Digital Video Broadcasting

Aram Cornelis Zeno Verstegen (aczid)

January 16, 2010

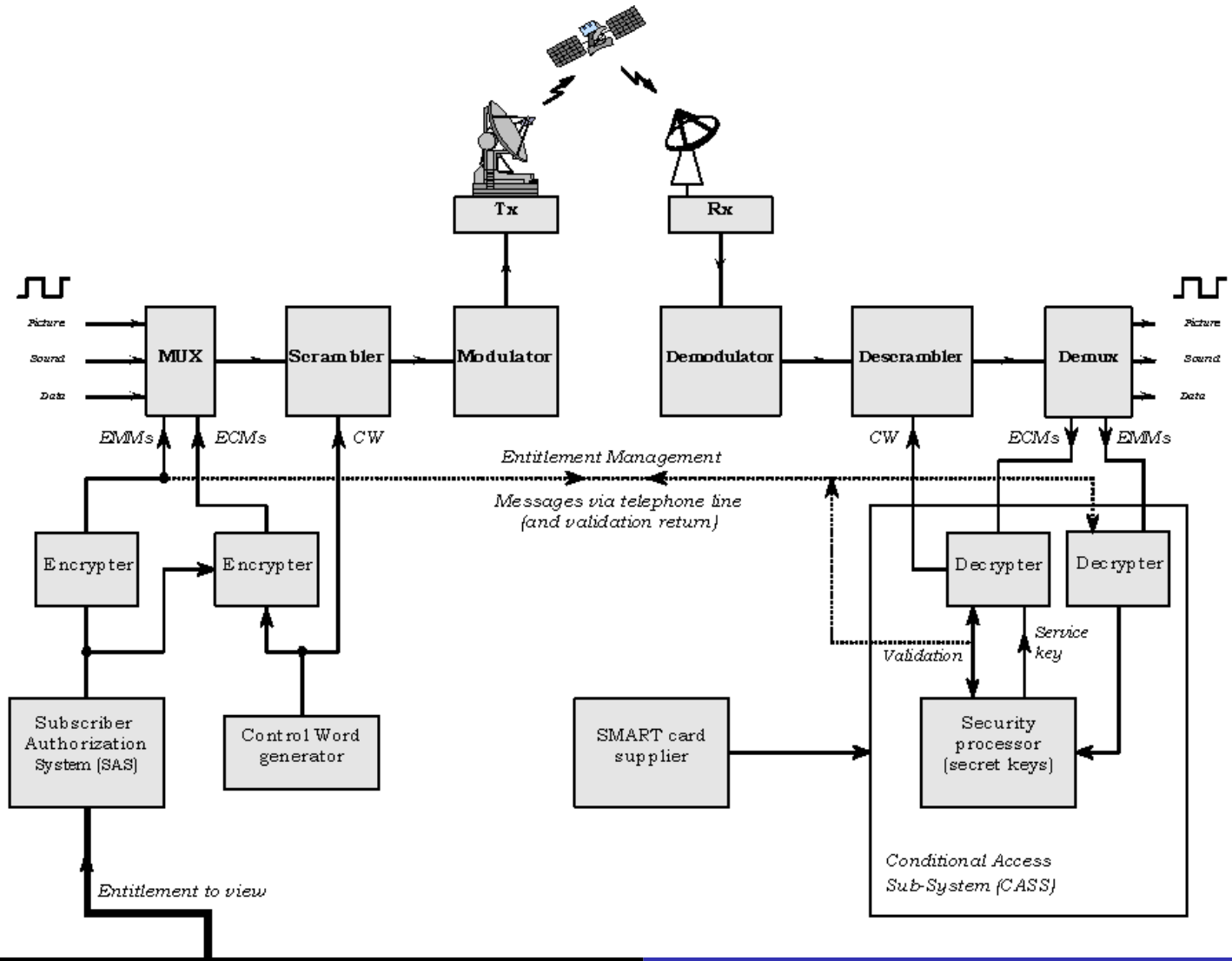
Digital Video Broadcasting

- DVB-T: Terrestrial
- DVB-S: Satellite
- DVB-C: Cable

Content bescherming

- ongecodeerde, ongescramblede gratis uitzendingen (free to air)
- gecodeerde, ongescramblede gratis uitzendingen (free to view)
- gecodeerde, gescramblede betaalde uitzendingen (pay tv)
- gecodeerde, gescramblede betaalde uitzendingen die buiten het standaard-pakket vallen (pay per view)

Content bescherming



Common Scrambling Algorithm

- Gespecificeerd door ETSI
- Door DVB Project geadopteerd als encryptiealgoritme in 1994
- Specificatie was tot 2002 alleen beschikbaar na tekenen NDA (software implementaties verboden)
- Softwareimplementatie FreeDec in 2002

Common Scrambling Algorithm

- Symmetrisch
- Shared key
- 64 bits bytewise block cipher + stream cipher
- Bekende zwakheden

CSA key: Control Word

- Wisselt meerdere keren per minuut
- Wordt *in band* meegestuurd met de MPEG stream in een gecrypte Entitlement Control Message (ECM)
- Decoderen van de ECM vereist een CAM met een smartcard
- Smartcard bevat hetzelfde algoritme en IVs als hetgene dat in de backend gebruikt wordt om de CWs te genereren

CSA authorisatie

- Entitlement Management Message (EMM)
- Wordt *out of band* meegestuurd met de MPEG stream
- Bepaalt welke CAMs mogen proberen de CW te decoderen uit de ECM

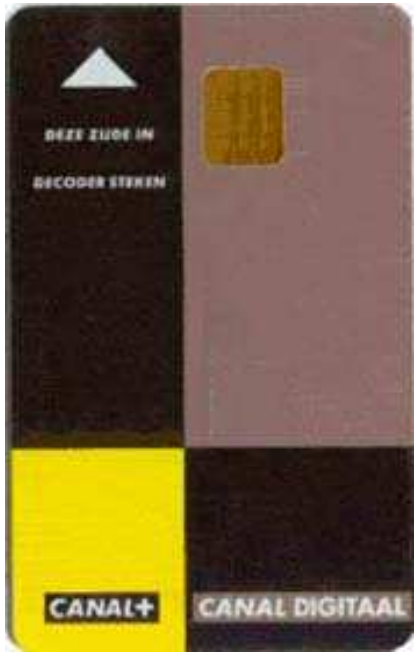
Coderingen

Aanbieder	Type	Fabrikant CAM
KPN Digitenne	DVB-T	Conax
CanalDigitaal	DVB-S	Mediaguard
UPC	DVB-C	Nagravision
Overige aanbieders	DVB-C	Irdeto

Conditional Access Module

Third party, special purpose PCMCIA met ingebouwde smartcard lezer

Smartcards



- CPU met key generatie algoritme
- (E)EPROM met keys
- In staat om eigen keys te updaten
- Gekozen omdat het destijds lastig te reverse engineeren was

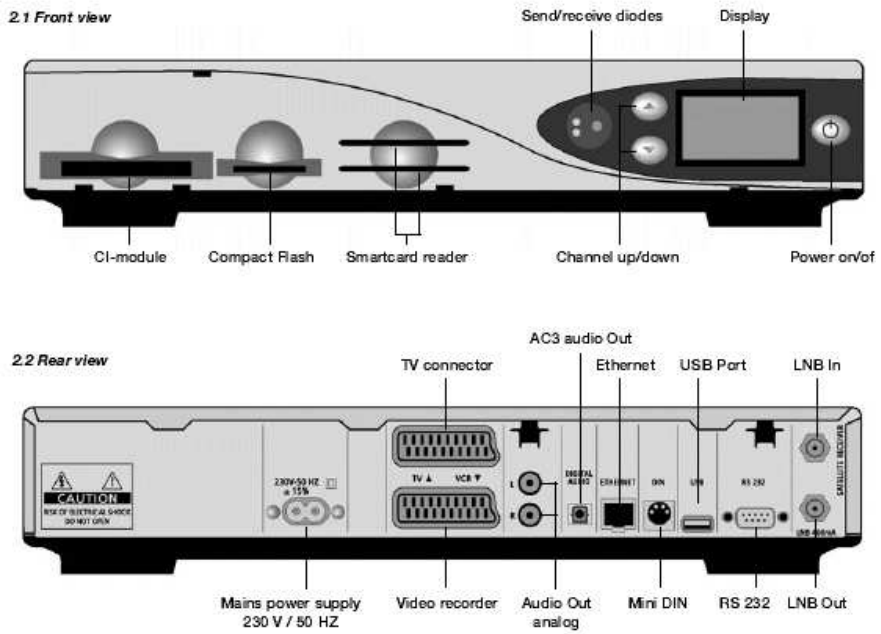
CAM hacks

- CAMs met meerdere ciphers
- Software emulatie van CAM

Smartcard hacks

- Smartcards met meerdere ciphers
- Card files
- Card sharing

Dreambox



- GNU/Linux based PowerPC
- DVB-{C,S,T} uitvoeringen of combinaties
- Softcam emuatie
- PVR

Tegenmaatregelen

- Attacks d.m.v. fake ECMs
- Frequent wijzigende EMMs
- ?

Links

- http://www.dvb.org/about_dvb/
- http://www.duwgati.com/
- http://blog.aczid.nl/