Fraunhofer FOKUS

Fraunhofer Institut für Offene Kommunikationssysteme (FOKUS)

Interoperabilitätssicherung der Zugangssicherung für IPTV

Studie

14.08.2009

Interoperabilitätssicherung der Zugangssicherung für IPTV
Studie im Auftrag der Deutschen Telekom

Erstellt von
FOKUS
Fraunhofer-Institut
für Offene Kommunikationssysteme
Kaiserin-Augusta-Allee 31
10589 Berlin

Inhalt

Executive Summary

Ziel der Studie war die Untersuchung von Zugangssicherungssystemen für IPTV aus technischer Sicht unter Berücksichtigung der durch das Telekommunikationsgesetz (TKG) vorgeschriebenen Interoperabilitätssicherung.

Digitales Fernsehen in Europa wurde in der Vergangenheit ausschließlich durch die vom DVB-Projekt vorgegebenen Standards definiert. Im Bereich der Zugangssicherung führt dieses zur Festschreibung von hardwarebasierten Mechanismen auf Basis des sog. Common Scrambling Algorithmus (CSA), zusammen mit der Anbindung von SmartCards über sog. Common Interface-Schnittstellen (CI). Diese Vorgabe aus der Universaldienstrichtlinie wird in Deutschland durch das Telekommunikationsgesetzt übernommen.

Im Rahmen der Studie galt es zu ermitteln, ob und in welchem Umfang die direkte Übernahme dieser Technologie für IPTV Anbieter sinnvoll und angemessen ist.

Die Studie kommt zu dem Schluss, dass sich IPTV technologisch als auch bei der Etablierung von konvergenten Zusatzdiensten noch in der Einführungsphase befindet. Erste Basisdienste, welche sich noch stark am existierenden TV-Erlebnis orientieren, sind kommerziell verfügbar. Darüber hinausreichende Anwendungen befinden sich derzeit jedoch zu einem großen Teil noch in der Entwicklung am Markt. Zurzeit sind Entwicklungstendenzen erkennbar, die vor allem auf die Konvergenz und Bereitstellung von Diensten auf dem TV, PC und mobilen Endgräten abzielen, jedoch haben sich noch keine klaren Trends entwickelt.

Im Bereich der Standardisierung von IPTV innerhalb der DVB, dem Open IPTV Forum und ETSI TISPAN gibt es derzeit eine Reihe von Aktivitäten, bei denen besonders die unterschiedlichen Ansichten der Marktteilnehmer zum Thema Zugangssicherung zu Tage treten und für Diskussion sorgen. Bisher sind auch hier keine klaren Vorgaben verabschiedet worden und Empfehlungen sind frühestens Ende 2009 zu erwarten.

Content-Provider entscheiden sich am Markt naturgemäß für das System, welches die meisten Nutzer und damit potentiellen Kunden erreicht. Eine Festlegung auf ein spezifisches Verschlüsselungssystem, welches die Anforderungen an ein modernes DRM nur begrenzt erfüllt, würde die Marktchancen von IPTV negativ beeinflussen.

Da dem IPTV Markt aufgrund des Potentials als Konvergenztechnologie kein eindeutiges Marktsegment zugeordnet werden kann und sich auch hier das primäre Anwendungsgebiet in den nächsten Jahren erst herausbilden muss, reduziert eine vorzeitige Festlegung eines Teilaspektes die IPTV Marktchancen. Dieses ist insbesondere der Fall, da es sich bei der derzeit anvisierten CSA Technologie um ein hardware-basiertes System handelt, welches später am Markt nur schwer wieder auszutauschen ist, insbesondere aufgrund der Tatsache, dass das Verfahren technisch nicht sicherstellen kann, dass die vom Gesetzgeber geforderte Interoperabilität gewährleistet ist. Das Festschreiben einer spezifischen Verschlüsselungstechnologie nähme der IPTV-Technologie die nötige Flexibilität, um sich in einem schnell wandelnden Markt behaupten zu können.

Die Studie empfiehlt daher, die Entwicklung für einen Übergangszeitraum dem Markt und den Standardisierungsgremien zu überlassen und nur dann regulierend eingreifen, wenn die Interoperabilität aus Kundensicht gefährdet sein sollte. Auch dann scheint eine Regulierung auf Dienste-Ebene sinnvoller als eine Festschreibung technischer Details.

1 Einleitung

Ziel dieser Studie ist die Untersuchung von Zugangssicherungssystemen für IPTV aus technischer Sicht unter Berücksichtigung der durch das Telekommunikationsgesetz (TKG) vorgeschriebenen Interoperabilitätssicherung.

Digitales Fernsehen in Europa wurde in der Vergangenheit ausschließlich durch die vom DVB-Projekt vorgegebenen Standards definiert. Im Kontext der Zugangssicherung gehörte hierzu auch die Verwendung von hardwarebasierten Mechanismen auf Basis des sog. Common Scrambling Algorithmus (CSA) zusammen mit der Anbindung von SmartCards über sog. Common Interface-Schnittstellen (CI).

Mit dem Aufkommen von neuen Diensten und neuen Arten des Content-Vertriebs und interaktiven Zusatzdiensten, wie Internet TV und IPTV verschwimmen die Grenzen zwischen „klassischem“ digitalem Fernsehen und neuen Formen zusehend. Dies tritt insbesondere bei IPTV in den Vordergrund, da sowohl die Konvergenz mit anderen Internetdiensten ('Triple-Play', 'Quadruple Play') als auch die Nutzung jenseits des herkömmlichen Fernsehverhaltens auf mehreren Endgeräten („3-Screen TV“) Teile des Grundkonzeptes sind.

Die soeben aufgeführten – sich vom klassischen digitalen Fernsehen abhebenden Merkmale – werden teilweise auch an der Rechtslage erkennbar. Während derzeit IPTV formal unter die spezifischen Regelungen des Telekommunikationsgesetzes fällt, welche CSA als Verschlüsselungsalgorithmus vorschreiben, ist dieser Teil des Gesetzes vorläufig für IPTV ausgesetzt, da die direkte Übernahme der DVB Technologien für IPTV nicht notwendigerweise angemessen ist und derzeit kontrovers diskutiert wird.

Da die, der derzeitigen Fassung des TKG zugrundeliegende, Forderung nach Interoperabilität auch für IPTV gelten muss, stellt sich die Frage nach den technischen Maßnahmen, welche nötig sind, um Interoperabilität für den Endverbraucher bei der Nutzung von IPTV Diensten zu gewährleisten.

Im Rahmen der Studie werden hierbei primär die technischen Aspekte dieser Frage erörtert. Das rechtliche und marktwirtschaftliche Umfeld wird berücksichtigt, spielt bei der Betrachtung aber nur eine untergeordnete Rolle. Nach einem kurzen Abriss über die derzeitige im DVB-Umfeld vorherrschenden rechtlichen und technischen Rahmenbedingungen wird im weiteren Verlauf auf die Situation im Bereich IPTV und die spezifischen Besonderheiten von IPTV im Vergleich zu anderen Formen des digitalen Fernsehens eingegangen. Darüber hinaus werden Zugangssicherungsmechanismen in anderen Medien betrachtet, die teilweise marktbedingt eine turbulentere Historie haben und deren Entwicklung potentiell Hinweise auf die zukünftige Entwicklung bei Videodiensten geben kann. Außerdem werden hiermit Alternativen zur CSA/CI/SmartCard basierten Zugangssicherung und deren Anwendbarkeit für IPTV aufgezeigt.

2 Rechtlicher Rahmen

Der rechtliche Rahmen für Zugangsberechtigungssysteme in Deutschland wird primär durch das Telekommunikationsgesetz vorgegeben, welches in §48 "Interoperabilität von Fernsehgeräten", Absatz 3 vorschreibt:

> (3) Jedes zum Verkauf, zur Miete oder anderweitig angebotene digitale Fernsehempfangsgerät, das für eine Zugangsberechtigung vorgesehen ist, muss Signale darstellen können,
>
> 1. die dem einheitlichen europäischen Kodieralgorithmus "Common Scrambling" entsprechen, wie er von einer anerkannten europäischen Normenorganisation verwaltet wird; für Geräte, bei denen die Zugangsberechtigung mittels eines Digital Rights Management (DRM) Systems realisiert wird, kann die Bundesnetzagentur abweichende Anordnungen und andere geeignete Maßnahmen zur Sicherstellung der Interoperabilität für digitale Fernsehempfangsgeräte treffen,
>
> 2. die keine Zugangsberechtigung erfordern. Bei Mietgeräten gilt dies nur, sofern die mietvertraglichen Bestimmungen vom Mieter eingehalten werden.

Diese Vorschrift ist nicht an die klassische Broadcastingumgebung gebunden, sondern ist auch für IPTV bindend. Es ist allerdings zu bemerken, dass auch im Rahmen der bestehenden Richtlinie andere Verfahren als "Common Scrambling" zugelassen werden dürfen, welche eine andere DRM Methode nutzen. Derzeit ist die Anwendung dieser Vorschrift durch die Bundesnetzagentur für IPTV Boxen bis zum 30.September 2009 ausgesetzt.

Es besteht eine gewisse Ambiguität bezüglich der Begriffe "Common Scrambling" und "Interoperabilität".

Auch wenn die Normenorganisation nicht direkt benannt wird, ist davon auszugehen, dass sich "Common Scrambling" spezifisch auf den CSA (Common Scrambling Algorithm), bezieht, welcher von der ETSI (European Telecommunications Standards Institute) entwickelt wurde und sich hierbei nicht auf einen anderen genormten und 'gebräuchlichen'' oder "gemeinsamen" Algorithmus bezogen wird. Allerdings besteht derzeit Unklarheit darüber, ob sich hieraus ein Zwang zur Benutzung zukünftiger Versionen von CSA (beispielsweise CSAv3) ergibt, oder hiermit die Benutzung des aktuell etablierten Algorithmus festgeschrieben wird.

Interoperabilität im Sinne des TKG wird allgemein aus Sicht des Endkunden betrachtet. Grundprinzip hierbei ist es dem Endkunden zu ermöglichen möglichst problemlos zwischen unterschiedlichen Anbietern zu wechseln oder auch die Angebote mehrerer Anbieter gleichzeitig zu nutzen. Dieses hängt oft mit der technischen Interoperabilität zusammen, ist aber damit nicht notwendig gekoppelt. Beispielsweise benutzen verschiedene Pay-TV-Anbieter derzeit technisch unterschiedliche und technisch inkompatible Schlüsselübertragungsmechanismen. Solange diese Inkompatibilität jedoch dem Benutzer verborgen ist (beispielsweise durch Implementierung der Methoden in austauschbaren Smart Cards), bleibt die Interoperabilität im Sinne des TKG weiterhin gewahrt.

Unter anderem auch aufgrund dieser begrifflichen Unklarheiten vertrat das Europäische Parlament in 6. Mai 2009 im Hinblick auf den Erlass zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, (Universaldienstrichtlinie) den Standpunkt, dass der entsprechende Paragraph wie folgt umformuliert werden sollte:

Alle für den Empfang von konventionellen Digitalfernsehsignalen (d.h. terrestrische, kabelgebundene oder satellitengestützte Übertragung eines Sendesignals, das hauptsächlich für den ortsfesten Empfang bestimmt ist) vorgesehenen Verbrauchergeräte, die in der Gemeinschaft zum Verkauf, zur Miete oder anderweitig angeboten werden und in der Lage sind, Digitalfernsehsignale zu entschlüsseln, müssen über die Fähigkeit verfügen,

- Signale zu entschlüsseln, die einem einheitlichen europäischen Verschlüsselungsalgorithmus entsprechen, wie er von einer anerkannten europäischen Normenorganisation, derzeit ETSI, verwaltet wird;
- Signale anzuzeigen, die unverschlüsselt übertragen wurden, sofern bei Mietgeräten die mietvertraglichen Bestimmungen vom Mieter eingehalten werden.

Eine Erwähnung eines spezifischen Algorithmus findet nicht mehr statt und schafft dadurch Raum für die Einführung von CSA v3 durch ETSI. Der Interoperabilitätsbegriff findet keine Anwendung mehr, die Möglichkeit der Zulassung anderer DRM Systeme ebenfalls nicht mehr vorgesehen.

Festzustellen ist aber vor allem, dass sich die Richtlinie jetzt nur noch auf herkömmliche digitale Fernsehsysteme bezieht (also DVB-C/-T/-S) und keine Anwendung mehr auf IPTV vorsieht.

3 Überblick derzeitiger Situation Content Protection DVB

Derzeit ist im DVB-Projekt der Common Scrambling Algorithmus als einziges Encryption-Verfahren zugelassen. Dieser wurde vom ETSI spezifiziert und vom DVB übernommen. Ursprünglich wurde der Algorithmus geheim gehalten und Lizenznehmern aus Gründen der Geheimhaltung nur Hardware gestützte Implementierungen gestattet. Nachdem die Grundstruktur des Algorithmus jedoch durch einen Patentantrag an die Öffentlichkeit kam, wurde im Jahr 2002 dann aus unbekannter Quelle eine Softwareimplementierung publik, durch welche CSA im Detail bekannt wurde.

Es handelt sich bei CSA um die Kombination einer Stream- und einer Blockkodierung (arbeitend auf 64-bit Blöcken). Beide Verschlüsslungen nutzen denselben 64-bit Schlüssel, bei DVB "Kontrollwort" genannt. Der Algorithmus wurde durch starke Betonung auf parallel ausführbare Berechnungen gezielt gestaltet, um die Berechnung durch spezielle Hardware effizient gestalten zu können und eine Implementierung als Softwarelösung zu behindern, was allerdings durch die Prozessorenentwicklung seit Entwurf des Algorithmus kaum noch Relevanz hat. CSA wird nur für den Videocontent selbst genutzt. Für den sicheren Austausch der Kontrollworte werden von den Anbietern unterschiedliche Systeme genutzt, beispielsweise Videoguard, Cryptoworks, Conax oder Nagravision. Diese Systeme sind technisch nicht interoperabel, ihre Interoperabilität aus Benutzersicht wird bei DVB Set-Top-Boxen durch das Common Interface (CI) gewährleistet, welches den definierten Schlüsselaustausch mit einer Smart Card ermöglicht, ohne dabei ein bestimmtes Verschlüsselungsverfahren zu mandatieren.

Der CSA selbst hat sich bisher als kryptologisch sicher erwiesen und hat keine inhärent ausnutzbaren Schwachstellen, ist allerdings aufgrund seiner geringen Schlüssellänge von 64-bit bei steigender verfügbarer Rechenleistung in absehbarer Zeit angreifbar. Da der durch CSA verschlüsselte Content an bekannten Stellen Checksummen enthält, ist die effektive Schlüssellänge derzeit nur 48 bit, was die potentielle Angreifbarkeit weiter erhöht. Trotzdem ist bisher kein Exploit bekannt, welcher den CSA-Algorithmus direkt addressiert. Erfolgreiche Angriffe auf geschützten Content im DVB Bereich beruhen derzeit alle auf fehlerhaften oder unvollständig gesicherten SmartCards, welche das direkte Auslesen des aktuellen Kontrollwortes ermöglichen.

Da die auf PCMCIA basierende CI-Schnittstelle keine weiteren Sicherheitsmechanismen beinhaltet, sind auch bei sicheren SmartCards einige Nutzungen des Contents möglich, die vom Provider nicht gewünscht sind. Dabei handelt es sich beispielsweise um Card-Sharing, bei dem die SmartCard an einem PC betrieben wird und die dekodierten Kontrollworte im Internet verbreitet werden. Weniger kritisch, aber aus Sicht der Content-Besitzer in unkontrollierter Form ebenfalls unerwünscht ist die Nutzung einer SmartCard durch mehrere Receiver in einem Haushalt unter Benutzung eines Card-Servers. Auch können SmartCards nicht erkennen, ob die Eingabe einer Jugendschutz-PIN direkt durch den Benutzer erfolgt oder eine gespeicherte PIN von der Set-Top-Box übermittelt wird.

Als Maßnahme gegen das Card-Sharing ist die Frequenz der Kontrollwortänderungen in den letzten Jahren deutlich erhöht worden, um die zeitgerechte Verbreitung im Internet zu erschweren. Auch haben einige Anbieter das SmartCard-Pairing eingeführt, welches sicherstellen soll, dass eine Karte nur in einem spezifischen Receiver benutzt werden kann. Allerdings kann auch dieses Verfahren umgangen werden, da der SmartCard über die CI-Schnittstelle, beispielsweise durch einen PC, eine beliebige Information vorgetäuscht werden kann. Weiterhin reduziert SmartCard-Pairing die Kunden-Akzeptanz, da ein Receiver nicht einfach durch ein neues Gerät ersetzt werden kann. De-facto wird

dadurch die Interoperabilität behindert. Beispielsweise hat Entavio das Pairing im Oktober 2008 wieder beendet.

Langfristig soll die Erhöhung der Sicherheit durch Einführung von CI+ (einer inkompatiblen Variante des Common Interface, bei der sich die Set-Top-Box und die SmartCard gegenseitig authentifizieren müssen) erreicht werden, sowie durch die Ablösung von CSA durch eine verbesserte Variante.

Hierzu ist die Einführung von CSAv3 vorgesehen (CSAv2 ist noch vor der Markteinführung gescheitert). Details der CSAv3 Implementierung sind, wie schon bei CSA selbst, nicht öffentlich. Aus allgemein zugänglichen Quellen lässt sich jedoch schließen, dass es sich dabei um eine Kombination zweier Blockkodierungen (AES und ein nicht näher definiertes DVB eigenes Verfahren) mit einer Schlüssellänge von 128-bit handelt, welches bereits vom Design her hardwarefreundlich und softwareunfreundlich sein soll. Eine detaillierte Bewertung der Sicherheit von CSAv3 und Vorhersage seiner Zukunftssicherheit ist derzeit aufgrund der "Security by obscurity" Einstellung des DVB nicht möglich.

4 Überblick derzeitige Situation IPTV

Interaktivität ist wohl das am häufigsten genannten Schlagwort derzeitiger Diskussionen bezüglich der Thematik IPTV. Der Nutzer wird in die Lage versetzt, sein persönliches, auf seine Interessen zugeschnittenes Programm mitbestimmen zu können. Personalisierte Dienste sind dabei nur ein Bestandteil eines innovativen und interaktiven Fernsehangebotes, das folglich eine Möglichkeit bieten muss, Interaktionen des Nutzers erkennen und verarbeiten zu können. Aus diesen Anforderungen lässt sich eine Basisarchitektur ableiten, die als minimale Voraussetzung einen Rückkanal für Steuerbefehle und Informationen des Nutzers bietet. Für diese Anforderungen haben sich besonders auf dem Internet-Protokoll (IP) basierte Netze empfohlen. Das populärste Beispiel eines IP-basierten Netzes ist ohne Zweifel das Internet. Folglich kristallisierte sich die Namensgebung des neuen Distributionsweges für Fernsehinhalte heraus, das „IPTV“ (Internet Protocol Television). Konkurrierend zum Begriff IPTV wird häufig auch fälschlicherweise die Bezeichnung „Internet-TV“ oder „Web-TV“ im Sprachgebrauch verwendet. Beide Ausdrücke bezeichnen aber keineswegs einen identischen Sachverhalt, sondern vielmehr zwei differenziert zu betrachtende Technologien und Anwendungsgebiete die sich unter anderem auch mit der Übertragung von Bewegtbild-Inhalten auseinandersetzen (siehe 4.1).

Ausgehend von den überlegenen technischen Möglichkeiten, die ein derartiges IP-basiertes TV-System gegenüber den herkömmlichen Broadcast-basierten Wegen, Fernsehen zu verbreiten, besitzt, könnte die Feststellung getroffen werden, dass es nur eine Frage der Zeit sein sollte, bis IPTV das zumeist lineare Fernsehen, wie wir es heute kennen, ablösen wird. Allerdings sollte man sich hier bewusst machen, dass die Entscheidung über Erfolg oder Misserfolg der neuen Technik im Endeffekt beim Nutzer liegt. Es muss demnach gelingen, bekannte Dienste wie Live-TV, Pay-TV (Bezahlfernsehen) und Radio mit neuartigen Diensten wie beispielsweise Video-on-Demand (VoD), interactive-TV (iTV), EPG, Wetten, Shopping, e-Commerce, Quiz, Spiele, Communities, netzwerkbasierte Videorekorder (Network PVR), Mobile-TV, HDTV und vor allem Telekommunikationsdiensten zu kombinieren. Im Ergebnis muss sich für den Endanwender ein Mehrwert an Nutzen ergeben, der sich mit hoher Wahrscheinlichkeit nur durch eine gesicherte Interoperabilität der Endgeräte und Dienste erreichen lässt. Für diesen komplementären Übertragungsweg zum klassischen analogen und digitalen Rundfunk empfehlen sich insbesondere Telekommunikationsnetze, deren Infrastrukturausbau in den letzten Jahren massiv durch die Betreiber vorangetrieben wurde. Netzbetreiber entwickeln sich damit zunehmend auch zu Plattformbetreibern, da für die Distribution der Dienste die notwendige Systemarchitektur in die neue Netzinfrastruktur integriert werden muss.

IPTV kann dabei nicht ausschließlich als neuer Distributionskanal neben den etablierten Übertragungswegen Kabel, Satellit und Terrestrisch angesehen werden, sondern stellt vielmehr eine völlig neue Basis für die Entwicklung und Verbreitung innovativer Dienste bereit, deren Marktpotential sich derzeit nur erahnen lässt. Als exemplarisches Bespiel nichtvorhersehbarer Marktpotentiale und Entwicklungsmöglichkeiten von Diensten kann der *Short Message Service*, besser bekannt unter der Abkürzung *SMS* herangezogen werden. Ursprünglich als Teil des Signalisierungskanals ausgelegt um Störungen oder ähnliche Informationen an die Nutzer zu übermitteln, entwickelte sich dieses regelrechte Nebenprodukt zu einem der bisher erfolgreichsten Dienste und größten Ertragsbringer der Netzbetreiber. Heute werden in Deutschland jährlich SMS im zweistelligen Milliardenbereich versendet. Im Hinblick auf die noch junge Geschichte von IPTV können hier Parallelen gezogen werden: Der Markt für IP-basierte TV Dienste ist noch

vergleichsweise neu, die Dienste selbst befinden sich gerade in der Entstehungsphase und derzeitige IPTV Angebote repräsentieren allenfalls den ersten Schritt der Provider in die neue Technologie. Das tatsächliche Potential von IPTV-Diensten wird sich erst nach erfolgtem Netzausbau und Findung des Marktes zeigen. Von immenser Bedeutung bleibt hier die Möglichkeit der Angebotsentfaltung für alle Marktteilnehmer (Service Provider, Netzbetreiber, Gerätehersteller, Content-Industrie), deren Grundlage ein möglichst offenes und damit möglichst wenig reglementiertes Umfeld sein muss. Nur so können optimale Entwicklungsmöglichkeiten für eine innovations-affine Technologie geschaffen werden.

4.1 Abgrenzung des Begriffs IPTV und Potentiale

Die derzeit stattfindende Industrie- und marktweite Diskussion über IP-basierte Videodienste geht mit der Vermischung der Begriffe IPTV und Internet-TV einher. Abgesehen von der Tatsache, dass beide Technologien unter anderem die Idee verfolgen, Videoinhalte über IP-basierte Netzwerke zu übertragen, sind die Ansätze, dies zu realisieren, jedoch aus Plattform-, Dienst- und Marktperspektive grundsätzlich differenziert zu betrachten. Zur Klassifizierung und Unterscheidung werden nachfolgend charakteristische Merkmale wie Netzwerkarchitektur, Bereitstellung von Inhalten und mögliche Dienste beider Technologien erläutert.

Das Internet-TV basiert auf existierenden Internettechnologien, die es ermöglichen Videoinhalte ohne zusätzliche Hardware oder spezielle Endgeräte weltweit mit dem PC empfangen zu können. Damit ist Internet-TV unabhängig von Service-Providern, Internetdienstanbietern, speziellen Set-Top-Boxen (STB) und benötigt außerdem keine erweiterte Infrastruktur. Ein herkömmlicher Personal-Computer (PC) mit einem Breitband-Internetanschluss genügt, um Internet-TV-Angebote nutzen zu können. Damit wird deutlich, dass Internet-TV auf einem offenen Netz aufbaut, das es jedem Rechteinhaber ermöglicht, seine Inhalte anzubieten. Selbst der private Nutzer ist damit in der Lage, eigene Inhalte über diese Technologie anzubieten. Es ist somit einerseits möglich nahezu jedes Nischenangebot zu bedienen, andererseits macht es die Kontrolle der angebotenen Inhalte hinsichtlich Rechten und Vermarktung nahezu unmöglich. Auch die Qualität von Bild und Ton, die Verfügbarkeit sowie der Inhalt des Angebotes unterliegen somit großen Schwankungen, die der gewohnten Dienstgüte des klassischen Fernsehens entgegenstehen.

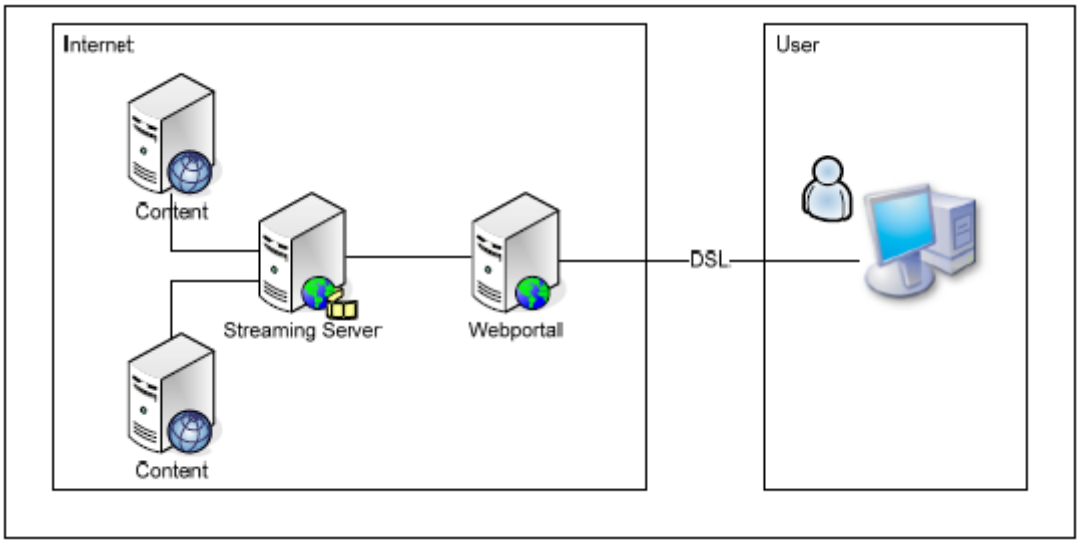

Abbildung 1 - Basisarchitektur eines Internet-TV-Systems

Abbildung 1 zeigt den prinzipiellen Aufbau eines Internet-TV-Systems. Internet-TV präsentiert sich dem Nutzer als eingebetteter Dienst im gewohnten Surferlebnis, dessen Qualität maßgeblich von der verfügbaren Internetanbindung des Nutzers abhängt (*best-effort Prinzip*). Als Beispiele für Internet-TV sind Live-Streams diverser Fernsehsender, Shows und Videos unabhängiger Produzenten, on-demand verfügbare Serien und Videoportale zu nennen. Es zeigt sich, dass Internet-TV ein breites Spektrum der Netzkultur abdeckt, durch die Breite des Angebotes für viele Nutzer interessant ist, andererseits aber keine technologische Alternative zu den bestehenden Broadcast- bzw. Rundfunksystemen bietet, da nicht die selbe Übertragungsqualität zugesichert werden kann. Auch ist der Inhalte-Schutz oft gering, da viele Anbieter, wie auch beim Internet-Radio, auf eine Verschlüsselung der Inhalte bei der Übertragung verzichten.

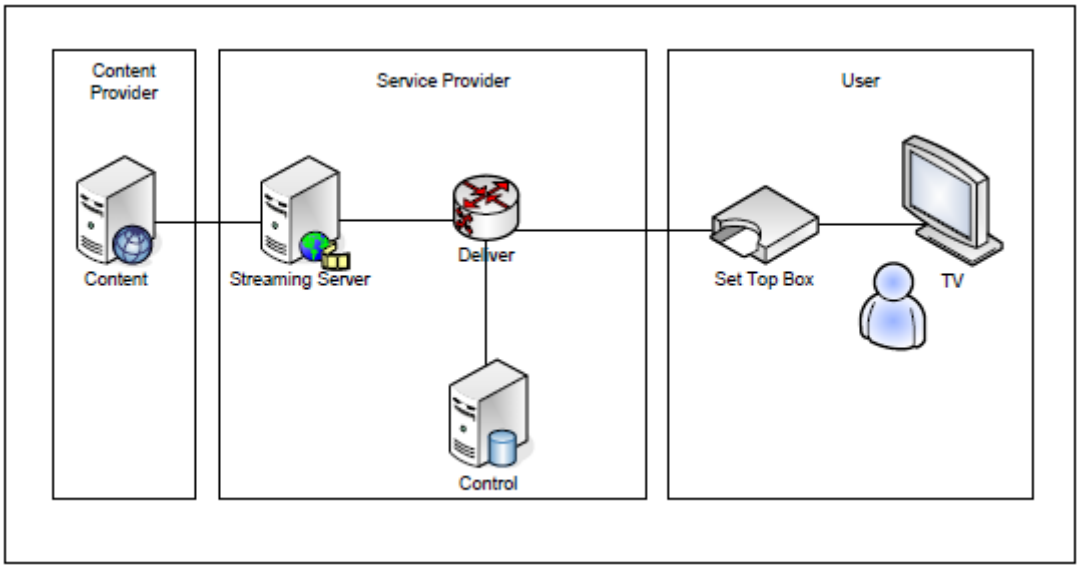

Abbildung 2 - Basisarchitektur eines IPTV-Systems

IPTV hingegen bezeichnet eine grundlegend andere Philosophie, Video und TV in die Haushalte und auf die Endgeräte des Nutzers zu transportieren. Abbildung 2 zeigt die prinzipielle Architektur eines IPTV-System. IPTV bezeichnet bereits in seinem Namen eine Übertragungstechnik, das Internet Protokoll, und ist im Gesamten als gänzlich neuer Übertragungsstandard für Video- und Fernsehsignale über IP-basierte Netze zu charakterisieren.

Der bedeutendste technische Unterschied zum Internet-TV besteht darin, dass die Ausstrahlung der Inhalte ausschließlich in kontrollierten, paketorientierten Netzen stattfindet. Dadurch ist auch eine Trennung zwischen Service- und Content-Providern möglich. Inhaber dieser Netze sind zumeist national agierende Telekommunikationsanbieter. IPTV bietet, im Gegensatz zu Internet-TV, auch traditionelles Fernsehen in gewohnter Qualität, also mit einer Bildqualität, welche auch bei einer Bewertung nach ITU-R BT 500-7 anhand der "Double Stimulus Continuous Quality Scale, (DSCQS)" jetzigem Broadcast-Fernsehen entspricht, unter Benutzung eines IP-basierten Transportnetzwerkes und bildet damit eine konkurrierende Plattform zum etablierten Broadcast. Es stellt neben den Übertragungswegen Kabel, Satellit und Antenne einen vierten Distributionskanal für Fernsehdienste dar. Telekommunikationsbieter schaffen sich damit die Möglichkeit, zum Triple Play-Anbieter aufzusteigen und Daten- (Internet), Sprach- (Voice-over-IP) und TV-Dienste aus einer Hand anzubieten. Als Übertragungstechnologie von linearen TV Programmen kommt das IP-Multicast-Verfahren zum Einsatz.

Derzeitige IPTV-Lösungen bilden geschlossene, zumeist proprietäre Systeme, die Inhalte über IP-basierte sichere Kanäle übertragen. Dies ermöglicht den Betreibern von Breitbandnetzen (in der Regel DSL Netze) die Verteilung von Inhalten gezielt zu steuern, um beispielsweise abonnierte Inhalte für registrierte Nutzer frei zu schalten und insbesondere ein gewisses Maß an Dienstgüte (Quality of Service) sicherstellen zu können. Ein kontrollierbares, geschlossenes Netz eignet sich desweiteren besonders zur Sicherung von Rechten an den ausgestrahlten Inhalten und Etablierung von zukunftsträchtigen Schutzmechanismen zur Kontrolle digitaler (IP-basierter) Telemedien.

Das Angebotsspektrum an Diensten im IPTV geht dabei deutlich über die lineare Weiterleitung von analogem und digitalem Rundfunk hinaus und impliziert folglich erweiterte Nutzungs- und Dienstszenarien, Anforderungen an das Content-Schutzsystem sowie die Endgeräte selbst. Diese Aspekte bedürfen insbesondere auch einer gesonderten Betrachtung hinsichtlich regulatorischer Rahmenbedingungen und standardisierter Content-Schutzmechanismen als Grundlage möglichst umfassender Interoperabilität aus Kundensicht.

Ein weiteres Merkmal von IPTV ist die Interaktivität, die durch den verfügbaren Rückkanal vom Nutzer zum Dienstanbieter entsteht. Auf dieser Grundlage wird IPTV zur idealen Plattform für personalisierte Dienste und setzt sich hier maßgeblich von bisher definierten interaktiven Lösungen für Fernsehdienste ab. Bei IPTV ist der Rückkanal nicht nur optional verfügbar (vgl. DVB MHP-Systeme), sondern es ist vielmehr sichergestellt, dass jedes Endgerät in jeder Nutzungssituation auch tatsächlich die Verbindung über den Rückkanal ohne wahrnehmbaren Medienbruch aufbauen kann. Dies bildet die technische und marktpolitische Basis zur Etablierung vielfältiger neuer Geschäftsmodelle und interaktiver TV-Dienste, wie beispielsweise Inhalte-bezogene Zusatzinformationen, Video on-Demand, Shopping, Interaktive Voting und Quiz-Applikationen, EPG/BCG, PVR, oder e-Commerce, die im Gegensatz zu bekannten Fernsehsystemen auf Wünsche, Verhalten und Aktivitäten des Nutzers eingehen können. Infolge der bidirektionalen Kommunikation, die in IPTV Systemen unerlässlich ist und gleichzeitig die Authentifizierung des Endkunden am netzwerkterminierenden Breitbandanschluss sicherstellt, kann dem Nutzer eine völlig neue Bandbreite an digitalen TV- und Telemediendiensten durch die jeweiligen Provider zur Verfügung gestellt werden.

Als eines der ersten Standardisierungsgremien formulierte die ATIS IPTV Exploration Group eine Antwort auf die Frage: „Was ist IPTV?“. Sie fasst alle angesprochenen charakteristischen Kernpunkte von IPTV zusammen und dient seither als Referenz zur Begriffsdefinition:

“The secure and reliable delivery to subscribers of entertainment video and related services. These services may include, for example, Live TV, Video On Demand (VOD) and Interactive TV (iTV). These services are delivered across an access-agnostic, packet-switched network that employs the IP protocol to transport the audio, video and control signals. In contrast to video over the public Internet, with IPTV deployments, network security and performance are tightly managed to ensure a superior entertainment experience, resulting in a compelling business environment for content providers, advertisers and customers alike”.

4.2 Systeme am Markt

Heute im Markt befindliche IPTV Systeme sind infolge der sich noch im Entwicklungsprozess befindlichen Standardisierung von IP-basiertem digitalen Fernsehen hinsichtlich Dienstzugang, Signalisierung und Content-Schutz zumeist proprietär bzw. bedienen sich Marktstandards aus der

Internet-Welt. Für den Zugang zu IPTV-Diensten benötigt der Endkunde sowohl einen speziellen Breitbandzugang, zumeist ADSL bzw. VDSL, als auch ein spezielles, vom jeweiligen Anbieter abhängiges Empfangsgerät in Form eines Receivers. Dieses auch Set-Top-Box genannte Endgerät wird mit dem TV-Gerät als auch dem Breitbandrouter im Heimnetz verbunden. Die Set-Top-Box übernimmt dabei üblicherweise den Empfang der IP-basierten Datenströme (sowohl Multicast als auch Unicast), die Entschlüsselung (Decryption) und Decodierung der AV-Inhalte, die Ausführung der gewünschten Applikationen und letztendlich die Darstellung der Dienste in Bild und Ton an den Geräteausgängen. Neben den genannten Basisfunktionalitäten verfügen IPTV Set-Top-Boxen über weitere Ausstattungsmerkmale zur Unterstützung von beispielsweise zeitversetztem Fernsehen (Time-Shift), Personal Video Recorder (PVR) Funktionalität, Abrufen von interaktiven Zusatzdiensten oder die Übertragung von Inhalten und Daten an Drittgeräte. Das verfügbare Funktionsspektrum ist dabei momentan von den angebotenen Diensten und Geschäftsmodellen des jeweiligen Anbieters abhängig. Grundlegende Voraussetzung zur Nutzung der IPTV-Dienste ist die Buchung eines entsprechenden Produktes des IPTV-Anbieters. In der Regel werden IPTV-Dienste heute als Bestandteil von Triple-Play Lösungen, also einem Dienstpaket aus Telefonie, Breitbandinternetzugang und Fernsehen angeboten. Der Kunde kann folglich über seinen Breitbandanschluss gegenüber dem IPTV-Anbieter bzw. Plattformbetreiber authentifiziert werden. Eine Authentifizierung kann abweichend davon auch direkt über die zur Verfügung gestellte Set-Top-Box realisiert werden. In beiden Fällen ist somit sichergestellt, dass dem Endkunden die gebuchten Dienste zur Nutzung bereitgestellt werden können. Zum Einsatz kommen dabei Verfahren, die auf einen bidirektionalen Austausch von Zertifikaten aufbauen, um sowohl die Zugangsberechtigung als auch die Verschlüsselung bzw. den Schutz von Inhalten und Diensten sicherzustellen. Infolge des breiten Dienstspektrums, das im IPTV realisiert werden kann kommen hierbei Verfahren zum Einsatz, die in ihrer Funktionsweise grundlegend verschieden zu bekannten Verfahren im klassischen Broadcast-TV Bereich sind.

Bei Betrachtung der verschiedenen am Markt aktiven IPTV Plattformbetreiber lässt sich feststellen, dass diese naturgemäß unterschiedliche Technologien in ihren Systemen einsetzen. Dies ist zusätzlich durch das Fehlen systemweiter Standards und der derzeitigen Marktphase von IPTV begründet. Auf den gesamten Produktzyklus gesehen, befindet sich IPTV noch immer in der Einführungsphase. Geschäftsmodelle und Dienste unterliegen einem stetigen Weiterentwicklungsprozess und fordern in diesem Stadium der neuen Technologie eine möglichst einfache und zeitunkritische Abstimmung der einzelnen Systemkomponenten zur Sicherstellung eines stabilen Dienstangebots.

Konvergenz durch NGN Architekturen - Getrennte Welten wachsen zusammen

Um mit der Ausweitung des Dienstangebots erfolgreich zu sein, müssen die Anbieter von Telekommunikationsdienstleistungen die volle Kompatibilität zwischen verschiedenen Technologien sowie die Konvergenz von Fest- und Mobilfunknetzen gewährleisten, das gilt insbesondere auch für IPTV. Die Telekommunikation-Industrie versucht diesbezüglich Rahmenwerke für einheitliche Standards und Schnittstellen für zukünftige Dienstinfrastrukturen zu erarbeiten. Das IP Multimedia Subsystem (IMS) ist dafür ein exemplarisches Beispiel.IMS (IP Multimedia Subsystem) steht für eine NGN-Architektur (Next Generation Network), die es ermöglicht, Multimedia-Dienste in Fest- und Mobilfunknetzen zu realisieren.

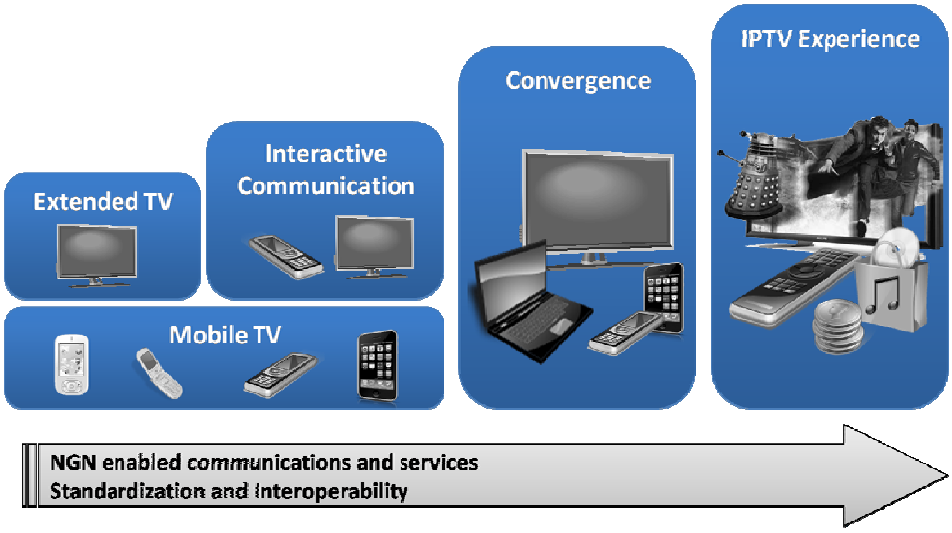

Abbildung 3 - Evolution von TV Services

IMS basiert auf dem Internet Protocol (IP) und soll dazu dienen, die Lücke zwischen der traditionellen Telekommunikations- und der Internet-Technologie zu schließen. Ein wichtiges Ziel ist es, identische Dienste über verschiedene Zugänge anbieten zu können, also kabelgebunden oder mobil, im Inland wie im Ausland. Mit IMS lässt sich ein TV-Service also an jedes Endgerät in jedem Netzwerk ausliefern. IMS macht es auch möglich, eine laufende Datenübertragung vom Fest- zum Mobilfunknetz (und umgekehrt) zu übergeben. Inhalte werden ortsunabhängig abrufbar, eine Bindung des Nutzers an bestimmte Endgeräte oder Nutzungsumgebungen entfallen und verschaffen dem Endkunden mehr Freiraum und Entscheidungsgewalt im Umgang mit Telemedien. Mit Dienstarchitekturen wie IMS wird es möglich an jedem Aufenthaltsort VoD-Dienste (Video-on-demand) zu nutzen, zu telefonieren, zu chatten, Textnachrichten zu senden und empfangen sowie sich an elektronischen Abstimmungen zu beteiligen. Über mobile Endgeräte kann von unterwegs mit dem TV- und HiFi-Geräten daheim kommuniziert werden, digitale Filme lassen sich beispielsweise vom Fernsehapparat drahtlos aufs Handy übertragen und Fotos und Multimediainhalte werden vom Heim-PC auf das mobile Endgerät heruntergeladen. NGN-basierte IPTV Plattformen fördern die Entwicklung von konvergenten und übergreifenden Kommunikations- und Unterhaltungsdiensten und bieten neue Dienst- und Marktperspektiven. Die Mediennutzung wird individueller und überwindet technologische Plattformbarrieren – Interoperabilität findet in einer neuen Qualität statt.

4.2.1 Ericsson IPTV Solution

Der schwedische Konzern Ericsson verfügt als erster Anbieter von Telekommunikationslösungen über eine IPTV-Middleware die den IMS-Standard unterstützt. Ericsson stellte die komplette Lösung erstmals zur International Broadcast Conference (IBC) im September 2008 der breiten Öffentlichkeit vor. Als offene, auf Standards basierende End-to-End Lösung bietet Ericsson IPTV im Vergleich zu proprietären Plattformen ein höheres Maß an Flexibilität und erleichtert die Integration von Technologien und Diensten Dritter.

Ericsson folgt damit der technologischen Entwicklung von konvergenten und übergreifenden Kommunikations- und Unterhaltungsdiensten im Telekommunikationssektor. Dabei setzt das entwickelte System auf den ersten verwertbaren Spezifikationen des sog. ETSI TISPAN Release 2 hinsichtlich NGN basierter IPTV Dienstplattformen auf. Zentrale Technologien beziehen sich auf IPTV

Middleware, die IPTV Netzinfrastruktur (in Verbindung mit IMS / NGN), Video Processing und Video On-Demand Lösungen, die auch Produkte von Drittanbietern integrieren.

Der mögliche Funktionsumfang geht dabei weit über die Broadcast-Dienste klassischen Digitalfernsehens hinaus. Neben Basisdiensten heutiger TV Lösungen wie hochauflösendes Fernsehen (HDTV), EPG, der persönliche Videorekorder (PVR) oder Video On-Demand Funktionalitäten stellt die NGN-basierte Lösung eine Reihe an innovativen Mehrwertdiensten bereit. Infolge konvergenter Dienstplattformen und einer eindeutigen Nutzer-Authentifizierung (ähnlich heutiger Mechanismen im Mobilfunk) werden personalisierte und interaktive Dienste auf Endgeräten aller Art ermöglicht. TV-Dienste können infolge der technologischen Konvergenz individualisiert und plattformübergreifend angeboten werden. Durch IMS kommen zusätzliche Kommunikationsdienste wie Anwesenheitsanzeigen der Nutzer (Presence Information), Chat- und Messaging Funktionen, Videotelefonie, effiziente Kinder- und Jugendschutzmechanismen und mobile Nutzungsszenarien hinzu.

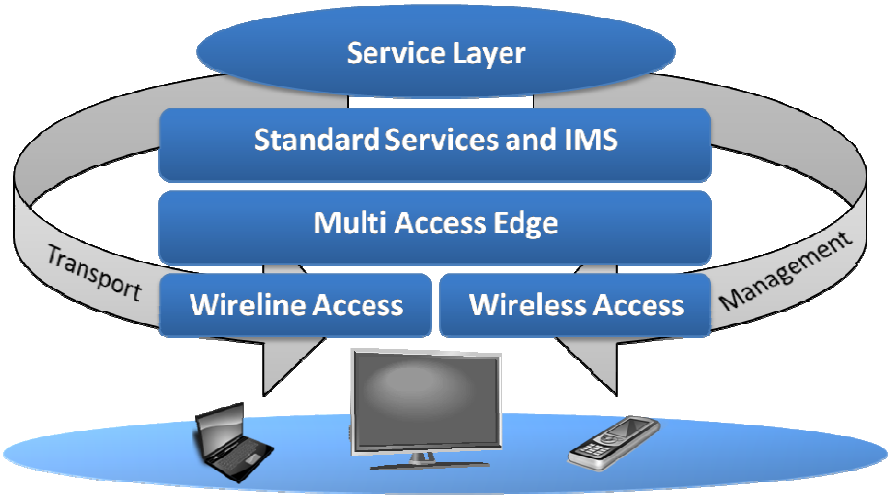

Abbildung 4 – NGN basierte End-to-End IPTV Lösung

Ericssons Lösung versteht sich als Integrationsplattform für ein umfassendes Dienstportfolio mit dem Ziel eine möglichst hochintegrierte End-to-End Lösung für IPTV bereitzustellen. Standards als Basis für Interoperabilität von Plattformen, Diensten und Endgeräten spielen dabei eine zentrale Rolle. Die potentielle Bandbreite von IPTV Diensten und damit verbundenen neuen Herausforderungen an die Marktteilnehmer in NGN basierten IPTV Lösungen werden durch Ericssons Lösung aufgezeigt. Die Evolution von Fernsehdiensten vollzieht sich dabei von ersten Erweiterungen zu klassischen digitalen Broadcast TV Angeboten (Extended TV) über die Integration von interaktiven Kommunikationsdiensten hin zu einer konvergenten und aus Nutzersicht individualisierbaren TV- und Mediennutzung. Das Dienstspektrum von NGN-basierten IPTV Lösungen geht weit über die Angebote digitalen Fernsehens hinaus.

4.2.2 Nokia Siemens Networks – Home Entertainment

„Ein multimediales Erlebnis für den Endkunden, dass es ihm gleichzeitig ermöglicht eigenen Content, verteilte Inhalte sowie die Teilnahme an Communities wahrzunehmen – zu jeder Zeit an jedem Ort mit jedem Gerät“, so stellt sich Nokia Siemens Networks (NSN) eigenen Angaben zufolge das

Fernsehen der Zukunft vor. Die passende technische Plattform soll dafür die hauseigene IPTV-Lösung bieten. Sie hört auf den Namen „Nokia Siemens Networks – Home Entertainment“ und steht in der aktuellen Release Version 3.0 bereit. Wie andere Mitstreiter am Markt, stellt sich auch NSN dem gegenwärtigen Paradigmenwechsel des Telekommunikationsmarktes und entwickelt Lösungen, die letztlich ein Angebot durch Service-Provider ermöglichen, das den wachsenden Ansprüchen des Endkunden Rechnung trägt. Neben Breitband-Internetzugang und (mobilen) Telefonie-Diensten, die heute das traditionelle Telekommunikationsgeschäft bereits abgelöst haben, gehen Kabelnetzbetreiber und Medienunternehmen dazu über ihrerseits traditionelle Märkte auszuweiten und selbst TK-Dienste wie Internet und Voice anzubieten. IPTV wird in diesem Zusammenhang von Telekommunikationsbetreibern oftmals als Chance verstanden die eigenen Kunden durch neue innovative Dienste zu erhalten bzw. auszubauen und gleichzeitig größtmöglichen Nutzen aus dem ohnehin stattfindenden Breitbandausbau zu ziehen. Dieser Zielsetzung folgt auch NSN Home Entertainment und versteht sich dabei als offene Plattform für IPTV Dienste.

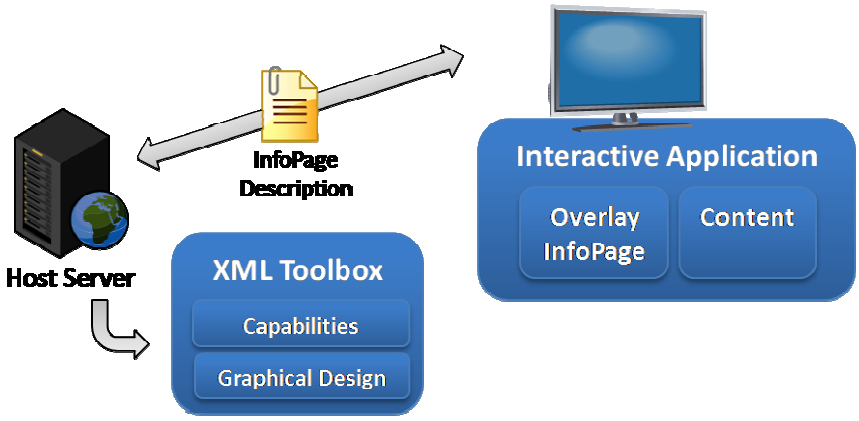

Abbildung 5 - Interaktive Applikation über NSN Web Media Ansatz

Neben bekannten Standarddiensten wie HDTV, Personal Video Recorder (PVR) und Video on Demand setzt die NSN Lösung insbesondere auf Integrationsmöglichkeiten von Drittanbieter-Anwendungen aus der Web 2.0 Welt. Dieses offener gestaltete Modell-Ansatz steht den bisherigen meist proprietären IPTV Systemlösungen entgegen. Dazu bietet NSN ein Software Development Kit (SDK), das die Entwicklung einer an Drittanbieteranwendungen anpassbaren Benutzeroberfläche (UI) ermöglichen soll. IPTV Betreiber können so ihre Angebote entsprechend den eigenen Anforderungen anpassen und optimieren. Die Technologie basiert auf heutigen Internet-Standards wie Java und HTML und erlaubt das Einbinden von Plug-ins und sogenannten Scriptables, kleinen Codebausteinen für erweitere Dienste.

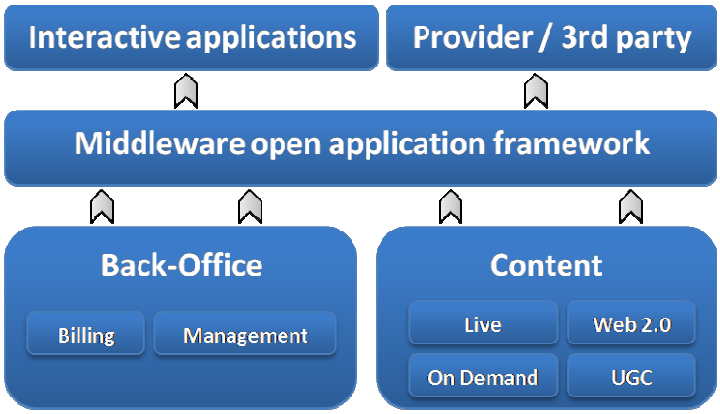

Abbildung 6 - NSN Web Media Middleware Architektur

Damit bietet auch NSN potentielle Dienstfunktionalitäten, deren Nutzungsverhalten und Erscheinungsbild bekannten Internetanwendungen aus dem Web 2.0 deutlich näher sind als klassischen digitalen Rundfunk. Das Funktionsspektrum und den damit einhergehenden Anforderungen an das Gesamtsystem hinsichtlich Dienststeuerung, Provisionierung und nicht zuletzt Schutz der Inhalte wird signifikant erweitert und erforderte andere und erweiterte Verfahren die auf eine derartige Nutzung zugeschnitten sind. Dies macht auch NSN mit weiteren verfügbaren Systemkomponenten wie beispielsweise der NSN Home Media Server-Lösung deutlich. Sie erweitert IPTV Dienste auf den PC und stellt umgekehrt von Nutzern generierte Inhalte (User-generated Content) von verschiedensten Medienquellen auf der IPTV Set-Top-Box bereit. Anwendungsszenarien werden infolge der technischen Fortschritte komplexer und erfordern gleichzeitig flexibler anpassbare Einstellungsmöglichkeiten durch den Nutzer. Denn der Nutzer ist es, der die Web-basierten Dienste mit TV-Support und deren Inhalte über Gerätegrenzen hinweg und unabhängig vom klassischen IPTV Endgerät Set-Top-Box nutzen möchte. Es zeichnet sich ein Migrationspfad NGN-basierter IPTV Plattformen ab, der es dem Kunden ermöglicht trotz der technologische Vielfalt der Bereiche Broadcast TV, IPTV und Mobile TV unkompliziert, jederzeit und ortsunabhängig auf die gewünschten Inhalte zugreifen zu können. Auch NSN bezeichnet diese Entwicklung als *Rich Media Experience*, die es dem Kunden zukünftig ermöglichen soll TV und Medien in einer verbesserten Nutzungs- und Dienstqualität zu erleben.

Demgegenüber steht allerdings die Feststellung, dass auch die NSN Lösung als offene Lösung propagiert wird aber letztlich eine in sich geschlossene Komplettlösung darstellt. Dies zeigt sich auch im SDK, dass es basierend auf Standard-Internettechnologie ermöglicht interaktive Applikationen zu entwickeln, andererseits aber keinem der sich entwickelnden Standards für IPTV entspricht. Beim Thema Schutz der Inhalte setzt NSN auf die Verschlüsselungslösung *Video Content Authority System (VCAS)* des Unternehmens *Verimatrix*. VCAS verfügt u.a. über die für IPTV Systeme konzipierte *Verimatrix MultiCAS/IP* Technologie, die es Herstellerangaben zufolge erlaubt IPTV Headend Scrambler Equipment von Drittanbietern unter einem robusten Software-basierten Content Secutity Systems zu vereinen. Dazu baut MultiCAS/IP auf das von DVB standardisierte Simulcrypt Verfahren auf, um innerhalb der eigenen Lösung VCAS kompatible Encryption multipler Datenströme zu ermöglichen. Auf Client-Seite, d.h. auf der IPTV Set-Top-Box findet die *Verimatrix ViewRight STB for IPTV Client* Technologie Anwendung. Als portabler embedded Code implementiert *ViewRight* die erforderlichen Sicherheitsfunktionen des VCAS Systems auf verschiedenen Set-Top-Boxen.

4.2.3 Microsoft Mediaroom

Microsoft stellte Ende 2004 die Systemlösung Microsoft IPTV Edition als Nachfolger von Microsoft TV vor. Drei Jahre später erfolgte die Umbenennung des Produktes in Mediaroom. Unter dieser Marke wird es heute B2B vertrieben.

Microsoft Mediaroom wurde als schlüsselfertige Lösung zur Verfügung gestellt und von vielen Telcos weltweit ausgewählt, um ein umfangreiches IPTV-Produkt über das jeweilige Netz auf den Markt zu bringen. Die Übertragung erfolgt stets IP-basiert und in den meisten Fällen über Gigabit-Ethernet-Netzwerke und zum Endkunden über DSL-Technologie (VDSL2 und ADSL2+) auf den vorhandenen Telefon-Teilnehmeranschlussleitungen.[1]

Microsoft Mediaroom genießt heute weltweit den größten Marktanteil. Mediaroom wird u. a. genutzt von Deutsche Telekom (Deutschland), Portugal Telecom (Portugal), Swisscom (Schweiz), AT&T (Vereinigte Staaten von Amerika), Reliance (Indien), MTS Allstream (Kanada), SingTel (Singapur), BT (UK) und Guangzhou Digital Media Group (China).

Über Mediaroom verbreitete Fernsehsender können neben einer Set-Top Box mit Microsoft Mediaroom Betriebssystem und Client Software auch mit Microsofts Xbox 360 empfangen werden. Die Plattform ist grundsätzlich proprietär, bedient sich jedoch diverser Standards aus dem IT- und Broadcast-Umfeld. So erfolgt die Übertragung der linearen TV-Programme als MPEG2 Transport Stream nach DVB-Standard über einen IP/UDP/RTP Protokoll Stack. Zum Schutz von linearen und non-linearen (Video on Demand) Inhalten kommt anstelle des CSA (Common Scrambling Algorithm) der AES (Advanced Encryption Standard) zum Einsatz. Mediaroom bietet den Vorzug, sowohl die linearen als auch die non-linearen Inhalte mit dem gleichen DRM System zu verschlüsseln. Ein Vorteil der Verwendung des gleichen Algorithmus liegt in der Distribution der gleichen Inhalte auf unterschiedliche Endgeräte, wie Spielekonsolen, portable Wiedergabegeräte, Mobiltelefone, die für gewöhnlich nicht mit CSA ausgestattet sind oder ausgestattet werden können.

Der besondere Vorteil von Mediaroom liegt in der Vielfalt der Mehrwerte und Funktionen, die über rein lineares Fernsehen hinaus gehen. Die Plattform bietet Inhalte in Standard Definition und High Definition (HDTV). Timeshift- und PVR Recording (Personal Video Recorder) sind in Abhängigkeit von den über das DRM signalisierten Nutzungsrechten möglich. Gleichzeitig sind der Konsum und die Aufzeichnung mehrerer Programme möglich (in Abhängigkeit von der zur Verfügung stehenden Übertragungsbandbreite auf der Teilnehmeranschlussleitung). Die Übertragung von Video on Demand Inhalten erfolgt als Unicast und damit zu einem vom Kunden bestimmten Zeitpunkt. Der EPG wird außer mit SI-Daten auch über separat redaktionell aufbereitete Informationen versorgt. Ein Browser und ein spezielles Application Framework bieten Diensteanbietern die Möglichkeit, Zusatzdienste zu implementieren. Darüber lassen sich vielfältige interaktive Applikationen realisieren. Beispiele hierfür sind etwa die T-Home Bundesliga-Applikation, das Spieleangebot der British Telecom und Applikationen von AT&T.

[1] Der Dienst Zhujiang Digital der Guangzhou Digital Media Group in China überträgt stattdessen erstmals Mediaroom TV-Programme und Dienste über ein Fernsehkabelnetzwerk (IP over Cable). Bei der British Telecom wurde dagegen die Übertragung der linearen TV-Programme auf die terrestrische Übertragung verlagert und nur Video on Demand Inhalte und weitere Dienste werden über DSL zum Kunden übertragen. Im Falle dieser Hybrid-Lösung kann somit nur bedingt von IPTV gesprochen werden.

Das DRM System der Mediaroom Plattform ist ein eingebettetes System und verzichtet auf Hardware-Formfaktoren wie CI (Common Interface), CAM (Conditional Access Module) und Smart Card. Eine Ausnahme bildet die hybride Lösung der British Telecom, wobei das dort für den DVB-T Empfang eingesetzte CA-System isoliert vom IPTV-Übertragungsweg zu betrachten ist.

Neben der Möglichkeit zur Authentifizierung des Endkunden über den Breitband-Anschluss (heute noch mittels PPPoE) erfolgt bei Mediaroom immer auch eine Authentifizierung des Endgeräts (Set-Top Box). Da Mediaroom auf Smart Cards verzichtet, erfolgt die Authentifizierung und Autorisierung über ein Endgeräte-Zertifikat im X.509 Format, welches bei der Herstellung in das Endgerät eingebracht wird. Das Endgerät muss sich gegenüber einem Server im Backend mittels des Zertifikats ausweisen, um Inhalte und Dienste empfangen zu können. Während der Authentifizierung mittels Zertifikat werden im Rahmen eines PKI Verfahrens (Public Key Infrastructure) auch die DRM-Schlüssel ausgehandelt, die für die spätere Entschlüsselung des Datenverkehrs benötigt werden.

Auch für die Entschlüsselung der Inhalte ist eine Client-Server-Kommunikation erforderlich, da die Kontrollwörter nicht im Transport Stream (oder mit dem Video on Demand Inhalt), sondern „out of band“ zum Client übertragen werden. Die Schlüssel werden dabei erst zum Client übertragen, nachdem im Headend/Backend geprüft wurde, ob eine Berechtigung zum Abruf des Inhalts vorliegt.

4.3 Standardisierung

Weltweit arbeiten Unternehmen der IT- und Telekommunikationsbranche mit Hochdruck daran, IPTV-Dienste mit maßgeschneiderten und hochwertigen Inhalten anzubieten. Von Standardisierungsgremien und Industrieorganisationen gebildete Konsortien koordinieren dazu die Aktivitäten, die mit der technologischen Weiterentwicklung und Standardisierung der IPTV-Dienste, Systemarchitekturen und Protokollen in Verbindung stehen. Sie forcieren die Entwicklung neuer Standards hinsichtlich geeigneten Szenarien, Netzwerk- und Softwarearchitekturen, Bereitstellung von Diensten, Signalisierungs- und Transportprotokollen zur Übertragung und Steuerung multimedialer Inhalte sowie geeigneten Content-Schutzmechanismen. In diesem Zusammenhang ist insbesondere die Integration von IPTV-Systemen in Telekommunikationsnetze der nächsten Generation (NGN) zu beachten, die als All-IP Infrastruktur eine Fülle an Möglichkeiten zur Entwicklung innovativer multimedialer (TV) Anwendungen auf Basis von netzübergreifenden Dienstplattformen ermöglichen. Getrieben durch den Wunsch aller beteiligten Marktteilnehmer nach möglichst hoher Planungssicherheit für die Entwicklung von Endgeräten, Dienstinfrastruktur und Geschäftsmodellen sowie dem Bestreben nach möglichst hoher Interoperabilität aus Kundesicht, besteht heute mehr denn je der Bedarf zur Standardisierung von Komponenten – trotz der immer kürzer werdenden Innovations- und Produktzyklen am Markt. Darüber hinaus schafft eine Harmonisierung über möglichst viele Märkte hinweg die Chance, vom sogenannten Skaleneffekt (Economy of Scale) profitieren zu können. Internationale anerkannte Normen und verbreitete Marktstandards bilden hier für gewöhnlich die Basis. Unabhängig davon bleibt auch zu beachten, dass sich ein zukunftsträchtiger Markt nur dann dynamisch weiterentwickeln kann, wenn für die Entwicklung neuer innovativer Geräte und Dienste genügend Spielraum zur Verfügung steht.

Zusammenfassend lassen sich folgende Hauptmotive für Standards und Normen identifizieren:

- Interoperable Lösungen
  Offene und standardisierte Schnittstellen von Systemen sichern eine umfassende und übergreifende Zusammenarbeit von Diensten und Netzen.

- Produktinnovation
  Standards und Normen spielen eine zentrale Rolle bei der Produktentwicklung und unterstützen die Forschungs- und Entwicklungs- (FuE) Bestrebungen innovativer Unternehmen.

- Neue Märkte
  Standards und Normen lassen Märkte von Skaleneffekten (Economy of Scales) profitieren und fördert einen ausbalancierten Wettbewerb unter den Beteiligten.

- Standardisierte Lösungen
  Standardisierte Lösungen reduzieren Kostenfaktoren hinsichtlich einer vereinfachten Entwicklung und Inbetriebnahme komplexer Systeme sowie der Integration verschiedenster proprietärer, nicht-standardisierten Lösungen.

- Regulatorische Anforderungen
  Standardisierung und Normung erfüllt essentielle regulatorische Anforderungen und sichert deren Umsetzung in technischen Systemen.

In Kontrast zur Standardisierung der Komponenten für klassisches, digitales Broadcastfernsehen, deren Entwicklungen in Europa und größeren Teilen der Welt hauptsächlich auf die DVB-Organisation zurückzuführen ist, beteiligen sich weltweit verschiedenste Organisationen und Gremien aus den Bereichen Telekommunikation, Informationstechnik und Rundfunk an der Entwicklung entsprechender Standards oder Spezifikationen für IPTV.

4.3.1 DVB-IP

Mit der Einführung erster Standards für IP-basiertes Fernsehen im Frühjahr 2005 war die Digital Video Broadcasting Group das weltweit erste Gremium welches Standards für IPTV anbieten konnte. Das bereitgestellte Dokument mit dem Namen „Transport of MPEG-2 TS based DVB Services over IP Based Networks“[2] fokussiert vollends auf das Mapping der bereits etablierten und erfolgreichen Standards für digitales TV auf die Übertragung in IP-basierten Netzen.

Der zunächst begrüßenswerte Ansatz, der eine einfache und kostengünstige Adaptierung von bereits verbreiteten Broadcastdiensten ermöglichen sollte, entwickelte sich allerdings durch die nicht durchführbare Übertragbarkeit der Ansätze auf die sich vom herkömmlichen digitalen Broadcast unterscheidenden Geschäftsmodelle und technischen Plattformen nicht vorteilhaft für diesen Ansatz. Besonders hervorzuheben ist hierbei, dass die Gründe für den Eintritt der Telcos in den Markt mit und um Mediendienste vor allem Aspekte der Dienst- und Netzkonvergenz waren und neben den reinen Streaming-Diensten (auch Endgeräte übergreifende) Zusatzdienste eine große Rolle spielen sollen.

Die vom DVB-IP- Standard abgedeckten herkömmlichen linearen Fernsehdienste, sowie Video on Demand werden somit lediglich einen von vielen Basisdiensten in einer sich noch zu entwickelnden Dienstelandschaft darstellen.

Hinsichtlich der Verschlüsselung bzw. des Inhalteschutzes lässt sich die oben geführte Diskussion fortführen: Im derzeitigen Status Quo sorgt ein Lagerkampf zwischen einem von den Broadcastern

2 ETSI TS 102 034 Digital Video Broadcasting (DVB); Transport of MPEG-2 Based DVB Services over IP Based Networks

getriebenen Ansatz zur Mandatierung von CSA als einzigen Verschlüsselungsalgorithmus auf der einen Seite und auf der anderen zur Nutzung eines Toolbox-Ansatzes und der freiwilligen Implementierung auf dem Endgerät für einen Stillstand bei der weiteren Standardisierung.

Zur Lösungsfindung dieser divergenten Ansätze wurde im Rahmen des Commercial Modules IPTV (CM-IPTV) die sogenannte Content Security Taskforce beauftragt die unterschiedlichen Sichtweisen darzustellen und Kompromisse zu finden[3].

Im Rahmen der Konsensfindung wurde beiden Parteien Gelegenheit gegeben zu den Punkten

- Interoperabilität
- Sicherheit
- Regulierung und
- Neue Endgeräte

Stellung zu nehmen. Im Bereich der Interoperabilität werden als Grund für den Einsatz von CSA die uneingeschränkte Nutzbarkeit von Endgeräten genannt, die sich aber gerade nicht auf potentielle mobile IPTV-Empfänger oder PC-basierte Lösungen adaptieren lässt.

Im Bereich der Sicherheit bzw. der Gegenüberstellung von Software- und hardwarebasierten Algorithmen wird darauf verwiesen, dass CSA bisher nicht kompromittiert worden ist und somit als sicher gilt, was sicher nicht in Frage zu stellen ist. Die Begründung, dass sich nur so hochwertiger Premiumcontent schützen ließe ist jedoch schlichtweg falsch, da vor allem DRM-basierte Ansätze von der Filmindustrie ausdrücklich unterstützt werden und gerade die parallel zu CSA gewünschte Simulcrypt-Funktionalität die Sicherheit des Gesamtsystems aus CSA und CA in Frage stellt.

Im Rahmen der Regulierung wird darauf hingewiesen, dass die DVB Group ihre Empfehlungen als ETSI Standards publiziert und somit europäisches Recht erfüllen müsse und somit die in der Universaldienstrichtlinie mandatierte Nutzung von CSA. Dies wird vom gegnerischen Lager in Frage gestellt, da zum einen nicht alle nationalen Regulierungsbehörden diese Sicht teilen, dass IPTV unter den Schirm dieser Richtlinie passe und zum anderen hierzu in zukünftigen Versionen der USD IPTV explizit nicht mit einbezogen wird.[4]

Im letzen Aspekt der potentiellen neuen Endgeräte für IP-basiertes Fernsehen führen die Verfechter des CSA-basierten Ansatzes das Argument an, dass der Kern von IPTV noch immer der Empfang von konventionellem digitalen Fernsehen sei und dass die Diskussion um neue Endgeräte wie Spielekonsolen und PCs zu komplex sei, um diese in die Verschlüsselungsthematik mit einzubeziehen. Genau dieser Position widersprechen die Gegner der CSA-Lösung, da durch diese Kurzsichtigkeit die Entwicklung neuer Dienste verhindert werden würde.

Parallel zu den eben beleuchteten Aspekten stellt ein Beschluss des DVB Steering Boards[5] die Benutzung von Toolbox-Ansätzen für Zukünftige DVB-Standards generell in Frage, um die Kosten für

[3] DVB-CM-IPTV Content Security Task Force: Status of the work item on Content Scrambling Algorithms CM-IPTV0490r4 20th March 2009

[4] Anmerkung der Autoren: In diesem Zusammenhang muss die die Frage gestellt werden, warum andere ETSI-Gruppen (vgl. ETSI TISPAN) im Rahmen der IPTV Standardisierung, die fragwürdige Mandatierung nicht berücksichtigen. Technische Aspekte zur Spezifikation konvergenter Dienstszenarien und die Erarbeitung eines hierfür technisch sinnvollen Ansatzes scheinen hier im Vordergrund zu stehen

[5] TM Chairman's report of DVB Steering Board meeting on 12th February 2009 (TM4169)

Hersteller gering zu halten und maximale Interoperabilität zu gewährleisten. Im gleichen Kontext wird jedoch ausdrücklich darauf hingewiesen, dass in Bereichen in denen andere Funktionalitäten, die außerhalb des eigentlichen Auftrags der DVB Group liegen durchaus auf Toolbox-Ansätze zurückgreifen können. Hierbei wird explizit auf den Standard DVB-H verwiesen, der durch die Benutzung mobiler Netze für den Rückkanal andere Industriestandards berührt. Da im Rahmen von IPTV ebenfalls andere Internet- oder Quasistandards das Marktgeschehen prägen und nicht etwa DVB-IP muss darüber nachgedacht werden, ob diese Ausnahme nicht auch für DVB-IP gelten sollte, um Aspekte der Netz- und Dienstkonvergenz endlich adressieren zu können.

4.3.2 ETSI TISPAN

Die ETSI Arbeitsgruppe *TISPAN* (Telecommunications and Internet converged Services and Protocols for Advanced Networking) beschäftigt sich mit der Spezifizierung von All-IP basierten Next Generation Networks, die auf sämtlichen Zugangsnetzen auf das Internet Protokoll setzen. Die Eingliederung aller Dienste in eine paketvermittelte Infrastruktur und der dazugehörigen Signalisierung soll erstmals eine Verschmelzung der entsprechenden Dienste aus der Internet, Telekommunikations-, Mobilefunk- und Medienwelt ermöglichen und bietet somit eine ideale Basis zur Realisierung konvergenter Triple- bzw. Quadruple Play Szenarien.

Im Rahmen der Standardisierung zum ETSI TISPAN NGN Release 2, welches nunmehr zur Verfügung steht, wurden eine Vielzahl von Spezifikationen für IPTV bzw. konvergente Telekommunikations- und Mediendienste über Next Generation Networks geschaffen.[6]

ETSI TISPAN spezifiziert das gesamte IPTV Ecosystem zum Einsatz in geschlossenen und gemanagten Netzwerken mit den folgenden Aspekten:

- Szenarien, Use-cases und Requirements (WG1)
- Architekturen (WG2)
- Signalisierung und entprechendes Protokollmapping (WG3)
- Medienstromkontrolle und Codecauswahl
- Mapping auf Heimnetze (WG5)
- Security und Inhalteschutz (WG7)

Für das derzeit in Arbeit befindliche ETSI TISPAN Release 3 werden die IPTV Spezifikationen nochmals mit besonderem Hinblick auf Konvergenzszenarien zur mobilen Welt, als auch mit Fokus auf die Interaktion zwischen Medien- und Telekommunikationsdiensten untersucht.

4.3.2.1 IPTV Zugangssicherung in TISPAN

Sicherheitsthemen sowie Aspekte zum Inhaltschutz für die Übertragung von IPTV-Signalen, d.h. linearem Fernsehen oder sogenanntem Content on Demand (CoD) werden im Rahmen der TISPAN

[6]Siehe hierzu:
ETSI TS 182 027: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IPTV functions supported by the IMS subsystem",
ETSI TS 182 028: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Dedicated IPTV Subsystem in NGN".ETSI TS 183 063, "Telecommunications and Internet converged Services and Protocols for
Advanced Networking (TISPAN); IMS based IPTV Stage 3 specification

Arbeitsgruppe 7 (WG7) erarbeitet. Die hierzu erarbeiteten Dokumente sind Teil der allgemeinen TISPAN NGN Release 2 Security Spezifikationen geworden.[7]

Eingangsdokumente waren insbesondere eine Machbarkeitsstudie zur Erweiterbarkeit der TISPAN NGN Architektur um IPTV Sicherheitsmechanismen und ein Studie zum Inhaltschutz im Heimnetzwerk (CPN)[8]

Im Rahmen der weiteren Arbeiten für das in Standardisierung befindliche ETSI TISPAN Release 3 (R3) wurden die folgenden Themen als relevant eingestuft:

- IPTV Security (Erweiterungen zum TISPAN R2)
- Security for Customer Premises Networks (CPN)
- Aspekte zur Sicherheit in Fixed Mobile Convergence (FMC) Szenarien

Ein besonderes Augenmerk liegt auf der Bereitstellung eines DRM-basierten Mechanismus zum Schutz der Inhalte unter Benutzung der von der 3GPP spezifizierten Generic Bootstrapping Architecture (GBA) [9]welche im Rahmen der derzeitigen Arbeiten am ETSI TISPAN Release 3 weiter erörtert wird. Erste Ergebnisse sind im Laufe des Jahres 2009 zu erwarten.

4.3.3 ETSI TC MCD

Zur Untersuchung der technischen Aspekte der Verteilung von Inhalten wurde vom ETSI das technische Komitee für Media Content Distribution (TC MCD) gegründet. Aufgabe dieses Komitees die Standardisierungsarbeit in diesem Bereich zu unterstützen und zu koordinieren.

Dabei soll neben IPTV auch Mobile TV und Broadcast-TV berücksichtigt werden. Aufgaben des TC sind dabei unter anderem die Sicherstellung der Interoperabilität zwischen ETSI, 3GPP und anderer Standards aus relevanten Bereichen, die Initiierung von neuen Standardisierungsinitiativen für Bereiche in denen Lücken gesehen werden, die von ETSI geschlossen werden können und die Integration von ETSI Tätigkeiten im internationalen Umfeld, in Anerkennung der Tatsache dass eine Beschränkung auf europäische Hersteller inhaltlich nicht sinnvoll ist.

Das technische Komitee ist erst vor kurzem gebildet worden und hat mit der inhaltlichen Arbeit erst im Januar dieses Jahres begonnen.

Derzeit existiert nur ein erster Working Draft des "Analysis & Requirement" Dokumentes, die Arbeit an weiteren Dokumenten hat erst kürzlich begonnen (Anfang Mai 2009). Für die meisten dieser Dokumente ist eine interne Fertigstellung für September 2009 mit dem Ziel der Veröffentlichung durch ETSI im Dezember 2009.

[7] Siehe hierzu ETSI TR 187 001 NGN Security Requirements, ETSI TS 187 002 NGN eTVRA und ETSI TS 187 003 NGN Security Architecture

[8] Siehe hierzu: WI 07033 IPTV SEC Architecture Feasibility Study Report und WI 05021 Feasibility Study of CPN Sec Machnisms

[9] 3GPP TS 33.220 (click spec number to see fileserver directory for this spec) Generic Authentication Architecture (GAA); Generic bootstrapping architecture http://www.3gpp.org/ftp/Specs/html-info/33220.htm

4.3.4 Open IPTV Forum

Das Open IPTV Forum wurde 2007 von acht Firmen aus dem Bereich der Kommunikations- und Unterhaltungsindustrie gegründet. Ziel des Forums ist es offene Standards zu entwickeln und zu promoten, welche Interoperabilität zwischen den Komponenten anstreben, um 'Plug and Play' Funktionalität für den Endbenutzer zu erreichen.

Das OIPF ist nicht auf die ursprünglichen Gründungsmitglieder beschränkt, sondern steht auch anderen Firmen offen. Seit der Gründung ist die Anzahl der Mitglieder auf 52 angestiegen.

Im Januar 2009 wurde vom OIPF das erste Release der Spezifikationen veröffentlicht, die auch Angaben zum Inhalte- und Diensteschutz enthält.

Die Spezifikation umfasst die Teile:

1. Overview
2. Media Formats
3. Content Meta Data
4. Protocols
5. Declarative Application Environment
6. Procedural Application Environment
7. Authentication, Content Protection and Service Protection

Das siebente Dokument ist dabei der für diese Studie relevante Teil. Das OIPF unterscheidet hierbei grundsätzlich zwischen zwei Ansätzen zur Umsetzung von Mechanismen zum Inhalte- und Diensteschutz:

- Terminal Centric Approach (TCA)
- Gateway Centric Approach (GCA)

Der Terminal Centric Approach präferiert hier Marlin (siehe hierzu Kapitel 8.1) als Content Protection System für IPTV, sowohl innerhalb einer Domain als auch als Zugangssicherungsformat des Providers, der Gateway Centric Approach hingegen terminiert ein beliebiges Zugangssicherungssystem im Gateway zum Plattformbetreiber und setzt im Heimnetz auf DTCP-IP bzw. CI+. Als Die Authentifizierungs-Mechanismen sind beim OIPF mit HTTP-Requests oder der Benutzung eines IMS Gateways stark an web-typische Mechanismen angelehnt. SmartCards spielen als Mittel der Authentifizierung bei IPTV keine Rolle. Die Spezifikation definiert das Verhalten im Falle des Vorhandenseins eines CI+ Interfaces, stellt aber explizit fest, dass die Umstände unter denen ein CI+ basierter Ansatz unterstützt wird außerhalb des Rahmens des Dokumentes liegt.

Eine Unterstützung von CI+ ist also möglich, wird aber vom OIPF nicht gezielt gefördert. Eine Unterstützung von CI ist nicht vorgesehen, da bei IPTV nicht die Notwendigkeit besteht CI-Legacy Devices zu unterstützen.

Zur Begründung der jeweiligen Ansätze, d.h. TCA bzw. GCA werden folgende Argumentationen herangezogen, wobei bei TCA die Endgeräteunabhängigkeit und bei GCA die Vorteile der weiteren Verwendbarkeit vorhandener CA/DRM Lösungen hervorgehoben werden:

"with TCA the rationale is to offer a solution that promises to be adopted in a large number of terminals, to establish the critical mass of industry standard terminals that enable mass-market deployment and

use of commercial content and services on many kinds of devices (i.e. not only PC and separate islands of handhelds) --> Service Provider-focused offering?"

"with GCA the rationale is to enable Service Providers to continue to use existing CA/DRM solutions while still (hopefully) being able to offer access to those services from the same population of compliant terminals. --> User-focused offering"[10]

Der GCA Approach verschiebt hierbei das Problem der Interoperabilität vom Endgerät auf das vom jeweiligen Service- oder Plattformbetreiber zu stellenden Gateways welches den hier jeweilig eingesetzten Mechanismus zum Inhalteschutz terminiert.

Der TCA-Approach erscheint zunächst als flexibler wird jedoch u.U. durch das Fehlen einer kritischen Masse an Endgeräten bzw. fehlender Deployments gebremst

Insgesamt erscheint die Situation im OIPF auch mit der derzeitigen Arbeit am zweiten Release dieser Spezifikation noch als extrem uneinheitlich und nicht reif zur Umsetzung. Eine Mandatierung eines dieser beiden Ansätze erscheint derzeit im OIPF nicht durchsetzbar.

4.4 Zusammenfassung derzeitige Situation

Die derzeitige Situation bei IPTV ist typisch für die Anfangsphase einer sich neu etablierenden Technologie. Es existiert ein starker Kontrast zwischen praktischen Anwendungen, welche sich momentan noch stark an bekannte Szenarien anlehnen und experimentellen Nutzungen, welche die erweiterten Möglichkeiten ohne direkten Blick auf den Markt nutzen.

Ein marktwirtschaftlich relevanter Zusatznutzen durch neue Möglichkeiten wird sich vermutlich erst nach einer Experimentalphase einstellen.

Ähnlich offen ist derzeit auch die Situation in der Standardisierung. Es gibt dort eine Reihe von Ansätzen aus verschiedenen Standardisierungs- und Industriegremien, aber bisher lassen sich nur vereinzelt Tendenzen erkennen, ein dominierender oder gemeinschaftlicher Trend ist jedoch noch nicht auszumachen. Auch hier ist eine Konsolidierungsphase von ein bis zwei Jahren zu erwarten.

[10] Internal Document – Profiling AHG Meeting Minutes – Conference Call 24 March 2009 On CSP Issues 24 March 2009

5 Aufgaben eines DRM Systems

Die Aufgaben eines DRM Systems unterscheiden sich von denen eines Zugangssicherungssystems. Allerdings werden beide Konzepte oft vermischt und eine klare Trennung der Bedeutungen ist in der Praxis eher selten. Dieses ist teilweise durch die Historie bedingt und teilweise durch die Nutzung ähnlicher Methoden wie der Verschlüsselung von Inhalten.

DRM Systeme beinhalten typischerweise die Zugangssicherung, erlauben aber eine feinere Gradierung als reine Zugangssicherungssysteme.

Zur Zeit der analogen Videoübertragung war die einzige Aufgabe eines Zugangssicherungssystems für Pay-TV die Beschränkung der Empfangbarkeit des Videosignales auf den Kreis der Abonnenten. Der Schutz vor der Verteilung und Aufzeichnung des Signales spielte keine signifikante Rolle.

Mit zunehmender Digitalisierung, portablen Geräten, der Verfügbarkeit von mehreren Bildschirmen im Haushalt und weit verbreiteter Heimvernetzung war die Beschränkung der Zugangssicherheit auf das lineare Signal eines einzigen Empfangsgerät nicht mehr hinreichend, so dass umfangreichere Systeme, die DRM Systeme, zum Management von Inhalten im Heimumfeld und deren Nutzungsrechte notwendig wurden.

Die Hauptfunktion eines DRM Systems ist zwar weiterhin die Bereitstellung eines Zugangsberechtigungssystems (Conditional Access), um sicherzustellen, dass Inhalte nur von berechtigten Adressaten genutzt werden können, über diese Basisfunktion der Zugangssicherung hinaus werden an moderne Systeme weitere Anforderungen gestellt. Die folgenden Abschnitte beschreiben die Anforderungen an ein solches System.

5.1 Zugangssicherung

Aufgabe der Zugangssicherung ist die Bereitstellung der Inhalte nur für berechtigte Benutzer. Hierzu werden die Inhalte vor der Übertragung an den Benutzer verschlüsselt, so dass andere Empfänger des Datenstroms keinen Zugang zu den enthaltenen Inhalten haben. Im Broadcast-Bereich werden Inhalte systembedingt mit einem für alle Benutzer identischen Schlüssel verschlüsselt. Systeme mit einer feineren Verteilgranularität erlauben auch individuell verschlüsselte Inhalte.

Da im Broadcast-Bereich derzeit noch kein Rückkanal als gegeben vorausgesetzt werden kann, erfolgt die Verteilung der Entschlüsselungs-Schlüssel im Allgemeinen in physischer Form, üblicherweise als SmartCard.

5.1.1 Authentifizierung, Autorisierung und Abrechnung (AAA)

Die Themenbereiche Authentifizierung, Autorisierung und Abrechnung werden üblicherweise als Teil der Zugangssicherung betrachtet. Im Broadcast-Bereich sind diese Themen jedoch zum großen Teil nicht Element der technischen Realisierung, sondern werden außerhalb dieser behandelt.

Eine spezifische Authentifizierung des Nutzers kann im Broadcast-Bereich durch den systemimmanent unidirektionalen Datenstrom nicht erfolgen. Die Authentifizierung erfolgt de-facto durch die Fähigkeit den Datenstrom zu entschlüsseln.

Die Abrechnung kann ohne Rückkanal ebenfalls nicht direkt aufgrund der spezifisch genutzten Dienste oder gesehenen Sendungen erfolgen, sondern geschieht, abgesehen von spezifischen Premium-Sendungen, üblicherweise durch das Abonnement von kompletten Programmbouquets über einen Zeitraum unabhängig von der tatsächlichen Nutzung.

Die Autorisierung des Ansehens spezifischer Sendungen oder Programbouquets erfolgt nachdem die Anforderung des Kunden auf separatem Wege (Telefon, SMS, Internet) gestellt worden ist durch spezielle Autorisierungsnachrichten an die individuelle SmartCard des Empfängersystems.

5.2 Rechteverwaltung

Eine spezifische Rechteverwaltung im engeren Sinne legt die Nutzungsrechte für Content fest. Diese Rechte beinhalten typischerweise das Kopierrecht, das Wiedergaberecht und das Modifikationsrecht, sowie detaillierte Unterkategorien dieser Rechte.

Im Broadcasting-Bereich findet eine detaillierte Rechteverwaltung derzeit kaum statt. Set-Top-Boxen und PVRs werden als geschlossene und eigenständige Systeme betrachtet auf denen die Wiedergabe üblicherweise (sofern für den Content autorisiert) beliebig erfolgen kann, während kopieren und modifizieren des Contents meist nicht zulässig ist.

Durch die weite Verbreitung von Heim-Netzwerken geht der Trend geht jedoch zum vermehrten Einsatz von Rechteverwaltungssystemen um die Nutzung innerhalb eines Haushaltes oder in Verbindung mit mobilen Systemen zu regeln.

5.3 Identifizierung von Rechteverletzungen

Die Identifizierung von Rechteverletzungen hat am Bereich der Zugangssicherung einen immer größeren Anteil. Hauptaufgabe hierbei ist die Identifikation von Rechteverletzern als Grundlage für juristische Maßnahmen ('Traitor tracing', "Forensic Marking"). Die gebräuchlichste Methode ist hierbei des Einbetten von nutzerspezifischen Daten und das digitale Watermarking, welches jedoch systemimmanent bei Broadcastsystemen keine Bedeutung hat.

5.4 Sperrung von kompromittierten Systemen

Sollten Zugangssicherungssysteme kompromittiert werden, müssen Mechanismen vorhanden sein, um solchen Systemen weitern Zugang zu geschütztem digitalem Content zu verwehren. Hierzu werden unterschiedliche Revocation-Strategien angewandt. welche derzeit in den meisten Fällen nur eine sehr grobe Granularität aufweisen und in vielen Bereichen nur das Sperren von ganzen Geräteklassen erlauben. Im Broadcast-Bereich steht hingegen die Möglichkeit zur Verfügung individuelle Geräte zu sperren, jedoch setzt dieses eine unabhängige Methode der Identifizierung von individuellen kompromittierten Systemen voraus, was im Broadcastbereich jedoch schwer zu erreichen ist. Ziel ist es kompromittierte Systeme spezifisch erkennen zu können und nur für diese eine Sperrung vorzunehmen.

5.5 Anforderungen an Zugangssicherungssysteme

Kocher et al.[11] definieren zehn Designziele und Requirements für Zugangssicherungssysteme.

Diese sind:

- **Renewability**
  Nach dem Auftreten von Sicherheitslücken oder dem Erkennen von potentiellen Schwachstellen muss es möglich sein das Zugangssystem erneut zu sichern.

- **Playability**
  Alle gültigen Abspielgeräte müssen, unter Berücksichtigung der aktuellen Sicherheitsrichtlinien, in der Lage sein allen gültigen Content wiederzugeben.

- **End-to-End Security**
  Content sollte auf dem Verteil- und Abspielweg durchgehend geschützt sein.

- **Cost**
  Kosten sollten minimiert werden.

- **Openness**
  Da bei jedem Sicherheitssystem zu erwarten ist, dass Interna bekannt werden können, darf die Sicherheit nicht von der Geheimhaltung von Implementierungsdetails abhängen.

- **Player Diversity**
  Die Sicherheit muss auf einer breiten Basis von Abspielgeräten gewährleistet werden können.

- **Migration Path**
  Der Übergang von einem etablierten Zugangsschutzsystem zu einem anderen System sollte zu möglichst keinen für den Benutzer erkennbaren Effekten führen.

- **Assurance**
  Das zugrundelegende Sicherungssystem muss ein hohes Vertrauen rechtfertigen können, selbst wenn individuelle Implementierungen Schwachstellen besitzen können.

- **Incentives for Security**
  Hersteller von Zugangssicherungssystemen müssen ein Marktinteresse daran haben die Sicherheit aufrechtzuhalten und zu verbessern, auch und gerade nachdem sich das System am Markt etabliert hat.

- **Forensic Reporting**
  Nach dem Auftreten von Sicherheitslücken sollte es möglich sein die kompromittierten Systeme und die Methoden zur Überwindung des Sicherheitssystemes zu identifizieren.

Nicht alle dieser Anforderungen sind für IPTV und Broadcasting gleicherweise anwendbar oder relevant, die Kriterien sind aber bei dem Vergleich und der Bewertung von unterschiedlichen Systemen als Klassifizierungsmerkmale hilfreich.

[11] Self-Protecting Digital Content by Kocher, Paul; Jaffe, Joshua; Jun,Benjamin; Laren, Carter; Lawson, Nate

6 Spezifische Herausforderungen IPTV

Im Rahmen des IPTV Standardisierungsprozesses kommt es innerhalb und außerhalb der jeweiligen Standardisierungsorganisationen zu einer zum Teil leidenschaftlichen Diskussion um die Definition des Begriffs IPTV und seiner verschiedenen Ausprägungen. Die wohl prägnanteste Definition wurde im Rahmen der Arbeiten der Focus Group IPTV der ITU-T gefunden und wird bis heute gerne als Referenz herangezogen:

"IPTV is defined as multimedia services such as television/video/audio/text/graphics/data delivered over IP-based networks managed to support the required level of QoS/QoE, security, interactivity and reliability."

Der klare Fokus liegt hierbei auf der Abgrenzung zu Web TV- bzw. reinen Internet-Streaming-Angeboten wie sie heute bereits im großen Umfang angeboten werden.

Als Hauptmerkmal von gemanagten Netzen sind hierbei vor allem Mechanismen hervorzuheben, wie sie im offenen Internet noch nicht zur Verfügung stehen:

- Authentifizierungs, Authorisierungs und Accounting Mechansimen (AAA)
- Quality of Service (QoS)
- Fähigkeit zum IP Multicast

Im Rahmen der Standardisierung dieser Dienste standen bzw. stehen weiterhin die folgenden Aspekte im Vordergrund:

- Einheitliche Mechanismen für Service Discovery & Selection
- Einheitliche Metadatenformate
- Standardisierte Mechanismen und Protokolle zur Content-Anforderung
- Einheitliche Nutzerverwaltung und Profile
- Schnittstellen zu Inhalteanbietern
- Inhalteschutz und Verschlüsselung
- Interaktive Applikationen
- Interaktion und Integration mit Telekommunikationsdiensten

Die Vielzahl an Aspekten, welche bereits bei der Verabschiedung erster Standards im Jahre 2007 im Rahmen von ITU-T/TISPAN/OIPF angesprochen wurden macht deutlich, dass ein bloßes Mapping der Basisdienste des digitalen Fernsehens (DTV) auf den neuen Übertragungsweg IP, wie im Rahmen der Definition von DVB-IP geschehen, nicht zielführend ist, da hiermit die tatsächlichen technologischen Vorteile (Dienst -und Netzkonvergenz), als auch wirtschaftliche Überlegungen keinerlei Rechnung getragen wird.

Abgesehen von der grundsätzlichen Fähigkeit digitales Fernsehen anzubieten, sind die technischen Übereinstimmungen von IPTV und herkömmlichen DVB Diensten relativ klein.

Bei IPTV dient DSL/DOCSIS als Transportschicht, womit immer eine bidirektionale Verbindung zum Nutzer besteht, welche sowohl andere Dienste als auch andere Authentifizierungs-, Abrechnungs- und Sicherheitsmechanismen ermöglicht, als diese bei bisherigen DVB Diensten, welche zumindest auch immer unidirektionale Vertriebswege mit unterstützen mussten, möglich waren.

Auch die Nutzung von MPEG-2 als Transportstrom ist im Rahmen von IPTV keine Notwendigkeit. Abhängig vom Anwendungsgebiet könnten hier auch andere Videoübertragungsformate (beispielsweise für Endgeräte mir kleinen Bildschirmen oder begrenzten Übertragungskapazitäten) zum Einsatz kommen. Eine Beschränkung ausschließlich auf MPEG-2 TS würde hier den technologischen Fortschritt hemmen.

Während das Zielgebiet von DVB-C/-S/-T weiterhin primär das lineare Live-Fernsehen bleibt, ist IPTV konzeptionell sowohl für lineares Fernsehen als auch auf Content on Demand Szenarien ausgelegt. Über die Nutzung von Bewegtbild-Inhalten hinaus, erlaubt IPTV integrierte Dienste mit anderen Medien, für welche gegebenenfalls andere Formen der Zugangssicherung notwendig oder geeigneter sind. Ein speziell auf Bewegtbild zugeschnittenes Zugangssicherungsverfahren ist für andere Medien nicht notwendigerweise geeignet.

IPTV Szenarien erlauben häufig auch eine Mischung aus kommerziellen und benutzergenerierten Inhalten. Ist auch für die Verschlüsselung spezifische Hardware nötigt, wie derzeit bei DVB, bedingt dies den Ausschluss von Kleinstanbietern vom Markt.. Ein Beispiel wäre die Bereitstellung von Videoaufnahmen aus einem Sportverein nur für Mitglieder dieses Vereins. Eine Verschlüsselung der Videoinhalte mit Verteilung der Schlüssel nur an Vereinsmitglieder wäre beim derzeitigen DVB-Ansatz unrealistisch, stellt aber durchaus ein plausibles IPTV Szenario dar.

Weitere Eigenschaften von IPTV Szenarien sind die Nutzbarkeit der Dienste auf unterschiedlichen Geräteklassen, sowie der Mehrwert (Added Value) der 'Gelegenheits-Nutzung' auf Systemen, die nicht primär zum Fernsehempfang dienen. Dabei ist aber nicht auf allen potentiellen Zielgeräten der Einsatz spezifischer Entschlüsselungshardware durchsetzbar.

Zusätzlich bietet IPTV, über den Vertrieb von konventionellem Fernsehen über einen weiteren Vertriebsweg hinaus die Möglichkeit, Kunden individuell zu adressieren. Dadurch werden Dienste wie gezielte, kundenspezifische Werbeeinblendungen und Mehrwertangebote sowie erweiterte Abrechnungsmechanismen möglich. Die Bezahlung von Inhalten in Abhängigkeit der tatsächlichen Nutzungszeit stellt dafür von potentiell vielen möglichen Anwendungsfällen dar.

IPTV erlaubt echtes 'Video on Demand ' und verfügt damit im Gegensatz zu „Pre-Download“ Angeboten, bei denen durch vorherigen Download die Inhalten auf das Endgerät mit nachträglicher Freischaltung übertragen werden, das Potential klassische Vertriebswege von hochwertigen Kinofilmen (Videothekenlandschaft) abzulösen.

Dabei können natürlich auch weiterhin herkömmliche Verschlüsselungsverfahren, bei denen die Inhalte beim Dienstanbieter bereits komplett in verschlüsselter Form vorliegen, genutzt werden. Gleichzeitig können sich aber auch Dienste entwickeln, bei denen die Verschlüsselung entweder komplett oder in einzelnen Segmenten kundenspezifisch vorgenommen wird, beispielsweise zur Identifizierung kopierter Inhalte oder zur Beschränkung der Nutzung auf spezifische Benutzergruppen.

Auch die Bereitstellung von DVD-ähnlichen Funktionen, wie der schnelle Wechsel zwischen zwei verschiedenen Videoströmen derselben Szene sowie die Ausblendung oder der Ersatz einzelner Szenen im Rahmen des Jugendschutzes ist bei einem inhärent stream-basierten Verschlüsselungsverfahren wie CSA möglich, aber problematisch. Andere Verfahren können für derartige Anwendungsgebiete geeigneter sein.

Durch die enge Verknüpfung von IPTV und Internetwelt sind auf IPTV Plattformen deutlich mehr gemischte Dienste als auf herkömmlichen fernsehorientierten Set-Top-Boxen zu erwarten. Dazu gehört die Integration von existierenden Internetinhalten in den Fernsehmedienkonsum wie auch zusätzlich geschaffener Internet-basierter Mehrwertdienst.

Wie andere Internet-basierte Systeme ist IPTV, abweichend von herkömmlichen Vertriebswegen für digitales Fernsehen, nicht auf nationaler Ebene oder ein geographisches Gebiet beschränkt. Viele Nutzer werden voraussichtlich nationale oder lokale Angebote nutzen, es werden sich aber auch internationale Spartenkanäle etablieren. Desweiteren besteht ein besonderes Interesse von IPTV Nutzern darin, anders als bei bisherigen Systemen, heimische Programme und Sender auch auf Reisen oder bei längeren Auslandsaufenthalten nutzen zu können.

Auch die Integration von Telekommunikationsdiensten wie VoIP, Messaging (zwischen Fernsehteilnehmern, aber auch zwischen Fernsehteilnehmern und Mobilfunknutzern oder Computernutzern) spielt in IPTV Szenarien eine ebenso wichtige Rolle wie die Integration von In-Home Diensten in die IPTV Plattform.

Abschließend sollte noch erwähnt werden, dass sich Zusatzdienste für IPTV derzeit noch in einer frühen Phase befinden und sich daher endgültige Anforderungen an ein Zugangssicherungssystem nur schwer definieren oder abschätzen lassen.

7 Rechtemanagement in anderen Medien

Während der kommerzielle Vertrieb von Video-Content, speziell von Streaming-Inhalten, in größerem Umfang noch vergleichsweise neu ist, haben andere Content-Arten und Vertriebsmedien schon eine längere Geschichte hinter sich. Dort sind verschiedene Ansätze entwickelt und hinreichend am Markt erprobt worden. Diese Ansätze lassen sich natürlich nicht direkt auf die IPTV Situation übertragen, erlauben aber Analogieschlüsse und Vermutungen über die zukünftige Entwicklung.

7.1 Audio

7.1.1 Vertrieb auf Tonträgern

Der Standard für Audio CD sieht keinerlei Zugangsbeschränkungs- oder Kopierschutzmechanismen vor. Ein minimales DRM System in Form eines Copy Protection Signalling System („Don't Copy Bit") ist im Standard definiert, hat jedoch in der Praxis keine Bedeutung.

Kopiergeschützte Audio-CDs kamen erst mehr als 20 Jahre nach der Markteinführung des Mediums auf den Markt. Kopiergeschützte CDs sind jedoch nicht Standard-konform und nutzen Seiteneffekte, um das Auslesen auf PCs zu erschweren und dabei die Abspielbarkeit auf reinen Audio-CD-Spielern weiterhin zu gewährleisten.

Da dieses Verfahren nicht im Standard genormt ist, sondern auf dem vermuteten Verhalten von verschiedenen Wiedergabesystemen beruht, führte es zu unerwünschten Seiteneffekten (wie die Nichtabspielbarkeit auf einigen Audio-CD Spielern), bei nur geringer Reduktion der Kopierbarkeit der CDs. Heutzutage werden Kopierschutzmechanismen auf Audio CDs nur noch von kleineren Labeln eingesetzt.

7.1.2 Digitaler Audio Broadcast

Die Situation beim Digitalen Audio Broadcast (DAB und DAB+) ist ähnlich wie bei der Audio CD. Der Standard sieht keine Kopierschutzmechanismen oder Verschlüsslungen vor. Es existiert, ebenfalls wie bei der Audio CD ein Copy Protection Signalling System, welches jedoch in der Praxis ebenfalls keine Bedeutung hat.

7.1.3 Internet Radio

Das Internet Radio ist von der technischen Grundlage vermutlich das System, bei dem die Verbreitung von Audio-Content der IPTV Methodik am nächsten kommt. Beim Internet Radio werden die Radioprogramme typischerweise über IP Multicast an die Benutzer verteilt, allerdings sind auch andere Verteilungsmechanismen gebräuchlich. Internet Radio findet heute sowohl als Zweitverwertung herkömmlicher Radiosender,, als auch als Plattform für kleinere kommerzielle und nichtkommerzielle Sender, Spartenprogramme und lokaler Angebote Verwendung.

Dabei wird Internet Radio zunehmend international genutzt. Trotz der inhärent größeren Wortlastigkeit von Audio-Content gegenüber Video-Content werden viele Programme auch in fremden Sprachen konsumiert. Umgekehrt nutzen viele Hörer das Internet Radio, um bei Auslandsaufenthalten ihre heimatlichen Programme weiter verfolgen zu können.

Internet Radio ist vom Format her nicht reguliert und definiert keine spezifischen Features. Nachdem in der Anfangsphase eine Reihe verschiedener und inkompatibler Lösungen auf dem Markt waren,

haben sich interoperable, MP3-basierte Server und Clients weitgehend durchgesetzt, wobei sich allerdings (ursprünglich recht erfolgreiche) proprietäre Lösungen wie RealAudio weiterhin in speziellen Nischen am Markt halten können.

Aus Sicht der Hardwarehersteller eröffnete die Vorbereitung des Internet Radios neue Absatzmöglichkeiten, durch das Aufkommen einer völlig neuen Geräteklasse, dem dedizierten Webradio-Empfänger.

Obwohl technisch möglich, findet im Internet Radio meist keine Verschlüsselung des Contents statt. Speicher- und Kopierschutz wird, wenn überhaupt vorgesehen, über die Funktionalität des Abspielprogrammes erreicht. Der Grund hierfür ist sicher in der leichten Umgehbarkeit jedes Kopierschutzes durch die mögliche Aufzeichnung des Analogsignales zu sehen, welche auch beim herkömmlichen analogen Radio gegeben ist. Eine wirksame technische Sperre ergibt hier keinen signifikanten Sicherheitsgewinn für den Content-Provider.

7.1.4 Internet Stores

Nach der Etablierung von MP3 als gebräuchliches Musikaustauschformat gab es anfänglich keine kommerzielle Verwertung von Audio-Content im Internet. Es existierte jedoch eine umfangreichen Konsumentengruppe, welche über File-Sharing-Programme (das bekannteste davon sicherlich Napster) auf Audio-Content (zumeist illegal) zugriff.

Um diesen Markt auch kommerziell zu nutzen, stellten die Content-Provider ihren Audio-Content dann als kostenpflichtige, legale Downloads zur Verfügung. Erste Versionen, bei denen die Downloadportale noch eng an die Content-Eigner (Platten- und Vertriebslabel) gebunden waren, erwiesen sich als wenig erfolgreich. Erst mit der Verbreitung von label-übergreifenden Stores (wie iTunes oder Musicload) stellte sich der kommerzielle Erfolg ein.

Zur Vermeidung des Austauschs der gekauften Musikstücke unter den Nutzern setzten die Stores auf umfangreiche DRM Systeme. Hierbei kamen zumeist unterschiedliche und inkompatible Systeme zum Einsatz, von denen FairPlay (Apple) und Windows Media DRM (Microsoft) die größte Verbreitung fanden.

Bei all diesen Systemen, soweit Details bekannt sind, liegt der Audio-Content bereits in verschlüsselter Form vor, er wird bisher nicht benutzerspezifisch verschlüsselt. Der eigentliche Entschlüsselungs-Key für den Content wird dabei mit einem benutzerspezifischen Schlüssel verschlüsselt. Darüber hinaus werden bei einigen Anbietern der ausgelieferten Audio-Datei benutzerspezifische Informationen hinzugefügt. Diese erlauben die Identifikation des individuellen Käufers im Falle einer nicht legitimierten Verbreitung des Audio-Contents.

Während sich der eigentliche Verschlüsselungsalgorithmus bei keinem der auf dem Markt befindlichen Geräte als angreifbar erwiesen hat, waren für alle Systeme bald Lösungen zum Abspielen des Audio-Contents auf nicht autorisierten Systemen verfügbar, üblicherweise durch Auslesen des Content-Keys während der autorisierten Entschlüsselung. Sicherheitslücken der Systeme sind jedoch meist kurzfristig durch Softwareupdates geschlossen worden.

"While we have had a few breaches in FairPlay, we have been able to successfully repair them through updating the iTunes store software, the iTunes jukebox software and software in the iPods themselves."
Steve Jobs, Thoughts on music, Februar 2007

Seit der Ankündigung von iTunes im April 2007 einen signifikanten Teil des Audio-Contents ohne Verschlüsselung anzubieten (inzwischen den kompletten Katalog), haben andere große Anbieter (Amazon, Musicload) ebenfalls auf Content-Verschlüsselung verzichtet.

7.1.5 Bezug zu IPTV

Für die IPTV-Thematik sind dabei folgende Punkte interessant:

- Es existierte kein zentral vorgegebenes Content-Sicherungssystem, die Entwicklung wurde dem Markt überlassen.
- Mehrere Systeme konnten sich parallel am Markt etablieren
- Obwohl der Verschlüsselungsalgorithmus selbst sicher war, haben sich bei allen Systemen Sicherheitslücken ergeben.
- Sicherheitslücken konnten durch Softwareupdates behoben werden.
- Nach einer Phase sehr stringenter DRM Handhabung wird Content heute meist weniger geschützt ausgeliefert. Die Sicherheit vor Missbrauch wird derzeit primär durch juristische Begleitmaßnahmen, Marktmechanismen und die Individualisierung des Contents geschaffen.
- Internet Radio funktioniert auch mit kommerziellen Inhalten ohne Zugangssicherungssystem und bietet eine Plattform auf der sowohl etablierte Radiosender als auch innovative Dienste miteinander erfolgreich existieren.

7.2 DVD / Blue-ray Disc

7.2.1 DVD

Für DVDs wurde als Abspielschutzverfahren das Content Scramble System CSS als einziges zulässiges Verfahren festgelegt. Das System beruht auf einem festen Satz von 408 Geräteschlüsseln, die zur Entschlüsselung des DVD-Schlüssels (Disk-Keys) dienen, welcher in den 408 möglichen Verschlüsslungen auf der DVD abgelegt sind.

Durch Veröffentlichung aller 408 Geräteschlüssel im Oktober 1999 wurde CSS technisch irrelevant. Aufgrund von kryptologischen Mängeln der CSS Verschlüsselung war es jedoch vorher schon möglich den Disk-Key einer DVD innerhalb weniger Sekunden auch ohne Kenntnis eines Gerätes zu ermitteln.

Obwohl es sich bei CSS primär um ein Verfahren handelte, um das Abspielen der DVDs nur auf autorisierten Geräten zu erzwingen, diente es ebenfalls als Kopierschutz, da die Schlüsselinformation im Lead-In Bereich der DVD gespeichert ist, welcher bei DVD±R Medien nicht direkt beschreibbar ist. In der Praxis hatte die Aushebelung des CSS Verfahrens jedoch kaum Auswirkungen auf den DVD Markt. Der Haupteffekt war vielmehr die Implementierung von DVD Spielern auf nicht autorisierten Plattformen, hauptsächlich Linux-Systemen, für die davor aus lizenzrechtlichen Gründen keine offiziellen DVD Abspielprogramm existierten.

7.2.2 Blue-ray Discs

Blue-rays Discs bieten zwei getrennte Sicherungsmechanismen, AACS und BD+.

7.2.2.1 AACS

Das derzeit primäre Schutzsystem bei Blue-ray Discs ist das Advanced Access Content System AACS. Es nutzt den Advanced Encryption Standard (AES) mit 128-bit Verschlüsselung. Die technischen Verbesserungen gegenüber dem bei DVD verwendeten CSS System sind die größere Schlüssellänge, die Nutzung eines erprobten Verschlüsselungsverfahrens, sowie die implizierte Berücksichtigung der speziellen Eigenschaften von Software-Playern durch eine zeitlich befristete Schlüsselvergabe, die es notwendig macht Software Player in regelmäßigen Abständen zu erneuern.

AACS erlaubt eine feinere Granularität beim Sperren von kompromittierten Geräten als CSS (welches nur 408 mögliche Gerätetypen unterscheiden kann). Darüber hinaus werden Watermarking Techniken eingesetzt, um kompromittierte Systems zu identifizieren ("traitor tracing"). Dadurch können unsichere Systeme spezifisch am Abspielen zukünftiger Blue-ray Discs gehindert werden. In der Praxis setzt das jedoch voraus, dass Blue-ray Disc Spieler aktualisiert werden können. Ein 'Blacklisting' und damit eine de-facto Sperrung einer kompletten Serie von Hardware-Spielern wird am Markt kaum durchsetzbar sein, wenn keine Möglichkeit des Updates auf eine sicherere Version besteht.

7.2.2.2 BD+

Anders als AACS, bei dem die Entschlüsselung des Contents systembedingt außerhalb der Kontrolle der DVD liegt und die Vertrauenswürdigkeit des Abspielsystems nicht überprüft werden kann, erlaubt BD+ eine aktive Verifikation des Spielers. BD+ stellt eine virtuelle Maschine auf dem Blue-ray Disc Spieler zur Verfügung, in welcher auf der Blue-ray Disc befindlicher Code ausgeführt wird. Aufgabe dieses Codes ist sicherzustellen, dass der Blue-ray Disc Spieler nicht modifiziert worden ist.

Der Vorteil des Verfahrens besteht darin, dass die Integrität des Spielers individuell überprüft werden kann und die Wiedergabe von Blue-ray Discs nur auf kompromittierten Spielern verhindert wird, ohne dass dabei eine ganze Klasse von Blue-ray Disc Spielern gesperrt werden muss.

Da bei BD+, anders als bei CSS und AACS, die Sicherungsalgorithmen frei gewählt werden können, kann leichter auf spezifische Sicherheitslücken reagiert werden. Auch ist die Reaktion auf bisher unvorhergesehene Sicherheitsprobleme möglich.

7.2.3 Bezug zu IPTV

Für die IPTV-Thematik sind dabei folgende Punkte interessant:

- CSS als statisches Sicherheitssystem war nach dem Auftreten von Sicherheitsproblemen nicht mehr durch ein verbessertest System ersetzbar.
- Das neuere AACS System geht, zumindest implizit, davon aus, dass auf Software-Spielern Sicherheitslücken auftreten werden und beinhaltet Mechanismen, um den Upgrade von Software-Spielern zu erzwingen.
- Über das passive Sicherheitssystem hinaus, welches davon ausgehen muss, dass das Endsystem nicht kompromittiert ist, wird zusätzlich ein aktives und flexibles System eingesetzt, welches die Integrität des Client-Systems überprüft.

8 Alternativen zu CSA

Entsprechend der Festlegung nach § 48 Abs. 3 Nr. 1 S. 1 TKG müssen alle digitalen Fernsehempfangsgeräte in der Lage sein, Signale darzustellen, die den standardisierten europäischen Kodieralgorithmus „Common Scrambling“ (CSA) verwenden. Der Algorithmus ist seit seiner Annahme durch das DVB-Projekt 1994 Bestandteil der DVB-Übertragungsstandards für digitalen Rundfunk (DVB-S/C/T). Mit der Markteinführung von IPTV Systemen in Deutschland, deren potentieller Funktionsumfang hinsichtlich interaktiver, geräteübergreifender Dienste und damit verbundenen Synergie-Effekten im Umgang mit TV und Medieninhalten das von digitalem Rundfunk bekannte Spektrum in hohem Maße übersteigen wird, stellt sich auch die Frage, inwieweit die bestehenden Regulierungen, im konkreten Fall die Mandatierung des DVB-CSA, auch auf IPTV-Systeme übertragbar sind. Insbesondere die technischen Innovationen von IPTV Systemen und damit verbundenen Mehrwertdiensten und Geschäftsmodellen erfordern mit hoher Wahrscheinlichkeit erweiterte bzw. gänzlich neue Möglichkeiten Inhalteschutz und Verschlüsselung zu realisieren. Die Sicherung von Interoperabilität gemäß den grundsätzlichen Vorgaben des TG sollte dabei auch innerhalb der Technologie IPTV Beachtung finden, wenngleich eine erweiterte Regelung bzw. die Anpassung derzeitiger Festlegungen in Betracht gezogen werden müssen. Das Zugangs-berechtigungssystem organisiert die Verwendung von Inhalten geräteübergreifend und verfolgt das Ziel einen wirksamen Schutz der Inhalte gegen unberechtigte Nutzung sowie Zugang sicherzustellen. Selbstredend sollten derartige Systeme auch in IPTV-Netzen Verwendung finden. Im Hinblick auf §48 Abs. 3 TGK und in Bezug auf die Fülle und Komplexität zukünftiger Dienste und Geschäftsmodelle ist allerdings festzuhalten, dass hierfür nicht ausschließlich der Common Scrambling Algorithmus eingesetzt werden muss bzw. kann. Für IPTV-Systeme empfehlen sich vornehmlich andere, der Telekommunikations- und Internet-Welt angelehnte Verschlüsselungstechniken, wie beispielsweise DRM-basierte Systeme. Sie bieten ein hohes Maß an Flexibilität und Sicherheit, können geräteübergreifend und differenziert angewendet werden und sichern damit letztlich ein hohes Maß an Dienst-Interoperabilität für den Endanwender. Die nachfolgende Auswahl an Verschlüsselungstechnologien soll einen Überblick über bereits am Markt etablierte als auch derzeit in der Standardisierung befindlicher Systeme hinsichtlich ihrer Verwendbarkeit in IPTV-Systemen geben. Diese Technologien stellen den State-of-the-Art derzeitiger Zugangskontrollsysteme dar, bieten ein hohes Maß an Funktionalität für zukünftige, konvergente und geräteübergreifende Dienstszenarien und empfehlen sich nicht zuletzt aus diesen Gründen für deren Einsatz in erweiterten TV Umgebungen, wie beispielsweise den hier im Fokus stehenden IPTV Systemen.

8.1 Marlin

Im Jahre 2005 gründeten die fünf Unternehmen Intertrust, Panasonic, Philips, Samsung und Sony die Marlin Developer Community, die das Ziel verfolgt Spezifikationen für ein Content und Rechtemanagementsystem der nächsten Generation zu entwickeln. Dies soll insbesondere eine maximale Interoperabilität zwischen Endgeräten auf dem immer stärker wachsenden Elektronik- und Entertainmentgerätemarkt erwirken.

So wurde z.B. speziell für den Markt von mobilen Endgeräten eine Schnittstelle, genannt OMArlin, zu OMA Version 2.0 spezifiziert. OMArlin verbindet dabei OMA kompatible Endgeräte mit der Marlin Technologie, womit der interoperable Austausch von sogenannten Content Objekten zwischen OMA und Marlin DRM Systemen möglich ist.

Funktional betrachtet ist das Content Objekt auf verschiedenen Endgeräten abspielbar, welche einer definierten Gerätegruppe angehören, z.B. einer Gruppe “Familie“, oder dem Nutzer zuzuordnen sind. Neue Geräte werden automatisch im Netzwerk erkannt und können ebenfalls Gruppen oder Nutzern zugeordnet werden. Somit ist es dem Nutzer möglich, seinen geschützten Content auf verschiedene Endgeräte zu portieren. Dies gewährleistet eine maximale Interoperabilität zwischen allen Endgeräten, welche die Funktionalitäten des Marlin DRM Prinzips unterstützen. Bei jedem erneuten Abspielen wird durch den Marlin DRM Client mittels Links geprüft, ob das Gerät verifiziert ist den Content wiederzugeben. Dieses Link System basiert auf den Octopus Spezifikationen, welche in der Marlin Technologie Verwendung finden.

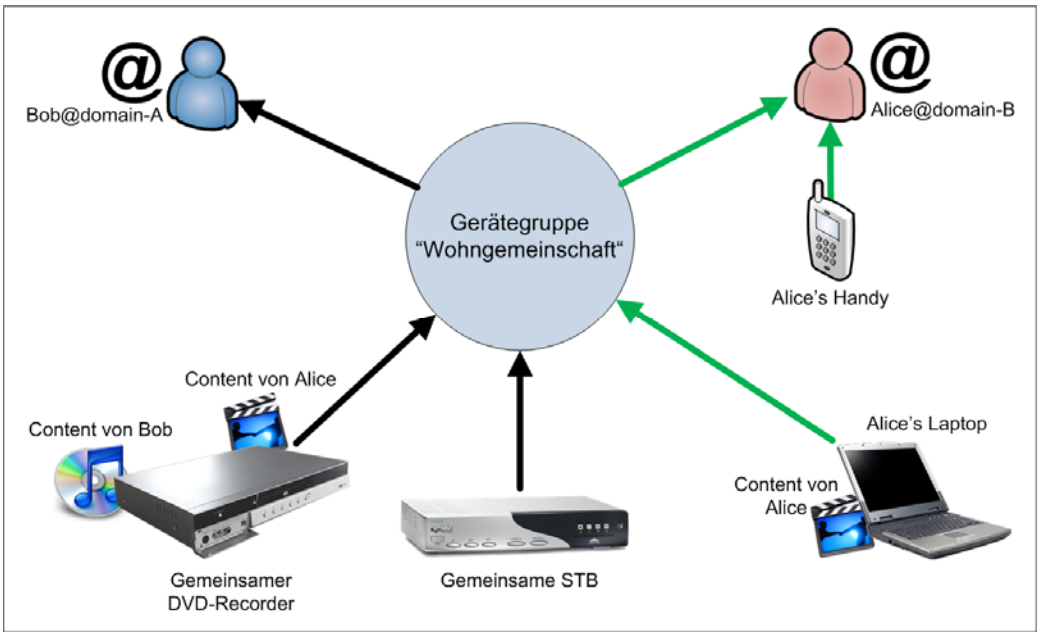

Abbildung 7 - Beispiel Marlin DRM Client

Abbildung 7 demonstriert ein typisches Anwendungsszenario des Marlin DRM Systems. In diesem Beispiel möchte Benutzer “Alice“ mit Ihrem mobilen Endgerät auf ein Content Objekt Ihres Laptops zugreifen. “Alice“ hat das gewünschte Content Objekt bereits in einem Videoportal erstanden. Es ist somit zu Ihrem Benutzerkonto verlinkt. Wie bereits erwähnt, ist neben der Verlinkung zu Benutzerkonten die Bildung von Gerätegruppen möglich. In diesem Beispiel sind verschiedene Endgeräte, wie z.B. ein DVD-Recorder und eine Set Top Box, aus dem Haushalt der Wohngemeinschaft mit der Gerätegruppe “Wohngemeinschaft“ verlinkt. “Alice“ möchte nun ein Content Objekt, welches Sie auf Ihr Handy kopiert hat, wiedergeben. Der Marlin DRM Client im Handy von “Alice“ prüft nun, ob die Berechtigung zur Wiedergabe gegeben ist. In diesem Fall ist es für “Alice“ möglich, den Content wiederzugeben, da Sie Ihr Benutzerkonto mit der Gerätegruppe “Wohngemeinschaft“ sowie Ihrem Handy verlinkt hat.

In einem anderen Beispiel erhält “Alice“ von “Bob“ eine E-Mail mit einem Content Objekt als Anhang, welches er in einem Portal erstanden hat. Der Versuch von “Alice“, das Content Objekt auf ihrem Handy wiederzugeben scheitert, da dieses Endgerät nicht der Gerätegruppe “Wohngemeinschaft“ angehört. Es besteht somit kein Link zu den Content Objekten von “Bob“. Abschließend ist für das Beispiel zu erwähnen, dass auf dem Endgerät “Gemeinsamer DVD-Recorder“ Content Objekte von beiden Benutzern abspielbar sind, weil es der Gerätegruppe “Wohngemeinschaft“ angehört, die wiederum mit beiden Benutzerkonten verlinkt ist.

Das Open IPTV Forum (OIPF) spezifiziert in seinem Dokument [OIPFVol7] eine “Content and Service Protection“ (CSP), welche den Schutz von Content und Services innerhalb des Terminals definiert. Dabei übernimmt die CSP die Rolle eines Marlin DRM Clients, sofern das Terminal diese Funktion unterstützt. Die CSP führt bei Interaktionen mit dem Providernetzwerk Marlin Aktionen, wie z.B. Linküberprüfung und Lizenzkontrolle, aus. Somit wird in dem Dokument des OIPF der Einsatz einer DRM Engine, hier Marlin, spezifiziert, welche eine größere Interoperabilität für den Endverbraucher zur Folge hat. Dabei spezifiziert das “Marlin Architecture Overview“ Dokument der Marlin Developer Community in Sektion 4.4.1, dass ein Marlin DRM Client sowohl in Hardware als auch Client Applikation, wie z.B. ein PC Software Media Player, realisiert werden kann. Durch die Verschlüsselung des Contents mit einem AES 128 Bit Key , welcher ebenfalls in Hard- oder Software implementiert werden kann, sind dem Endgerätemarkt dahingehend keine Grenzen aufgezwungen und entsprechend Spielraum bei der Umsetzung des Standards gegeben.

8.2 CI+

Im Jahre 1997 wurde das “Common Interface“ (CI) durch das DVB Projekt standardisiert. Es ist im Dokument EN 50221 beschrieben und dient als Schnittstelle zwischen einem Host und einem externen Modul. Ein Host, beispielsweise eine Set-Top-Box, übernimmt die Funktionalität für den Empfang von MPEG-2 Video, Audio und Daten während das externe Modul, beispielsweise ein “Conditional Access Modul“ (CAM), für das Entschlüsseln des MPEG-2 Transportstroms verantwortlich ist.

Die CI Schnittstelle basiert auf dem Industriestandard “PCMCIA“. Dementsprechend sind die CAM-Module aufgebaut. Sie enthalten optional eine Smartcard oder einen Mikroprozessor zur Entschlüsselung des MPEG2 Transportstroms. In der folgenden Abbildung wird in roter Farbe dargestellt, dass nach der Entschlüsselung des MPEG2 Transportstroms die Daten unverschlüsselt über das Common Interface an den Host zurückgegeben werden. An dieser Stelle ist es Angreifern möglich, den Datenstrom abzugreifen und darzustellen, was eine Schwachstelle darstellt.

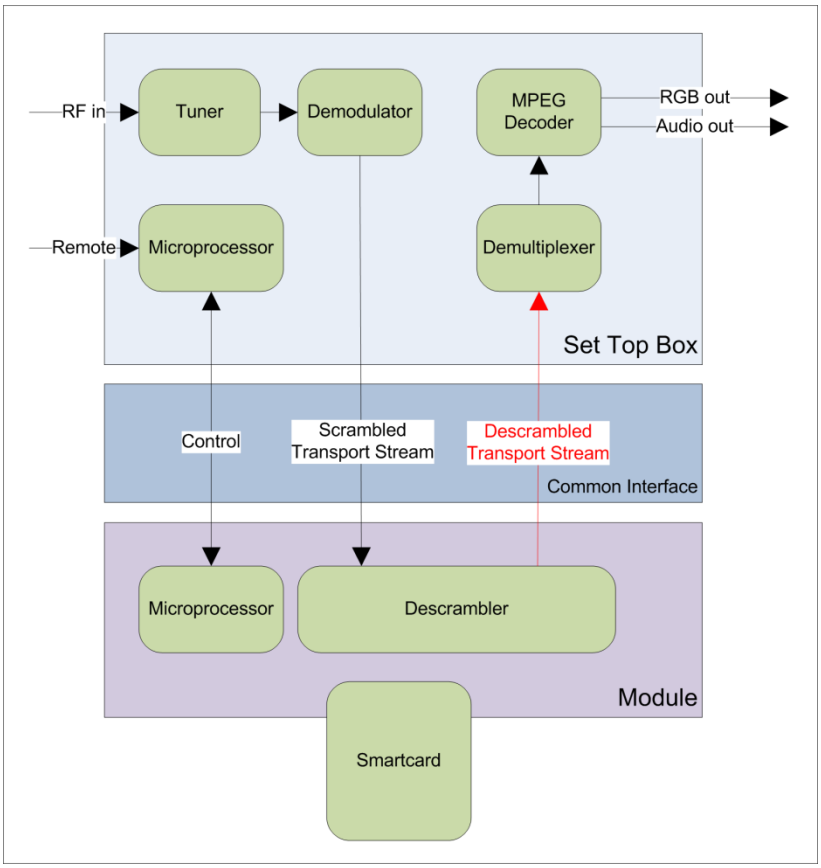

Abbildung 8 - CI Modul

Aufgrund der potentiellen Sicherheitslücke und aufgrund einiger weiterer Unzulänglichkeiten der CI Schnittstelle (beispielsweise beim Jugendschutz) begann das DVB Projekt mit der Entwicklung des Nachfolgestandards CI v2. Es konnte allerdings im DVB Rahmen keine Einigung über die technische Ausprägung der Schnittstelle erzielt werden und die Entwicklung wurde eingestellt.

Dies führte dazu, dass die Firmen Neotion, Panasonic, Philips, Samsung, SmarDTV und Sony das "Common Interface Plus" (CI+) Forum gründeten, mit dem Ziel, den bestehenden CI Standard des DVB Projekts zu erweitern. Im Januar 2008 veröffentlichte das CI+ Forum die "V1.00 CI Plus Specification", mit dem Schwerpunkt die Schwachstelle des Common Interfaces zu schließen.

Die CI+ Spezifikation baut auf der CI Spezifikation EN 50 221 auf und erweitert diese. Dafür werden etablierte und von der Industrie akzeptierte Techniken verwendet, wie Geräte- und Nachrichten-Authentifizierung und Verschlüsselung. CI+ nutzt geteilte private Schlüssel, welche vom CAM Modul und vom Host separat berechnet werden. Es reicht nicht aus die Schlüssel am Common Interface abzufangen. Sie können aus diesen Informationen nicht berechnet werden. Dieses Verfahren nutzt etablierte und getestete Methoden, welche zur Zeit der Erstellung der Spezifikation keine bekannten Schwachstellen besitzen.

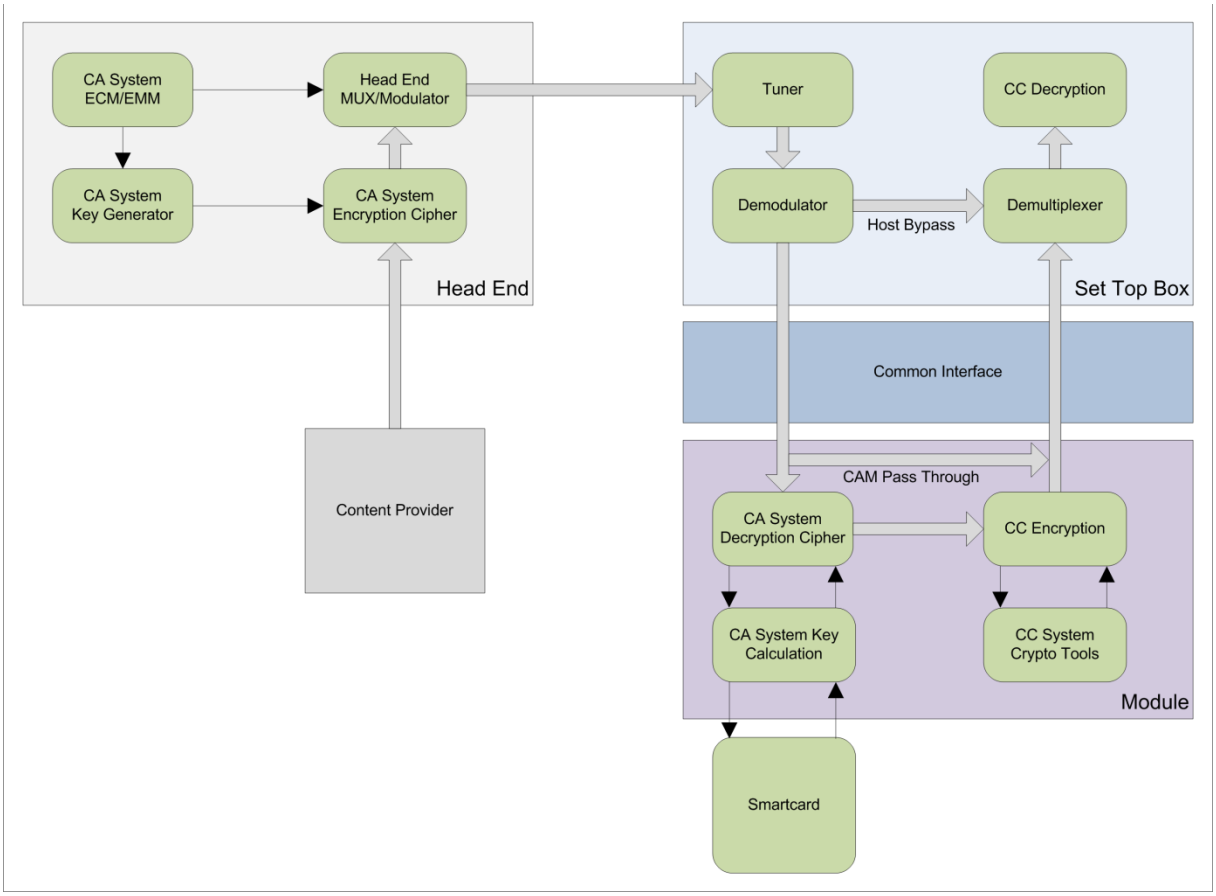

Abbildung 9 - CI+ Content Control System

Die obenstehende Abbildung zeigt die Funktionalität des bei CI+ eingesetzten Content Control Systems. Dabei wird im Head End der Content durch ein CA System mittels des CA Systemkeys kodiert. Die Set Top Box empfängt den Transportstrom und leitet ihn über das Common Interface zu dem Conditional Access Modul. Das Modul entfernt den CA Schutz und verschlüsselt den Content erneut mit dem Content Control System. Dieses erneut verschlüsselte Signal wird zurück an die Set-Top-Box geleitet, wo es letztendlich entschlüsselt und somit dargestellt werden kann. Das erneute Verschlüsseln schließt die bekannte Sicherheitslücke des CI Systems.

Obwohl der Standard erst seit Anfang 2008 verfügbar ist, stößt er bei Kabelnetzbetreibern und Endgeräteherstellern auf großes Interesse. So kündigte der größte niederländische Kabelnetzbetreiber Ziggo den Einsatz des CI+ Standards an. Sony zieht nach und setzt CI+ in den Flachbildschirmen der WE5 Reihe ein, welche seit Mai 2009 verfügbar sind. Tandberg möchte in einem Konsortium mit Sony, Neotion und S&T Kabelnetzbetreibern die Einführung von CI+ vorantreiben, indem Sie eine Video on Demand Plattform auf Basis von CI+ bereitstellen. In Deutschland kündigten die Kabelnetzbetreiber Kabel Deutschland und Tele Columbus die Einführung des CI+ Standards an. Jedoch gibt es auch Endgerätehersteller, die sich gegen die Einführung von CI+ am Markt stark machen. So kündigte die Firma Dream-Multimedia (Hersteller der Dreambox) an, dass sie die Einführung des CI+ Standards nicht unterstützen werde. Der Alphacrypt-Hersteller Mascom reiht sich ebenso in die Reihe der öffentlichen Gegner ein.

Somit ist abschließend festzustellen, dass der CI+ Standard von Kabelnetzbetreibern und Endgeräteherstellern teilweise akzeptiert, gefördert und bereits eingeführt wird. Ob und wie dies beim Endverbraucher akzeptiert wird, bleibt abzuwarten.

8.3 OMA DRM

Eines der am weitesten verbreiteten Zugangsschutzsysteme, welches auch explizit DRM Funktionalität beinhaltet ist das System der Open Mobile Alliance (OMA), in der sowohl alle namhaften Telefonhersteller, als auch die Netzwerkbetreiber vertreten sind.

Technisch beruht das Verfahren auf gerätespezifischer individueller Verschlüsselung eines Rechteobjektes, welches sowohl eine Rechtebeschreibung, als auch den Schlüssel für den Content selbst enthält. Hierbei existiert für jedes Endgerät ein eigener Public Key, welcher vom Content-Provider (der bei OMA konzeptionell in Content-Issuer und Rights-Issuer getrennt wird, wobei beide Rollen in der Praxis aber von einem Provider übernommen werden) zur Verschlüsselung des Rechte-Objektes genutzt wird. Dieses rechte-Objekt kann wiederum nur mit dem Private Key des Gerätes entschlüsselt werden.

Die Nutzungsrechte werden mit Hilfe von Open Digital Rights Language (ODRL) beschrieben, einer XML-basierenden Rechtebeschreibungssprache. ODRL definiert nicht nur Kopierrechte, sondern darüber hinaus auch Nutzungs-, Modifikations- und Management-Rechte, sowie den Ausdruck dieser Rechte in Abhängigkeit verschiedener Parameter wie Nutzer, Nutzergruppen, verfügbare Hardware, Zeit, Datum, Nutzungshäufigkeit, der Anwesenheit von Wasserzeichen, Art des Speichermediums und weiterer Kriterien.

Mit OMA DRM hat sich im Rahmen eines Industriekonsortiums ein DRM Standard entwickelt, der sich, obwohl er für OMA Mitglieder nicht bindend ist, am Markt etabliert hat. Da bei mobilen Geräten der Telekommunikation, anders als in der Broadcast-Welt, eine eindeutig identifizierbare Verbindung zwischen Provider und Endgerät besteht, konnte sich hier ein neues und auf den einzelnen Kunden spezifischer zugeschnittenes Zugangssicherungssystem durchsetzen.

8.4 Microsoft Windows Media DRM

Das derzeit am weitesten verbreitete Zugangssicherungssystem für Audio- und Videoinhalte im Heimbereich ist das von Microsoft verwendete Windows Media DRM. Das System wird bereits in vielen IPTV Systemen zur Zugangssicherung eingesetzt. Neben IPTV wird Windows Media DRM derzeit auch von zahlreichen VoD Diensten eingesetzt, das VoD Angebot von Premiere ist dafür ein prominentes Beispiel.

Audio- und Videoinhalte werden dabei einmal verschlüsselt und gespeichert (seit Windows Media DRM ist auch die Verschlüsselung von Live-Content möglich). Zur Verschlüsselung dient eine Mischung aus verschiedenen Verschlüsselungsmethoden, darunter ein ECC (Elliptic Curve Crypto-system) Verfahren, eine DES Blockverschlüsselung, eine RC4 Stromchiffre und ein SHA-1 Hash-Algorithmus. Letztendlich wird aber nur mit einem Key verschlüsselt. Zur Entschlüsselung benötigt der Endverbraucher ein sogenanntes Lizenzpaket, welches neben dem Key zur Entschlüsselung der Inhalte die Nutzungsrechte für die Inhalte enthält, beispielsweise

- wie oft eine Datei abgespielt gespielt werden darf,
- auf welchen Geräten die Dateien abgespielt werden dürfen (beispielsweise das Recht das Audiodateien auch auf bestimmten mobilen Audio-Playern verwenden zu können),
- in welchem Zeitrahmen die Dateien genutzt werden können,
- ob die Dateien auf Audio-CDs gebrannt werden dürfen,

- welche Sicherheitsanforderungen ein Abspielgerät erfüllen muss.

Besonderheiten des Windows Media DRM sind die bereits erwähnte Eignung für Live-Streams, die Möglichkeit durch Stammlizenzen die Lizenzen hierarchisch zu verknüpfen, so dass Zugangsrechte auch für Gruppen von Content erteilt werden können, wodurch beispielsweise zeitlich begrenzte Abonnements für heruntergeladene Dateien zentral verlängert werden können ohne für alle Dateien die Lizenzen einzeln modifizieren zu müssen.

Durch die enge Verknüpfung von DRM System, dem Windows Media Player und dem Betriebssystem kann darüber hinaus, zumindest für PCs mit Microsoft Betriebssystemen, ein "Secure Audio Path" zugesichert werden, d.h. eine geschlossene und jeweils gegenseitig zertifizierte Abspielkette vom Softwareplayer zur Soundkarte, welches ein Auslesen der unverschlüsselten Daten durch zwischengeschaltete Software verhindern soll. (Ein entsprechender "Secure Video Path" steht jedoch derzeit nicht zur Verfügung.)

Naturgemäß richtet sich Microsoft Windows Media DRM primär an Systeme mit Microsoft Betriebssystem, es stehen inzwischen aber auch Tools und SDKs zur Integration von Microsoft auf Nicht-Windows-Betriebssystemen, beispielsweise für netzwerkbasierte Audiospieler oder portable Geräte zur Verfügung.

Eine Erweiterung des Microsoft Windows Media DRM namens "Microsoft PlayReady DRM" zielt spezifisch auf den Markt der portablen Geräte. Microsoft PlayReady DRM ist abwärtskompatibel zu Microsoft Windows Media DRM, fügt jedoch einige Features hinzu:

- Das Konzept der 'Domain', welches es erlaubt Lizenzen für einen kompletten Haushalt zu erwerben, so dass Content auf allen Geräten innerhalb eines Haushaltes genutzt werden kann, ohne für jedes individuelle Gerät eine Lizenz erwerben zu müssen.
- 'Embedded Licenses', welche Content und DRM Information in einer Datei bündeln und das Problem der Trennung von Content und Lizenz bei der Übertragung auf mobile Geräte vermeiden,
- Die Möglichkeit auch Nicht-Mediendateien zu verschlüsseln und zu lizensieren.
- Bei der Entwicklung wurde gezielt auf Portabilität, auch auf nicht von Microsoft produzierte Betriebssysteme, sowie die Möglichkeit beliebige Player und Codecs verwenden zu können, geachtet, um einen größeren Markt erreichen und die marktführende Stellung ausbauen zu können.

Microsoft PlayReady DRM wird auch bei Silverlight als DRM System eingesetzt.

Die Microsoft DRM Varianten sind jeweils vollständig in Software implementiert. Die Rechenleistung moderner Systeme ist also durchaus hinreichend um eine Entschlüsselung (auch von HD Inhalten) in Echtzeit vorzunehmen, ohne dass spezifische Entschlüsselungshardware technisch notwendig ist.

Die reine Software-Implementierung erlaubt auch den Austausch angreifbarer oder fehlerhafter Komponenten. Explizit wird von Microsoft festgestellt: "Because any DRM system can potentially be compromised, Microsoft designed the Windows Media DRM system to support dynamic updates, should a security compromise like this occur." Die Ersetzbarkeit von Komponenten wird hier also als Teil des Sicherheitskonzeptes angesehen.

8.5 Apple FairPlay

Bei FairPlay handelt es sich um das von Apple verwendete DRM System. Die technische Realisierung besteht in der Nutzung von AES verschlüsseltem Audiocontent, welcher sich in einer MP4 Container-Datei befindet. Der zum Abspielen benötigte "Master Key" (von Apple "User Key" genannt) wird beim Kauf des Contents benutzerspezifisch verschlüsselt und dem Endkunden bereitgestellt. Auf dessen System werden alle erworbenen Schlüssel in verschlüsselter Form in einem Key-Repository gespeichert. Soll Content abgespielt werden, entschlüsselt das Abspielprogramm den "Master Key" und nutzt diesen zur Entschlüsselung des Contents.

Das Management der Schlüssel auf einem System und zwischen Systemen (beispielsweise zwischen mehreren PCs und einem iPod) wird durch das Abspiel- und Managementprogramm (typischerweise iTunes oder die Firmware auf einem mobilen Gerät) gesichert. Beispielsweise erlaubt die iTunes Software die Übertragung von Musikstücken und der dazugehörigen Schlüssel auf beliebig viele iPods, jedoch stellt die Firmware auf dem iPod sicher, dass nur Content von maximal fünf PCs gespeichert werden können.

Spezifische Nutzungslizenzen oder dateiabhängige Nutzungsbeschränkungen sind bei FairPlay nicht vorgesehen, da hier nur die Schlüsselinformationen ausgetauscht werden. Darüber hinaus gehende Funktionen müssen durch Softwarefunktionalität zur Verfügung gestellt werden.

FairPlay ist eng in die Apple-Vertriebskette integriert und ist nur in Apple-Produkten verfügbar (als Firmware in iPods/iPhones, als Software in Quicktime und iTunes), Lizenzen für andere Hersteller werden nicht erteilt, was in der Vergangenheit zu juristischen Problemen führte.

Inzwischen hat FairPlay am Markt für Audio-Inhalte keine Bedeutung mehr, da Apple im iTunes Store seit April 2009 nur noch DRM-freie Inhalte anbietet. Für Video-Inhalte wird jedoch weiterhin FairPlay genutzt.

Interessant an FairPlay ist vor allem, dass Apple hier einen vertikalen Vertriebsweg aufgebaut hat, bei dem iTunes Store, iTunes, iPod eine durchgehende Verwertungskette aus einer Hand darstellen und eine durchgehende DRM Lösung vom Shop bis zum Endgerät genutzt wurde.

Weiterhin zeigt gerade der Fall des iPod, dass auch aus Sicht der Rechenleistung technologisch 'schwache' Systeme durchaus in der Lage sind eine Realzeit-Entschlüsselung, auch von Video-Inhalten, in Software vorzunehmen.

Abschließend ist festzustellen, dass es anfänglich einen starken Druck der Content-Provider gab, sichere DRM Verfahren einzusetzen.

> However, a key provision of our agreements with the music companies is that if our DRM system is compromised and their music becomes playable on unauthorized devices, we have only a small number of weeks to fix the problem or they can withdraw their entire music catalog from our iTunes store.
>
> Steve Jobs, Thoughts on music, Februar 2007

Im Endeffekt erwies sich DRM im Bereich des Downloads von Audio-Inhalten eher als marktschädigend, hauptsächlich durch die traditionelle Verfügbarkeit höherwertiger Versionen derselben Inhalte auf DRM-freien CDs. Letztendlich präferierten die Content-Anbieter einen erweiterten Marktzugang gegenüber der Zugangssicherung von Inhalten.

8.6 AACS

Eine technische Beschreibung des AACS Standards findet sich bereits bei der Beschreibung von Blue-ray Discs im Abschnitt "7.2.2.1AACS". Marktwirtschaftlich wäre der Einsatz für IPTV vor allem dadurch interessant, dass das Verfahren schon jetzt zur Zugangssicherung, auch von HD Video-Inhalten, eingesetzt wird.

Abgesehen von der Art der Bereitstellung des verschlüsselten Videostromes (bei IPTV über eine Netzverbindung, bei Blue-ray Disc vom Spieler), welche AACS inhaltlich jedoch keinen Unterschied machen, sind die Anforderungen für beide Anwendungsbereiche nahezu identisch.

Da mit AACS bereits eine im Heim eingesetzte Technologie zur Verfügung steht, der auch von Herstellern von HD Premium-Content hinreichend Vertrauen entgegengebracht wird und welche bereits die meisten Erfordernisse für die Nutzung im IPTV–Bereich erfüllt, stellt AACS eine potentielle Zugangssicherungslösung für IPTV dar.

8.7 DVB Content Protection und Management (CPCM)

Bei DVB CPCM handelt es sich um ein vom DVB Projekt definiertes und im Juni 2008 als ETSI Standard verabschiedetes System zur Regelung von Nutzungsrechten innerhalb von Haushalten. DVB-CPCM befasst sich explizit nicht mit der Übertragung der Inhalte zum Konsumenten, sondern adressiert die Verwaltung der Inhalte nachdem sie beim Verbraucher angekommen sind.

Dazu definiert DVB CPM eine "Authorized Domain" (AD), in dem alle zu einem Haushalt gehörenden Geräte zusammengefasst sind. Dabei sind nicht nur fest im Haushalt installierte Geräte erfasst, sondern auch portable Geräte, In-Car Devices und gegebenenfalls auch ein weiterer Haushalt (z.B. Ferienhaus oder Freunde).

Nutzungsrechte innerhalb der "Authorized Domain" werden anhand von "Usage Rules" festgelegt, welche sowohl explizit durch den Content- oder Service-Provider als auch implizit durch den Übertragungsweg (beispielsweise "Free-to-air broadcasting") festgelegt werden können.

Neben der Festlegung von Nutzungsrechten für die "Authorized Domain" besteht die Möglichkeit spezifische Regeln für eine "Localized Authorized Domain" (der eigentliche Haushalt, ohne bewegliche oder externe Geräte) oder einen "Geographically Constrained Authorized Domain" (beispielsweise ein spezifisches Land) festzulegen.

Nutzungsrechte umfassen dabei die Kontrolle von Kopieren und Verschieben von Inhalten, der Anzahl und dem Zeitraum der Nutzung von Inhalten, der Möglichkeit der parallelen Nutzung auf mehreren Geräten und der Definition der Wiedergabequalität für verschiedene Geräteklassen.

Zum Austausch der Lizenzinformationen wird zwischen zwei CPCM Geräten nach gegenseitigem Austausch von "CPCM Instance Certificates" ein "Secure Authenticated Channel" etabliert, über den dann die Lizenzinformationen übertragen werden. Da die Video-Inhalte auf den Geräten nur in verschlüsselter Form gespeichert werden dürfen, kann deren Austausch auch über ungesicherte und nicht authentifizierte Verbindungen geschehen.

Derzeit wird DVB-CPCM jedoch noch nicht eingesetzt, da derzeit noch keine Zertifizierungsstelle eingerichtet wurde und daher keine Geräte-Zertifikate erteilt werden können, welche verschiedene

CPCM konforme Geräte in die Lage versetzen würden sich anderen Geräten gegenüber zu authentifizieren.

8.8 DTCP

Ein von den Firmen Intel, Matsushita, Sony, Toshiba und Hitachi gebildete Konsortium, welches sich mit der Entwicklung von Content Schutz für digitale Entertainment Inhalte im Heimumfeld befasste, veröffentlichte 1999 die Spezifikation 1.0 der “Digital Transmission Content Protection“ (DTCP). DTCP definiert ein kryptografisches Protokoll zum Schutz von Audio- und Videoinhalten gegen illegales Kopieren. Ziel war es die Verteilung im Heimbereich über verschiedene digitale Schnittstellen wie Firewire, Bluetooth, Universal Serial Bus (USB) oder IP zu ermöglichen, jedoch die Verbreitung der Inhalte außerhalb des Heimbereichs, beispielsweise über das Internet, zu verhindern.

Bei DTCP handelt es sich um einen proprietären Standard der sogenannten “Five Companies“ (5C). Dabei wird die Interoperabilität zu anderen Content Protection Systemen im Heimnetzwerk wie AACS, CPRM, CSS, D-VHS, Magic Gate und VCPS gewährleistet. DTCP kann Content, der mit diesen Systemen geschützt ist, übertragen und umgekehrt kann mit DTCP geschützter Content an andere Technologien wie HDCP oder Windows Media DRM übergeben werden.

Jedes Endgerät authentifiziert sich den anderen Geräten gegenüber, mit denen es kommunizieren möchte, um eine gesicherte und verschlüsselte Verbindung herzustellen. Die folgende Grafik stellt den typischen Ablauf des Austauschs von Content mittels DTCP dar. Bei einer Anfrage nach Content sendet die Quelle einen Stream mit verschlüsseltem Content inklusive Encryption Mode Indicator (EMI). Dieser Indikator enthält Informationen über den Kopierschutz, wie copy-freely, copy-never, copy-one-generation oder no-more-copies, und ist bei der Übertragung von IPTV Inhalten im MPEG2 Transportstrom enthalten. Nach dem Erhalt des Content Streams analysiert der Empfänger die EMI Bits. Anschließend authentifizieren sich die Endgeräte und die Schlüssel, so genannte “content keys“, werden ausgetauscht (Authentication and Key Exchange – AKE). Dieser Content Key wird zum Ver- und Entschlüsseln des Contents genutzt. Bei der Übertragung über IP Netzwerke kommt hierbei ein AES 128 Bit Schlüssel zum Einsatz. Dieser Schlüssel wird bei Verwendung des Real-time Transport Protocols (RTP) für die Übertragung von Medieninhalten mindestens alle 30 Sekunden oder maximal alle 120 Sekunden erneuert. Bei Nutzung des Hypertext Transport Protocols (HTTP) wird der Schlüssel alle 128 Megabyte erneuert. Ein wichtiges Feature bei der Nutzung von DTCP-IP ist der Verfall der Exchange-Keys, welcher nach 2 Stunden nachdem der Inhalt vollständig übermittelt wurde in Kraft tritt. DTCP ist mit anderen DRM und Content Protection Systemen interoperabel.

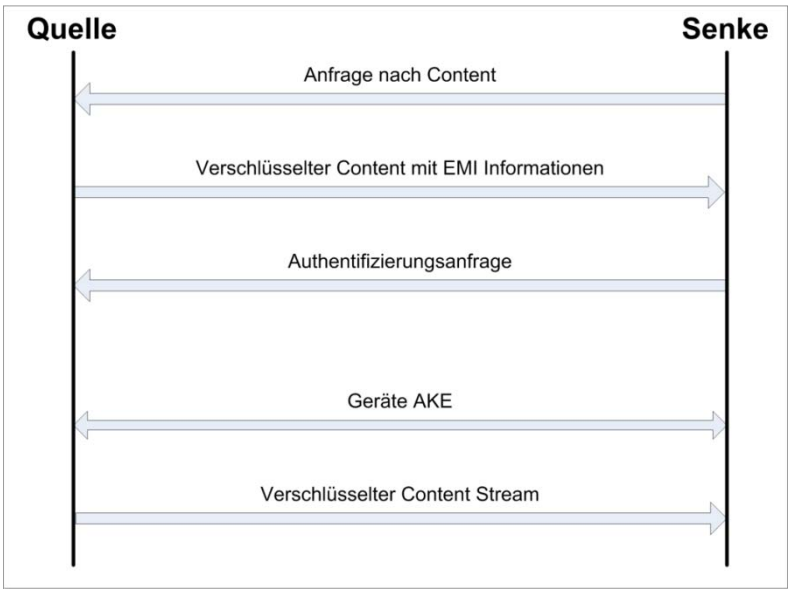

Abbildung 10: Austausch von DTCP verschlüsselten Inhalt zwischen zwei Endgeräten

Nach Aussage des DTCP Konsortiums wurde DTCP inzwischen an über 140 Hersteller aus verschiedenen Bereichen lizensiert und wird auch von Content-Providern und Filmstudios als sicherer Schutzmechanismus akzeptiert.

Allerdings muss festgestellt werden, dass DTCP, um die Verbreitung von Content außerhalb des Heimnetzwerkes zu verhindern, eine Reihe von übertragungstechnischen Kriterien beinhaltet (beispielsweise die Begrenzung der Übertragung auf maximal drei "Hops" oder eine erforderliche Round-Trip-Time auf weniger als acht Millisekunden, welche das 'Tunneln' von Content über das Internet blockieren sollen, aber auch die Anwendbarkeit für IPTV verhindern.

8.9 Zusammenfassung Zugangssicherungsverfahren

Allgemein lässt sich feststellen, dass es bei Zugangssicherungs- und DRM-Verfahren im Heimbereich zwei gegenläufige Tendenzen gibt. Bei den Verfahren selbst geht der Trend zunehmend zu Lösungen für den Gesamthaushalt, also weg von der einfachen Verbindung vom Provider zum Endgerät, sondern vielmehr zu Systemen, welche konzeptionell die Kette vom Provider zu einem Server im Haus und von dort weiter zu mehreren Endgeräten innerhalb des Haushaltes umfassen.

Dem hingegen wird bei am Markt etablierten Vertriebssystemen wie iTunes Store oder Musicload zunehmend auf Zugangssicherungsmaßnahmen verzichtet, da diese meist vom Verbraucher negativ beurteilt werden und der Verzicht auf diese Maßnahmen einen größeren Markt erschließt.

9 Feste vs. auswechselbare DRM und CA Systeme

Für derzeitige DVB-Empfangsgeräte ist die Verwendung des Common Scrambling Algorithmus in Hardwareform vorgeschrieben. Bei der Entwicklung von CSAv3 wurde darauf geachtet, dass der Algorithmus Hardware-freundlich und Software-feindlich ist, eine effiziente Softwareimplementierung also gezielt erschwert wird.

9.1 Diskussion bei DVB

Der Zwang zur Verwendung von chipbasierten Sicherheitslösungen für IPTV ist auch im DVB nicht unumstritten. Im Protokoll der DVB-CM-IPTV Content Security Task Force vom 20. März 2009 wird zum Thema Content Scrambling Algorithms festgestellt, dass es derzeit zwei unvereinbare Lager gibt.

Eine Gruppe besteht darauf, dass alle Empfangsgeräte zumindest die CSA Implementierung in Hardware vornehmen müssen und die Implementierungsform von anderen Algorithmen noch zu entscheiden ist.

Die Gegenposition besteht nur darauf, dass mindestens ein Zugangssicherungsalgorithmus auf den Empfangsgeräten implementiert seins muss. Kein einzelner, spezifischer Algorithmus soll vorgeschrieben werden und die Implementierungsform bleibt dem Gerätehersteller überlassen.

Ursprünglich war geplant verschiedene Geräteklassen zu spezifizieren und für diese verschiedene Richtlinien festzulegen. Durch die zunehmende Vermischung der Geräteklassen wurde dieser Plan jedoch als nicht durchführbar angesehen.

Als Argumente zu den einzelnen Positionen wurden genannt:

Befürworter der Hardwarelösung argumentierten, dass Interoperabilität mit nur einem, dem etablierten DVB-CSA, System leichter zu gewährleisten sei, da Broadcaster denselben verschlüsselten Content für Satelliten- und IPTV-Set-Top-Boxen nutzen können und es kostengünstiger ist existente Hardware weiterzuverwenden. Weiterhin sichert nur eine identische Lösung auf allen Endgeräten eine unbeschränkte Nutzbarkeit durch den Endverbraucher. Weiterhin sei CSA durch die European Universal Service Directive vorgeschrieben, welche von Ländern der EU in nationales Recht umgesetzt werden muss. Daher müsste CSA in allen Endgeräten, die digitales Fernsehen empfangen können (PCs, Spielekonsolen, Set-Top-Boxen, Mobiltelefone) implementiert werden.

Gegner der hardwarebasierten CSA Lösung argumentierten dass dadurch Inkompatibilitäten mit derzeit existierenden IPTV fähigen Endgeräten (primär PCs) entstehen würden und das weiterhin einer der Hauptgründe für eine softwarebasierten Lösung darin liegt, dass nicht auf allen Geräten eine hardwarebasierte Lösung möglich ist. Eine Kompatibilität mit existierenden CSA Systemen wäre nur relevant, wenn diese weiterhin CSAv1 nutzen. Da ein Umstieg auf CSAv3 geplant ist, müssten existierende Systeme ohnehin erneuert werden. Der Bezug auf die europäische Gesetzgebung ist nur begrenzt relevant, da DVB auch außerhalb der EU genutzt wird und daher nicht primär durch europäische Regelungen präjudiziert werden sollte. Weiterhin wird die European Universal Service Directive nicht von allen Staaten als relevant für IPTV Dienste angesehen. Desweiteren bezieht sich die Direktive nur auf lineare Fernsehprogramme, jedoch nicht auf andere Dienste wie Video On Demand.

Darüber hinaus gibt es derzeit Bestrebungen zur Modifikation der European Universal Service Directive, spezifisch zur Ersetzung von “the common scrambling algorithm” durch “a common

scrambling algorithm” und Beschränkung auf terrestrisches, Satelliten- und Kabelfernsehen und somit ohne notwendige Anwendung auf IPTV.

Laut Befürwortern des derzeitigen Systems hat die Implementierung von CSA in Hardware gute Gründe. 'Reverse Engineering' chipbasierter Lösungen ist signifikant schwerer und derart gewonnene Informationen können zur Findung von Schwachstellen des Algorithmus genutzt werden. Eine hardwarebasierte Lösung erleichtert weiterhin die Geheimhaltung einzelner Teile des CSA und damit getrennte Lizenzen für Verschlüsselungs- und Entschlüsselungssysteme. Weiterhin wird, jedoch ohne weitere Begründung, festgestellt, dass es für Broadcaster und Content-Eigner leichter ist gegen kompromittierte Systeme vorzugehen, wenn diese hardwarebasiert sind.

Gegner der Hardwarelösung argumentieren dass die Erzwingung von CSA die Einführung neuer Geräteklassen am Markt verhindern würde. Schon heute sind moderne Spielekonsolen technisch in der Lage IPTV Dienste zu empfangen und zu präsentieren. Der Einbau von CSA Hardware in solche Geräte ist jedoch am Markt nicht durchzusetzen.

9.2 Weitere Argumente für eine Hardware-basierte Lösung

Zusätzlich zu den bereits in der Diskussion erwähnten Argumenten gibt es eine Reihe von weiteren Gründen, den Entschlüsselungsalgorithmus in Hardware zu implementieren.

Bei Softwarelösungen besteht ein höheres Risiko, dass einzelne Teile der Komponente modifiziert werden, so dass die Entschlüsselung der Inhalte weiterhin möglich ist, aber zusätzliche Sicherungs-mechanismen (wie SmartCard-Pairing, Jugendschutz-PIN-Eingabe, Identifikationsinformationen), ausgetauscht oder entfernt werden. Bei Hardwarelösungen ist das Modifizieren deutlich schwieriger und kann durch weitere Sicherheitsmaßnahmen wie Verifizierung und Authentifizierung der Komponenten untereinander nahezu ausgeschlossen werden.Da hardwarebasierte Sicherungssysteme typischerweise nur eine einzelne Aufgabe erfüllen, ist ihre Zuverlässigkeit im Betrieb besser als bei Softwarelösungen, bei denen auf der CPU meist mehrere Tasks ausgeführt werden und es potentiell zu Resource-Problemen und Verzögerungen kommen kann, insbesondere bei Prozessoren mit geringer Leistungsfähigkeit, wie sie bei Set-Top Boxen häufig eingesetzt werden. Durch die konstantere Qualität, wie auch durch die bereits angesprochene Verfälschungssicherheit ist das Vertrauen von Content Providern und Broadcastern in eine Hardware-Lösung typischerweise höher.

Auch reduziert die geringe Anzahl von Lizenznehmern für eine Hardwareimplementierung die Anzahl der Implementierungen, was das Risiko von unerwarteten Inkompatibilitäten zwischen verschiedenen Implementierungen verringert. Im Rahmen der Qualitätskontrolle der Set-Top Boxen muss mit weniger Systemen, Versionen und Konfigurationen getestet werden, als bei Verwendung von Software-Playern.

9.3 Zusätzliche Argumente für eine Software-basierte Lösung

Den Vorteilen einer Hardware-Lösung stehen eine Reihe von Argumenten für eine Software-Lösung entgegen.

Im einzelnen sind diese:

Schließen von Sicherheitslücken
Kein System ist unangreifbar, praktisch alle Sicherungssysteme sind irgendwann kompromittiert worden. Sollte bei einer hardwarebasierten Lösung eine Schwachstelle bekannt werden, ist es kaum möglich das Problem ohne hohen finanziellen Aufwand zu beheben. Softwarebasierte Lösungen können hingegen durch verbesserte Versionen ersetzt werden.

Reagieren auf spezifische Sicherheitslücken
Dem Sperren von kompromittierten Systemen kommt eine immer größere Bedeutung zu. Derzeit besteht nur die Möglichkeit individuelle Systeme zu sperren (wenn beispielsweise die ID einer Smart Card bekannt ist) oder ganze Geräteklassen, wobei letzteres am Markt praktisch nicht durchsetzbar ist. Ein über Softwareupdates modifizierbares Sicherheitssystem wäre (wie BD+ bei Blue-ray Discs) in der Lage nach spezifischen Exploits zu suchen und nur solche Systems zu sperren, die tatsächlich kompromittiert sind.

Reagieren auf neue Anforderungen
IPTV ist noch in der Entwicklungsphase. Zukünftige Anwendungsbereiche sind nicht im Detail vorhersagbar. Softwarebasierte Sicherungssystems können auf neue Anforderungen reagieren, wie beispielsweise Heimvernetzungen oder den Austausch von Content zwischen fest installierten und mobilen Systemen.

Sonderstellung von CSA nicht begründbar
Im IPTV-Bereich werden voraussichtlich außer Video-Sicherungsmechanismen auch in anderen Diensten Schutz- und Rechteverwaltungsmechanismen Verwendung finden, beispielsweise aus dem Internet und dem Mobilfunkbereich, welche auch heute bereits in Software implementiert sind. Darüber hinaus sind auch in jetzigen Set-Top-Boxen die meisten Sicherungsmechanismen, wie das Kopiermanagement, Jugendschutz und Schlüsselverwaltung in Software realisiert. Eine Sonderstellung von CSA scheint antiquiert, insbesondere da die Rechenleistung aktueller Systeme inzwischen hinreichend ist, um auch Video in Echtzeit zu entschlüsseln.

Algorithmen sind nicht dauerhaft geheim zu halten
Auch wenn das 'Reverse Engineering' bei Hardwarelösungen deutlich schwerer ist als bei Softwarelösungen, ist wie auch schon am Beispiel von CSAv1 erkennbar, die dauerhafte Geheimhaltung des zugrundeliegenden Algorithmus nicht zu gewährleisten. Der postulierte zusätzliche Sicherheitsgewinn durch "Security by obscurity" ist in der Praxis eher minimal.

Anzahl der möglichen Endgeräte wird erweitert
Ein Zwang zum Einbau von CSA Hardware würde die potentiellen Endgeräte für IPTV auf 'klassische' Set-Top-Boxen beschränken, also Systeme, deren primäre Funktion der Videokonsum ist. Eine Softwarelösung würde es erlauben IPTV Dienste auch auf Systemen zu nutzen, die primär zu anderen Zwecken benutzt werden (Mobiltelefone, Spielekonsolen, PCs, mobile Videoplayer) und bei denen sich der Einbau spezifischer Hardware am Markt nicht durchsetzen lässt. Durch Einbeziehung zusätzlicher Geräteklassen würde der Markt für IPTV Dienste erweitert. Wie sich schon im Bereich von Audio DRM gezeigt hat, bevorzugen Content-Owner Systeme mit höherer Content-Sicherheit, entscheiden sich aber im Konflikt zwischen DRM und Marktgröße dann doch für den größeren Markt.

10 Empfehlung für IPTV Verschlüsselung

Derzeit gibt es am Markt und in der Standardisierung keine klare Tendenz zu einem spezifischen Zugangssicherungssystem.

In der Standardisierung wird derzeit vom OIPF als Zugangssicherungssystem Marlin favorisiert, während sowohl ETSI TISPAN als auch ETSI TC MCD Aktivitäten erst in einer frühen Phase sind und erste Empfehlungen erst gegen Ende 2009 erwartet werden.

Auch auf dem Markt hat sich kein Zugangssicherungssystem deutlich von anderen Systemen abheben können. Derzeit basieren jedoch alle gebräuchlichen Systeme auf Softwarelösungen, was jedoch nicht unbedingt für die Zukunft präjudizierend ist, da viele IPTV Anwendungen derzeit auf PCs entwickelt worden sind und dort gebräuchliche Konzepte direkt übernommen haben. In einem im Wandel befindlichen Markt erlauben derzeit auch nur Softwarelösungen auf geänderte Anforderungen in kurzer Zeit einzugehen.

IPTV wurde dabei ursprünglich von vielen Anbietern als Mittel zur Zweitverwertung von bereits als 'free to air' ausgestrahlter Fernsehprogramme angesehen, so dass Zugangssicherungsmaßnahmen bisher nur geringe Sicherheitsanforderungen erfüllen mussten. Es ist zu erwarten, dass die Anforderungen für die Verbreitung von Premium-Inhalten von Seiten der Rechteinhaber deutlich höher sein werden.

Mit mehr Weitblick ist parallel zu den derzeitigen Betrachtungen und Diskussionen zur Verschlüsselung der Inhalte im IPTV auch die bereits angesprochene nicht vorhandene direkte Vergleichbarkeit von IPTV und herkömmlichen digitalen Verbreitungswegen über DVB-C/-S und –T heranzuziehen. Hervorzuheben ist vor allem die der Verschlüsselungsdiskussion folgende Diskussion um einheitliche Plattformen und die Signalisierung und Kontrolle interaktiver Inhalte, die mit der in IPTV-Systemen nun tatsächlich und vor allem flächendeckend bereitstehenden Adressierbarkeit Einzug halten werden.

Aus dem derzeitigen Markt und den Standardisierungsaktivitäten lässt sich also zum jetzigen Zeitpunkt keine spezifische Empfehlung ableiten.

Eine optimale Erfüllung des Interoperabilitätsgedankens aus Kundensicht wäre sicher die Vermeidung jeglicher Zugangssicherungsmaßnahmen. Diese ist in der Praxis am Markt, speziell für Premium-Inhalte, derzeit nicht durchzusetzen, auch wenn eine entsprechende Entwicklung langfristig, ähnlich wie bei Audio-Inhalten geschehen, möglich wäre.

Aus Sicht der Content-Provider wäre vermutlich die Etablierung von einem AACS/BD+ basierendem System für IPTV die optimale Lösung. Bereits jetzt werden Premium-Inhalte auf Blue-ray Discs durch solche Systeme geschützt und von den Rechteinhabern akzeptiert und ein einheitliches Schutzverfahren für alle Vertriebswege wäre sicherlich wünschenswert. Auch würde dadurch die Nutzung im Heimnetzwerk vereinfacht werden, da die weitere Verteilung im Haushalt unabhängig von der ursprünglichen Datenquelle erfolgen würde. Verfahren zur individuellen Markierung von Inhalten, 'Traitor Tracing' und zum Auffinden und Blockieren kompromittierter Systeme könnten einheitlich entwickelt und genutzt werden, ohne den Mehrfachaufwand durch ähnliche, aber nicht kompatible Systeme. Allerdings gibt es derzeit keine konkreten Ansätze AACS/BD+ im IPTV Bereich einzusetzen.

Eine regulatorische Festschreibung eines spezifischen Zugangssicherungssystems, speziell eines aus der herkömmlichen Digitalfernsehwelt stammenden Verfahrens wie CSA, scheint zum derzeitigen Zeitpunkt aus mehreren Gründen nicht wünschenswert. Auch die derzeitigen Aktivitäten im Europäischen Parlament, welche eine Umformulierung der Universaldienstrichtlinie anstreben, welche dazu führen würde, dass sich die Pflicht zu einem einheitlichen Verschlüsselungsverfahren nur auf herkömmliche digitale Fernsehdienste beziehen würde, zeigen eine Abkehr vom bisherigen regulatorischen Ansatz auf.

IPTV ist nicht nur ein Fernsehübertragungsverfahren, sondern unterscheidet sich in grundlegenden Aspekten von herkömmlichem digitalem Fernsehen, so dass dortige Lösungen nur bedingt übertragbar sind. Da IPTB noch neu am Markt ist, kann noch nicht vorausgesehen werden, in welchen Marktsegmenten es sich etablieren wird und welche Anforderungen erfüllt werden müssen. Selbst als reines Fernsehübertragungsverfahren hat IPTV als Nachverwertung von Free-to-air Programmen andere Erfordernisse als für Video-on-Demand oder interaktiver Videodienste.

Der Zwang zu spezifischen Verfahren, insbesondere spezifischer Hardware, kann spätere, bisher nicht geplante Dienste blockieren. Ein Beispiel für einen nicht vorhergesehenen Dienst von großer Marktbedeutung ist die Nutzung von Klingeltönen auf Mobiltelefonen. Hätte eine Regulierung hier aus historischen Gründen heraus feste Klingeltöne mandatiert, wäre die Entwicklung blockiert worden.

Darüber hinaus weist die spezifische Festlegung eines Verschlüsselungsstandards diesem eine Sonderrolle zu, welcher in der Praxis nicht gegeben ist. Weitere Aufgabengebiete wie Jugendschutz und In-Home Vernetzung werden hingegen nicht im technischen Detail festgelegt.

Das Ziel einer Interoperabilität im technischen Sinne ist mit dem etablierten Verfahren im Broadcastbereich auch heute nicht gegeben. Anbieter verwenden auch jetzt unterschiedliche Zugangssicherungsverfahren, beispielsweise für den Schlüsselaustausch, wobei die proprietäre Lösung dann in die SmartCard ausgelagert wird. Dadurch entsteht aus Sicht des Anwenders eine Austauschbarkeit, die jedoch auch dadurch realisiert werden könnte, dass der komplette Entschlüsselungsvorgang in SmartCards ausgelagert wird, wo anbieterspezifisch Soft- oder Hardwarelösungen zum Tragen kommen können.

Auch wird durch die Erzwingung der Nutzung eines Hardware-Interfaces wie CI oder CI+ und entsprechender SmartCards die Anzahl der gleichzeitig nutzbaren (meist zwei) SmartCards begrenzt, das für den Endkunden einfach zugängliche Angebot also reduziert. Dieses behindert den Marktzugang für Klein- und Spartenanbieter und verringert die Attraktivität von IPTV insgesamt. Bei der Verwendung von Software-Lösungen könnten mehrere unabhängige Systeme gleichzeitig auf einem Endgerät vorhanden sein und die Angebotsvielfalt für den Endkunden erhöhen. Dieses ist insbesondere der Fall, da die Funktion der SmartCard als Mittel der Authentifizierung, welche durch die unidirektionale Technologie herkömmlicher Broadcastverfahren notwendig ist, bei IPTV entfällt, da hier andere, aus der Internetwelt entnommene Verfahren, genutzt werden können. Eine direkte Übernahme der Konzepte derzeitiger Set-Top-Boxen entspricht auch hier nicht aktuellen Bedürfnissen.

Es hat sich auch am Markt im Hinblick auf Set-Top-Boxen für DVB-C/-S/-T gezeigt, dass einzelne Anbieter die Interoperabilität ihrer Set-Top-Boxen mit Diensten anderer Anbieter auch bei gemeinsamer Verschlüsselungstechnologie stark beeinflussen konnten. Ziel der Regulierung sollte es

daher sein die Interoperabilität von Plattformen auf Dienstebene vorzuschreiben, statt spezifische technische Teillösungen zu forcieren.

Da IPTV aus technischer Sicht, anders als herkömmliche Broadcast-Verfahren, inhärent eine internationale Nutzung erlaubt, riskiert eine spezifisch deutsche Regulierung oder eine, wie derzeit abzusehen, Regulierung für nur wenige europäische Staaten eine Loslösung und Stillstand der IPTV Entwicklung in Deutschland und damit ein Scheitern am hiesigen Markt, insbesondere, da die internationale Nutzung von IPTV zusätzliche Marktchancen bietet, die es vom konventionellen Fernsehen abheben, beispielsweise durch Anbindung des Nutzers an gewohnte Sender, auch bei Auslandsaufenthalten.

Auch steht IPTV im direkten Wettbewerb zu anderen, kaum regulierten oder regulierbaren Video-Angeboten im Internet, so dass eine zu starke Regulierung die Marktmöglichkeiten zu Ungunsten von IPTV beeinflussen würde, und beispielsweise YouTube-ähnliche Dienste und andere nicht-IPTV "Internet TV" Dienste) den Markt beherrschen und IPTV zu einem Nischendasein reduzieren würden.Zusammenfassend wird daher empfohlen für die nahe Zukunft, außer der Verpflichtung zu interoperablen Lösungen als allgemeine Zielvorgabe, keine spezifische Regulierung vorzunehmen.

In etwa 3-5 Jahren, nachdem erkennbar ist, in welche Richtung sich sowohl die Standardisierung, also auch der Markt und die Anwendungsbereiche für IPTV entwickelt haben, kann dann eine behutsame Regulierung sinnvoll sein.

11 Zusammenfassung

IPTV befindet sich als Technologie noch in der Experimentalphase. Derzeit sind erste Basisdienste, welche sich noch stark an existierende Services anlehnen, kommerziell verfügbar, darüber hinaus reichende Anwendungen befinden sich derzeit jedoch zu einem großen Teil noch in der Entwicklung und Erprobung. Zurzeit sind Entwicklungstendenzen erkennbar, jedoch haben sich noch keine klaren Trends entwickelt.

Auch im Bereich der Standardisierung gibt es derzeit eine Reihe von Aktivitäten, primär durch das firmenorientierte Open IPTV Forum, aber auch durch andere Standardisierungsgremien wie ETSI und DVB. Allerdings sind auch hier bisher keine klaren Vorgaben verabschiedet worden.

Da dem IPTV Bereich aufgrund des Potentials als Konvergenztechnologie kein eindeutiges Marktsegment zugeordnet werden kann und sich auch hier das primäre Anwendungsgebiet in den nächsten Jahren erst herausbilden muss, ist eine Festlegung eines Teilaspektes (die technische Zugangssicherung) durch eine nationale oder auch eingeschränkt europäische Lösung für die IPTV Marktchancen schädlich. Dieses ist insbesondere der Fall, da es sich bei der derzeit anvisierten CSA Technologie um ein Hardware-basiertes System handelt, welches später am Markt nur schwer wieder auszutauschen ist.

Dieses wiegt umso schwerer, als dass Internet-basierte Videotechnologien, anders als herkömmliche Broadcastverfahren, sich nicht auf eine kleine Zahl von Providern beschränken und damit regulatorisch kontrollieren lassen. Dadurch steht IPTV im direkten Wettbewerb mit anderen Internet-Videodiensten wie dem Video-Vertrieb von iTunes Store und Amazon oder Podcast-Diensten wie YouTube oder auch neuen Videodiensten wie SmoothHD für Silverlight.

Das Festschreiben einer spezifischen Verschlüsselungstechnologie und die damit implizite Festlegung von MPEG-2 als Videostandard würde IPTV die nötige Flexibilität nehmen, um sich an einem schnell wandelnden Markt behaupten zu können.

Selbst wenn CSA als Zugangssicherungssytem technologisch anderen Systemen überlegen wäre und inhärent einen eine höhere Sicherheit gegen Content-Missbrauch bieten würde (wofür es allerdings keine Anzeichen gibt), hat die Entwicklung auf dem Audio-Markt gezeigt, dass Content-Provider (bei ansonsten identischer Situation) ein DRM-System mit hoher Sicherheit wünschen, sich aber am Markt dann für das System entscheiden, welches die meisten Nutzer und damit potentiellen Kunden erreicht, selbst wenn dieses System (iTunes, Musicload) die Inhalte ungeschützt verteilt.

Daher ist auch bei IPTV eine höhere Marktpenetration, welche auch implizit die Interoperabilität steigern wird, als wichtiger zu bewerten als die Festlegung auf ein spezifisches Verschlüsselungssystem.

12 Abkürzungsverzeichnis

AAA	Authentication, Authorization and Accounting
AACS	Advanced Access Content System
AES	Advanced Encryption Standard
AKE	Authentication and Key Exchange
ATIS	Alliance for Telecommunications Industry Solutions
BCD	Broadband Content Guide
BD+	Blu-ray Disc Digital Rights Management
CA	Conditional Access
CAM	Conditional Access Modul
CD	Compact Disk
CI	Common Interface
CPCM	Content Protection and Management
CPN	Customer Premises Network
CSA	Common Scrambling Algorithm
CSP	Content and Service Protection
CSS	Content Scramble System,
DAB	Digital Audio Broadcasting
DOCSIS	Data Over Cable Service Interface Specification
DRM	Digital Rights Management
DSL	Digital Subscriber Line
DTCP	Digital Transmission Content Protection
DTCP-IP	Digital Transmission Content Protection over Internet Protocol
DVB	Digital Video Broadcasting
DVB-C	Digital Video Broadcasting - Cable
DVB-H	Digital Video Broadcasting - Handheld

DVB-S	Digital Video Broadcasting – Satellite
DVB-T	Digital Video Broadcasting - Terrestrial
EPG	Electronic program guide,
ETSI	European Telecommunications Standards Institute
ETSI TISPAN	European Telecommunications Standards Institute - Telecommunications and Internet converged Services and Protocols for Advanced Networking
ETSI TC MCD	European Telecommunications Standards Institute - Technical Comitee for Media Content Distribution
GBA	Generic Bootstrapping Architecture
GCA	Gateway Centric Approach
HD	High Definition
HDTV	High Definition Television
HTTP	Hypertext Transfer Protocol
IBC	International Broadcasting Convention
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPTV	Internet Protocol Television
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
iTV	Interactive TV
MHP	Multimedia Home Platform
MP3	MPEG-1 Audio Layer 3
MP4	MPEG-4 Part 14
MPEG	Moving Picture Experts Group
NGN	Next Generation Networking
NSN	Nokia Siemens Networks
OIPF	Open IPTV Forum
OMA	Open Mobile Alliance

PCMCIA	Personal Computer Memory Card International Association
PVR	Personal Video Recorder
QoS	Quality of Service
RTP	Real-time Transport Protocols
SDK	Software Development Kit
SMS	Short Message Service
STB	Set-Top-Box
TISPAN	Telecommunications and Internet converged Services and Protocols for Advanced Networking
TKG	Telekommunikationsgesetz
TS	Transport Stream
USB	Universal Serial Bus
USD	Universaldienstrichtlinie
VCAS	Video Content Authority System
VDSL	Very High Bitrate Digital Subscriber Line
VoD	Video on Demand
VoIP	Voice over IP

13 Literaturverzeichnis

AACS Blu-ray Disc Pre-recorded Book [Online] / Verf. AACS LA. - http://www.aacsla.com/specifications/AACS_Spec_BD_Prerecorded.921.pdf.

AACS Introduction and Common Cryptographic Elements [Online] / Verf. AACS LA. - http://www.aacsla.com/specifications/specs091/AACS_Spec_Common_0.91.pdf.

Abschlußbericht der Projektgruppe CA/DRM des ATRT [Bericht] / Verf. Lütteke Georg und Illgner-Fehns Dr. Klaus. - 2009.

An introduction to Internet Radio [Online] / Verf. Kozamernik Franc und Michael Mullane.. - 2005. - http://www.ebu.ch/fr/technical/trev/trev_304-webcasting.pdf.

Analysis of the DVB Common Scrambling Algorithm [Online] / Verf. Weinmann Ralf-Philipp und Wirt Kai. - 2004. - http://www.cdc.informatik.tu-darmstadt.de/~kwirt/csa.pdf.

Anmerkungen des VPRT zu den Entwicklungen zum Common Interface Plus (CI-Plus) [Online] / Verf. VPRT - Verband privater Rundfunk und Telemedien e.V.. - 2009. - http://www.vprt.de/get_pdf.php?m=positions&langkey=de&id=80.

Anmerkungen des VPRT zum Workshop der Studie "Sicherung der Interoperabilität als Ziel der Regulierung der Rundfunkübertragung" [Online] / Verf. VPRT - Verband privater Rundfunk und Telemedien e.V.. - 2008. - http://www.vprt.de/index.html/de/positions/article/id/63/?year={-1}&or=0&page=2.

Apple FairPlay DRM [Online] / Verf. Wikipedia. - http://en.wikipedia.org/wiki/FairPlay.

Bericht Projektgruppe CA/DRM - ATRT Jahrestagung [Bericht] / Verf. Illgner-Fehns Dr.Klaus und Lütteke Dr.Georg. - 2008.

CI Plus Specification - Content Security Extensions to the Common Interface [Online] / Verf. CI Plus LLP. - 2009. - http://www.ci-plus.com/data/ci_plus_specification_v1.2.pdf.

Declassifying Content Security - Buzzwords, Myths, BS and How to Get Rich Quick [Bericht] / Verf. Wilson Robert (Nagra). - 2004.

DVB Security: Why Bother? [Bericht] / Verf. McCann Ken (ZetaCast). - 2009.

DVB-CPCM Frequently Asked Questions [Online] / Verf. DVB. - 2007. - http://www.dvb.org/technology/dvb-cpcm/CPCM_FAQ_160507.pdf.

Encryption and Security Tutorial [Bericht] / Verf. Gutmann Peter. - Auckland : University of Auckland, 2005.

Fernsehen über einen Breitband Internet Zugang [Online] / Verf. Monitor - das Magazin für Internettechnologie. - http://www.monitor.co.at/index.cfm/storyid/11276_IPTV-Fernsehen_ueber_einen_Breitband_Internet_Zugang.

Introduction of basic concepts in OMA DRM [Bericht] / Verf. Motorola Developer Network. - 2007.

Marlin Architecture Overview [Online] / Verf. Marlin Developer Community. - 2007. - http://www.marlin-community.com/public/MarlinArchitectureOverview.pdf.

Marlin Broadband Architecture Overview [Online] / Verf. Marlin Developer Community. - 2007. - http://www.marlin-community.com/public/MarlinBroadbandArchitectureOverview.pdf.

Microsoft PlayReady: Content Access and Protection Technology for Digital Entertainment Services, Devices and Applications [Online] / Verf. Microsoft. - http://www.microsoft.com/PlayReady/Overview.mspx.

N 300 401 V1.4. - Radio Broadcasting Systems;Digital Audio Broadcasting (DAB) to mobile, portable and fixed receivers [Bericht] / Verf. ETSI. - 2006.

Network infrastructure for IPTV [Online] / Verf. Arberg Peter [et al.]. - http://www.ericsson.com/ericsson/corpinfo/publications/review/2007_03/files/2_NetworkInfastructure.pdf.

New generation DVB scrambling [Online] / Verf. Nagravision. - http://www.nagravision.com/online/online02/article_7.html.

Next Generation IPTV Solution Home Entertainment Release 3.0 [Online] / Verf. Nokia Siemens Networks. - http://www.nokiasiemensnetworks.com/NR/rdonlyres/46FD93F4-9BC3-4154-BCB3-B516A5780AAB/0/1_NSNIPTVHE30Datasheet.pdf.

Nokia Siemens Networks Launches Next Generation IPTV Solution [Online] / Verf. Soft32.com. - http://news.soft32.com/nokia-siemens-networks-launches-next-generation-iptv-solution_7086.html.

Nokia Siemens Networks setzt mit IPTV-Lösung der nächsten Generation auf Plattform-Offenheit und -Interaktivität [Online] / Verf. Nokia Siemens Networks. - http://www.nokiasiemensnetworks.com/de/Press/Press+releases/news-archive/Nokia+Siemens+Networks+Launches+Next+Generation+IPTV+Solution.htm?languagecode=de.

OMA Digital Rights Management V2.1 [Online] / Verf. Open Mobile Alliance. - 2008. - http://www.openmobilealliance.org/Technical/release_program/drm_v2_1.aspx.

OMA-Download-ARCH-V1_0-20040625-A - Download Architecture [Bericht] / Verf. Open Mobile Alliance. - 2004.

OMA-Download-DRMCF-V1_0-20040615-A - DRM Content Format [Bericht] / Verf. Open Mobile Alliance. - 2004.

OMA-Download-DRMREL-V1_0-20040615-A - Rights Expression Language [Bericht] / Verf. Open Mobile Alliance. - 2004.

OMA-Download-DRM-V1_0-20040615-A - Digital Rights Management [Bericht] / Verf. Open Mobile Alliance. - 2004.

OMA-ERELD-DRM-V1_0-20040625-A - Enabler Release Definition for DRM [Bericht] / Verf. Open Mobile Alliance. - 2004.

OMA-ETS-DRM-v1_0-20040917-a - Enabler Test Specification for DRM 1.0 [Bericht] / Verf. Open Mobile Alliance. - 2004.

Open IPTV Forum – Toward an open IPTV standard [Online] / Verf. Cedervall Mats [et al.]. - 2007. - http://www.ericsson.com/ericsson/corpinfo/publications/review/2007_03/files/1_OpenIPTVForum.pdf.

Personalized and interactive TV enabled by IMS [Online] / Verf. Ericsson. - http://www.ericsson.com/technology/whitepapers/IMS_TV_4.pdf.

Proposed Definition and Description of IPTV services for IPTV service scenario [Online] / Verf. ITU. - 2006. - http://www.itu.int/md/dologin_md.asp?lang=en&id=T05-FG.IPTV-C-0132!!MSW-E.

Refusal, Remediation and Renewability in Marlin [Online] / Verf. Marlin Developer Community. - 2008. - http://www.marlin-community.com/public/RRR_WhitePaper_v.1.3_14Jan08.pdf.

Richtlinie des Europäischen Parlaments und des Rates über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten (Universaldienstrichtlinie) [Online] / Verf. Europäisches Parlament. - 2002. - http://www.bmvit.gv.at/telekommunikation/recht/downloads/rl2002de22.pdf.

Self-Protecting Digital Content [Online] / Verf. Kocher Paul [et al.]. - http://www.cryptography.com/resources/whitepapers/SelfProtectingContent.pdf.

Staatsvertrag für Rundfunk und Telemedien (Rundfunkstaatsvertrag RStV) [Bericht] / Verf. ALM - Arbeitsgemeinschaft der Landesmedienanstalten inder Bundesrepublik Deutschland. - 2008.

Status of the work item on Content Scrambling Algorithms [Bericht] / Verf. DVB CM IPTV Content Security Task Force. - 2009.

Supplementary CI Plus Specification for Service / Network Operators - Version 1.2 [Online] / Verf. CI Plus LLP. - 2009. - http://www.ci-plus.com/data/Supplementary_CI_Plus_specification_v1.2.pdf.

Telekommunikationsgesetz [Online] / Verf. Bundesministerium der Justiz. - 2004. - http://www.gesetze-im-internet.de/bundesrecht/tkg_2004/gesamt.pdf.

Terms of Reference of Technical Committee (TC) on Media Content Distribution (MCD) [Online] / Verf. ETSI. - 2008. - http://portal.etsi.org/mcd/MCD_ToR.asp.

The Role of NEMO in Marlin [Online] / Verf. Marlin Developer Community. - 2006. - http://www.marlin-community.com/public/RoleofNEMOinMarlin.pdf.

The Role of Octopus in Marlin [Online] / Verf. Marlin Developer Community. - 2006. - http://www.marlin-community.com/public/RoleofOctopusinMarlin.pdf.

The technology vision for the DTCP standard [Online] / Verf. IBM. - http://www.intel.com/standards/case/case_dtcp.htm.

Thoughts on Music [Online] / Verf. Jobs Steve. - Februar 2007. - www.apple.com/hotnews/thoughtsonmusic/.

TISPAN NGN Security standards [Bericht] / Verf. Rossebø Judith E. Y.. - Sophia-Antipolis : 4th ETSI Security Workshop, 2009.

TR 102 033 V1.1.1 - Architectural Framework for the Delivery of DVB-Services over IP-based Networks [Bericht] / Verf. ETSI. - 2002.

TR 187 002 - TISPAN NGN Security (NGN_SEC) Threat, Vulnerability and Risk Analysis - Release 2 [Bericht] / Verf. ETSI. - 2007.

TR 187 013 - TISPAN - Feasibility study on IPTV Security Architecture [Bericht] / Verf. ETSI. - 2008.

TS 102 034 V1.3.1 DVB-IPTV 1.3: Transport of MPEG-2 TS Based DVB Services over IP Based Networks (and associated XML) [Bericht] / Verf. ETSI. - 2007.

TS 102 825-10 - Content Protection and Copy Management (DVB-CPCM); Part 10: CPCM Acquisition, Consumption and Export Mappings [Bericht] / Verf. ETSI. - 2008.

TS 102 825-2 - Content Protection and Copy Management (DVB-CPCM); Part 2: CPCM Reference Model [Bericht] / Verf. ETSI. - 2008.

TS 102 825-4 - Content Protection and Copy Management (DVB-CPCM); Part 4: CPCM System Specification [Bericht] / Verf. ETSI. - 2008.

TS 102 825-5 - Content Protection and Copy Management (DVB-CPCM); Part 5: CPCM Security Toolbox [Bericht] / Verf. ETSI. - 2008.

TS 182 027 - IPTV functions supported by the IMS subsystem [Bericht] / Verf. ETSI.

TS 182 028 - Dedicated IPTV Subsystem in NGN [Bericht] / Verf. ETSI.

TS 183 063 - IMS based IPTV Stage 3 specification [Bericht] / Verf. ETSI .

TS 187 001 - NGN SECurity (SEC) Requirements – Release 2 [Bericht] / Verf. ETSI. - 2008.

TS 187 003 - NGN Security Architecture [Bericht] / Verf. ETSI . - 2007.

Volume 1 - Overview V1.0 [Bericht] / Verf. Open IPTV Forum. - 2009.

Volume 2 - Media Formats V1.0 [Bericht] / Verf. Open IPTV Forum. - 2009.

Volume 3 - Content Meta Data V1.0 [Bericht] / Verf. Open IPTV Forum. - 2009.

Volume 4 - Protocols V1.0 [Bericht] / Verf. Open IPTV Forum. - 2009.

Volume 5 - Declarative Application Environment V1.0 [Bericht] / Verf. Open IPTV Forum. - 2009.

Volume 6 - Procedural Application Environment V1.0 [Bericht] / Verf. Open IPTV Forum. - 2009.

Volume 7 - Authentication, Content Protection and Service Protection V1.0 [Bericht] / Verf. Open IPTV Forum. - 2009.

Windows Media DRM FAQ [Online] / Verf. Microsoft. - 2005. - http://www.microsoft.com/windows/windowsmedia/forpros/DRM/FAQ.aspx.

Windows Media Rights Manager 10.1.2 Software Development Kit Programming Reference [Online] / Verf. Microsoft. - http://msdn.microsoft.com/en-us/library/bb614742(VS.85).aspx.