Digitales Fernsehen

Alexander Schmidt
BetaResearch

11. Juni 2002

Themenübersicht

- Analoges und digitales TV in Deutschland
- Digital Video Broadcast – ein europäischer Standard
- Monopol oder Markt – die Verschlüsselung
- Interaktives Fernsehen

Analogtechnik:

- Erste Übertragungen bewegter Bilder 1928
- Seit 1967 Farbfernsehen gemäß PAL-Norm
- Übertragung entweder terrestrisch, per Kabel oder über Satellit
- Feste Bandbreite pro Kanal: 7 bzw. 8 MHz

Vorteile der Digitaltechnik:

- Bessere Kanalnutzung: Bis zu sechs Programme pro 7/8 MHz-Band
- Übertragung beliebiger Metadaten möglich (z.B. Programminformation)
- Flexible Aufteilung der Bandbreite, beliebige Audio-/Video-/Datenströme
- Electronic Program Guides (EPG) und interaktives TV realisierbar
- Wirksamer Schutz der Programminhalte: Conditional Access (Verschlüsselung)

Standardisierung

- Gründung des Gremiums „Digital Video Broadcast" (DVB) im Jahr 1993 in Genf
- Bis 1995: Standardisierung für alle Übertragungsarten: DVB-S, DVB-C, DVB-T
- Weltweite Akzeptanz – bis auf USA und Japan

Einsatz in der Bundesrepublik

- 1996: DF1 (Kirch) als erstes digitales Programm
- Derzeit senden Premiere, ARD und ZDF digital
- Bundesweite Einstellung des analogen Sendebetriebs im Jahre 2010
- In Berlin: Einstellung des analogen terrestrischen Sendebetriebs bis Ende 2003

Wie sieht das konkret aus?

- Über Satellit (Astra, Eutelsat): 60cm-Schüssel erforderlich
- Im Kabel (z.B. nach Bayerischer Kanalbelegungssatzung):

Kanäle	Frequenz	Nutzung
K2 – K4	47 – 68 MHz	analog
S2 – S10	111 – 174 MHz	analog
K5 – K12	174 – 230 MHz	analog
S11 – S20	230 – 300 MHz	analog
S21 – S38	302 – 446 MHz	analog/**digital**
K21 – K39	*470 – 622 MHz*	*analog /digital*
K40 – K39	*622 – 862 MHz*	*analog /digital*

(bei entspr. Netzausbau)

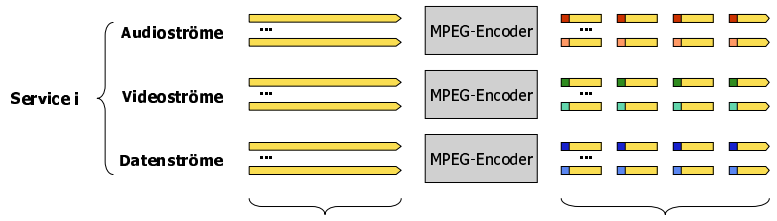
Premiere: S27 – S31, S33 • ZDF: S32 • ARD: S34, S36

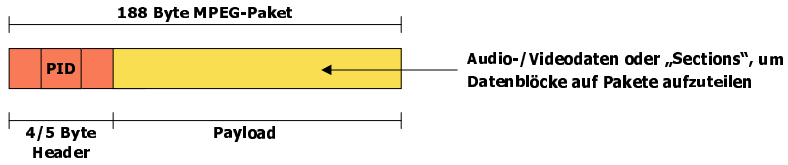
- Terrestrisch: Bisher nur Feldversuche, z.B. in Berlin
- Spezielles Empfangsgerät (Digitalreceiver, „Set Top Box") notwendig

DVB

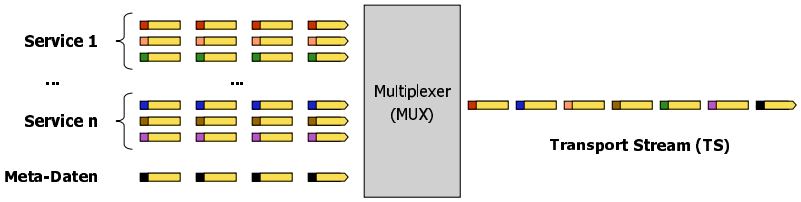
- Standardisiert Codierung, Übertragung und Metainformationen
- Videocodierung basiert auf MPEG 2, Audiocodierung auf MPEG 1 Layer 2
- Terminologie:
  - Fernsehkanal heißt bei DVB „Service", bei MPEG „Program"
  - Sendungen sind „Events"
- Services können aus beliebigen Audio-, Video- und Datenströmen bestehen, z.B.
  - 4:3-Format, 19:9-Format
  - Mehrere Sprachen, Dolby Surround
  - Metainfo, beliebige Daten, Videotext

Encoding





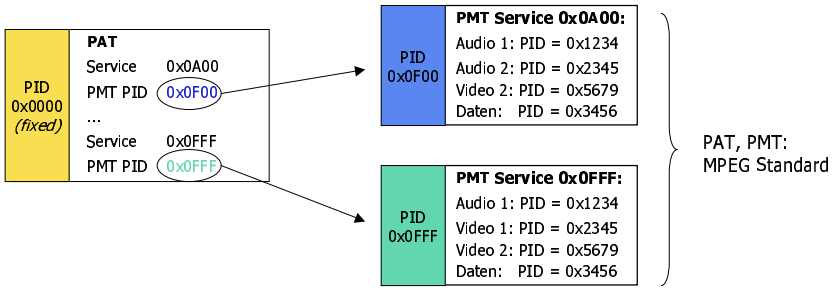
Multiplexing



- Ein Transport Stream überträgt 38 Mbit/s
- Entspricht einem Satelliten-Transponder, Modulation durch QPSK
- Im Kabel durch QAM-Modulation innerhalb eines 8 MHz-Kanals
- Auf einen Transport Stream wird physikalisch getunt

Übertragung von Meta-Information (1)

- Welche Pakete gehören zu welchem Service?
- Verknüpfung durch **PSI- Tabellen** (Program Specific Information):
  - Pro Transport Stream eine Program Association Table (PAT)
  - Pro Service eine Program Map Table (PMT)



- weitere CA-Tabellen folgen...

Übertragung von Meta-Information (2)

- DVB definiert weitere fernsehspezifische Tabellen (Service Information):
- Service Description Table (SDT, PID = 0x0011). Enthält für alle Services eines Transport Streams z.B.:

  Service-Typ, Service-Name, Name des Anbieters, Verschlüsselungssystem, etc

- Event Information Table (EIT, PID = 0x0012). Beschreibt pro Transponder z.B.:

  Service ID, Startzeit, Endzeit, Kurztitel, Inhaltsangabe, Jugendschutz, Genre, Sprache, folgender Event, nächste Startzeit, etc.

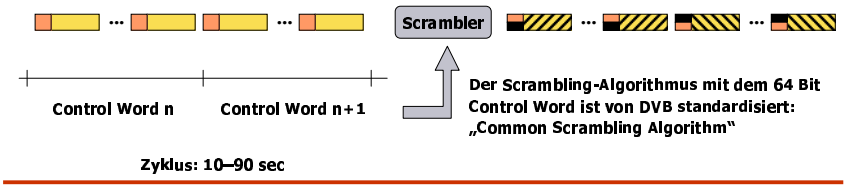
- Bouquet Association Table (BAT): Beschreibt die über TS hinweg die Zusammengehörigkeit von Services, z.B. alle Services von „ARD digital" (3. Programme)

Übertragung von Meta-Information (3)

- Weitere Tabellen:
  - Übertragungsdaten des Netzwerks, Sat-Parameter: Network Information Table (NIT)
  - Transport von Zeitbasen: Time and Date Table (TDT), Time and Offset Table (TOT)
  - Aktualisieren von Events: Running Status Table (RST)
  - Überschreiben von Tabellenteilen: Stuffing Table (ST)
- Verlinkung über Transport Streams hinweg möglich
- Tabellen bestehen aus Sequenzen von Deskriptoren: [tag, length, data]
- DVB gibt nur vor, welcher Deskriptor in welcher Tabelle zulässig ist!
- *Verwendung* der SI-Tabellen von DVB ist Sache der Broadcaster

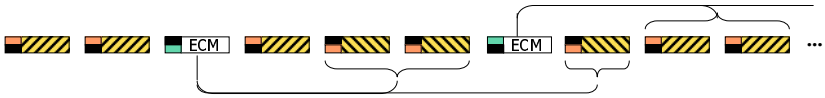
Conditional Access (CA)

- Anwendung hauptsächlich für PayTV, aber auch für Business-TV
- Anwendung auch zur Einhaltung von Sendelizenzen („Grundverschlüsselung"):
  - Lizenz pro Land, Satellitensignal macht nicht an Ländergrenzen halt
  - Jeder Einwohner erhält einen Schlüssel, wie z.B. in Österreich
  - Weil ARD/ZDF nicht verschlüsseln (können), dürfen sie die WM nicht digital über Satellit ausstrahlen ⇒ 100000 ausschließlich digital über Sat versorgte Haushalte, die nicht Premiere-Kunden sind, schauen in die Röhre
- Prinzip: Audio-, Video- und Datenströme werden *gescrambled*



Descrambling (1)

- Das Control Word muß mit ausgestrahlt werden
- Dazu wird es in **Entitlement Control Messages** (ECM) verpackt...
- ...die einen eigenen Datenstrom in jedem verschlüsselten Service bilden...
- ...und deren PID von der Program Map Table des Service signalisiert wird.



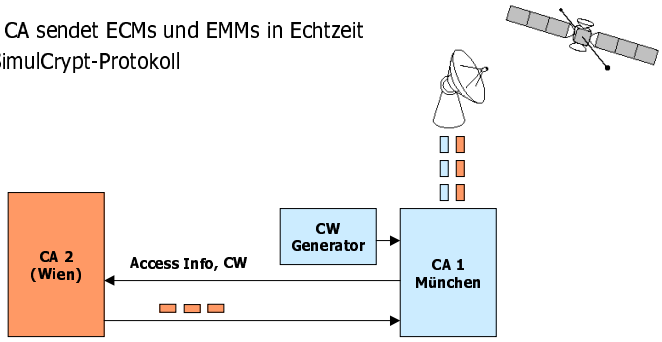
- Offensichtlich kann man die ECM nicht unverschlüsselt ausstrahlen
- Die Information, um ECMs zu entschlüsseln, kann in **Entitlement Management Messages** (EMM) ausgespielt werden
- Pro Transport Stream und Anbieter wird der PID des EMM-Stroms in der Conditional Access Table (CAT) signalisiert

Descrambling (2)

- DVB standardisiert im wesentlichen nur:
  - die Länge des CW: 64 Bit
  - den Common Scrambling Algorithm
- Aber nicht, wie das CW in der ECM verschlüsselt ist sowie wann und auf welche Weise die Box durch EMMs den Schlüssel für ECMs erhält
- Beispiel **Betacrypt:**
  - Das sichere Element ist eine Smart Card, die in der Box steckt und keine Schlüssel preisgibt
  - Das Control Word ist in der ECM unter einem Offset Key verschlüsselt
  - Möchte ein Kunde einen Kanal (Pay-per-Channel) oder eine Sendung (Pay-per-View) sehen, erhält seine Smart Card „over Air" das entsprechende „Produkt"
  - Mit dem passenden Produkt kann die Karte den Offset Key entschlüsseln, der unter einem weiteren Schlüssel verschlüsselt übertragen wird.
  - Alle Produkte, Schlüssel und sonstigen Parameter können vom Head End für jede Karte einzeln modifiziert werden

SimulCrypt

- Verschlüsselung *eines* Services mit *mehreren* CA-Systemen
- Beispiel: Premiere über Astra ist mit dem deutschen und österr. CA-System verschl.
- Service wird mit *einem* CW verschlüsselt, das mit *mehreren* ECMs (und EMMs) übertragen werden muß
- Entferntes CA sendet ECMs und EMMs in Echtzeit über das SimulCrypt-Protokoll

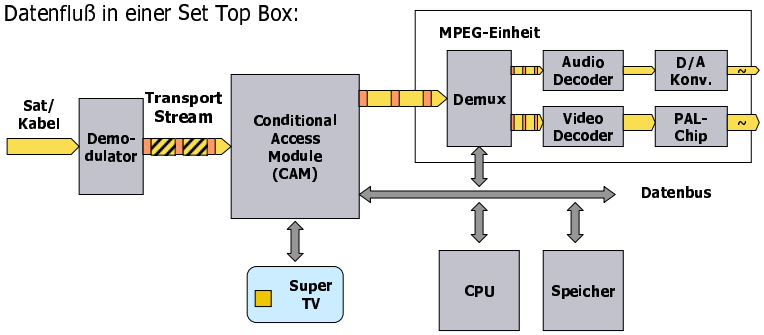


CA Systeme

- Riesiger TV-Markt, der bis ca. 2010 mit CA-Systemen versorgt werden muß
- Jeder Betreiber verwendet ein anderes Conditional Acces System: Betacrypt (Premiere), Viaccess (Frankreich), Mediaguard (UK), ...
- Bei Betacrypt: mehrere Betreiber weitgehend unabhängig voneinander auf einer Karte möglich (z.B. ORF/Premiere)
- Jedoch sind dann Lizenzgebühren fällig, zudem besteht gewisse Abhängigkeit
- d-box-Population (2,5 Mio): CA-System fest eingebaut $\Rightarrow$ Monopol von Kirch
- Alle Betreiber sind sich einig: kein Zuschauer soll Boxen stapeln müssen
- Lösung: das CA-System einer Box austauschbar machen: **Common Interface**

Common Interface

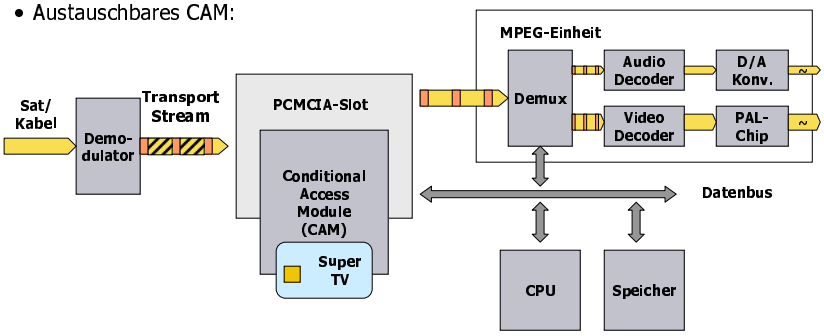
- Datenfluß in einer Set Top Box:



- Das CAM filtert alle notwendigen Nachrichten, um den gewünschten Service entschlüsseln zu können
- Das CAM ist immer proprietär
- Arbeitet zumeist mit einer Smart Card, die die kryptographischen Elemente enthält

Common Interface (2)

- Austauschbares CAM:



- Sehr aufwendige Lösung, verteuert die Boxen
- Kunde kauft eine beliebige Box und erhält vom Betreiber CA-Modul und Karte

Voraussetzungen

- Im MPEG-Strom können beliebige Daten übertragen werden
- Boxen verfügen über einen leistungsfähigen Prozessor (ca. 50-100 MHz)
- Download von Applikationen für interaktives Fernsehen möglich
- Beispiele:
  - Komfortable EPGs (Electronic Program Guides)
  - Begleitende Applikationen (Quiz, Spiele, Informationen)
  - Internetzugang in „walled gardens"
- Mit Rückkanal auch
  - Homebanking, Homeshopping
  - E-Mail, Chat, vollständiger Internet-Zugang
  - Marktanalysen, Umfragen
- Aber: TV ist „lean backward activity"

Markt

- Bis heute nur proprietäre APIs der Boxen: betanova (Kirch), OpenTV, Media Highway
- SDKs kosten viel Geld, zudem Abhängigkeit vom Hersteller
- Daher: Vorwurf eines weiteren Monopols neben dem CA-System (vertikaler Markt)
- Seit 1998 wird vom DVB-Gremium ein universelles API standardisiert:
  die **Multimedia Home Platform** (MHP)
- MHP standardisiert die Umgebung, die Applikationen in der Box vorfinden
- Ziel: Eine Applikation für alle Boxen
- Derzeit ist MHP 1.0.2 aktuell, MHP 1.1 in Vorbereitung
- Drei verschiedene Profile:
  - Enhanced Broadcast (lokale Interaktivität, kein Rückkanal)
  - Interactive Broadcast (Interaktivität mit Rückkanal)
  - Full Internet Access (volle Internetfunktionalität)

MHP

- MHP standardisiert APIs, Protokolle, Datenformate und Box-Eigenschaften
- MHP basiert auf Java
- MHP 1.0.2 definiert unter anderem:
  - Rahmen für Applikationen: Signalisierung, Starten, Stoppen, Suspend, Resume, Ressourcen
  - APIs für Tuning, Decoding, Demuxing
  - für den Zugriff auf alle Tabellen und Metadaten
  - für die Bild- und Tondarstellung
  - zur Speicherung von Applikationen und Daten (Persistant Storage)
  - für den Zugriff auf das Conditional Access System
  - für die Kommunikation über den Rückkanal
  - Definiton von Widgets mit austauschbarem Look&Feel
  - Zertifizierung von Applikationen, Permission Request Files
  - Verschlüsselung für den Rückkanal
  - Datenformate für Audio, Video, Bilder

- Mit MHP 1.1 kommen hinzu:
  - Interface für PlugIns, die weitere Datenformate darstellen können
  - DVB-HTML: Videoinhalte in HTML-Seiten, ECMA-Script, Eventmodell
- Technisch basiert das MHP-API auf
  - PersonalJava 1.1, reduziert um einige Widgets (Fenster etc.)
  - Java Media Framework 1.0 (JMF): API für zeitabhängige Medien (javax.media)
  - JavaTV: API für Fernsehfunktionalität (Zappen, Bild, Ton, FB-Kommandos, Meta-Info), enthält auch die Basisklasse aller Apps: Xlet, XletContext (Package javax.tv)
  - HAVi 1.1: Widgets (in org.havi)
  - DAVIC (org.dvb): Repräsentation von MPEG-Objekten (TS, PES, Tabellen, PSI-/SI-Info), Filtering, CA-Zugriff, Resource Notification
  - org.dvb: DVB-spez. Tabellen, Signalisierung von Applikationen, User Preferences, Objektkarussel von DSM-CC
- Viele weitere Standards: IP-Protokolle, HTTP, JPEG, GIF, XML, X.509, ...

Beurteilung

- MHP ist ein sehr großer Standard, viele Redundanzen, viele Sachen völlig unbehandelt (z.B. die Behandlung von Ressourcenkonflikten)
- Erfordert mindestens 100 MIPS, 16 MB RAM, 8 MB Flash
- Implementierung ist aufwendig, Interoperabilität derzeit noch offen
- Für Consumer-Geräte gelten andere Qualitätskriterien
- Vertikale Märkte haben Vorteile. Problemraum ist jetzt
  Box-Hersteller × Broadcaster × Applikationsprovider
- API zu kompliziert (> 1000 Klassen) für einfache Applikationen
- DVB-HTML (in MHP 1.1) ist der bessere Ansatz, aber wozu dann die APIs?
- Vielleicht kommt abgespecktes MHP, derzeit unter dem Decknamen MHP Car

Beurteilung

- Wird sich PayTV in Deutschland durchsetzen?
  - Es hat sich bereits durchgesetzt, seit über 30 Jahren
- Wird sich privates PayTV in Deutschland durchsetzen?
  - Ja, wenn es zielgruppenspezifische Angebote gibt (neben Fußball, F1)
  - Mit dem Übergang zur Digitaltechnik kommt automatisch die Verschlüsselung
  - Das Endstadium werbefinanzierter Sender ist wenig attraktiv für den Zuschauer
- Wird sich interaktives Fernsehen durchsetzen?
  - Ja, wenn die Technik den Bedürfnissen von Wohnzimmergeräten entspricht
  - Home Shopping im TV funktioniert blendend!