DRM für Multimedia-Broadcasts – wie sieht das PayTV der Zukunft aus?

Ulrich Greveler

Horst-Görtz-Institut für IT Sicherheit
Ruhr-Universität Bochum
44780 Bochum
ulrich.greveler@nds.rub.de

Zusammenfassung

Der Beitrag beschreibt neue Anforderungen an ein globales System für digitale Multimediaübertragungen und Lösungen zur Umsetzung dieser Anforderungen. Aufgrund des Erfolges der Standardisierung der Kodierung multimedialer Inhalte kann ein moderner PC als Set-Top-Box zum Empfang von kostenpflichtigen Inhalten dienen, der via Internet vermarktet und – wie bisher – via Ausstrahlung übertragen wird. Dies ermöglicht die Existenz globaler Anbieter für PayTV, Newsdienste und andere hochwertige Inhalte im Pay-per-View-Modell, die supranational ausgestrahlt und vermarktet werden, stellt aber hohe Anforderungen an das DRM-System, das die Interessen der Rechteinhaber durchsetzt. Die Herausforderung besteht in der Bindung der erworbenen Inhalte an Regionen, da die Rechte-Inhaber verschiedene Nutzungskonditionen abhängig von der Region, in der sich Konsumenten aufhalten, vorsehen.

1 Einführung

PayTV (Bezahlfernsehen) stellt seit den 80er Jahren ein erfolgreiches Geschäftsmodell für Multimedia-Inhalte dar. Viele Jahre bevor der Begriff *E-Commerce* erfunden wurde, war die Vermarktung (analoger) Fernsehproduktionen in vielen Ländern (z.B. Großbritannien) etabliert. Aufgrund der zunehmenden Digitalisierung der Fernseh- und Filmproduktionen auf der einen Seite und verbesserter Multimediafähigkeit von Privatanwender-PCs auf der anderen Seite ergibt sich die Fragestellung, wann diese Technologien zusammenwachsen. Ein zentraler Punkt bei der Einführung neuer Technologien im Bereich Vermarktung multimedialer Inhalte stellt die Durchsetzungsmöglichkeit der kommerziellen Interessen der Rechte-Inhaber mittels DRM (Digital Rights Management) dar. In diesem Beitrag werden verschiedene Mechanismen zur Durchsetzung vorgestellt und analysiert, insbesondere neue Anforderungen und Entwicklungen in diesem Bereich sollen aufgegriffen werden.

1.1 Technische Standardisierung

Aufgrund der weiten Verbreitung von Datenformat-Standards für Multimedia-Content (z. B. MPEG21 [6]) und dessen breitbandiger Übertragung (z. B. DVB) ist eine deutliche Konvergenz von PC-Technologien und Unterhaltungselektronik erkennbar. Der etablierte Standard für digitales PayTV (*Common Interface* [2] mit Smartcards) ist ebenfalls so-

wohl für klassische Empfangsgeräte (Digitale Receiver, SetTop-Boxen) als auch für PCs verfügbar. Die Übertragungen selbst können auch mit multipler Sprachunterstützung ausgestrahlt werden (Audio-„Kanäle“, wählbare Untertitel), so dass potentielle Kunden über ein nationales Gebiet hinweg mit einer Übertragung (z. B. via Satellit) versorgt werden können. Diese Entwicklung ermöglicht die Existenz von supranationalen (bzw. globalen) PayTV-Anbietern. Ein Pay-per-View-Modell eines globalen Anbieters kann dann in der Weise eines Webshops realisiert werden, d. h. die Kunden ordern einzelne Übertragungen (Filme, Sport-Events) mit dem Webbrowser und empfangen – wie gewohnt – eine Freischaltung über den Broadcast-Kanal, die speziell das Angebot für ihre Region (Sprachwahl) zum dort festgelegten Preis ermöglicht. Hierbei spielt die Durchsetzung des DRM eine wesentliche Rolle, denn einerseits könnte ein Anbieter erhebliche Kosten sparen, wenn er Übertragungen, die ohnehin Grenzen überschreiten, auch supranational vermarkten kann, andererseits muss die Preisstruktur, die letztlich der Rechteinhaber für jede Region festlegt, berücksichtigt und durchgesetzt werden. Es darf aus Sicht des Rechteinhabers nicht möglich sein, eine Übertragung für eine „günstige“ Region zu ordern und diese dann in einer „teuren“ Region zu konsumieren. Kann dies jedoch wirksam verhindert werden, ermöglicht die effiziente Nutzung der Übertragungskapazitäten für eine globale Zielgruppe eine Verringerung der Übertragungskosten, die auch mittelbar für den Rechteinhaber eine Erhöhung der Einkünfte ermöglicht.

1.2 Etablierte Standards

Das Ziel der von uns vorgeschlagenen Architektur besteht neben den Sicherheitsanforderungen darin, auf bestehenden Standards aufzubauen, d. h. eine geeignete technische Lösung erfordert kein Ausrollen einer neuen Technologie (Empfangsgeräte) auf Endbenutzerseite. Die etablierten Standards im Bereich digitale Übertragung von Filmen und Fernsehprogrammen sind DVB (Digital Video Broadcasting [8]) zur Übertragung der Inhalte über Satellit, Kabel und terrestrischem Funk, die MPEG-Standards [6] zur Kodierung der Inhalte und CAS (Conditional Access System [1]) mit der Schnittstelle CI (Common Interface, [2]) zur Durchsetzung der digitalen Rechte. Diese Standards werden von den derzeitigen PayTV-Anbietern verwendet und sind in den Empfangsgeräten (Set-Top Boxen für den Fernseher oder DVB-Karte für den PC) implementiert. Bemerkenswert ist an dieser Stelle, dass sowohl die Unterhaltungselektronik als auch der Personal Computer dieselben Multimediastandards unterstützen. Trotz der erfolgreichen Kovergenz der Technologien, können die digitalen Inhalte selbst mittelfristig noch nicht über das Internet übertragen werden, da dieses für den Privatanwender noch keine ausreichende Bandbreite für die erheblichen Datenmengen zur Verfügung stellt; es gibt zwar Multicast-Verfahren, die via Internet nutzbar wären [5], diese sind aber derzeit nicht für PayTV geeignet [7].

Die Endbenutzer erhalten von ihrem Anbieter bzw. Händler eine Smartcard und ein CAM (Conditional Access Module), in das die Karte gesteckt wird. Das Modul, das nur etwas größer als die Karte selbst ist, wird dann in einen CI-Slot gesteckt, um das PayTV-Abonnement zu nutzen. Die verbreiteten CA-Systeme (z. B. Irdeto, Nagravision, Beta-Crypt) sind allein über die Karte und das CAM realisiert; das Empfangsgerät selbst bietet CI als standardisierte Schnittstelle. Auf diese Weise können nach Bekanntwerden von Schwachstellen verbesserte CA-Systeme genutzt werden, ohne dass die Empfangsgeräte erneuert werden müssen. Die Entschlüsselung der Inhalte im Empfangsgerät geschieht

mittels *Common Scrambling Algorithm*; bisher sind keine wesentlichen Schwachstellen dieses Kryptoverfahrens bekannt geworden, es wurden aber bereits Teilmechanismen des Algorithmus gebrochen [11]. Die zur Entschlüsselung mittels CSA benötigten Schlüssel empfängt die Set-Top-Box in kurzen Abständen als sogenannte *Control Words* über das CI.

CAS ist eine etablierte Technologie in Bezug auf regionales (meist nationales) Bezahlfernsehen; die Anbieter in einer Region liefern die Karten an ihre Kunden und wählen die Preisstruktur für das Angebot in Abhängigkeit von den Entgelten, die der Rechte-Inhaber für die Vermarktung in dieser Region erhebt. Der Übertragungsinhalt kann dadurch in jeder Region zu anderen Konditionen vermarktet werden. Für die globale Vermarktung ist CAS jedoch auf den ersten Blick ungeeignet, da das Angebot mit jeder freigeschalteten Karte unabhängig vom Aufenthaltsort des Endbenutzers empfangen werden kann. Es kann also technisch vom Empfgangsgerät nicht ohne weiteres zwischen „günstigen“ und „teuren“ Regionen unterschieden werden.

2 Anforderungen der Rechteinhaber

Wir wollen nun Anforderungen seitens des Geschäftsmodells eines globalen Anbieters und der jeweiligen Rechteinhaber detaillieren. Zunächst legen wir fest, was wir in unserem Vorschlag unter einer Lizenz verstehen, die es einem bestimmten Nutzer in einer definierten Region erlaubt, eine Übertragung zu konsumieren (d. h. für seinen PC / seine SetTop-Box, diese Übertragung entschlüsseln zu können).

Wie in Abb. 1 dargestellt, soll der Rechteinhaber spezifizieren können, dass der Inhalt, der in diesem Beispiel dreimal übertragen wird, in jeder Region zu einem anderen Preis vermarktet wird und dass einzelne Regionen zu bestimmten Zeitpunkten ganz ausgeblendet werden. Im derzeitigen CAS-System kann dies realisiert werden, indem ein Nutzungsvertrag mit drei Anbietern (jeweils einer pro Region) geschlossen wird und die Kunden in einer Region die Karte ihres Anbieters erhalten. Die Übertragung wird dann für jede Region einzeln und gleichzeitig erfolgen, auch dann wenn alle Regionen vom selben Satelliten versorgt werden. Insgesamt wird der Inhalt in diesem Beispiel sieben Mal übertragen. Ein globaler Anbieter könnte Kosten sparen und den Inhalt jeweils für alle Regionen, d. h. insgesamt nur drei Mal, übertragen, muss dann aber sicherstellen, dass die Nutzung trotzdem an die Region gebunden bleibt. Beispielsweise darf es nicht möglich sein, dass ein Kunde in Region 3 seine Karte in Region 2 kauft, um die erste der drei Übertragungen zu sehen.

Die Rechteinhaber behalten sich vor, für jede Region Preise und Ausstrahlungszeitpunkte zu bestimmen. Bei jeder Ausstrahlung wird die Sprachauswahl (Audio und Untertitel) für jede Region festgelegt. Abb. 2 zeigt das Modell einer Lizenz als abstraktes Datenformat, das den Content an den Nutzer und eine Region bindet.

Diese Lizenz legt auf kryptographische Weise fest, welcher Content (Broadcast ID) für den Benutzer zur Verfügung steht; gleichzeitig wird die Festlegung an die spezifizierte Region (Region ID) vorgenommen, gemeinsam mit der Einschränkung der Nutzung, d. h. der Nutzer darf nur bestimmte Sprachinhalte (Audio stream, Subtitles) dieses Contents empfangen (d. h. entschlüsseln können). Die Restriktionen müssen nicht explizit angegeben sein; i. a. wird das Vorhandensein kryptographischer Schlüssel innerhalb des *Restriction*-Feldes ge-

	Region 1	Region 2	Region 3
Transmission 1 (**date:** Jan 15) **audio:** E, F, DE **subtitle:** E1, E2, F	per-view 5$ audio: all subtitle: all	per-view 3$ audio: DE subtitle: E1, DE	black out
Transmission 2 (**date:** Feb 12) **audio:** E, F, DE, ES, IT, CH, JP **subtitle:** E1, E2, F, DE1, DE2, ...	per-view 3$ audio: all subtitle: all	black out	per-view 5$ audio: E, JP subtitle: all
Transmission 3 (**date:** Jun 19) **audio:** E, F, DE **subtitle:** E1, E2, F	free for subscribers audio: all subtitle: all	per-view 1$ audio: DE subtitle: E1, DE	free for subscribers audio: E, JP subtitle: all

Abbildung 1: Mehrere Übertragungen des gleichen Inhalts, Beispiel

nau die Entschlüsselung bestimmter Sprachwahlen ermöglichen, so dass fehlende Schlüssel die Nutzung der (aus Sicht der Rechte-Inhaber „nichtzulässigen“) Sprachen verhindern.

Der Nutzer kann diese Lizenz grundsätzlich über einen beliebigen Weg (z. B. Webshop, telefonisch) unter Angabe seiner Aufenthaltsregion bzw. der Region, in der der Inhalt konsumiert werden wird, erwerben. Sein Empfangsgerät wird eine Lizenz in Form eines Lizenz-Tickets, das dann als kleine Datei vorliegt, empfangen und an die Smartcard weitergeben. Diese sendet dann die zur Entschlüsselung benötigten Daten an die Set-Top-Box. Das Ticket soll gegen Verfälschung kryptographisch geschützt sein (AuthCode), eine Nutzung außerhalb der spezifizierten Region muss unterbunden werden. Eine konkrete Festlegung des Datenformats soll nicht vorgenommen werden; das Ticket kann sowohl als Kontrollnachricht einer existierenden CAS-Anwendung aufgefasst werden als auch mittels einer Rights-Expression-Language (z. B. XrML) beschrieben sein.

3 Mögliche Maßnahmen zur Durchsetzung des DRM

Zur Durchsetzung der Anforderungen der Rechteinhaber sind unterschiedliche Ansätze denkbar. Diese unterscheiden sich im Hinblick auf Sicherheitseigenschaften, Kosten und Benutzerfreundlichkeit. Eine wünschenswerte Eigenschaft wäre die Möglichkeit, auf den im vorigen Abschnitt benannten Standards aufzubauen, so dass der Kunde des PayTV-Anbieters seine Empfangsgeräte weiterhin nutzen kann. Die Herausforderung für das DRM-System des globalen PayTV-Anbieters besteht in der Bindung der Rechte an Regionen; die CAS-Technologie hat sich als DRM-System für nationale PayTV-Anbieter

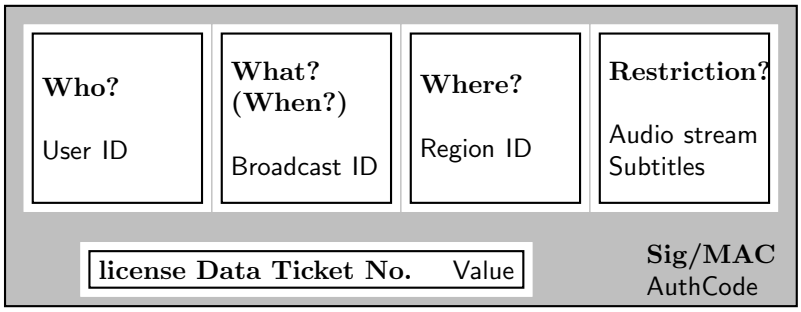

Abbildung 2: Lizenz Ticket

bewährt, unterstützt aber keine Regionalisierung abgesehen von der impliziten Bindung an Regionen, wenn es - wie zur Zeit- in jeder Region einen dedizierten Anbieter gibt, der für seine Kunden den Inhalt verschlüsselt und ausstrahlt.

Die Bindung an eine Region kann über eine sichere Lokalisierungsfunktion auf Seiten des Empfangsgerätes oder über eine senderseitige Lokalisierung bei der Erstellung des Lizenz-Tickets erfolgen; es sind aber auch Alternativen denkbar, die implizit die regionale Bindung durchsetzen. Wir betrachten folgende technische Maßnahmen.

1. Nutzung der etablierten CAS-Technologie in Kombination mit einer Lokalisierungsfunktion durch Call-Out-Funktionalität der SetTop-Box (ein als Empfangsgerät genutzter PC könnte via ISDN mit Nummernübertragung eine Verbindung aufbauen)
2. Positionsbestimmung mittels Navigationssatelliten (GPS, Galileo), ggf. unter Einsatz von Trusted-Computing-Funktionen des Multimedia-PCs
3. Einsatz eines von der Broadcast-Übertragung unabhängigen Funknetzes mit feiner örtlicher Auflösung (z.B. GSM-Netz mit Cell-Broadcast-Funktion) zur Übertragung der Schlüsselinformationen
4. Spezifikation eines modifizierten CAS mit inhärenter Lokalisierungsfunktion
5. Lokalisierung durch Auswertung der Netztopologie des Internets und Messungen zu Latenz und Durchsatz der übertragenen Daten
6. Nutzung der vom Betriebssystem bzw. von angeschlossenen Geräten verwalteten *Region Codes* gemäß DVD-Standard

Bewertung der technischen Maßnahmen

Die Maßnahmen unterscheiden sich deutlich bzgl. benötigter Ressourcen, Kosten für einen Roll-Out und erzieltem Sicherheitsniveau. Ein Vergleich der Wirksamkeit technischer Maßnahmen ist schwierig, insbesondere der realistische Aufwand seitens des Angreifers kann oft nur subjektiv abgeschätzt werden. Wir konzentrieren uns daher auf die Darlegung der Stärken und Schwächen sowie besonderer Eigenschaften der Alternativen. Es ist zu betonen: Je nach Gewichtung der Eigenschaften wird ein Anbieter in Bezug auf die Auswahl einer DRM-Architektur zu unterschiedlichen Ergebnissen kommen können.

Die Maßnahme 1 (Call-Out zur Lokalisierung, siehe [3]) bietet nur eine eingeschränkte Benutzerfreundlichkeit, da der PC oder die Set-Top-Box selbst einen Verbindungsaufbau über eine Wählleitung herstellen müsste. Eine solche Funktionalität ist in den Empfangsgeräten i. a. nicht vorhanden und auch PCs verfügen nicht regelmäßig über eine Verbin-

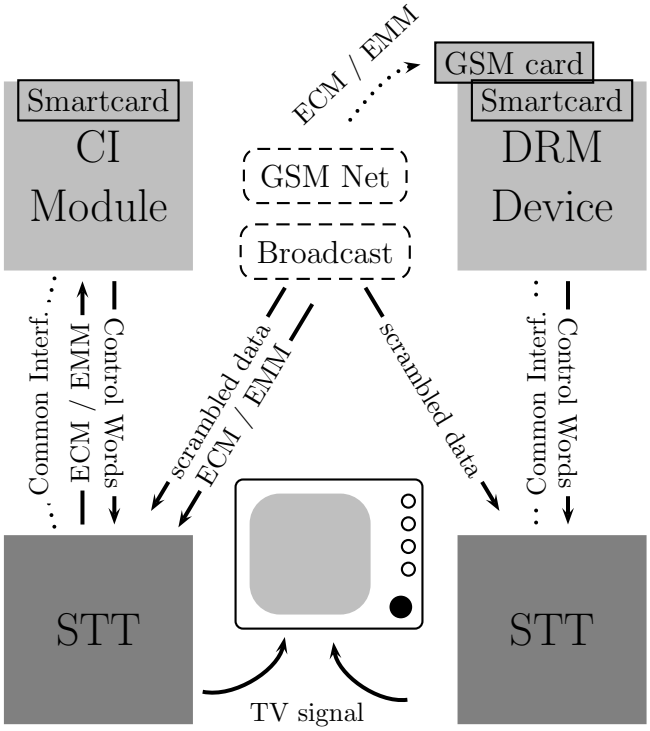

Abbildung 3: bisheriges CAS – neues CAS plus Funknetz

dung zum Telefonnetz; der Benutzer müsste dies dann erst eigenhändig bereitstellen. Da der Präfix einer Telefonnummer (die Vorwahl) einen Rückschluss nicht nur auf den Staat sondern auch auf kleinere Gebiete (z. B. Städte) zulässt, wäre die regelmäßige Erhebung dieser Ortsdaten auf Anbieterseite auch unter Datenschutzaspekten problematisch. Das Sicherheitsniveau hängt nicht nur von der Zuverlässigkeit der Rufnummernübertragung ab; denn weil es technisch möglich ist, Weiterleitungen einzurichten, so dass der Anruf aus Sicht des Anbieters scheinbar aus einer günstigen Region kommt, ist eine erfolgreiche Umgehung der Sicherheitsmaßnahme mit geringem bis mittlerem Aufwand möglich.

Die Maßnahme 2 (GPS) macht eine zusätzliche Hardware auf Nutzseite mit ensprechenden Mehrkosten erforlich. Wenn CAS-Technologie weitergenutzt werden soll, muss das CA-Modul bzw. mittelbar die Smartcard die Positionierungsdaten empfangen, um eine Überprüfung der Position unter Berücksichtigung des Lizenz-Tickets zu ermöglichen. Eine notwendige direkte Verbindung zwischen GPS-Hardware und dem Modul ist technisch aufwändig und stellt den Benutzer möglicherweise vor eine Herausforderung bei der Verkabelung der Geräte. Ist das Empfangsgerät ein PC könnte unter Nutzung von Trusted-Computing-Funktionalität [10] eine gesicherte Verbindung zur GPS-Hardware realisiert werden und eine Anbindung über PC-Schnittstellen wäre möglich. Der Angreifer hat in beiden Fällen jedoch die Möglichkeit, das GPS-Signal zu verfälschen, um dem Empfangsgerät eine andere Region vorzutäuschen. Die von den Satelliten empfangenen Daten sind nicht kryptographisch gesichert und können mittels spezieller Hardware simuliert oder nach Aufzeichnung abgespielt werden. Die Umgehung der Sicherheitsmaßnahme ist daher mit mittlerem bis hohem Aufwand möglich.

Die Alternative 3 setzt ebenfalls eine zusätzliche Hardware auf Empfängerseite voraus (eine GSM-Karte, die allerdings gemeinsam mit dem CAM implementiert werden kann).

Die Herstellung dieses speziellen CAM wäre mit höheren Kosten im Vergleich zu normalen CAMs verbunden. Die Architektur ist in Abb. 3 dargestellt. Die Wirksamkeit dieses von uns vorgeschlagenen Verfahrens [4] besteht in der Tatsache, dass ein essentieller Teil der zur Entschlüsselung benötigten Informationen (z. B. das Lizenz-Ticket und einige CAS-Kontrollnachrichten: ECM, EMM) nicht über den Übertragungskanal sondern über ein zweites Funknetz (hier: GSM mit Dienst *Cellbroadcast*) nur in der entsprechenden Region gesendet wird. Ein Angreifer kann zwar beim Erwerb der Lizenz eine falsche Region angeben, er kann diese aber nicht nutzen, da notwendige Daten nicht an seinem Standort erhältlich sind. Die Nutzerfreundlichkeit ist auch hier eingeschränkt, da eine GSM-Netzabdeckung des Empfangsgerätes erforderlich ist. Um das System zu brechen, müsste entweder eine Manipulation der GSM-Netze erfolgen, was für den Angreifer – selbst mit hohem Aufwand – nicht möglich sein sollte, oder es müsste das Signal des zweiten Funknetzes in Echtzeit zum Angreifer übermittelt werden. Letzteres ist mit hohem Aufwand möglich, allerdings ist es mit diesem Angriff ohnehin möglich, die gesamte CAS-Architektur zu brechen, da auch die Daten, die über das CI übertragen werden, weitergeleitet werden können, d. h. auch die Sicherheitsarchitektur der bestehenden regionalen Anbieter würden mit einem solchen erfolgreichen Angriff durchbrochen.

Eine Weiterentwicklung des CAS-Systems (Maßnahme 4) könnte nicht nur bestehende Sicherheitsschwächen ausmerzen, sondern auch eine sichere Lokalisierungsfunktion integrieren. Dies würde allerdings einen Roll-Out neuer Empfangsgeräte, die den neuen Standard unterstützen, erforderlich machen. Diese Möglichkeit, die sich ohne Kenntnis der neuen Standards sicherheitstechnisch nicht bewerten lässt, wäre bei kurzfristiger Umsetzung nicht kundenfreundlich, da die Kunden ihre Geräte nicht mehr nutzen können; langfristig wäre aber eine neue CAS-Architektur mit der nächsten Gerätegeneration zu erwarten.

Die Maßnahme 5 (Lokalisierung durch Auswertung der Internetverbindung) setzt voraus, dass die Verbindung tatsächlich vom Kunden initiiert wird und nicht von einem Mittelsmann, der sich in einer anderen Region aufhält. Sie kommt darüber hinaus nicht für Kunden in Frage, die über keine Verbindung zum Internet verfügen und ist daher als nur begrenzt kundenfreundlich einzustufen. Die im Internet verbreitete Proxy-Technologie liefert allerdings eine Umgehungsmöglichkeit dieser Lokalisierungstechnik; der Angreifer kann unter Nutzung eines Proxy-Services mit geringen Aufwand seine Position verschleiern und damit die Sicherheitsarchitektur durchbrechen.

Abschließend untersuchen wir die Maßnahme 6 (DVD-*Region Code*). Der DVD-Standard [9] sieht einen Regionalcode vor, der es ermöglicht, Medien gezielt in einer von sechs Weltregionen anzubieten, ohne dass diese von Abspielgeräten in anderen Regionen akzeptiert werden. Für DVD-Laufwerke wird die Regionalcodierung häufig so realisiert, dass sich der Nutzer für einen Regionalcode entscheiden muss, der nach einer maximalen Anzahl von Änderungen nicht mehr geändert werden kann. Wird der PC als Abspielgerät genutzt, könnte dieser Regionalcode auch zur Überprüfung der PayTV-Region herangezogen werden. Die DVD-Regionen sind jedoch viel größer als die Marktregionen, die beim PayTV Verwendung finden; eine vollständige Umsetzung der Regionenbindung ist daher nicht möglich. Zudem ist es mithilfe von Tools und Anleitungen, die teilweise via Internet verfügbar sind, für den Benutzer mit geringem Aufwand möglich, bei vielen Geräten die Regionalcode-Sicherung zu umgehen.

Zusammenfassend lässt sich feststellen, dass von den genannten Maßnahmen nur 2 und 3 die Regionalbindung auf gehobenem Sicherheitsniveau realisieren und gleichzeitig eine Unterstützung der bestehenden Infrastruktur und Standards ermöglichen. Ein direkter Vergleich der Maßnahmen 2 und 3 ist schwierig, da bei der Entscheidung für eine Systemarchitektur auch bisher nicht genannte Aspekte außerhalb der Sicherheitsüberlegungen beim globalen PayTV-Anbieter eine Rolle spielen können (z. B. Akzeptanzprobleme von Trusted-Computing-Lösungen, aufwändige Vertragsgestaltung mit GSM-Netzbetreibern, umständlicher Aufbau und Verkabelung eines GPS-Empfängers mit der Set-Top-Box etc.).

4 Zusammenfassung und Ausblick

Wir haben gezeigt, dass ein globales PayTV-Angebot unter Nutzung der etablierten Technologien und gleichzeitiger Wahrung der Interessen der Rechte-Inhaber grundsätzlich realisierbar ist. Zur Umsetzung sind eine Vielzahl technischer Maßnahmen denkbar; diese unterscheiden sich jedoch erheblich in Bezug auf Kosten, Benutzerfreundlichkeit und Sicherheit.

Wenn die Rechte-Inhaber zur Überzeugung gelangen, dass ein wirksames DRM-System zur Berücksichtigung regionaler Lizenzmodelle Bestand hat, kann dies einen globalen Markt für Multimediaübertragungen ermöglichen. Die Nutzer könnten dann beispielsweise über das Internet die Rechte am Konsum einzelner Übertragungen erwerben, so dass PayTV letztlich zu einer E-Commerce-Anwendung würde. Gleichzeitig würde die Anzahl der notwendigen Ausstrahlungen desselben Inhalts reduziert, wodurch Kosten gespart werden können, was sowohl dem Endkunden als auch dem Rechteinhaber zugute kommen könnte. Eine solche Entwicklung würde aber vermutlich auch die Anzahl der PayTV-Anbieter global reduzieren, denn ein Verdrängungswettbewerb ist wahrscheinlich.

Literatur

[1] Simon Bewic. Descrambling dvb data according to etsi common scrambling specification. Technical Report GB2322994A, GB2322995A, UK Patent Application, 1998.

[2] CENELEC. Common interface specification for conditional access and other digital video broadcasting decoder applications. Technical Report EN 50221, Technical Committee TC 206, October 1997.

[3] Eran Gabber and Avishai Wool. How to prove where you are. *Proceedings of the 5th ACM Conference on Computer and Communications Security*, pages 142–149, November 1998.

[4] Ulrich Greveler. Enforcing regional drm for multimedia broadcasts with and without trusted computing. In *First International Conference on Digital Rights Management DRMtics (Sydney)*. Springer LNCS, November 2005.

[5] R. Hinden and S. Deering. IP version 6 addressing architecture. RFC 2373, IETF, July 1998.

[6] Keith Hill Jan Bormans. Mpeg-21 overview v.5. Technical Report JTC1/SC29/WG11/N5231, ISO/IEC, Requirements Group, October 2002.

[7] Katia Obraczka. Multicast transport protocols: A survey and taxonomy. *IEEE Communications Magazine*, pages 94–102, January 1998.

[8] Ulrich Reimers. *DVB, The Family of International Standards for Digital Video Broadcasting*. Springer, second edition, September 2004.

[9] Jim Taylor. *DVD Demystified*. McGraw-Hill Professional, second edition, December 2000.

[10] Trusted Computing Group. Tcg tpm specification version 1.2 revision 85, tpm main, part 1, design principles. Technical report, Trusted Computing Group, February 2005.

[11] Ralf-Philipp Weinmann and Kai Wirt. Analysis of the dvb common scrambling algorithm. In *Proceedings of the 8th IFIP TC-6 TC-11 Conference on Communications and Multimedia Security (CMS 2004)*. Springer LNCS.