Digital Rights Management

Copy Protection und DVB CPRM

Dietrich Sauter
Öffentlichkeitsarbeit

Beiträge von Dr. Norbert P. Flechsig, Dr. Rainer Schäfer, Robert Sedlmeyer

§ 51 UrhG Zitatrecht

Zulässig ist die Vervielfältigung und öffentliche Wiedergabe eines veröffentlichten Werkes zum Zwecke des Zitats, sofern die Nutzung in ihrem Umfang durch den besonderen Zweck gerechtfertigt ist. Zulässig ist die insbesondere, wenn:

Einzelne Werke in wissenschaftlichen Werken Stellen eines Werkes in einem selbständigen Sprachwerk

Einzelne Stellen eines Musikwerkes in selbständigen Musikwerk genutzt werden.

§ 53 Abs. 1 UrhG – Vervielfältigung, insbesondere Donwload aus Internet nur von rechtmäßiger Quelle:

Zulässig sind einzelne Vervielfältigungen eines Werkes durch eine natürliche Person zum privaten Gebrauch auf beliebigen Trägern, sofern sie weder unmittelbar noch mittelbar Erwerbszwecken dienen, soweit nicht zur Vervielfältigung eine offensichtlich rechtswidrig hergestellte oder öffentlich zugänglich gemachte Vorlage verwendet wird.“

(2) Zulässig ist, einzelne Vervielfältigungsstücke eines Werkes herzustellen oder herstellen zu lassen

1. zum eigenen wissenschaftlichen Gebrauch, wenn und soweit die Vervielfältigung zu diesem Zweck geboten ist und sie keinen gewerblichen Zwecken dient

2. zur Aufnahme in ein eigenes Archiv, wenn und soweit die Vervielfältigung zu diesem Zweck geboten ist und als Vorlage für die Vervielfältigung ein eigenes Werkstück benutzt wird, ...

§ 52b UrhG Wiedergabe an elektronischen Leseplätzen in Bibliotheken

Wiedergabe veröffentlichter Werke ausschließlich in den Räumen öffentlich zugänglicher Bibliotheken, Museen und Archive ohne Erwerbszweck an eigenen Leseplätzen zur wissenschaftlichen Forschung und für private Studien.

Vergütungspflicht via Verwertungsgesellschaft.

§ 53a UrhG – Kopienversand auf Bestellung

Zulässig ist auf **Einzelbestellung die Vervielfältigung** und Übermittlung einzelner in Zeitungen und Zeitschriften erschienener Beiträge sowie kleiner Teile eines erschienenen Werkes im Weg des Post- oder Faxversands durch öffentliche Bibliotheken, sofern die Nutzung durch den Besteller nach § 53 zulässig ist.
Die Vervielfältigung und Übermittlung in sonstiger elektronischer Form ist ausschließlich als grafische Datei und nur dann zulässig, wenn der Zugang zu den Beiträgen oder kleinen Teilen eines Werkes den Mitgliedern der Öffentlichkeit nicht von Orten und zu Zeiten ihrer Wahl mittels einer vertraglichen Vereinbarung ermöglicht wird.

Vergütungspflicht via Verwertungsgesellschaft.

§ 106 Abs. 3 UrhG wird ergänzt:

(3) Nicht bestraft wird, wer Werke oder Bearbeitungen oder Umgestaltungen von Werken nur in geringer Zahl und ausschließlich zum eigenen privaten Gebrauch oder zum privaten Gebrauch von mit dem Täter persönlich verbundenen Personen vervielfältigt oder an solchen Vervielfältigungen teilnimmt (§§ 26, 27 des Strafgesetzbuchs).
Satz 1 gilt nicht für die Vervielfältigung von Computerprogrammen (§ 69a).

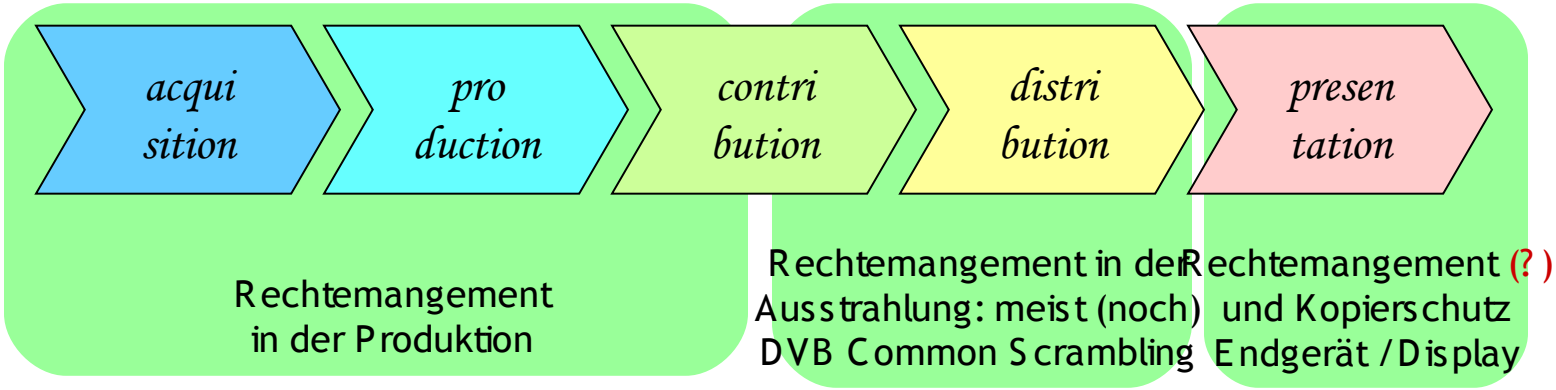
Begründung:

Strafausschließungsgrund soll Bagatellfälle ausnehmen.
Private Endnutzer begehen Urheberrechtsverletzungen - zwar nicht zu billigen, aber:
„Grenzüberschreitungen“ zu kriminalisieren ist rechtspolitisch nicht opportun.

Die "Schulhöfe" sollten nicht kriminalisiert werden.

Produktions- und Verteilkette

Schnitt-stellen:	HD-SDI (single, dual) IT-Welt, FireWire	HD-SDI (single, dual) IT-Welt (IP, FibreChannel)	HD-SDI, ASI, STM, ...	ASI, USB, FireWire	SCART, Component, HDMI, DVI, ...



Kopierschutz: Verschlüsselung auf digitaler Schnittstelle -> HDCP auf HDMI
Rechtemanagement: Kontrolle der Verschlüsselung

Digitale Schnittstelle als Grundlage für den Kopierschutz

Varianten von DVI und HDMI

„Integrated" „Digital" „Analog"

	VI-I Single Lin	DVI-I Dual Lin	DVI-D Single Li	DVI-D Dual Lin	DVI-A	HDMI Type A	HDMI Type B
	Digital Display Working Group (Intel, Compaq, Fujitsu, Hewlett Packard, IBM, NEC, Silicon Image)					Hitachi, Matsushite Electric Ind. (Panasonic), Philips, Sony,, Thomson (RCA), Toshiba, Silicon Image	
	Http://www.ddwg.org DVI 1.0 Specification					www.hdmi.org HDMI 1.2 Specification	
	T.M.D.S. (transition optimized 8 Bit payload on 10 Bit frames)					T.M.D.S.	
	RGB 8 bit	RGB 8 bit dual only: RGB, bis 16 Bit	RGB 8 bit	RGB 8 bit dual only: RGB, bis 16 Bit		RGB 8 bit YCrCb 8 Bit CrCb 4:2:2 12B	RGB 8 bit YCrCb 8 Bit CrCb 4:2:2 12 Bit
	Min. 25 MHz					Min. 25 MHz	
Takt	165 MHz	No limit spec.	165 MHz	No limit spec.		165 MHz	No limit spec.
Audio	-	-	-	-	-	in Austastung	in Austastung
Remote						CEC Remote control	CEC Remote control
Steckergröße	39,6x15,1 mm					13,9 x 4,5 mm	21,2 x 4,5 mm
Pins/benutzt	29/23	29/29	24/17	24/23	29/11	19/18	29/27
davon analog RGB H/V	6	6	-	-	6	-	-

Häufig: PCs Häufig: STBs Nicht spec. Kabel

Motivation, Parameter für HD ready

Motivation für Hersteller, PayTV Operator, HD Promoter

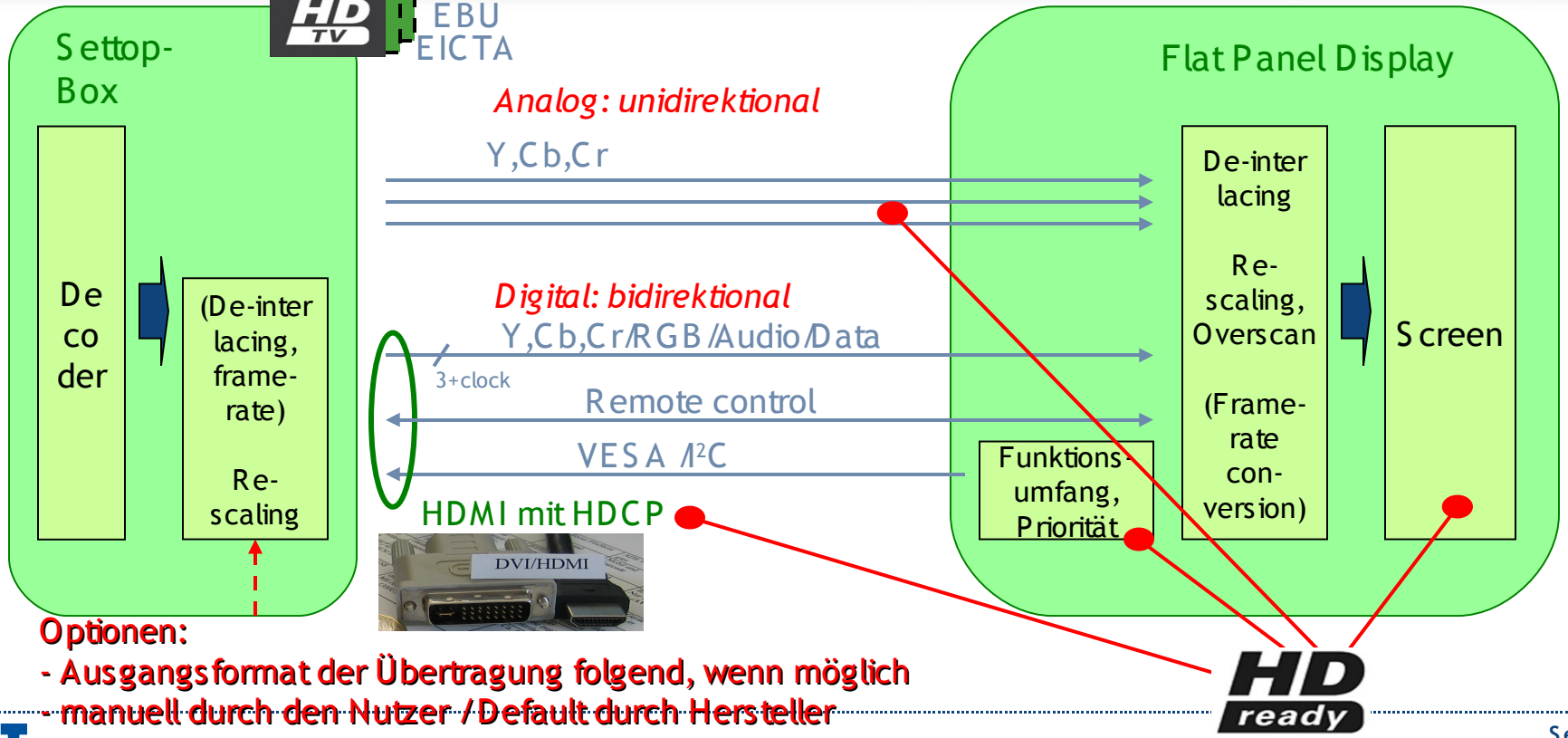
- Sicherung, dass Displays „kopiergeschützte“ Signale akzeptieren (meist einziges Ausgangssignal der STB bei PayTV und HDTV DVD)
  -> HDCP mandatory
- Sicherung, dass neue teure Flat Panel Displays bei HD nicht „schwarz“ bleiben
  -> müssen 720/50p and 1080/25i „unterstützen“
- Garantie minimaler Auflösung (evtl. Auflösung <> „Qualität“!)
  -> minimal 720 Zeilen

Interfaces

• digital (DVI und HDMI mit Copy Protection HDCP !)	mandatory
• SD Scart	recommended
• analog	mandatory

Derzeit etwa 20% der neu verkauften Geräte (Umsatz ?)

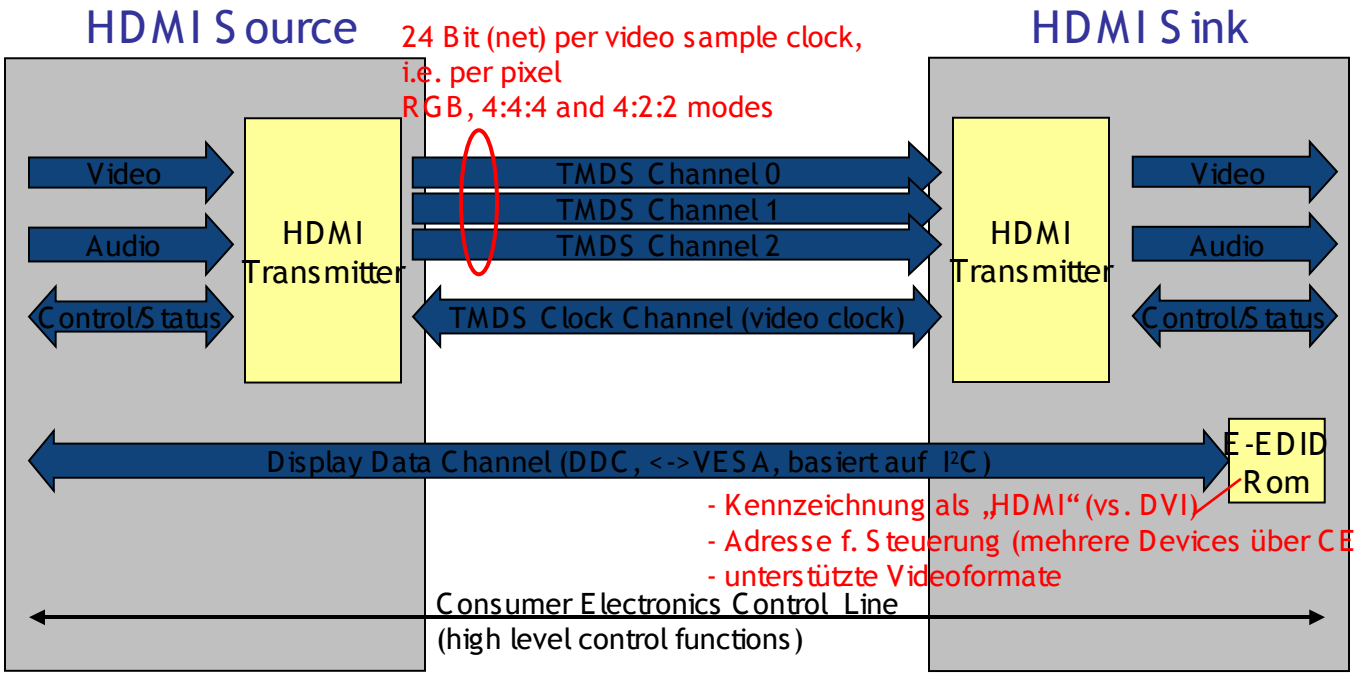
Settop-Box und Display



Optionen:

- Ausgangsformat der Übertragung folgend, wenn möglich
- manuell durch den Nutzer / Default durch Hersteller

HDMI-Interface



E-EDID: VESA Enhanced Extended Display Identification Data Stand

Display Data Channel (DDC)

E-EDID: Enhanced Extended Display Identification Data Standard

- Identifikation der Parameter/Fähigkeiten der Senke (Display)
  - > Video-Formate
  - > Audio-Kanäle
- Identifikation als „HDMI“-Senke (Gegensatz zu „nur“ DVI)
- Adresse für Selektion einzelner Geräte z.B. für Fernbedienung

Hot Plug - Mechanismus zeigt an

- Lesbarkeit der E-EDID
- Änderungen

Consumer Electronics Control Line (CEC)

Gemeinsamer „Datenbus“ sämtlicher verketteter HDMI-Geräte (PVR, DVD, STB, Display, ...)

- eine einzelne und einzige Leitung
- Hierarchie bis 5 Geräte in Serie

Beispiele für Funktionen

- Presets, One touch play/record, Timer/Tuner/Deck Control
- Meldungen für „On Screen Display“

Rechtemanagement

Verwaltung der Schlüssel für Authentifizierung

Geräte müssen (geheime) Schlüssel / Ids enthalten

Quellen müssen eine Liste der kompromittierten Senken-Ids verwalten

- Liste speichern
- Liste erneuern (-> Zuführung ?, „revocation lists“)

Verwaltung / Lizensierung über Digital-CP LLC

- 15 k$/Jahr für Hersteller, 0.5 cent pro Schlüssel
- 50 k$ für bisher zwei Teilnehmer (Warner & Disney)
- Selbstzertifizierung

Zusammenfassung: Das Label „HD ready“

Displays (Label „HD ready“):
Analoge Scart oder Cinch Schnittstelle
Digitale DVI oder HDMI Schnittstelle mit HDCP Entschlüsselung

Empfänger (Label „HDTV“):
Analoge Scart oder Cinch Schnittstelle abschaltbar, wenn es der Programmanbieter signalisiert
Digitale DVI oder HDMI Schnittstelle, mit HDCP Verschlüsselung, wenn es der Programmanbieter signalisiert

Kann der Kunde etwas von „HD ready“ Schnittstellen aufzeichnen, wenn es der Programmanbieter nicht will?

Die analoge Schnittstelle ist abgeschaltet
Die digitale Schnittstelle ist gut gesichert:
- Hohe Datenrate (1080i25: > 1Gbit/s) erschwert die vollständige Aufzeichnung oder Komprimierung in Echtzeit
- Patentierte TDMS macht es rechtlich unmöglich einen Recorder anzubieten
- HDCP Verschlüsselung

Kann der Kunde etwas aufzeichnen, wenn der Programmanbieter es erlaubt?

Die analoge Schnittstelle ist zwar eingeschaltet, aber es sind zur Zeit keine Aufzeichnungsgeräte für Consumer am Markt verfügbar
Die digitale Schnittstelle ist auch ohne HDCP gut gesichert:
- Hohe Datenrate (1080i25 > 1Gbit/s) erschwert die vollständige Aufzeichnung
- Patentierte TDMS macht es rechtlich unmöglich Recorder anzubieten

Welche theoretischen Alternativen gäbe es für die Industrie?

Anbindung der Aufzeichnung an analoge Schnittstellen
Anbindung über FireWire
Integration der Aufzeichnung in den Empfänger

Nachteil: jederzeit vom Programmanbieter abschaltbar

Fazit

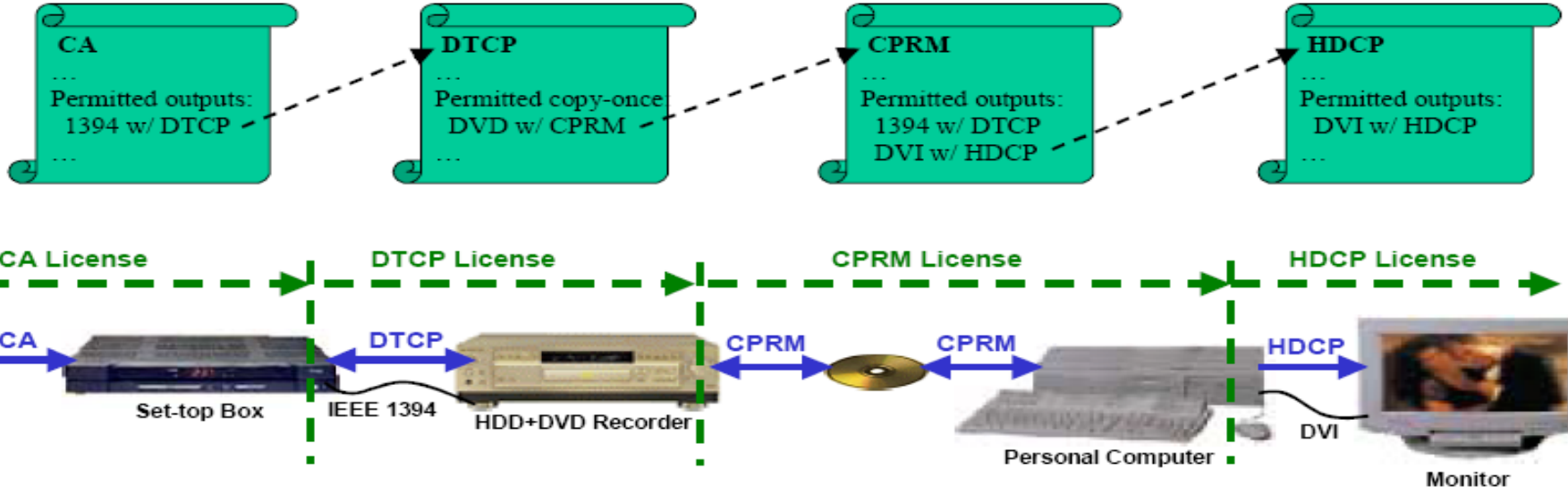
Funktion HDMI und HDCP

- bieten eine einfach zu nutzende Schnittstelle zum Display für Audio, Video, Control
- HDCP „verlängert“ Copy Protection und CA über den Verteilweg hinaus

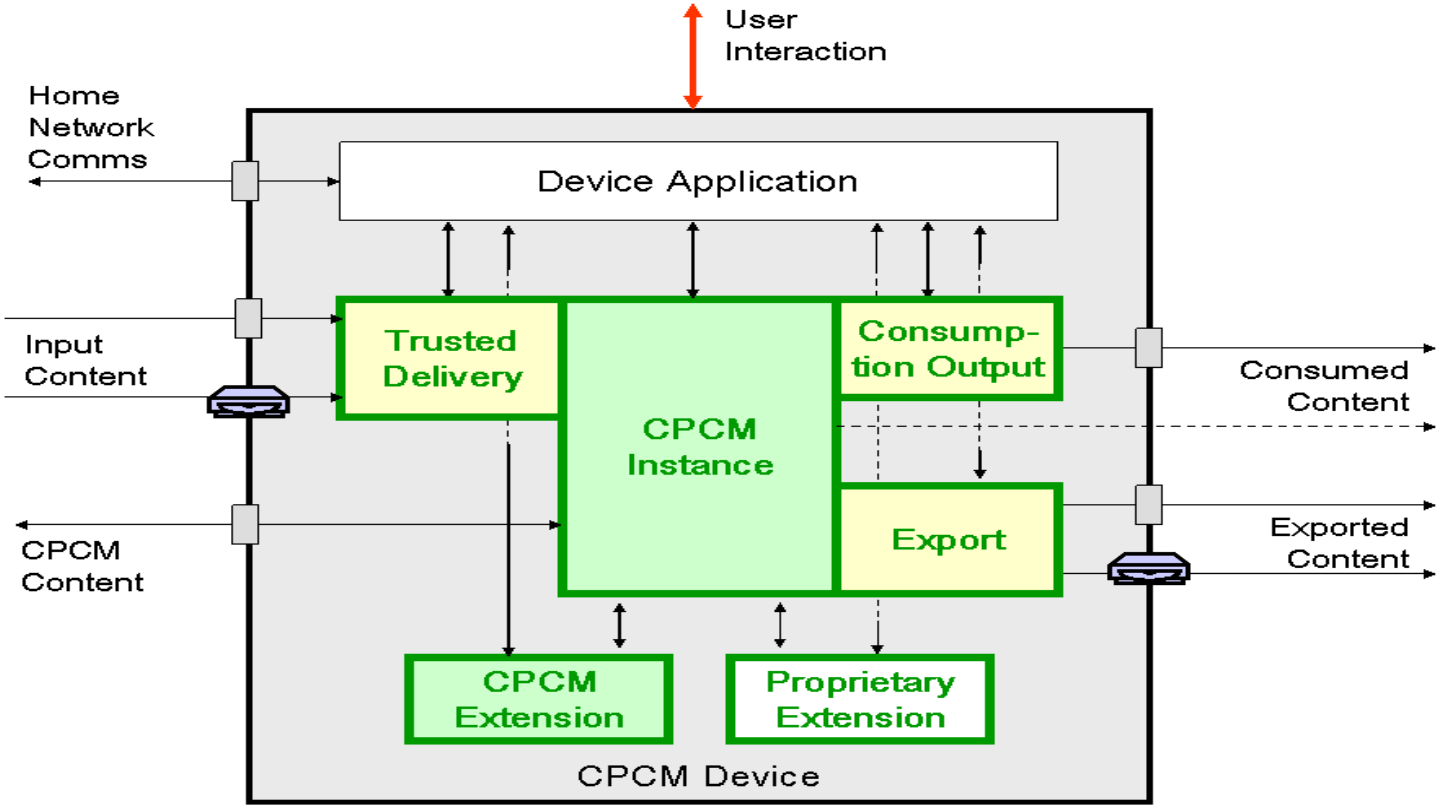
Risiken

- Im Falle nicht-kompatibler oder fehlerhaft implementierter Endgeräte könnten „Displays schwarz bleiben“, oder Verteiler/Umschalter in AV-Systemen (früher „Tuner“) Probleme verursachen
  - » Zertifizierungen und Plugfests, Informationen/Labels (HD ready)
- Die vollständige Ansteuerung/Kontrolle des „letzten Glieds in der DRM-Kette“ für Broadcast ist derzeit nur über proprietäre Systeme möglich, „Default-Werte“ am Markt sind durchaus sinnvoll gewählt, jedoch nicht zwingend und nicht zwingend einheitlich in Europa

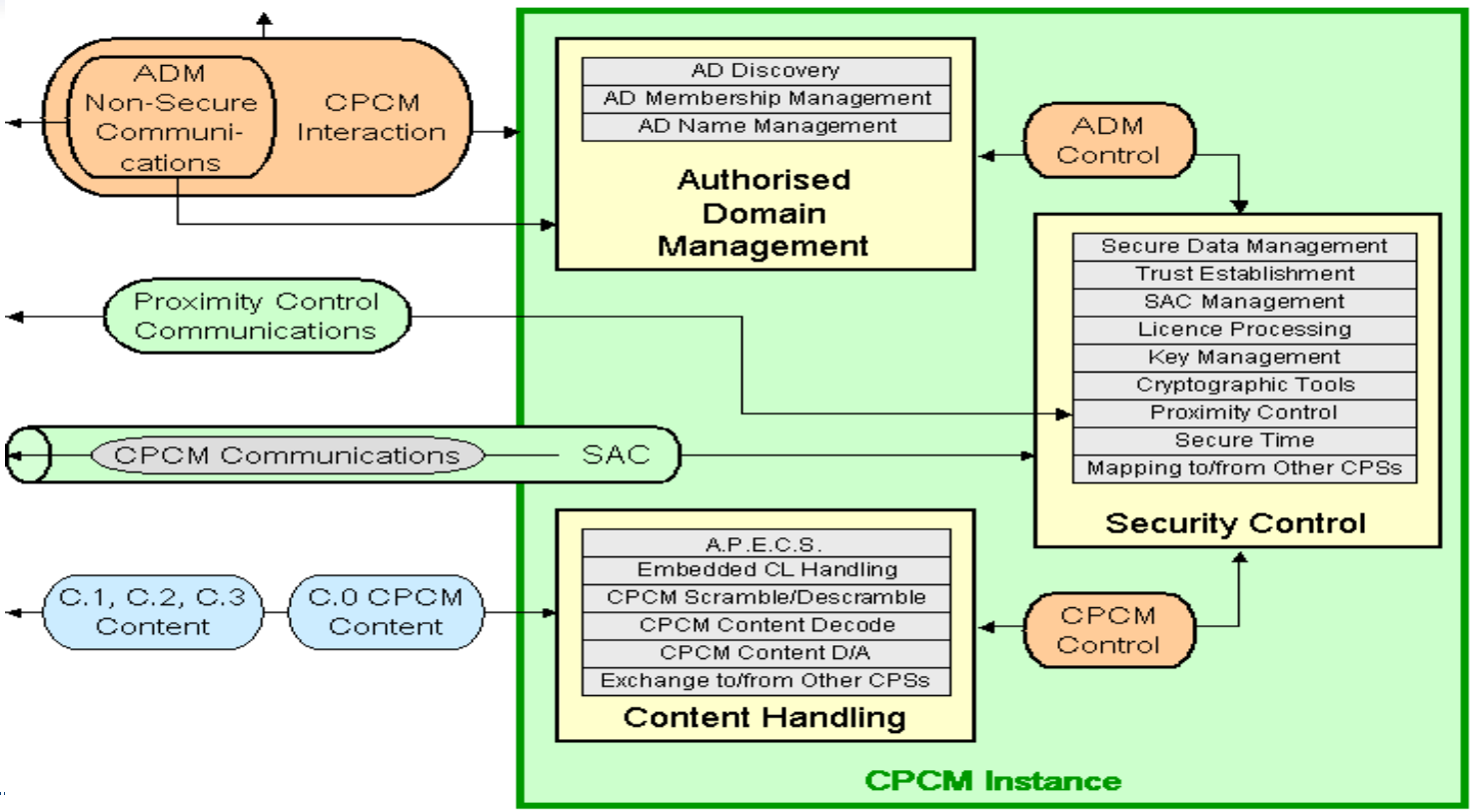
“Classical“ Link Encryption



CPCM Reference Model: Device



CPCM Reference Model: CPCM Instance



Wer will Copy Protection und Rights-Management und warum?

- **Rechte-Inhaber mit ‚wertvollen' Inhalten:**
  - **Hollywood-Studios:**
    Um Einnahme-Verluste durch illegale Verbreitung und Nutzung von rechtlich geschützten Inhalten zu vermeiden
    - Angst vor illegalem Inhalte-Austausch über das Internet (Peer to Peer)
    - Angst vor Raubkopien auf mobilen Datenträgern (DVD)
    - Verbreitung über den in Lizenzverträgen mit Broadcastern ausgehandelten Footprint hinaus führt zu schlechteren Vermarktungsmöglichkeiten

➔ **Beauftragung der Magazine Publishers of America (MPA)**

➔ **Beauftragung der Motion Picture Association of America (MPAA)**

Wer will Copy Protection und Rights-Management und warum?

Pay-TV-Broadcaster:

Um Einnahme-Verluste durch illegale Verbreitung und Nutzung von rechtlich geschützten Inhalten zu vermeiden

Angst vor illegalem Inhalte-Austausch über Heimnetzwerke und Internet

Angst vor Raubkopien auf mobilen Datenträgern (DVD)

Wer will Copy Protection und Rights-Management und warum?

- **Musik- und DVD-Industrie):**
  Um Einnahme-Verluste durch illegale Verbreitung und Nutzung von rechtlich geschützten Inhalten zu vermeiden

  - Angst vor illegalem Inhalte-Austausch über das Internet (Peer to Peer)
  - Angst vor Raubkopien auf mobilen Datenträgern (DVD)

➔ **Hersteller werden bei neuen technischen Systemen bereits bei der Entwicklung zur Verwendung von DRM-Systemen verpflichtet**
Beispiel: Blue-Ray High Definition DVD-Spieler dürfen von allen Geräte-Herstellern nur noch mit DRM ausgeliefert werden.

Wer will Copy Protection und Rights-Management und warum?

- **Copy Protection- und Rights-Management-System-Hersteller:**
  Erweiterung des Einnahme- und Produkt- Spektrums von bisherigen Conditional-Access-Systemen und einfachen analogen Copy-Protection-Systemen hin zu vollständigen DRM- oder CPCM-Systemen

Die Ideal-Vorstellungen der Hollywood-Studios, MPAA, sowie von Pay-TV-Broadcastern:

ständige Kontrolle des Konsumenten bezüglich der Nutzung von Inhalten

intergrund: Gewinnmaximierung. Inhalte und Rundfunk werden als reines Wirtschaftsgut betrachtet

- **Lokale Begrenzung der Nutzung von Inhalten**
  Keine Nutzung von Inhalten an anderen Orten (z.B. Ferienhaus). Maximaler Gewinn bei Rechte-Verkauf bei lokaler Aufsplitterung
  Keine (sekundäre) Weiterverbreitung von Inhalten über Internet

- **Zeitliche Begrenzung der Nutzung von Inhalten**
  Für jede Nutzung neu bezahlen. Pause bei zeitversetztem Fernsehen nur 90 Minuten lang.

Die Ideal-Vorstellungen der Hollywood-Studios, MPAA, sowie von Pay-TV-Broadcastern:

Beschränkung der Anzahl von Geräten, auf denen ein Inhalt genutzt werden kann
Angst vor riesigen Domains

- **Kenntnis der Identität des Zuschauers**
  Verfolgung der natürlichen Person bei Missbrauch

Die Ideal-Vorstellungen der Public Broadcaster:

Eine Kontrolle des Konsumenten bezüglich der Nutzung von Inhalten

Hintergrund: Sozialer Auftrag. Free Flow of Information. Inhalte und Rundfunk werden **nicht** als Wirtschaftsgut betrachtet

- Freie Empfangbarkeit und Nutzung von Inhalten
  Nutzung von Inhalten auch an anderen Orten (z.B. Ferienhaus).
  Nutzung und Weiterverbreitung von Inhalten entsprechend gesetzlicher Vorschriften
- Keine zeitliche Begrenzung der Nutzung von Inhalten notwendig

Keine Beschränkung der Anzahl von Geräten, auf denen ein Inhalt genutzt werden kann

- Kenntnis der Identität des Zuschauers eines Inhaltes nicht erlaubt
  Inhalte müssen ohne Kenntnis der Person anonym empfangbar sein

Welche Lösungs-Ansätze gibt es zu Copy Protection und Digital-Rights-Management?

- Verschlüsselung von Inhalten

- Kennzeichnung von Inhalten und technische Verfahren zur Auswertung dieser Kennzeichnung (Wasserzeichen und andere Verfahren)

- Rechtliche Maßnahmen

Welche Lösungs-Ansätze gibt es zu Copy Protection und Digital-Rights-Management?

- **Microsoft DRM:**
  Wiedergabe-Software und DRM ineinander verwoben.

- **OMA DRM 2 (Open Mobile Alliance):**
  Offener Standard aus der Mobilfunk-Szene. Wird auf mobilen Geräten mit großer Wahrscheinlichkeit eingeführt.

- **HDCP:**
  Verschlüsselung digitaler Bild- und Tonsignale für Displays. Bereits eingeführt.

Welche Lösungs-Ansätze gibt es zu Copy Protection und Digital-Rights-Management?

- **DTCP over IP (Digital Transmission Content Protection):**
  Ausschließlich ‚Link-Protection'-System zwischen Geräten auf IP-Schnittstellen.
  In DLNA (Digital Living Network Alliance) als obligatorisch beschlossen.
  Auf IP-Verbindungen zwischen Geräten bald Realität.

- **CA-Systeme (Conditional Access):**
  Nur Zugangs-Kontrolle. Gemeinsame Schnittstelle Common Interface für unterschiedliche Systeme.

- **DVB CPCM (Content Protection and Copy Management):**
  Noch nicht fertig spezifiziert

Beispiel DTCP

Quellen für Inhalte

Packaged Media

Recordable Media

Broadcast

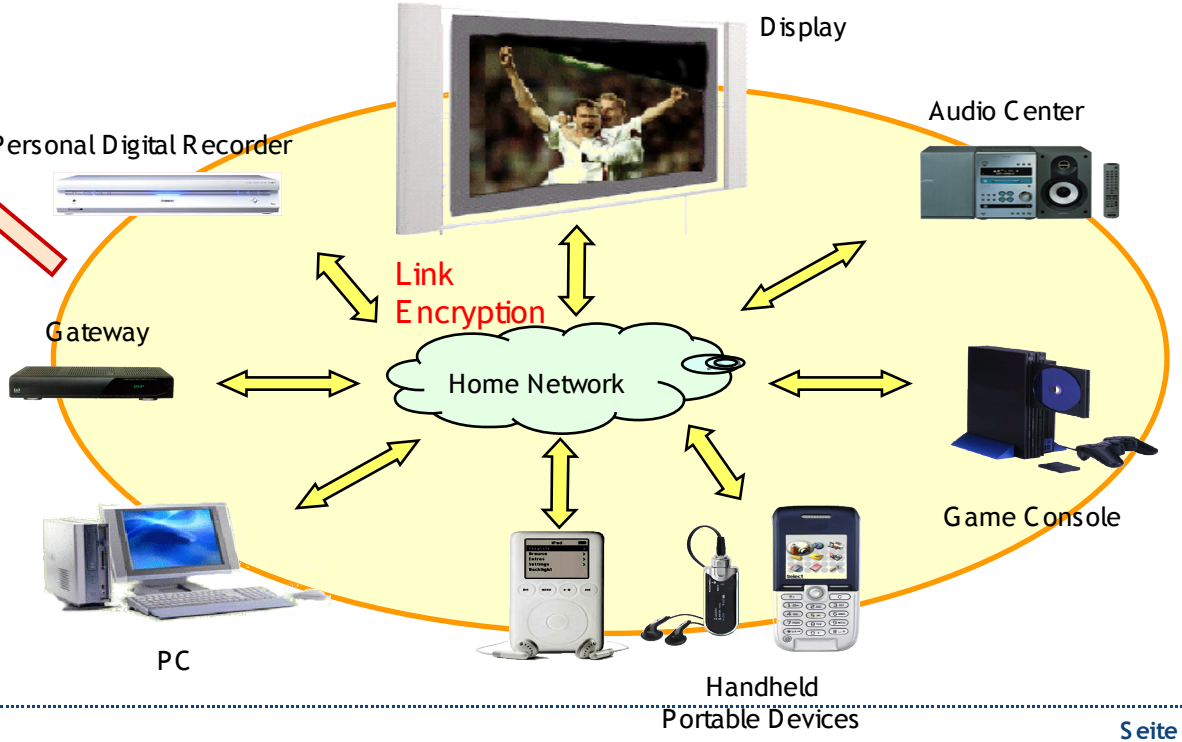
Cable

DSL

Internet

On Demand

Die Geräte-Sammlung eines Haushaltes



Conditional Access (CA) und HDMI

Quellen für Inhalte

Packaged Media

Broadcast

Cable

DSL

Internet

On Demand

Content Encrypted (CA)

Die Geräte-Sammlung eines Haushaltes

Display

Personal Digital Recorder

Audio Center

Content Encrypted (HDMI)

Gateway

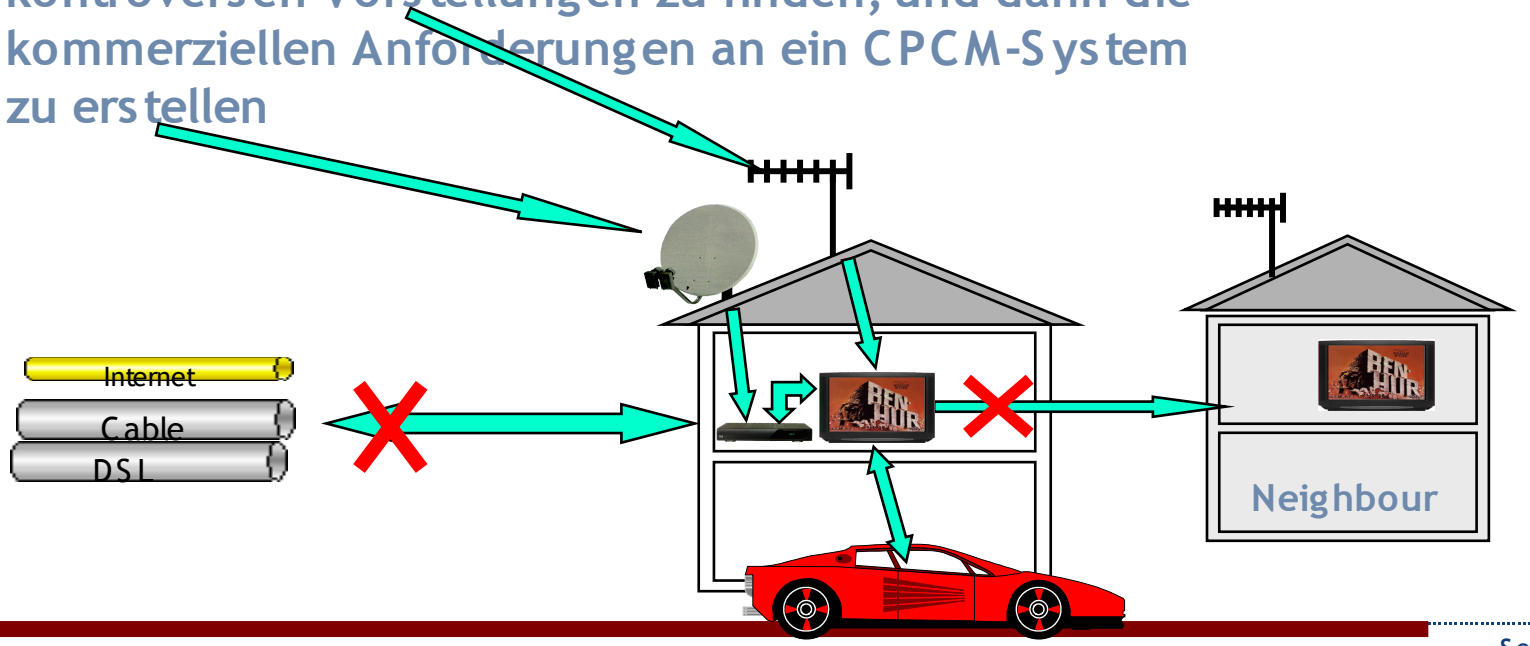
Home Network

Game Console

PC

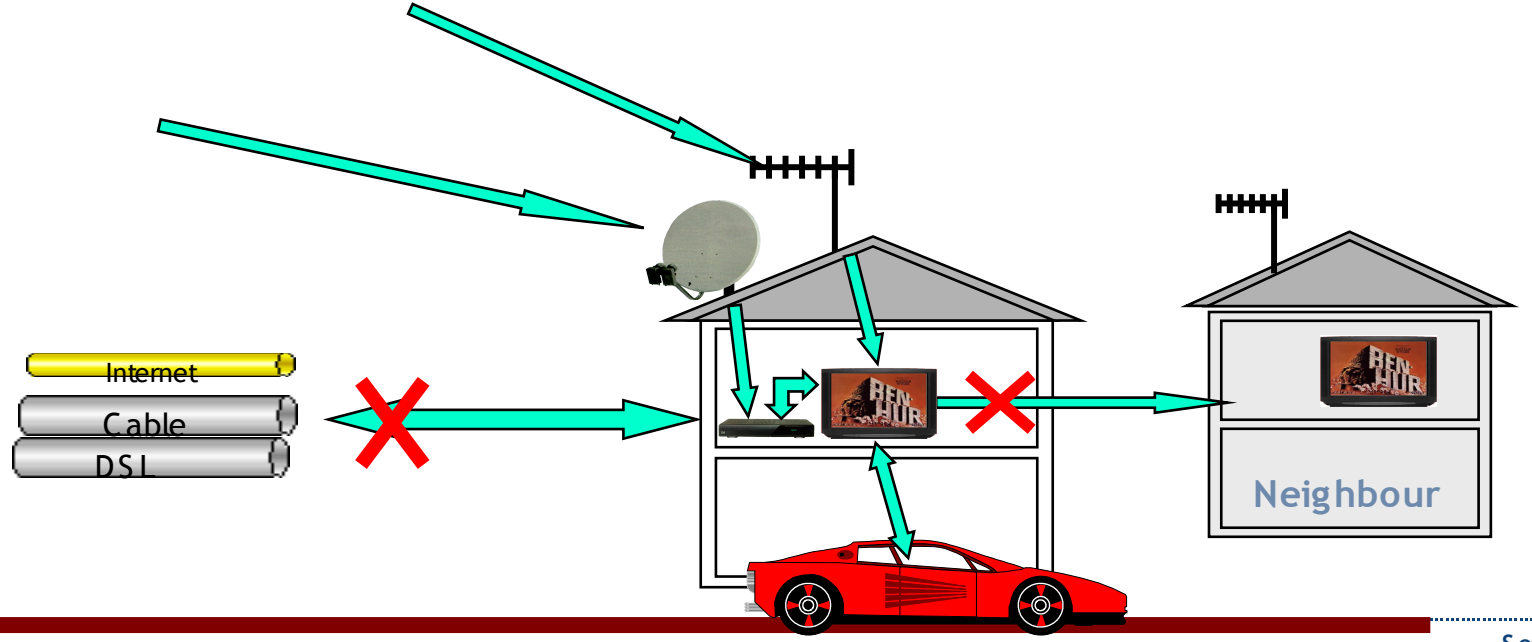
Handheld Portable Devices

VB-CM-CP: Die kommerzielle Gruppe von DVB hatte als erstes die Aufgabe, einen Kompromiss zwischen den kontroversen Vorstellungen zu finden, und dann die kommerziellen Anforderungen an ein CPCM-System zu erstellen

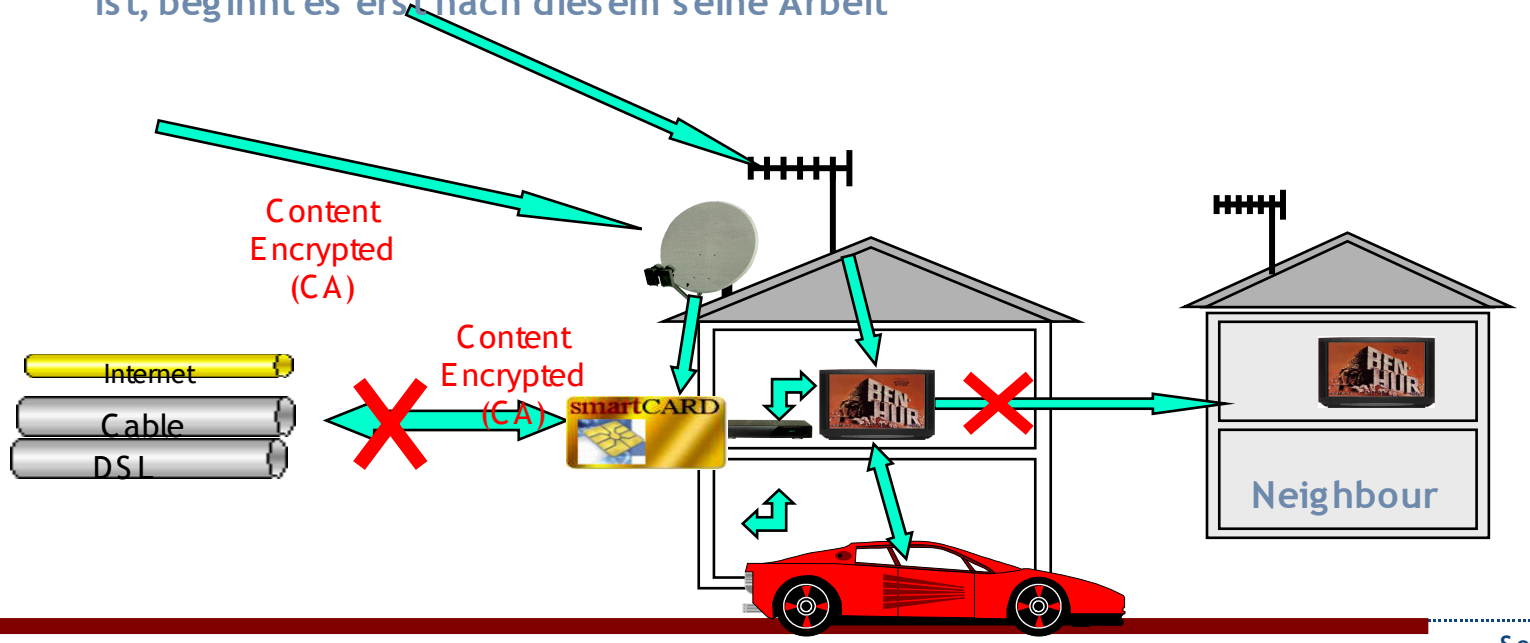


DVB-CM-CP: Eine unkontrollierte Weiterverbreitung besonders im Internet soll verhindert werden.
Die Nutzung von Inhalten des Konsumenten soll lokal und zeitlich begrenzt werden können.

End-to-End Protection



DVB-CM-CP: Das DVB Content Protection und Copy Management System soll kein Conditional-Access-System (CA) ersetzen. Wenn ein CA-System vorhanden ist, beginnt es erst nach diesem seine Arbeit



Die Authorized Domain

Local Delivery

Second Home

Content Delivery:

Broadcast

Broadband, On-demand

Packaged Media

Main Home

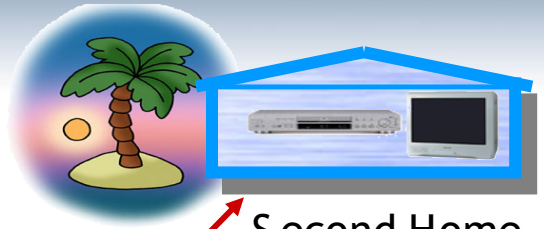
Mobile Delivery

Handheld Portable Devices

Mobile Delivery

In-Car Devices & Network

Proximity



Second Home

Content Delivery:

Broadcast

Broadband, On-demand

Packaged Media

Main Home

Über-Tragung

Handheld Portable Devices

nur, wenn in der Nähe

In-Car Devices & Network

esultierende Nutzungs-Szenarien bei Existenz von DVB-CPCM:

- Keine CPCM-Signalisierung

Nutzung wird nicht durch technische Mittel eingeschränkt
Entspricht bisherigem Zustand.
Inhalte wandern *nicht* in den CPCM-Bereich.

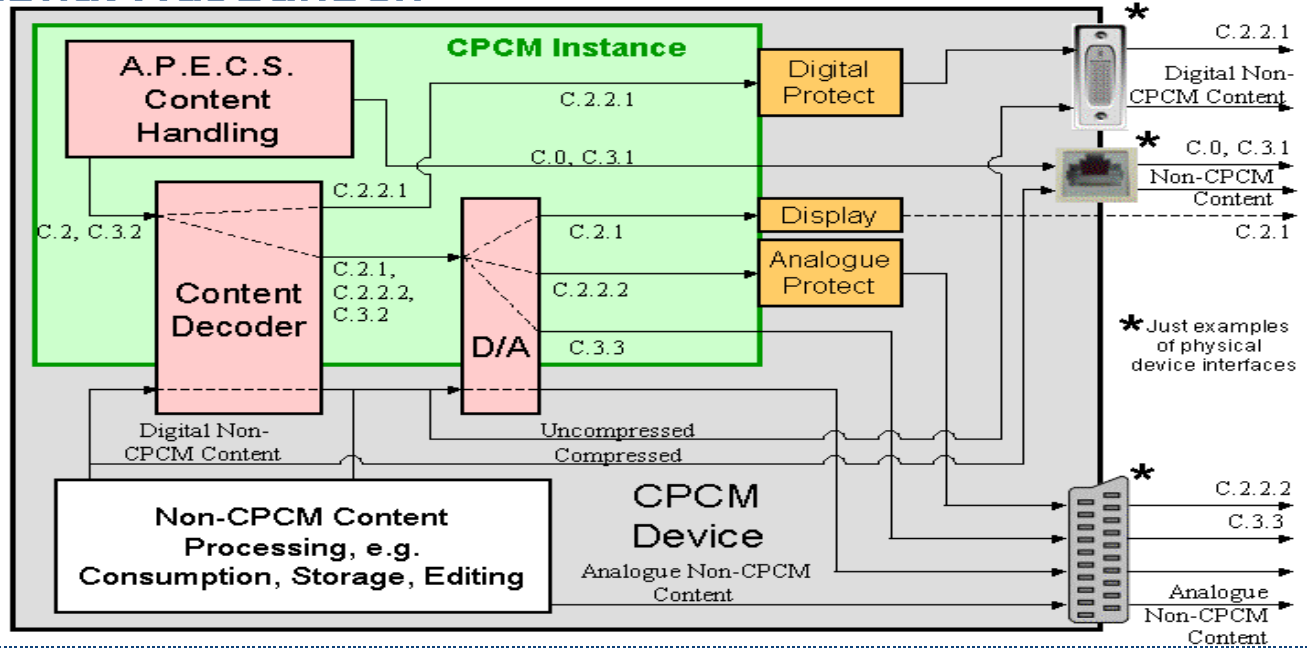
- ‚Free-to-Air'- CPCM-Signalisierung

Für ‚Free-to-Air' passende Nutzungs-Einschränkungen wählbar.
Unterschiedliche Erfordernisse auf unterschiedlichen Kontinenten.

- Pay-TV-CPCM-Signalisierung

Grosse Menge unterschiedlicher Nutzungs-Einschränkungen zur Auswahl.

Gerät mit CPCM-Bereich sowie Non-CPCM-Bereich und Signal-Ausgängen



EBU-Forderungen für ‚Free-to-Air':

Die Nutzungsmöglichkeiten sollen erweitert - nicht eingeschränkt werden.

- Vorhandene (Legacy) Geräte müssen weiter benutzbar sein

Einzige Einschränkung der Nutzung durch technische Mittel soll bei entsprechender Signalisierung eine Verhinderung der Weiterverbreitung empfangener Inhalte über das Internet sein.

Inhalte sollen bei entsprechender Signalisierung weder auf Schnittstellen zwischen unterschiedlichen Geräten, noch bei der Aufzeichnung verschlüsselt werden.

- Funktionalitäten der ‚Authorized Domain' sind nicht erforderlich

Werkzeuge zur Identifikation des lokalen Standortes sind nicht erforderlich.

esultierende Forderungen zur Signalisierung für ‚Free-to-Air':

- **‚Do not CPCM Scramble'**

Hiermit soll sichergestellt werden, dass Inhalte auf Interfaces zwischen Geräten und bei der Aufzeichnung nicht verschlüsselt werden, und selbst nach einer zeitweiligen Verschlüsselung, wie etwa auf drahtlosen Heim-Netzwerken immer wieder in eine unverschlüsselte Form zurückkehren

- **‚No Re-Distribution over the Internet'**

Vor Versenden eines Inhaltes soll mittels eines ‚Proximity-Tests' geprüft werden, ob sich der Empfänger in der Nähe befindet

Diese Signalisierungen sollen immer mit dem Inhalt mitgeführt werden, auch wenn dieser zeitweilig über andere DRM-Systeme geführt wird

Vielen Dank für Ihre Aufmerksamkeit.

Das IRT
Ihr Partner für das digitale Zeitalter

Professor Dietrich Sauter
089 3 23 99 204
sauter@irt.de

Digital Rights Management

Copy Protection und DVB CPRM

Dietrich Sauter
Öffentlichkeitsarbeit

Beiträge von Dr. Norbert P. Flechsig, Dr. Rainer Schäfer, Robert Sedlmeyer

§ 51 UrhG Zitatrecht

Zulässig ist die Vervielfältigung und öffentliche Wiedergabe eines veröffentlichten Werkes zum Zwecke des Zitats, sofern die Nutzung in ihrem Umfang durch den besonderen Zweck gerechtfertigt ist. Zulässig ist die insbesondere, wenn:

- Einzelne Werke in wissenschaftlichen Werken Stellen eines Werkes in einem selbständigen Sprachwerk
- Einzelne Stellen eines Musikwerkes in selbständigen Musikwerk genutzt werden.

§ 53 Abs. 1 UrhG – Vervielfältigung, insbesondere Donwload aus Internet nur von rechtmäßiger Quelle:

Zulässig sind einzelne Vervielfältigungen eines Werkes durch eine natürliche Person zum privaten Gebrauch auf beliebigen Trägern, sofern sie weder unmittelbar noch mittelbar Erwerbszwecken dienen, soweit nicht zur Vervielfältigung eine offensichtlich rechtswidrig hergestellte oder öffentlich zugänglich gemachte Vorlage verwendet wird."

(2) Zulässig ist, einzelne Vervielfältigungsstücke eines Werkes herzustellen oder herstellen zu lassen

1. zum eigenen wissenschaftlichen Gebrauch, wenn und soweit die Vervielfältigung zu diesem Zweck geboten ist und sie keinen gewerblichen Zwecken dient

2. zur Aufnahme in ein eigenes Archiv, wenn und soweit die Vervielfältigung zu diesem Zweck geboten ist und als Vorlage für die Vervielfältigung ein eigenes Werkstück benutzt wird, ...

§ 52b UrhG Wiedergabe an elektronischen Leseplätzen in Bibliotheken

Wiedergabe veröffentlichter Werke ausschließlich in den Räumen öffentlich zugänglicher Bibliotheken, Museen und Archive ohne Erwerbszweck an eigenen Leseplätzen zur wissenschaftlichen Forschung und für private Studien.

Vergütungspflicht via Verwertungsgesellschaft.

§ 53a UrhG – Kopienversand auf Bestellung

Zulässig ist auf **Einzelbestellung die Vervielfältigung** und Übermittlung einzelner in Zeitungen und Zeitschriften erschienener Beiträge sowie kleiner Teile eines erschienenen Werkes im Weg des Post- oder Faxversands durch öffentliche Bibliotheken, sofern die Nutzung durch den Besteller nach § 53 zulässig ist.
Die Vervielfältigung und Übermittlung in sonstiger elektronischer Form ist ausschließlich als grafische Datei und nur dann zulässig, wenn der Zugang zu den Beiträgen oder kleinen Teilen eines Werkes den Mitgliedern der Öffentlichkeit nicht von Orten und zu Zeiten ihrer Wahl mittels einer vertraglichen Vereinbarung ermöglicht wird.

Vergütungspflicht via Verwertungsgesellschaft.

§ 106 Abs. 3 UrhG wird ergänzt:

(3) Nicht bestraft wird, wer Werke oder Bearbeitungen oder Umgestaltungen von Werken nur in geringer Zahl und ausschließlich zum eigenen privaten Gebrauch oder zum privaten Gebrauch von mit dem Täter persönlich verbundenen Personen vervielfältigt oder an solchen Vervielfältigungen teilnimmt (§§ 26, 27 des Strafgesetzbuchs).
Satz 1 gilt nicht für die Vervielfältigung von Computerprogrammen (§ 69a).

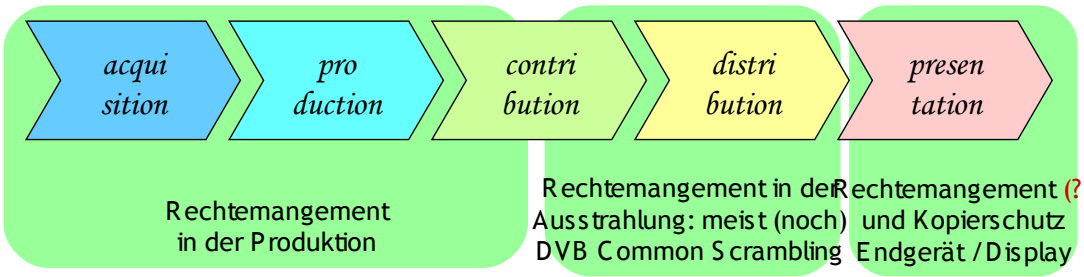
Begründung:

Strafausschließungsgrund soll Bagatellfälle ausnehmen.
Private Endnutzer begehen Urheberrechtsverletzungen - zwar nicht zu billigen, aber: „Grenzüberschreitungen“ zu kriminalisieren ist rechtspolitisch nicht opportun.

Die "Schulhöfe" sollten nicht kriminalisiert werden.

Produktions- und Verteilkette

Schnitt-stellen:	HD-SDI (single, dual) IT-Welt, FireWire	HD-SDI (single, dual) IT-Welt (IP, FibreChannel)	HD-SDI, ASI, STM, ...	ASI, USB, FireWire	SCART, Component, HDMI, DVI, ...



Kopierschutz: Verschlüsselung auf digitaler Schnittstelle -> HDCP auf HDMI
Rechtemanagement: Kontrolle der Verschlüsselung

Digitale Schnittstelle als Grundlage für den Kopierschutz

-> neue Zweige der Industrie

neue Produkte

Umbau der Entw/ / Produktion

Verschiebung des Umsatzes !!!

-> neue Konkurrenten

Beispiel aus Signalverteilung

IT-Welt -> nä. Bild

Varianten von DVI und HDMI

„Integrated" „Digital" „Analog"

	DVI-I Single Link	DVI-I Dual Link	DVI-D Single Link	DVI-D Dual Link	DVI-A	HDMI Type A	HDMI Type B
	Digital Display Working Group (Intel, Compaq, Fujitsu, Hewlett Packard, IBM, NEC, Silicon Image)					Hitachi, Matsushite Electric Ind. (Panasonic), Philips, Sony,, Thomson (RCA), Toshiba, Silicon Image	
	Http://www.ddwg.org DVI 1.0 Specification					www.hdmi.org HDMI 1.2 Specification	
	T.M.D.S. (transition optimized 8 Bit payload on 10 Bit frames)					T.M.D.S.	
	RGB 8 bit	RGB 8 bit dual only: RGB, bis 16 Bit	RGB 8 bit	RGB 8 bit dual only: RGB, bis 16 Bit		RGB 8 bit YCrCb 8 Bit YCrCb 4:2:2 12Bit	RGB 8 bit YCrCb 8 Bit YCrCb 4:2:2 12Bit
	Min. 25 MHz					Min. 25 MHz	
Takt	165 MHz	No limit spec.	165 MHz	No limit spec.		165 MHz	No limit spec.
Audio	-	-	-	-	-	in Austastung	in Austastung
Remote						CEC Remote control	CEC Remote control
Steckergröße	39,6x15,1 mm					13,9 x 4,5 mm	21,2 x 4,5 mm
Pins/benutzt	29/23	29/29	24/17	24/23	29/11	19/18	29/27
davon analog RGB H/V	6	6	-	-	6	-	-

Häufig: PCs Häufig: STBs Nicht spec. Kabel

Motivation, Parameter für HD ready

Motivation für Hersteller, PayTV Operator, HD Promoter

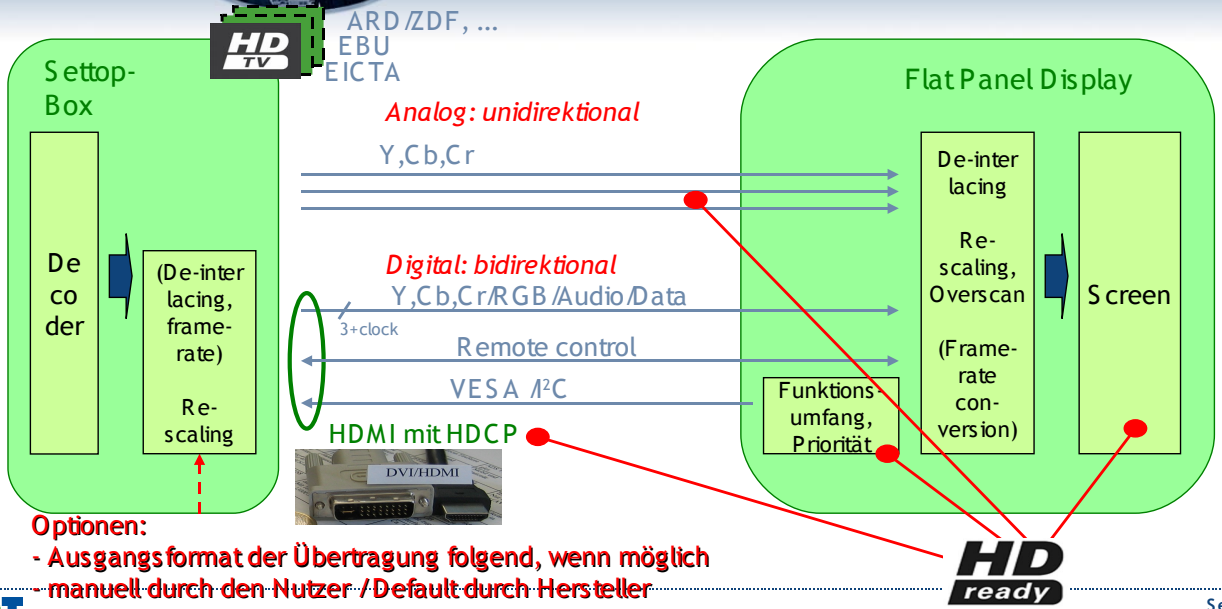
- Sicherung, dass Displays „kopiergeschützte" Signale akzeptieren (meist einziges Ausgangssignal der STB bei PayTV und HDTV DVD)
  -> HDCP mandatory
- Sicherung, dass neue teure Flat Panel Displays bei HD nicht „schwarz" bleiben
  -> müssen 720/50p and 1080/25i „unterstützen"
- Garantie minimaler Auflösung (evtl. Auflösung <> „Qualität"!)
  -> minimal 720 Zeilen

Interfaces

• digital (DVI und HDMI mit Copy Protection HDCP !)	mandatory
• SD Scart	recommended
• analog	mandatory

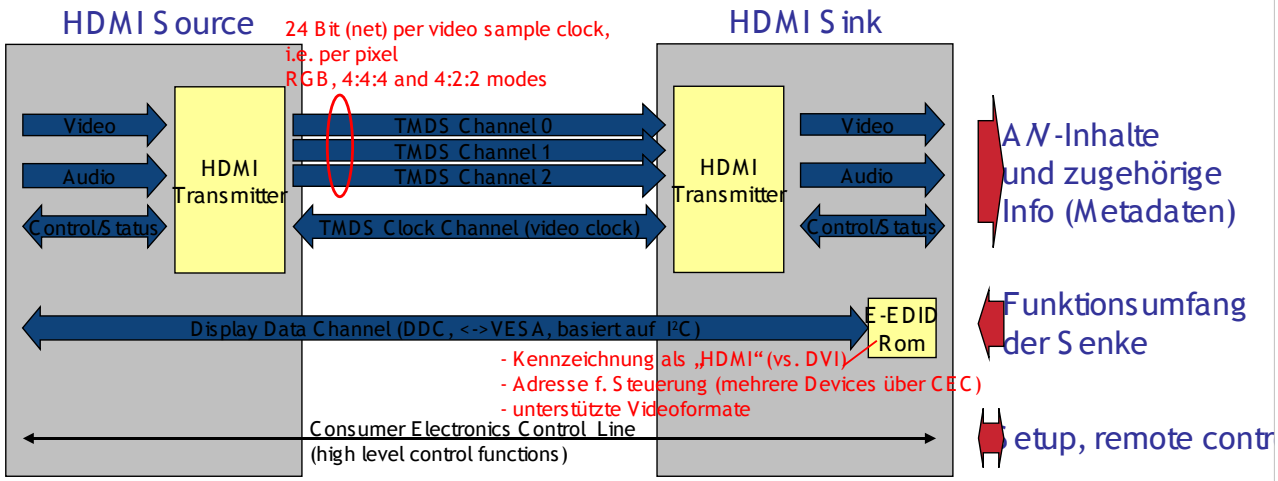
Derzeit etwa 20% der neu verkauften Geräte (Umsatz ?)

Settop-Box und Display



Optionen:
- Ausgangsformat der Übertragung folgend, wenn möglich
- manuell durch den Nutzer / Default durch Hersteller

HDMI-Interface



E-EDID: VESA Enhanced Extended Display Identification Data Stand

E-EDID: Enhanced Extended Display Identification Data Standard

- Identifikation der Parameter/Fähigkeiten der Senke (Display)
  - > Video-Formate
  - > Audio-Kanäle
- Identifikation als „HDMI“-Senke (Gegensatz zu „nur“ DVI)
- Adresse für Selektion einzelner Geräte z.B. für Fernbedienung

Hot Plug - Mechanismus zeigt an

- Lesbarkeit der E-EDID
- Änderungen

Gemeinsamer „Datenbus“ sämtlicher verketteter HDMI-Geräte (PVR, DVD, STB, Display, ...)

- eine einzelne und einzige Leitung
- Hierarchie bis 5 Geräte in Serie

Beispiele für Funktionen

- Presets, One touch play/record, Timer/Tuner/Deck Control
- Meldungen für „On Screen Display“

Rechtemanagement

-> neue Zweige der Industrie

neue Produkte

Umbau der Entw/ / Produktion

Verschiebung des Umsatzes !!!

-> neue Konkurrenten

Beispiel aus Signalverteilung

IT-Welt -> nä. Bild

Verwaltung der Schlüssel für Authentifizierung

Geräte müssen (geheime) Schlüssel / Ids enthalten

Quellen müssen eine Liste der kompromittierten Senken-Ids verwalten
- Liste speichern
- Liste erneuern (-> Zuführung ? , „revocation lists“)

Verwaltung / Lizensierung über Digital-CP LLC
- 15 k$/Jahr für Hersteller, 0.5 cent pro Schlüssel
- 50 k$ für bisher zwei Teilnehmer (Warner & Disney)
- Selbstzertifizierung

Zusammenfassung: Das Label „HD ready“

Displays (Label „HD ready“):
Analoge Scart oder Cinch Schnittstelle
Digitale DVI oder HDMI Schnittstelle mit HDCP Entschlüsselung

Empfänger (Label „HDTV“):
Analoge Scart oder Cinch Schnittstelle abschaltbar, wenn es der Programmanbieter signalisiert
Digitale DVI oder HDMI Schnittstelle, mit HDCP Verschlüsselung, wenn es der Programmanbieter signalisiert

Kann der Kunde etwas von „HD ready“ Schnittstellen aufzeichnen, wenn es der Programmanbieter nicht will?

Die analoge Schnittstelle ist abgeschaltet
Die digitale Schnittstelle ist gut gesichert:
- Hohe Datenrate (1080i25: > 1Gbit/s) erschwert die vollständige Aufzeichnung oder Komprimierung in Echtzeit
- Patentierte TDMS macht es rechtlich unmöglich einen Recorder anzubieten
- HDCP Verschlüsselung

Kann der Kunde etwas aufzeichnen, wenn der Programmanbieter es erlaubt?

Die analoge Schnittstelle ist zwar eingeschaltet, aber es sind zur Zeit keine Aufzeichnungsgeräte für Consumer am Markt verfügbar
Die digitale Schnittstelle ist auch ohne HDCP gut gesichert:
- Hohe Datenrate (1080i25 > 1Gbit/s) erschwert die vollständige Aufzeichnung
- Patentierte TDMS macht es rechtlich unmöglich Recorder anzubieten

Welche theoretischen Alternativen gäbe es für die Industrie?

Anbindung der Aufzeichnung an analoge Schnittstellen
Anbindung über FireWire
Integration der Aufzeichnung in den Empfänger

Nachteil: jederzeit vom Programmanbieter abschaltbar

Fazit

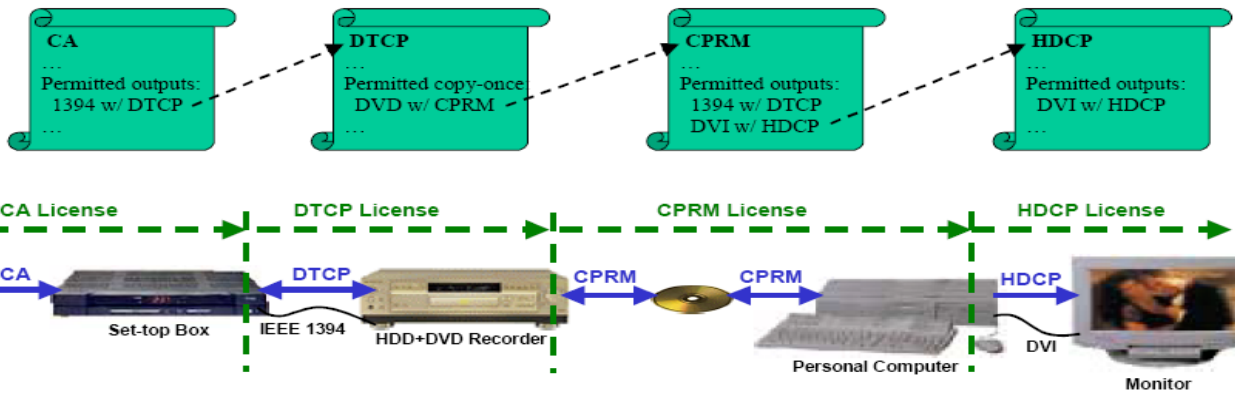
Funktion HDMI und HDCP

- bieten eine einfach zu nutzende Schnittstelle zum Display für Audio, Video, Control
- HDCP „verlängert“ Copy Protection und CA über den Verteilweg hinaus

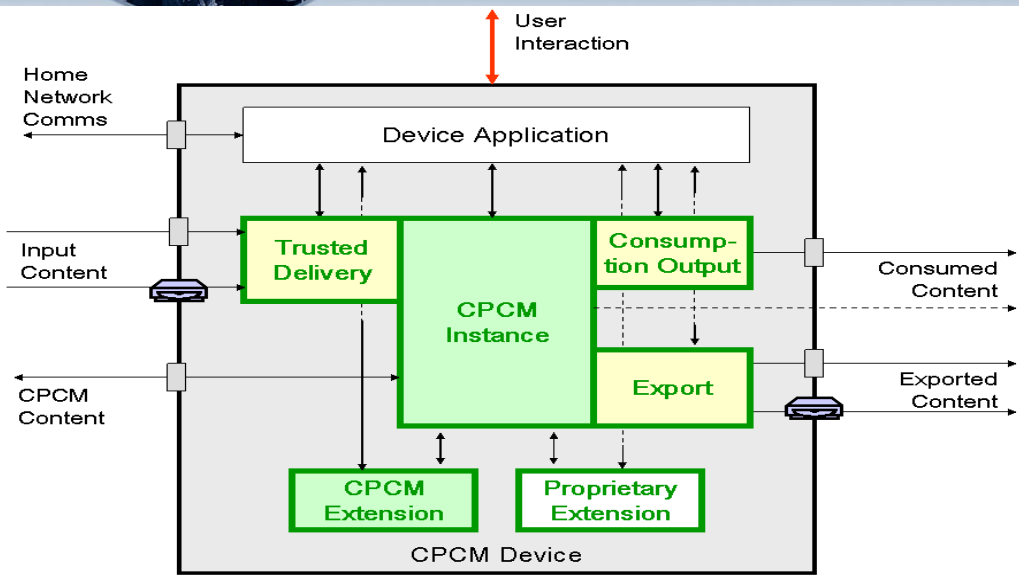
Risiken

- Im Falle nicht-kompatibler oder fehlerhaft implementierter Endgeräte könnten „Displays schwarz bleiben“, oder Verteiler/Umschalter in A/V-Systemen (früher „Tuner“) Probleme verursachen
  - » Zertifizierungen und Plugfests, Informationen/Labels (HD ready)
- Die vollständige Ansteuerung/Kontrolle des „letzten Glieds in der DRM-Kette“ für Broadcast ist derzeit nur über proprietäre Systeme möglich, „Default-Werte“ am Markt sind durchaus sinnvoll gewählt, jedoch nicht zwingend und nicht zwingend einheitlich in Europa

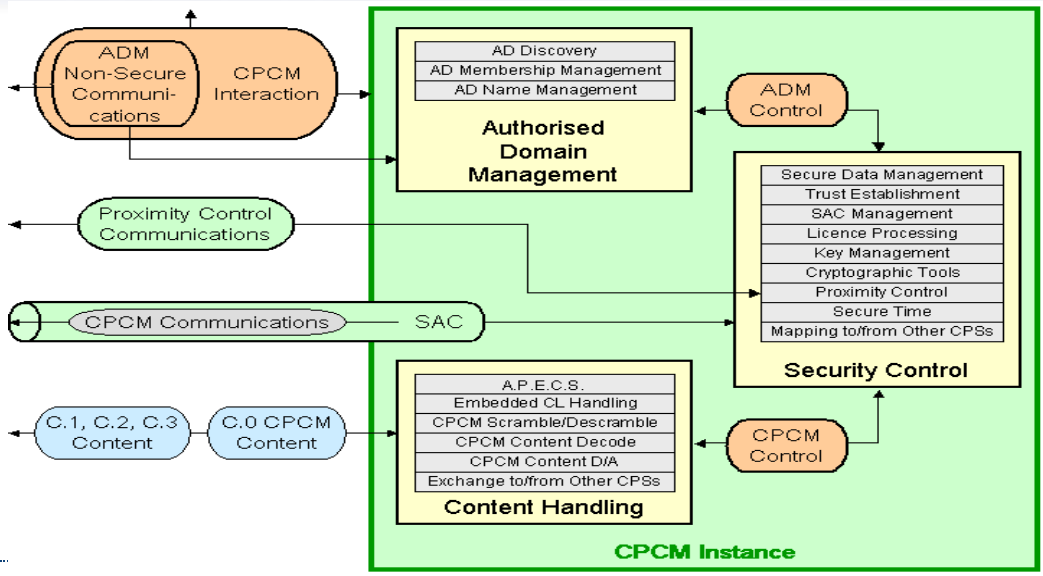
"Classical" Link Encryption



CPCM Reference Model: Device



CPCM Reference Model: CPCM Instance



Wer will Copy Protection und Rights-Management und warum?

- **Rechte-Inhaber mit ‚wertvollen' Inhalten:**
  - **Hollywood-Studios:**
    Um Einnahme-Verluste durch illegale Verbreitung und Nutzung von rechtlich geschützten Inhalten zu vermeiden
    - Angst vor illegalem Inhalte-Austausch über das Internet (Peer to Peer)
    - Angst vor Raubkopien auf mobilen Datenträgern (DVD)
    - Verbreitung über den in Lizenzverträgen mit Broadcastern ausgehandelten Footprint hinaus führt zu schlechteren Vermarktungsmöglichkeiten

➔ **Beauftragung der Magazine Publishers of America (MPA)**

➔ **Beauftragung der Motion Picture Association of America (MPAA)**

Wer will Copy Protection und Rights-Management und warum?

Pay-TV-Broadcaster:
Um Einnahme-Verluste durch illegale Verbreitung und Nutzung von rechtlich geschützten Inhalten zu vermeiden

Angst vor illegalem Inhalte-Austausch über Heimnetzwerke und Internet

Angst vor Raubkopien auf mobilen Datenträgern (DVD)

Wer will Copy Protection und Rights-Management und warum?

- **Musik- und DVD-Industrie):**
  Um Einnahme-Verluste durch illegale Verbreitung und Nutzung von rechtlich geschützten Inhalten zu vermeiden

  - Angst vor illegalem Inhalte-Austausch über das Internet (Peer to Peer)
  - Angst vor Raubkopien auf mobilen Datenträgern (DVD)

➔ **Hersteller werden bei neuen technischen Systemen bereits bei der Entwicklung zur Verwendung von DRM-Systemen verpflichtet**
Beispiel: Blue-Ray High Definition DVD-Spieler dürfen von allen Geräte-Herstellern nur noch mit DRM ausgeliefert werden.

Wer will Copy Protection und Rights-Management und warum?

- **Copy Protection- und Rights-Management-System-Hersteller:**
  Erweiterung des Einnahme- und Produkt-Spektrums von bisherigen Conditional-Access-Systemen und einfachen analogen Copy-Protection-Systemen hin zu vollständigen DRM- oder CPCM-Systemen

Die Ideal-Vorstellungen der Hollywood-Studios, MPAA, sowie von Pay-TV-Broadcastern:

ständige Kontrolle des Konsumenten bezüglich der Nutzung von Inhalten

intergrund: Gewinnmaximierung. Inhalte und Rundfunk
werden als reines Wirtschaftsgut betrachtet

- **Lokale Begrenzung der Nutzung von Inhalten**
  Keine Nutzung von Inhalten an anderen Orten (z.B. Ferienhaus). Maximaler Gewinn bei Rechte-Verkauf bei lokaler Aufsplitterung
  Keine (sekundäre) Weiterverbreitung von Inhalten über Internet

- **Zeitliche Begrenzung der Nutzung von Inhalten**
  Für jede Nutzung neu bezahlen. Pause bei zeitversetztem Fernsehen nur 90 Minuten lang.

Die Ideal-Vorstellungen der Hollywood-Studios, MPAA, sowie von Pay-TV-Broadcastern:

Beschränkung der Anzahl von Geräten, auf denen ein Inhalt genutzt werden kann
Angst vor riesigen Domains

- **Kenntnis der Identität des Zuschauers**
  Verfolgung der natürlichen Person bei Missbrauch

Die Ideal-Vorstellungen der Public Broadcaster:

Eine Kontrolle des Konsumenten bezüglich der Nutzung von Inhalten

Hintergrund: Sozialer Auftrag. Free Flow of Information. Inhalte und Rundfunk werden nicht als Wirtschaftsgut betrachtet

- **Freie Empfangbarkeit und Nutzung von Inhalten**
  Nutzung von Inhalten auch an anderen Orten (z.B. Ferienhaus).
  Nutzung und Weiterverbreitung von Inhalten entsprechend gesetzlicher Vorschriften
- **Keine zeitliche Begrenzung der Nutzung von Inhalten notwendig**

Keine Beschränkung der Anzahl von Geräten, auf denen ein Inhalt genutzt werden kann

- **Kenntnis der Identität des Zuschauers eines Inhaltes nicht erlaubt**
  Inhalte müssen ohne Kenntnis der Person anonym empfangbar sein

Welche Lösungs-Ansätze gibt es zu Copy Protection und Digital-Rights-Management?

- Verschlüsselung von Inhalten

  - Kennzeichnung von Inhalten und technische Verfahren zur Auswertung dieser Kennzeichnung (Wasserzeichen und andere Verfahren)

- Rechtliche Maßnahmen

.

Welche Lösungs-Ansätze gibt es zu Copy Protection und Digital-Rights-Management?

- **Microsoft DRM:**
  Wiedergabe-Software und DRM ineinander verwoben.

- **OMA DRM 2 (Open Mobile Alliance):**
  Offener Standard aus der Mobilfunk-Szene. Wird auf mobilen Geräten mit großer Wahrscheinlichkeit eingeführt.

- **HDCP:**
  Verschlüsselung digitaler Bild- und Tonsignale für Displays. Bereits eingeführt.

Welche Lösungs-Ansätze gibt es zu Copy Protection und Digital-Rights-Management?

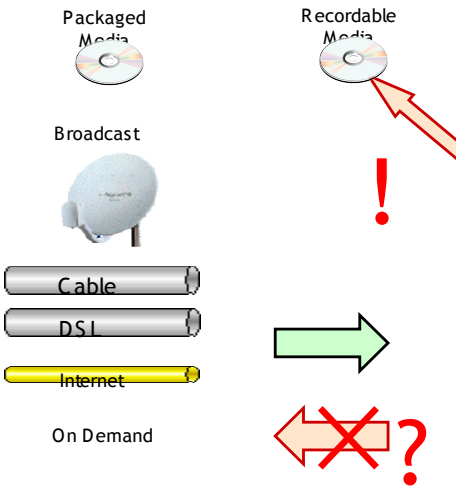
- **DTCP over IP (Digital Transmission Content Protection):**
  Ausschließlich ‚Link-Protection'-System zwischen Geräten auf IP-Schnittstellen.
  In DLNA (Digital Living Network Alliance) als obligatorisch beschlossen.
  Auf IP-Verbindungen zwischen Geräten bald Realität.

- **CA-Systeme (Conditional Access):**
  Nur Zugangs-Kontrolle. Gemeinsame Schnittstelle Common Interface für unterschiedliche Systeme.

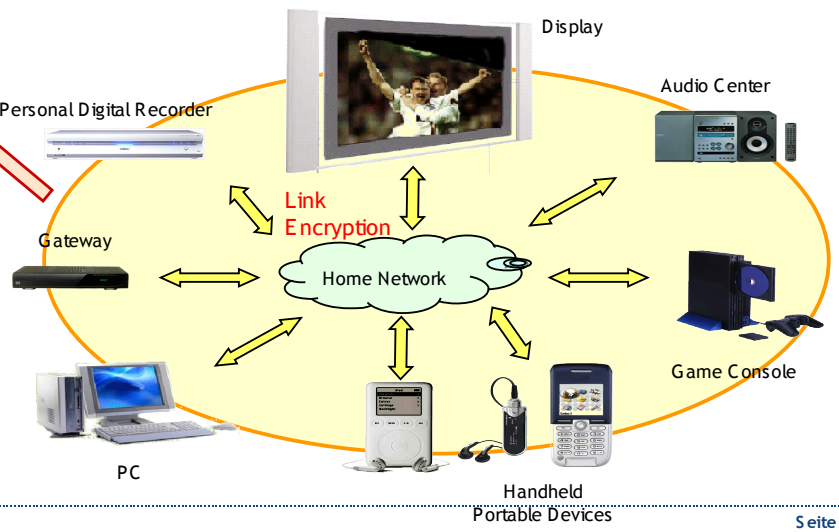
- **DVB CPCM (Content Protection and Copy Management):**
  Noch nicht fertig spezifiziert

Beispiel DTCP

Quellen für Inhalte



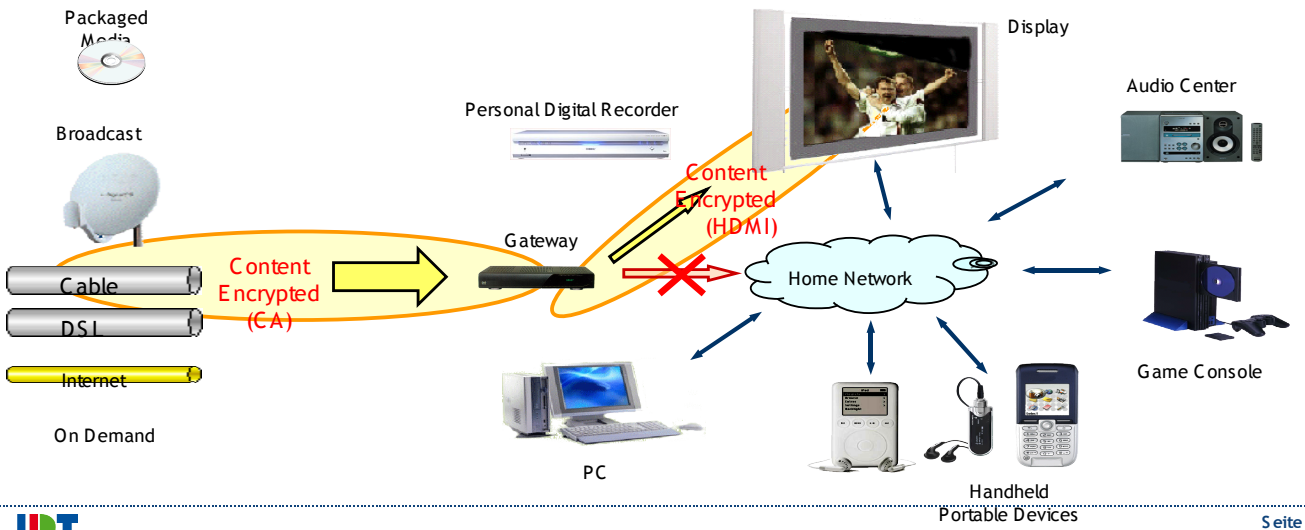
Die Geräte-Sammlung eines Haushaltes



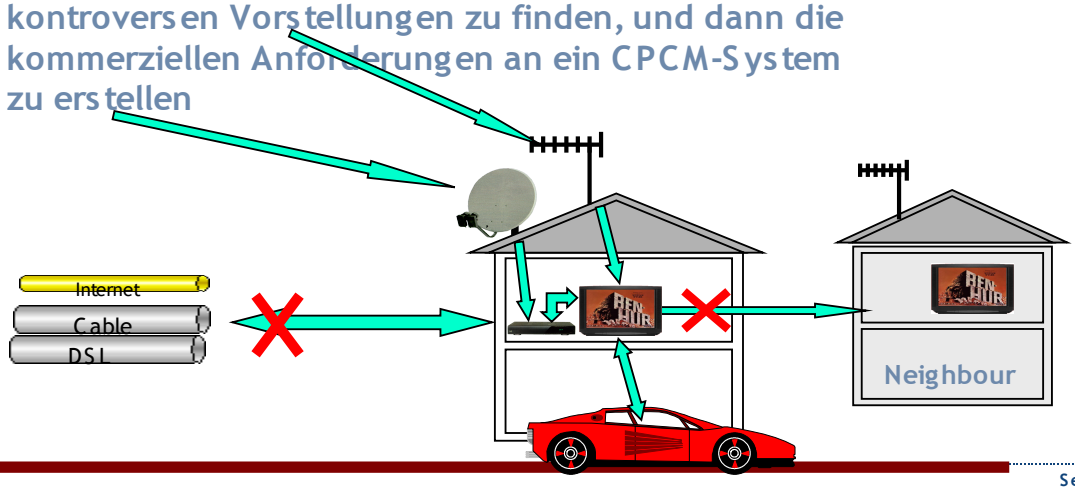
Conditional Access (CA) und HDMI

Quellen für Inhalte

Die Geräte-Sammlung eines Haushaltes

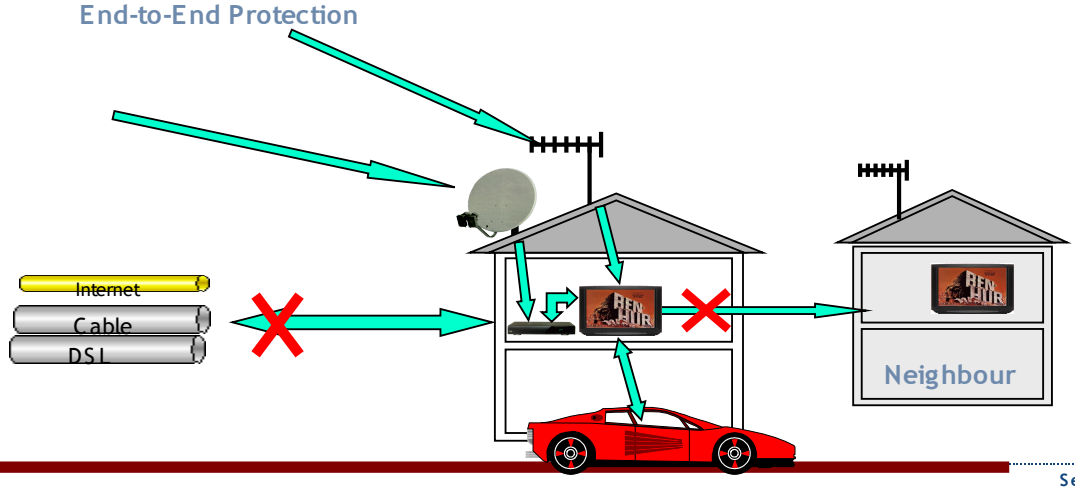


VB-CM-CP: Die kommerzielle Gruppe von DVB hatte als erstes die Aufgabe, einen Kompromiss zwischen den kontroversen Vorstellungen zu finden, und dann die kommerziellen Anforderungen an ein CPCM-System zu erstellen



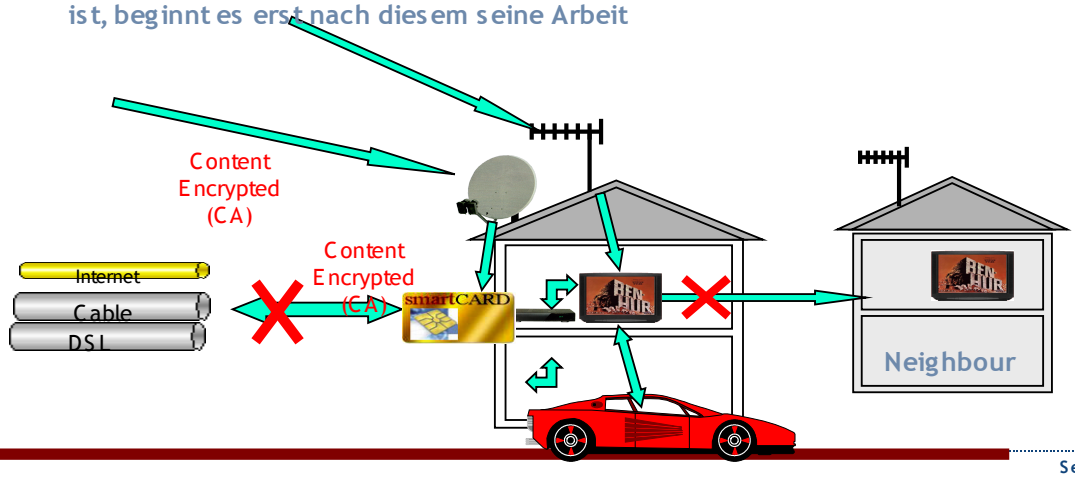
DVB-CM-CP: Eine unkontrollierte Weiterverbreitung besonders im Internet soll verhindert werden.
Die Nutzung von Inhalten des Konsumenten soll lokal und zeitlich begrenzt werden können.

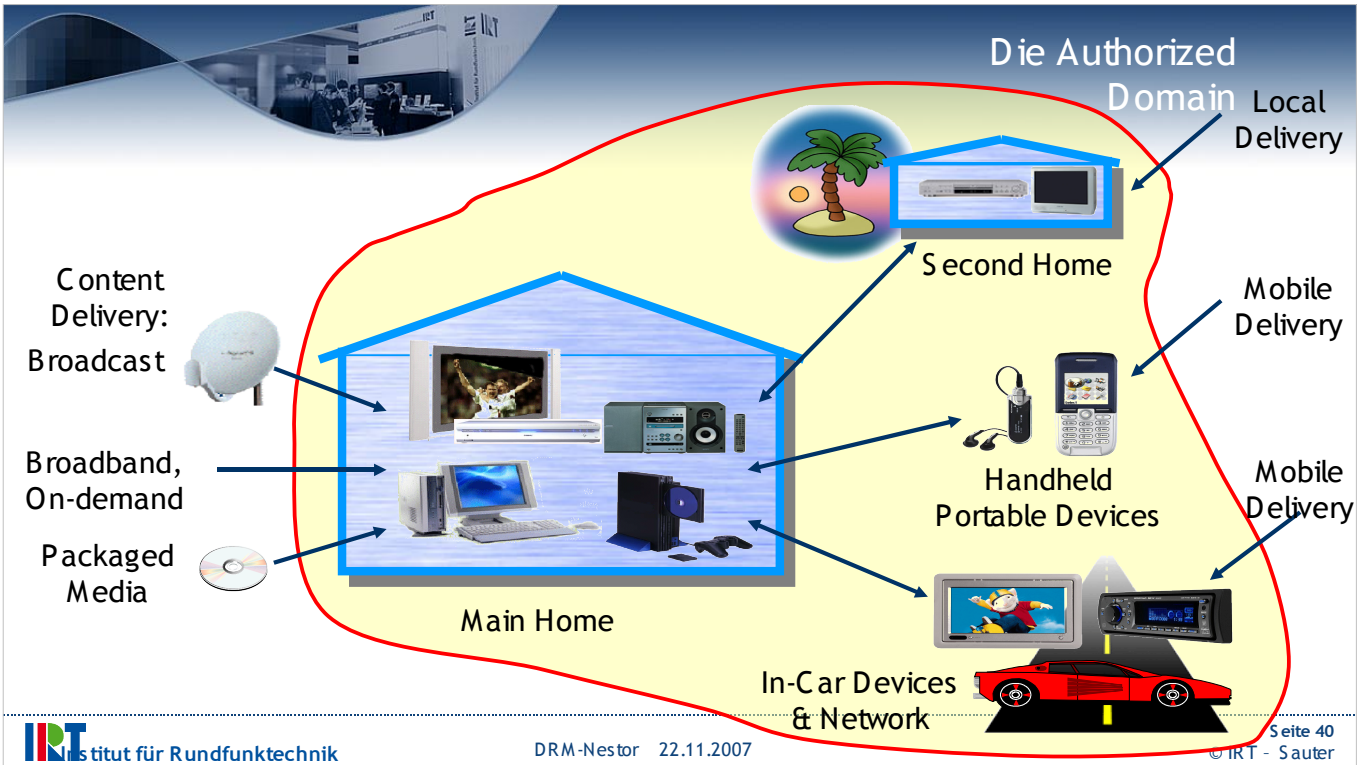
End-to-End Protection

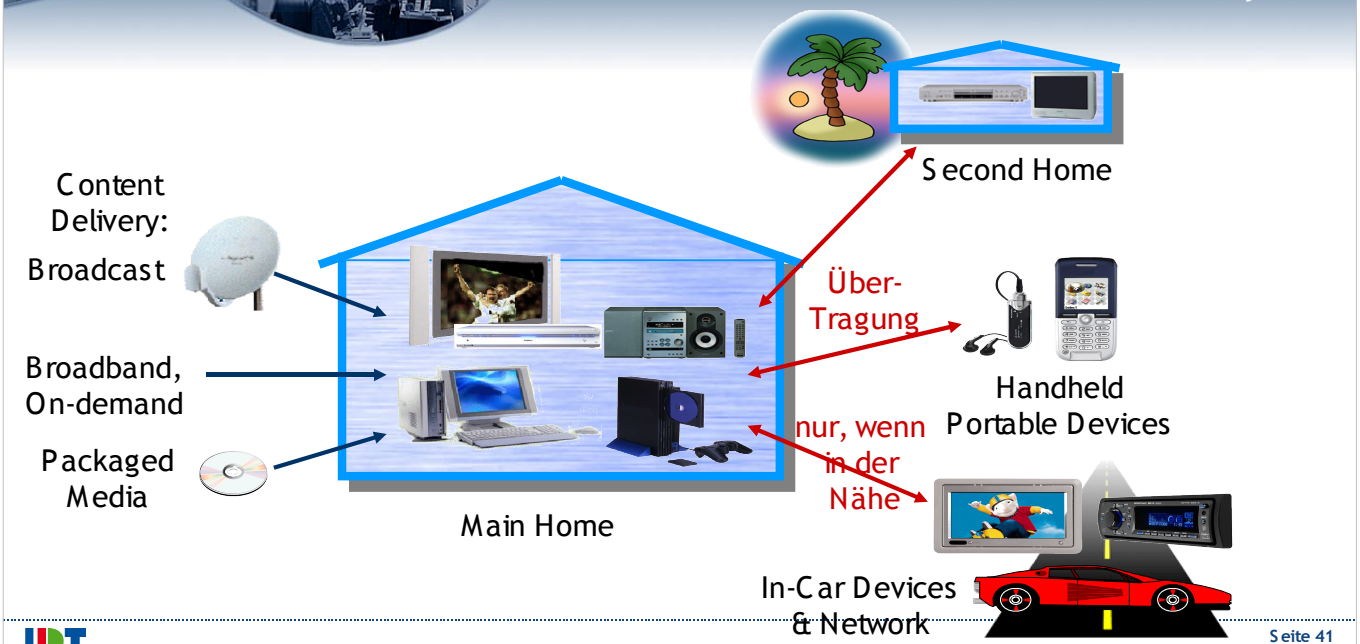


DVB-CM-CP:

Das DVB Content Protection und Copy Management System soll kein Conditional-Access-System (CA) ersetzen. Wenn ein CA-System vorhanden ist, beginnt es erst nach diesem seine Arbeit




Die Authorized Domain
Local Delivery
Second Home
Mobile Delivery
Content Delivery:
Broadcast
Broadband, On-demand
Packaged Media
Handheld Portable Devices
Mobile Delivery
Main Home
In-Car Devices & Network


Second Home
Content Delivery:
Broadcast
Broadband, On-demand
Packaged Media
Main Home
Über-Tragung
Handheld Portable Devices
nur, wenn in der Nähe
In-Car Devices & Network

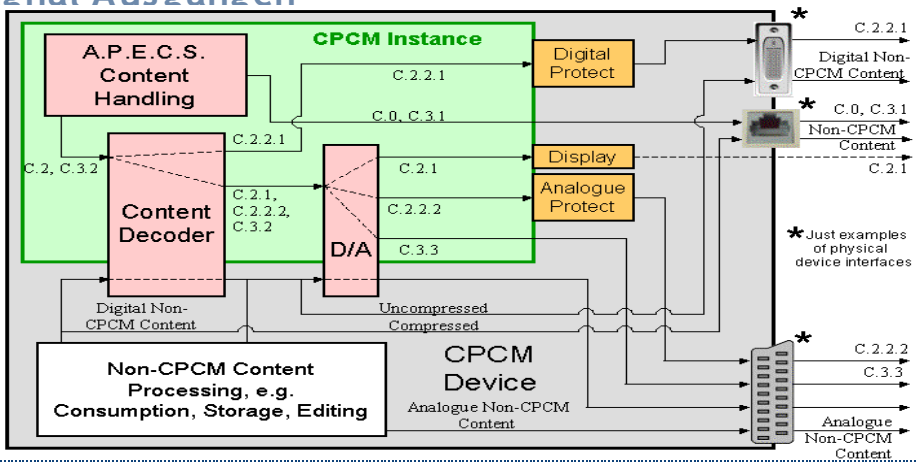
esultierende Nutzungs-Szenarien bei Existenz von DVB-CPCM:

- **Keine CPCM-Signalisierung**
  Nutzung wird nicht durch technische Mittel eingeschränkt
  Entspricht bisherigem Zustand.
  Inhalte wandern *nicht* in den CPCM-Bereich.

- **‚Free-to-Air'- CPCM-Signalisierung**
  Für ‚Free-to-Air' passende Nutzungs-Einschränkungen wählbar.
  Unterschiedliche Erfordernisse auf unterschiedlichen Kontinenten.

- **Pay-TV-CPCM-Signalisierung**
  Grosse Menge unterschiedlicher Nutzungs-Einschränkungen zur Auswahl.

Gerät mit CPCM-Bereich sowie Non-CPCM-Bereich und Signal-Ausgängen



EBU-Forderungen für ‚Free-to-Air':

Die Nutzungsmöglichkeiten sollen erweitert - nicht eingeschränkt werden.

- Vorhandene (Legacy) Geräte müssen weiter benutzbar sein

inzige Einschränkung der Nutzung durch technische Mittel soll bei entsprechender ignalisierung eine Verhinderung der Weiterverbreitung empfangener Inhalte über as Internet sein.

Inhalte sollen bei entsprechender Signalisierung weder auf Schnittstellen zwischen unterschiedlichen Geräten, noch bei der Aufzeichnung verschlüsselt werden.

- Funktionalitäten der ‚Authorized Domain' sind nicht erforderlich

Werkzeuge zur Identifikation des lokalen Standortes sind nicht erforderlich.

esultierende Forderungen zur Signalisierung für ‚Free-to-Air':

- ‚Do not CPCM Scramble'

Hiermit soll sichergestellt werden, dass Inhalte auf Interfaces zwischen Geräten und bei der Aufzeichnung nicht verschlüsselt werden, und selbst nach einer zeitweiligen Verschlüsselung, wie etwa auf drahtlosen Heim-Netzwerken immer wieder in eine unverschlüsselte Form zurückkehren

- ‚No Re-Distribution over the Internet'

Vor Versenden eines Inhaltes soll mittels eines ‚Proximity-Tests' geprüft werden, ob sich der Empfänger in der Nähe befindet

Diese Signalisierungen sollen immer mit dem Inhalt mitgeführt werden, auch wenn dieser zeitweilig über andere DRM-Systeme geführt wird

Vielen Dank für Ihre Aufmerksamkeit.

Das IRT
Ihr Partner für das digitale Zeitalter

Professor Dietrich Sauter
089 3 23 99 204
sauter@ irt.de