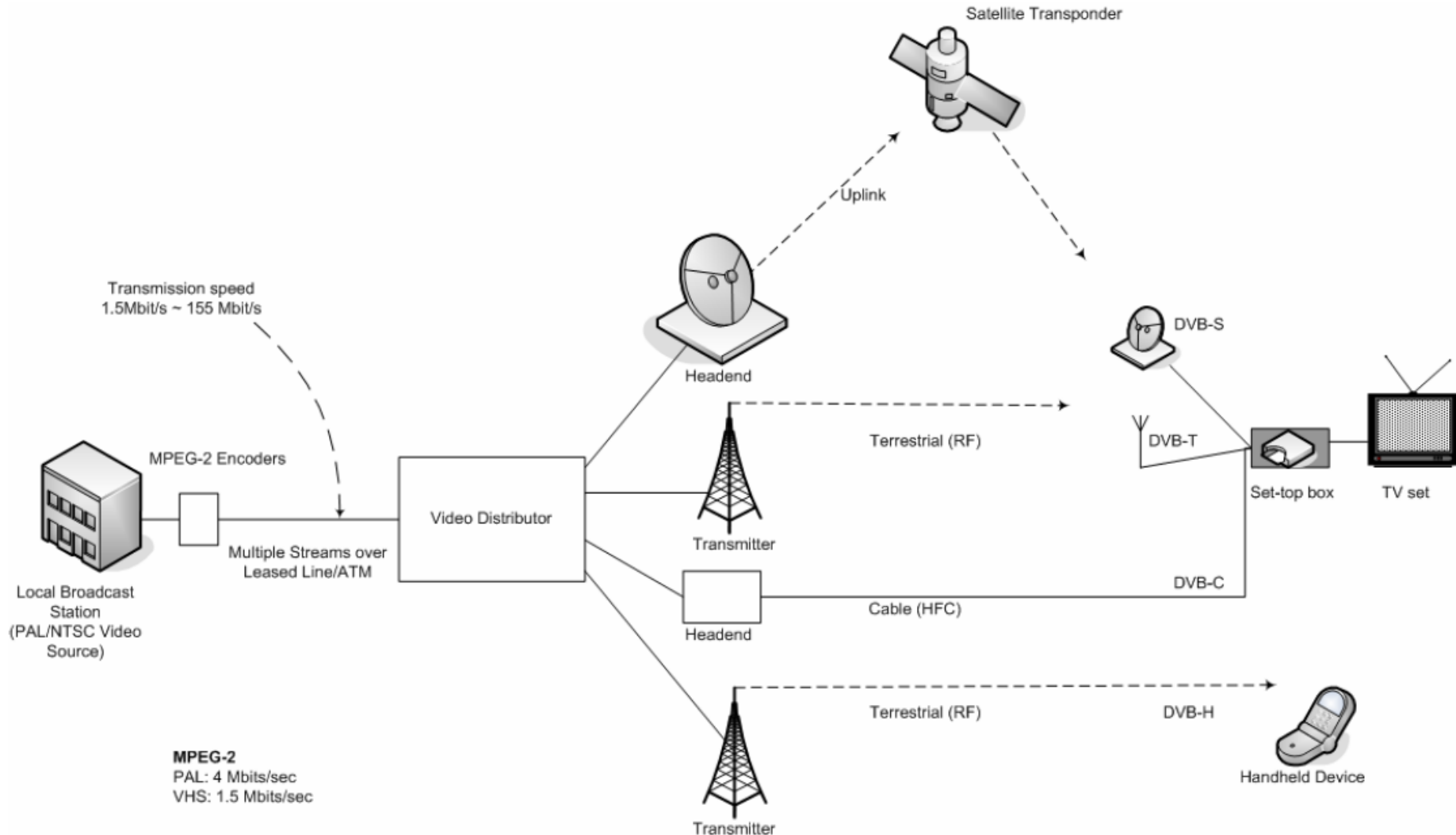
DVB-T2

ATSC

ISDB-T

DTMB

DVB – Digital Video Broadcasting



DVB Magyarországon

digitális átállás: az analóg műsorterjesztés helyébe a digitális műsorterjesztés lép

~~2011. 2012.~~ december 31.: analóg lekapcsolás végdátuma, megszűnik az analóg földfelszíni sugárzású televíziós műsorszórás, és helyébe a digitális földfelszíni sugárzás (DVB-T) lép

5/2013. (III. 11.) NMHH rendelet: két ütemben, 2013. július 31-én és 2013. október 31-én

hagyományos szoba- vagy tetőantenna mellé:

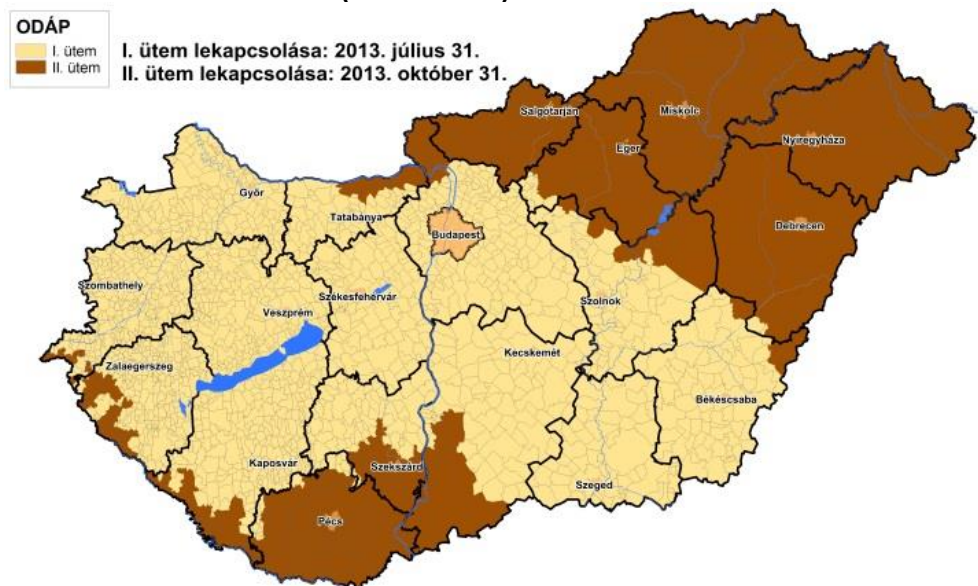
- set-top-box + hagyományos TV
- új TV beépített vevőegységgel

2013 februári előfizetők (szabad hozzáférésű nélkül):

- DVB-C: 900e
- DVB-S: 900e
- DVB-T: 85e
- analóg vezetékes: 1.050e

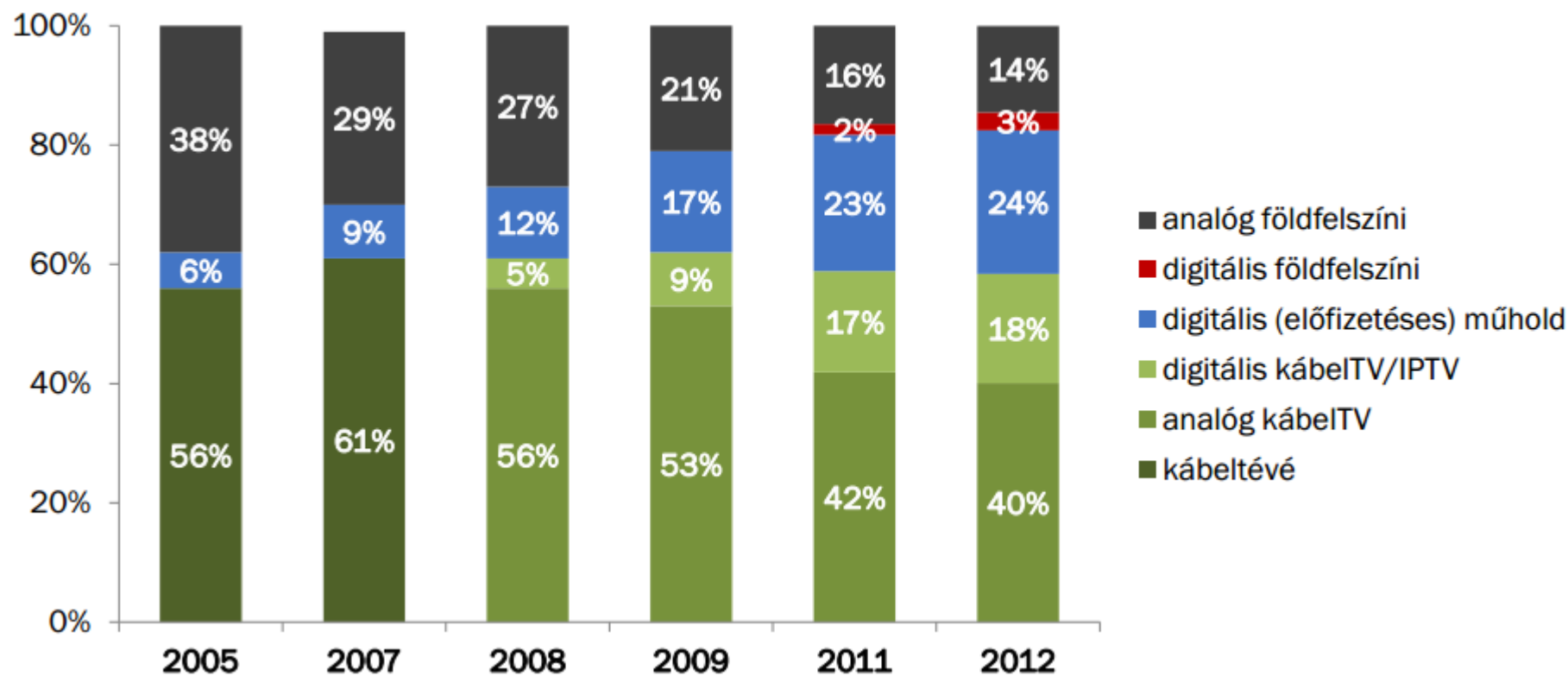
szabad hozzáférésű analóg:

- 500e (becslés)



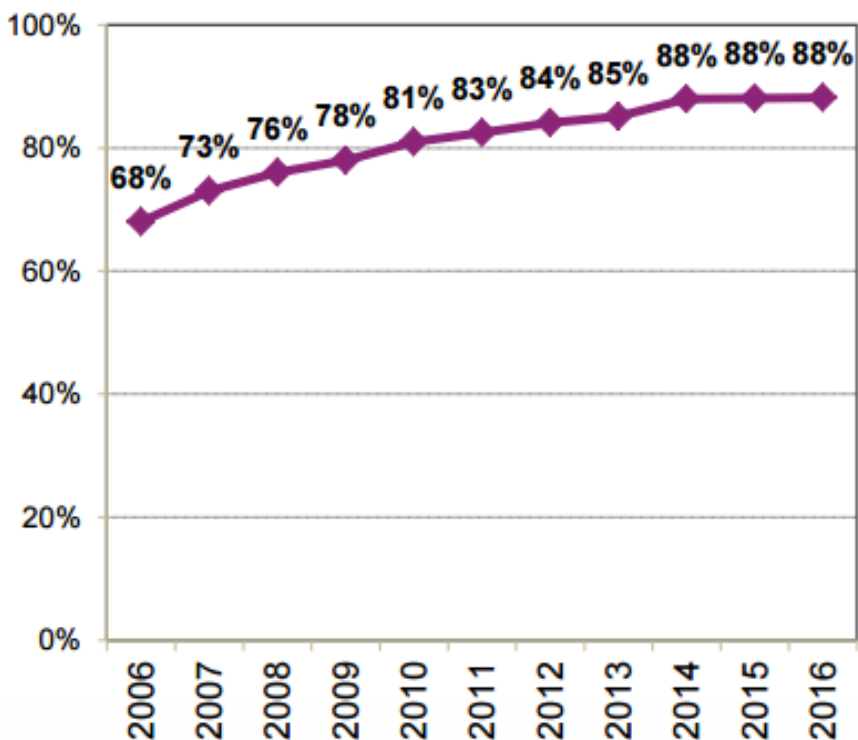
DVB Magyarországon (múlt)

Jelenleg a magyarországi tévésző háztartások 45 százaléka rendelkezik digitális tévévételi móddal



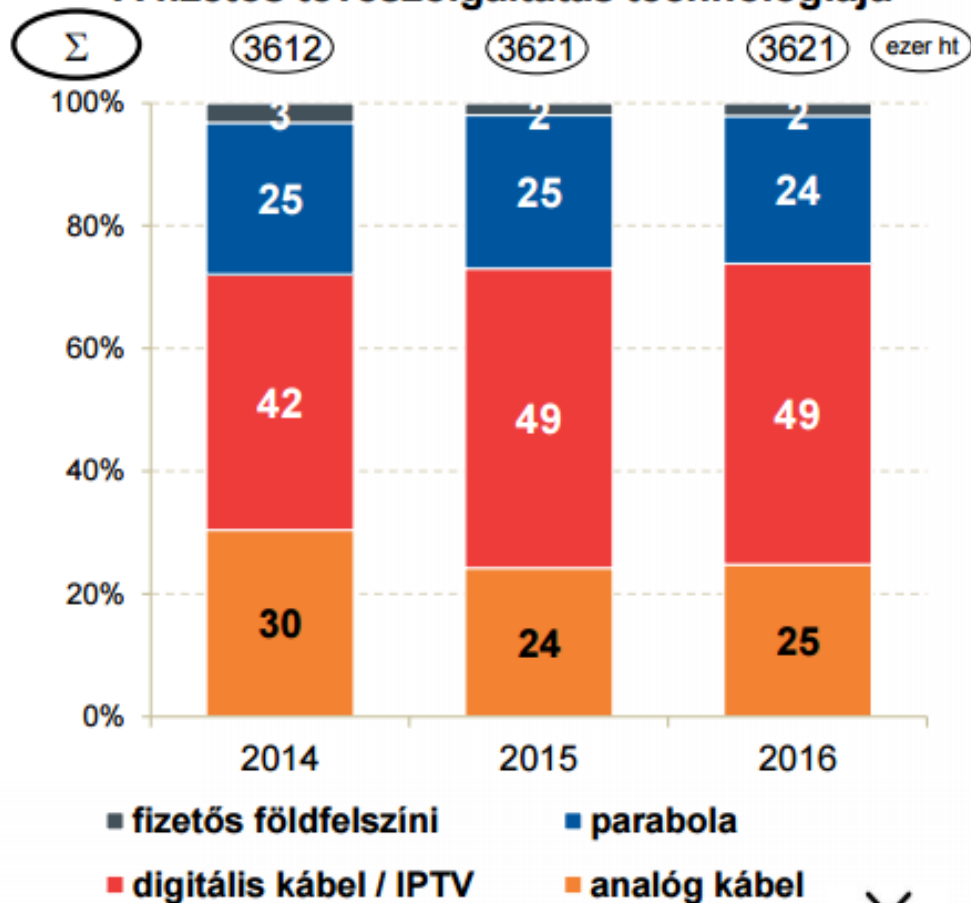
DVB Magyarországon (jelen)

A háztartások ellátottsága fizetős tévével



Bázis: Összes háztartás (N=4,106 millió; n=2020)

A fizetős tévészolgáltatás technológiája



Bázis: Fizetős tévével rendelkező háztartások
(N=3,621 millió HT; n=1776)



DVB átvitel



source coding & multiplexing: MPEG Transport Stream létrehozása

MPEG-2 vagy MPEG-4 (pl. Magyaró.)

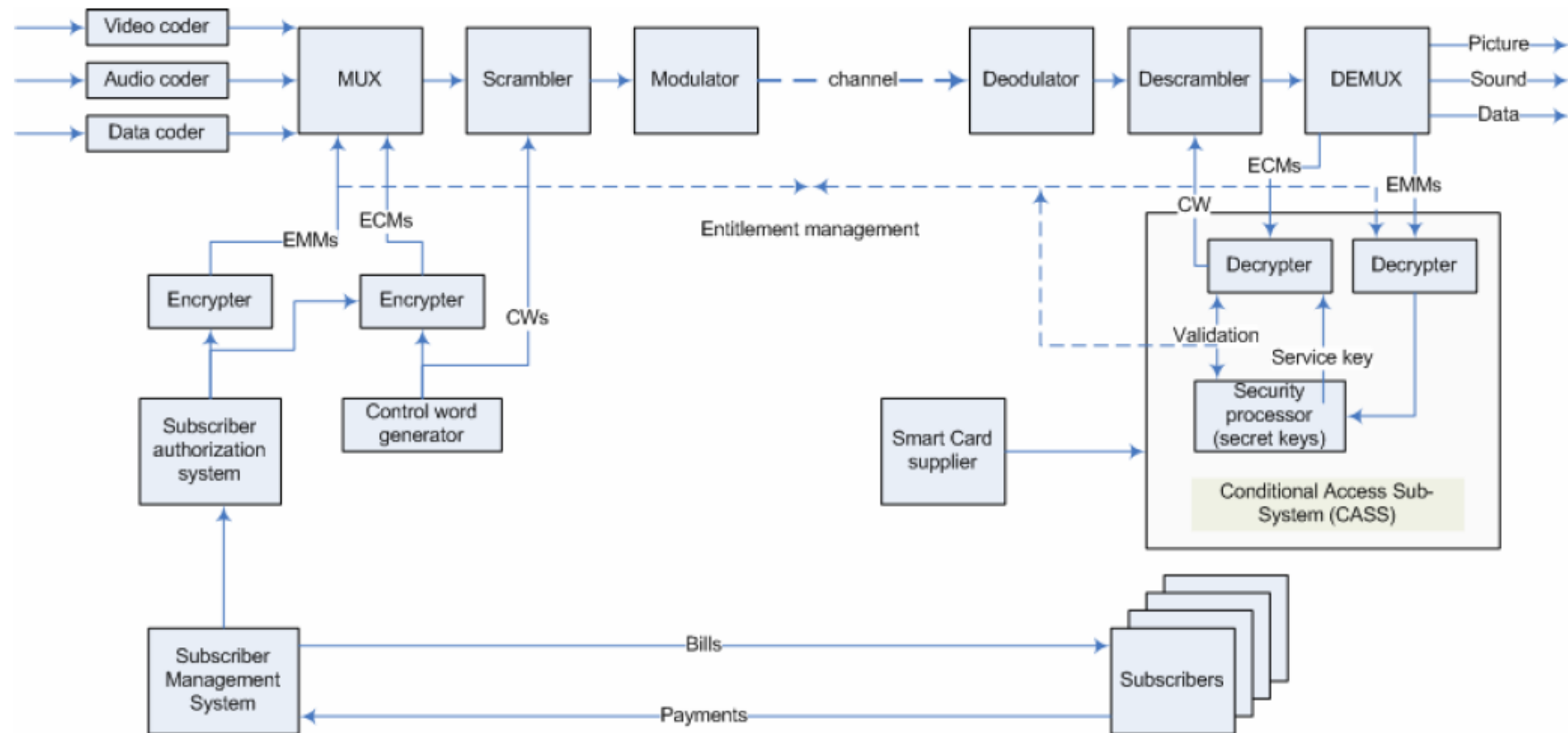
channel adaptation: az átvivő közegtől függően

transmission media: kábel, műhold, földi sugárzás, mobil

demodulation & decoding: MPEG-TS visszanyerése

presentation: függ a készülék, kábel képességeitől

DVB hozzáférés védelem



DVB hozzáférés védelem

DVB-CA (Conditional Access): fizetős adások hozzáférés védelmi mechanizmusa

DVB-CSA (Common Scrambling Algorithm): az adás rejtjelezésének algoritmus

CW (Control Word): vezérlőszó, gyakran változik, ezzel történik az MPEG-TS titkosítása

ECM (Entitlement Control Message): jogosultság vezérlő üzenet, a szolgáltatási kulccsal titkosított CW

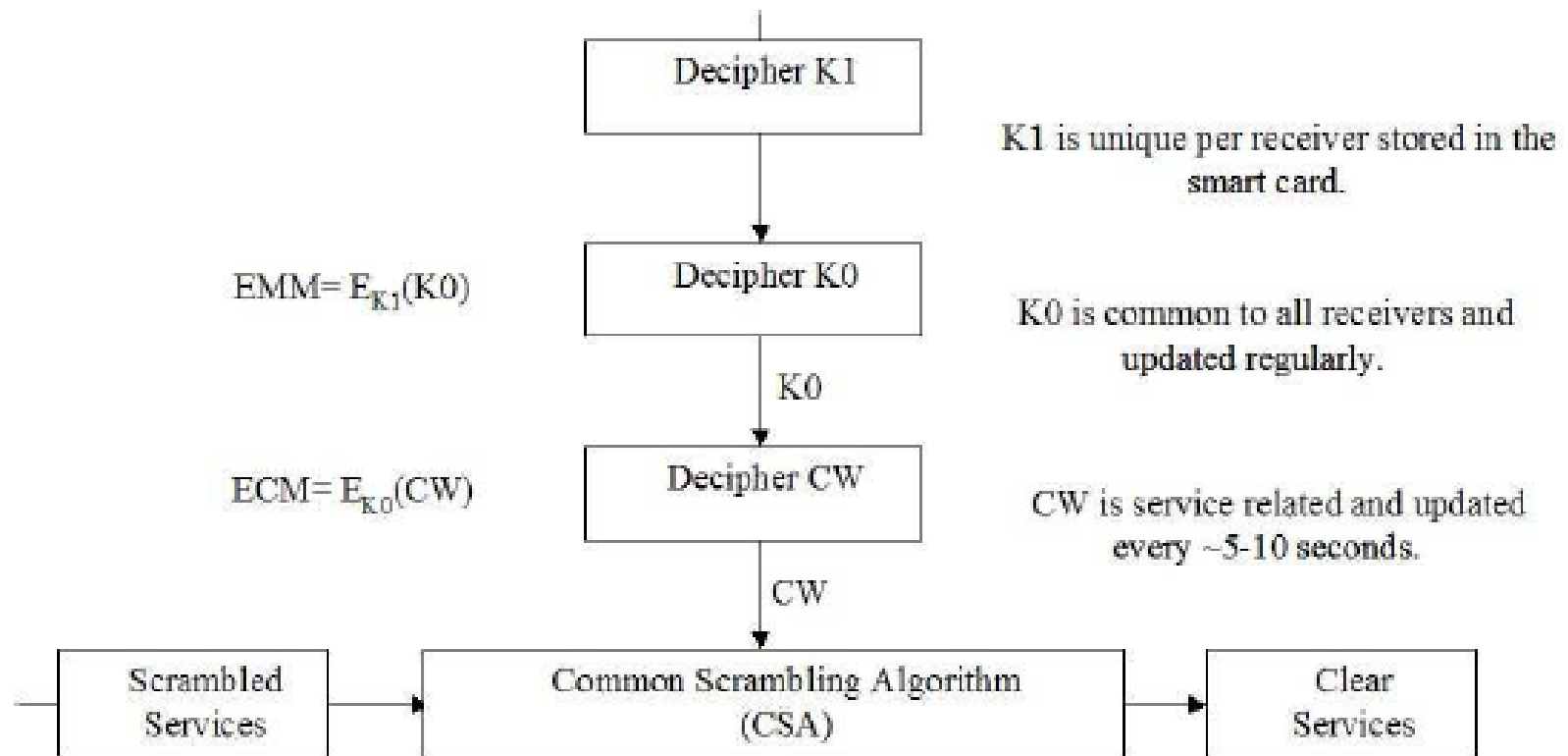
szolgáltatási kulcs: K0, ritkán változik, adott szolgáltatás tekintetében egységes mindenkinek

EMM (Entitlement Management Message): jogosultság kezelő üzenet, a felhasználói kulccsal titkosított szolgáltatási kulcs

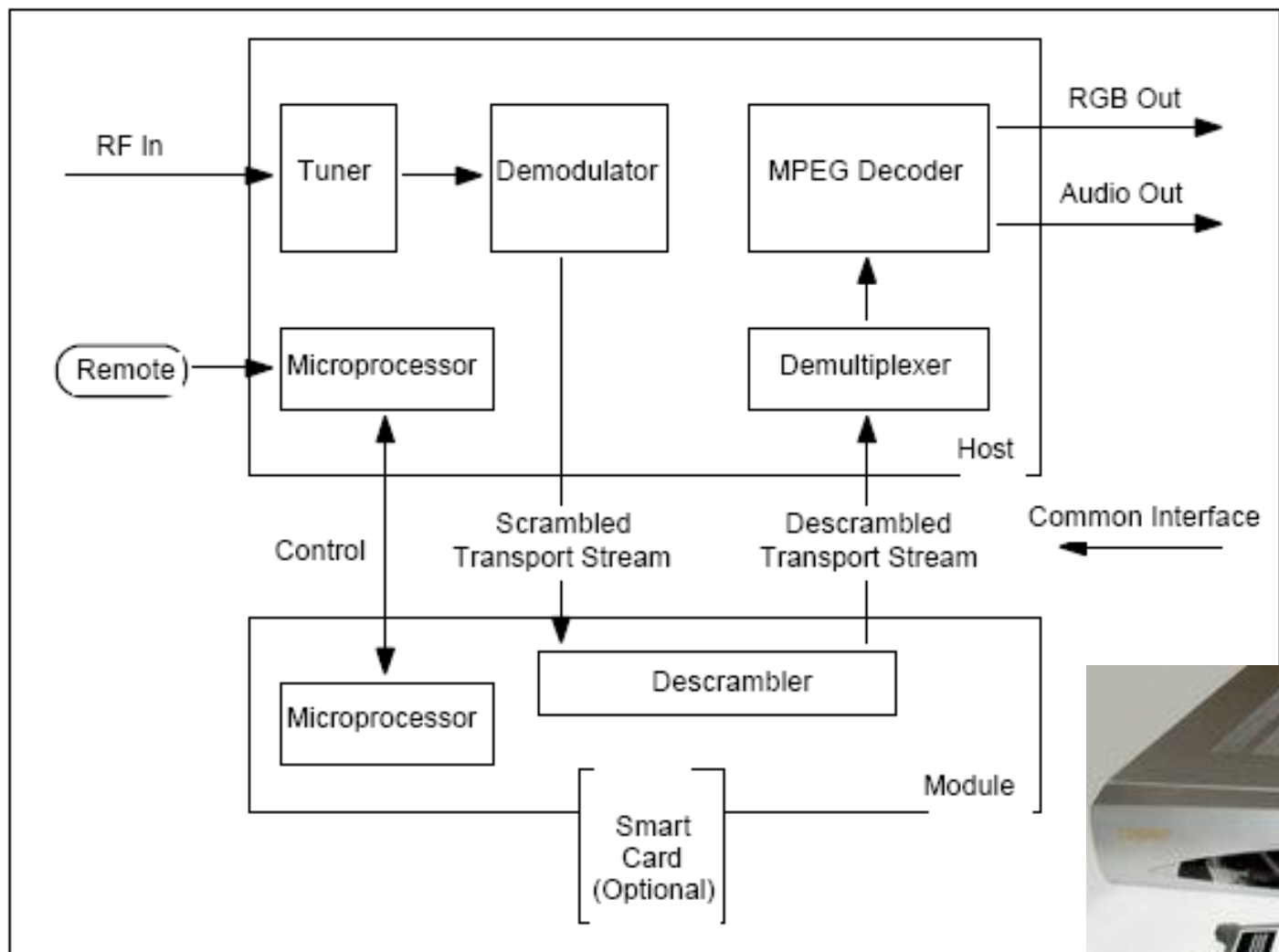
felhasználói kulcs: K1, állandó, készülékenként eltérő (valójában a felhasználók egy csoportja azonos kulccsal rendelkezik)

ECM és EMM az MPEG-TS-be beépül

DVB – Common Scrambling Algorithm



DVB – Common Interface



DVB – Common Interface

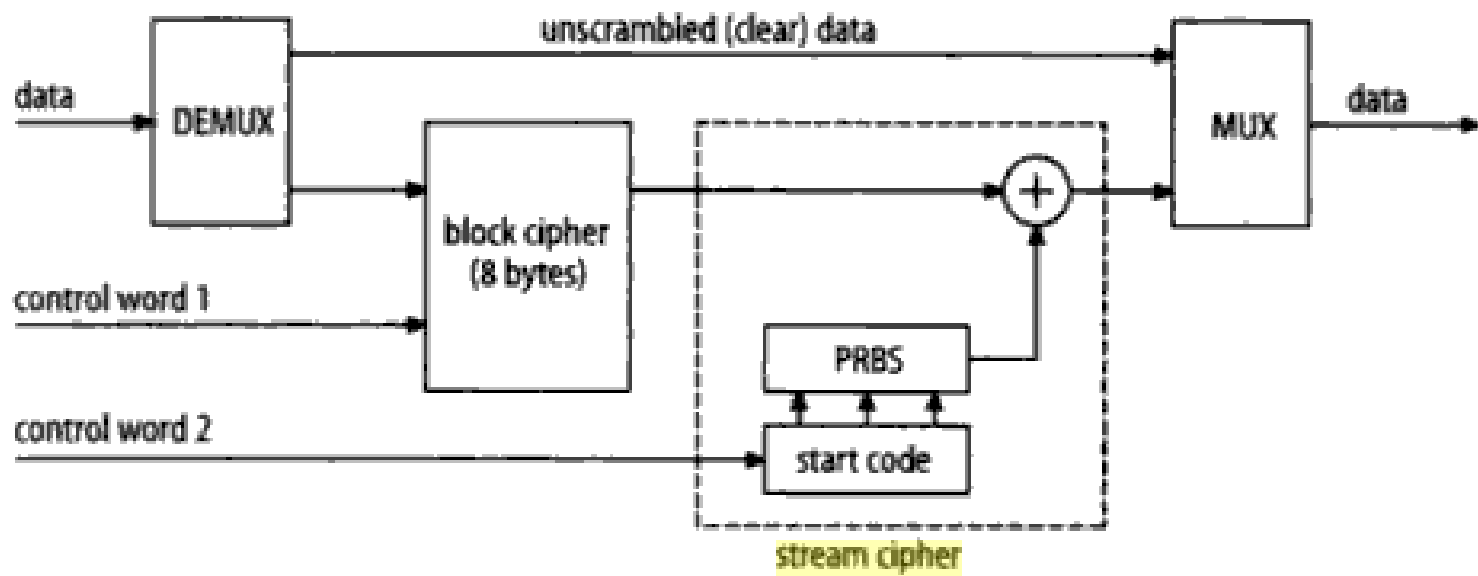
A set-top-box-ról, TV készülékről leválasztásra kerülnek a hozzáférés védelmi funkciók.

Célja: könnyebb szolgáltatóváltás

A Conditional Access alrendszer a PCMCIA szabványnak felel meg és tartalmazhat egy intelligens kártyát a felhasználói kulcs biztonságos tárolására.

A szolgáltatói kulcs és a vezérlőszó meghatározása, valamint a rejtjelezés dekódolása itt történik.

DVB – Common Scrambling Algorithm



ETSI szabvány, csak gyártók számára hozzáférhető

2002-ben megjelent egy szoftver implementációja a DVB-CA-nak

Rövid idő múlva visszafejtették

DVB biztonsági problémák

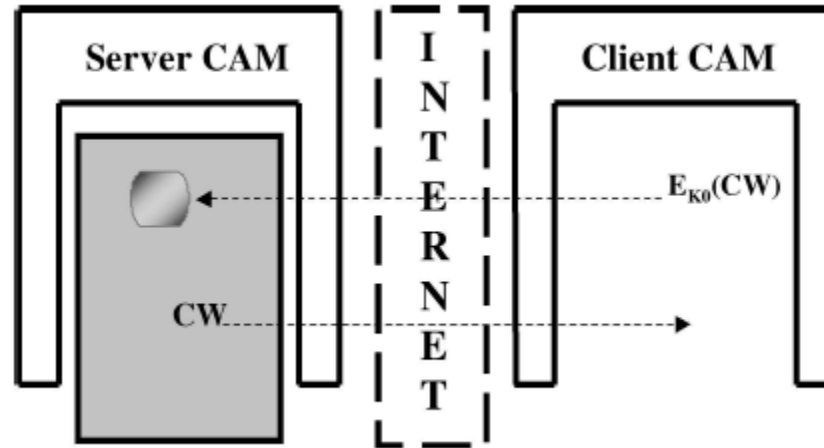
Jobb, mint az analóg hozzáférésvédelem, ahol elég volt egyféle kalózkártya

Itt a kulcsok folyamatos cseréjén és a különböző felhasználói kulcsokon alapul a védelem.

Problémák:

- mindenkihez eljut az adás
- nincs visszafelé irány, nem hitelesíthető a set-top-box, nem tudni, hányan használják ugyanazt a kulcsot
- a set-top-box és a CA modul lehet PC alapú, programok telepíthetők rá

DVB – Card Sharing Attack



www.cardsharingserver.com

<http://tvboom.net/en>

<http://blastoblogja.blogspot.hu/>

Kártyamegosztás ellenszere

Control Word encryption:

EMM dekódolása és a K0 (szolgáltatási kulcs) tárolása a smart card-on történik, de a CW elhagyja a kártyát, mert az MPEG-TS dekódolás nem a smart card-on, hanem a Conditional Access Module-ban (CAM) történik. Ekkor a CW megszerezhető. Ezt akadályozza meg, ha a kártya és a CAM között egy plusz titkosítást alkalmazunk.

DVB CSA3:

Új ETSI szabvány. Nem publikus a működése. „eXtended emulation Resistant Cipher”: hardverben gyors, szoftverben lassú a számítás.

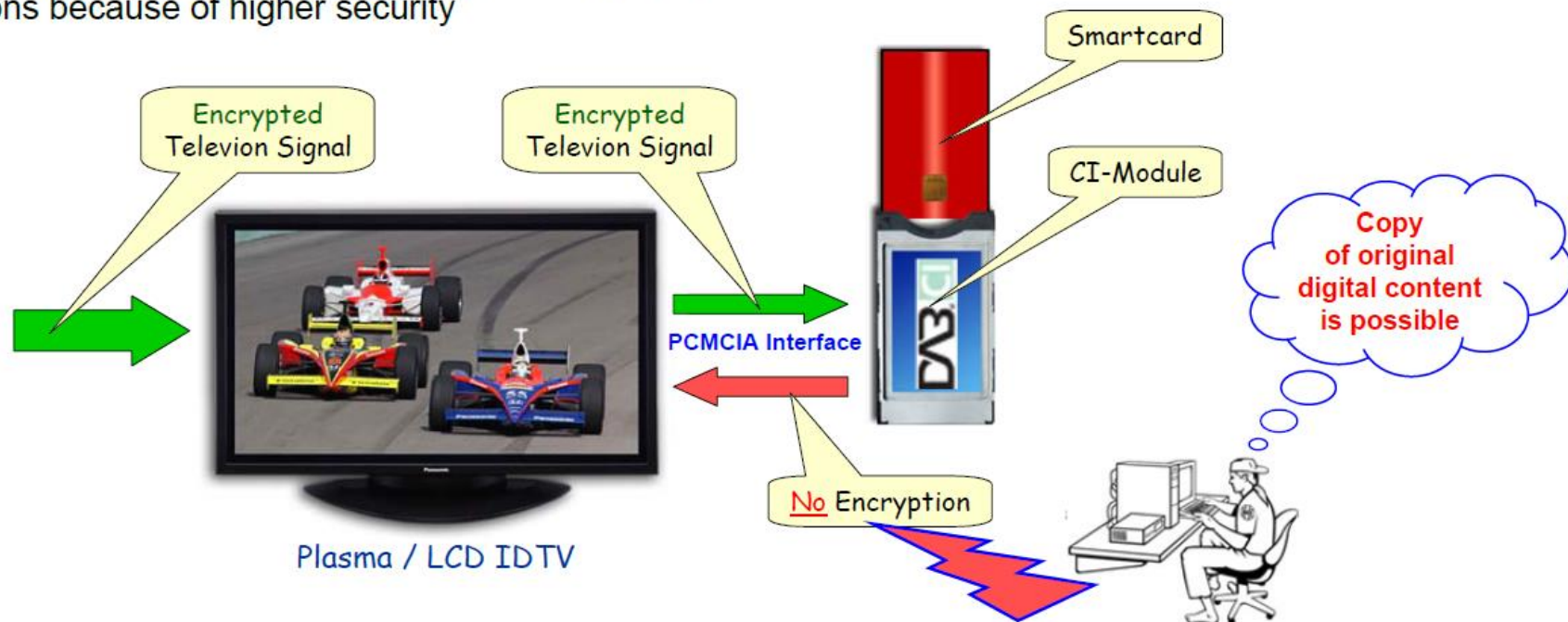
Common Interface Plus (CI+):

Másolásvédelemre is alkalmazható. UPC ilyen CAM-ot ad az ügyfeleinek. Ha a TV is támogatja a szabványt, a CAM és a TV kölcsönösen hitelesítik egymást eszköz tanúsítványok alapján. A CAM és a TV között titkosított adatáramlás van.

DVB CI - First Generation Standard v1



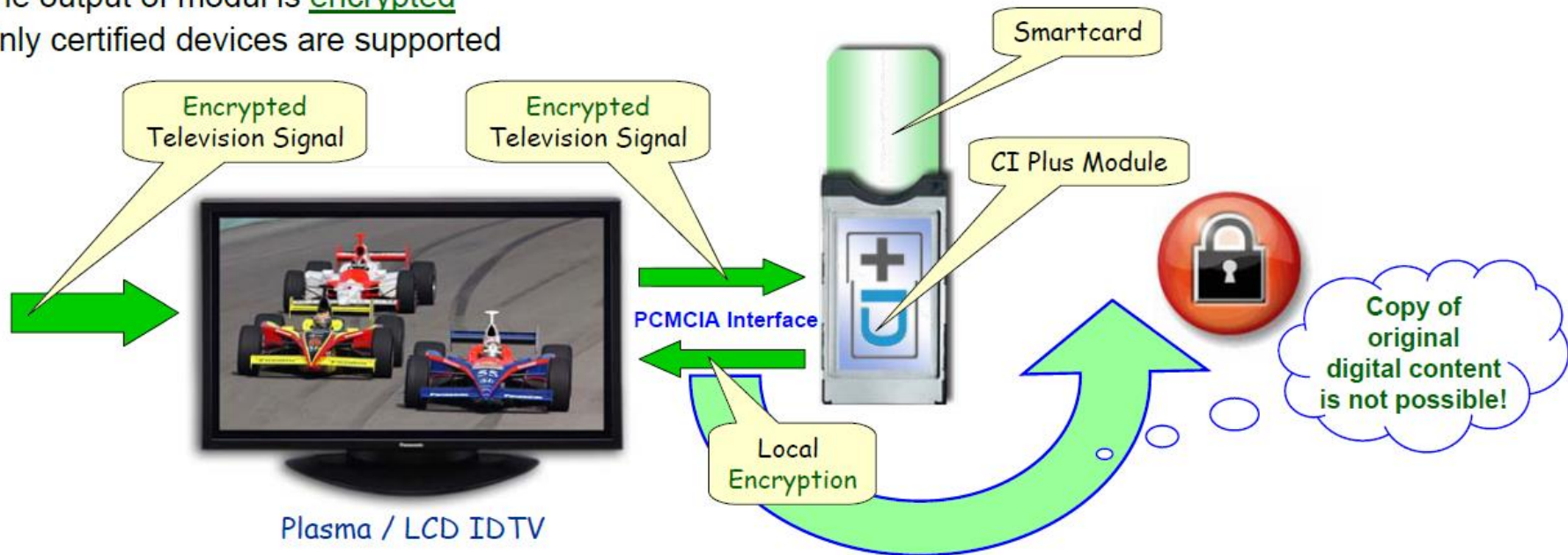
- CI-Module used with smartcard containing key-informationen
- CI-Module remove the encryption of protected content
- The output of CI-Module is unencrypted
- Due to this, most content providers prefer integrated solutions because of higher security



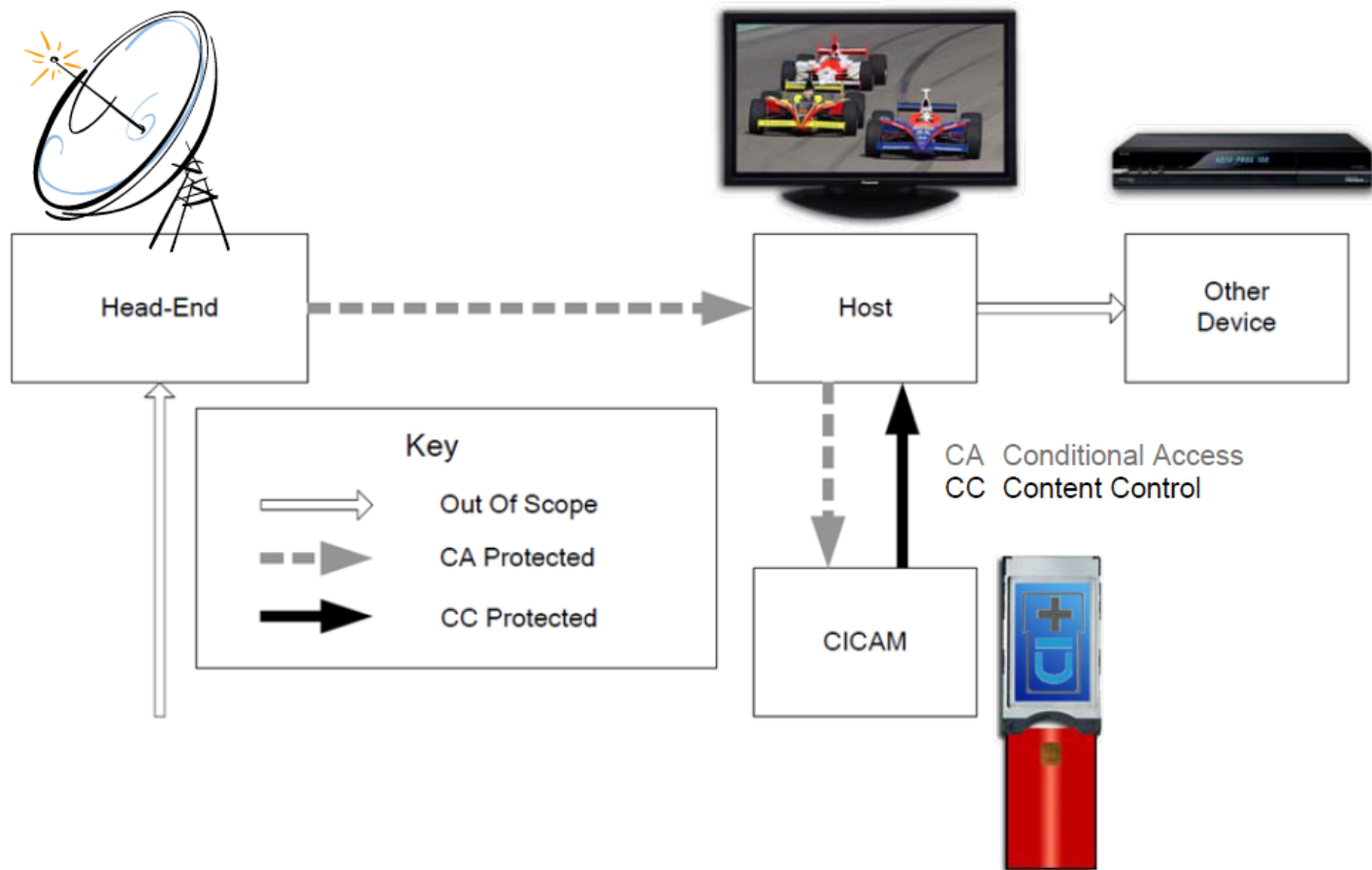
CI Plus - Protection of Content



- Based on existing DVB-CI Standard
- Main requirement: achieving the same level of security as embedded solutions
- CI Plus Modul and Receiver
 - Calculation & Usage of a secure key for content protection
 - Secure, authenticated channel for critical system messages
- The output of modul is encrypted
- Only certified devices are supported



CI Plus - Scope of Protection



CI Plus - System Overview

