Digitales Rechte Management

Anhang

Nachstehend sei noch einmal dargestellt, was man prinzipiell zum Schutz vor illegaler Nutzung von Inhalten tun kann, selbst wenn sie unverschlüsselt weitergegeben und aufgezeichnet werden: (Die Meinung der Hollywood-Studios hierzu ist wie gesagt, dass man wirkliche Sicherheit vor illegaler Nutzung – und die braucht man ihrer Meinung nach auch für Free-to-Air - im Gegensatz zu den unten dargestellten Methoden nur mit Verschlüsselung erreichen kann).

Ein wichtiger Punkt beim Schutz von Inhalten vor illegaler Nutzung ist der Schutz der Nutzungs-Rechte. Ein weiterer ist die sichere Verbindung der Inhalte mit der Signalisierung der Nutzungs-Rechte, um eine Manipulation der letzteren zu verhindern. Einige der Möglichkeiten sind:

1. Die Signalisierung der Nutzungs-Rechte wird einfach in Klartext zusammen oder parallel mit dem unverschlüsselten Inhalt übertragen oder gespeichert. Da die Nutzungsrechte im Klartext sind, und auch nur dieser Klartext vor einer Nutzung ausgewertet wird, besteht kaum eine Sicherung der Nutzungsrechte. Sie könnten eventuell leicht gegen erweiterte Rechte ausgetauscht werden (z.B. an einem gängigen PC).
2. Die Signalisierung der Nutzungs-Rechte wird verschlüsselt. Dies ergibt eine etwas größere Sicherung gegen Manipulation der Signalisierung. Es ergibt jedoch keine sichere Bindung an den unverschlüsselten Inhalt.
3. Die Signalisierung der Nutzungs-Rechte mit einem Teil des unverschlüsselten Inhaltes verrechnet wird anschließend verschlüsselt und (Der Inhalt selbst bleibt jedoch weiterhin unverschlüsselt). Dies ergibt eine sicherere Bindung an den unverschlüsselten Inhalt.
4. Die Signalisierung der Nutzungs-Rechte wird verschlüsselt und mit der Information eines Wasserzeichens verrechnet, welches vorher in den unverschlüsselten Inhalt eingefügt wurde. Alternativ hierzu können auch die verschlüsselten Nutzungs-Rechte in Form eines Wasserzeichens nach dem Empfang in den Inhalt eingebettet werden. Die Bindung an den unverschlüsselten Inhalt wird hierdurch noch weiter abgesichert.

Die genannten Optionen erfordern nach unten hin eine immer größere Komplexität.

Die Variante 1 wird von Sony und vermutlich auch von anderen Geräte-Herstellern favorisiert. Ihre Argumentation ist, dass es bei unverschlüsselten Inhalten nicht wirklich einen Sinn macht, die Nutzungsinformationen hochgradig zu schützen. Das Ziel, ‚to keep honest people honest' kann für „Free- to-Air" dennoch erreicht werden. Die Hersteler sagen, vor allem für die dritte Welt brauche man preisgünstige Geräte, vor allem für Free-to-Air. Mit der Variante 1 lässt sich dies einfach erreichen.

Bezüglich eines Wasserzeichens wurde mir von einem IC-Hersteller erklärt, dass es eines sehr viel größeren Aufwandes bedarf, ein Wasserzeichen in einem Inhalt zu

detektieren und auszuwerten, als ein Wasserzeichen in einen Inhalt einzufügen. Die Schwierigkeit steigt darüber hinaus um so mehr an, je sicherer ein Wasserzeichen gegenüber möglichen Manipulationen und Veränderungen des Inhaltes gemacht werden soll, da die notwendigen forensischen Methoden immer komplexer werden. Aus diesen Gründen sehen viele DVB-Mitglieder in der Verwendung von Wasserzeichen keine Alternative. Sie werden sogar als komplexer betrachtet als zu verschlüsseln. Und für 'Free-to-Air' komplexere Schutzmechanismen zu verwenden, als für ‚Pay-TV' macht keinen Sinn.

Mit dem deutlich verringerten Schutz unverschlüsselt weitergegebener und aufgezeichneter Inhalte ist es nach Meinung einiger DVB-Mitglieder nicht vereinbar, alle der prinzipiell möglichen Nutzungs- Einschränkungen in DVB-CPCM auch für diese Inhalte zur Verfügung zu stellen. So etwa eine Signalisierung ‚Copy Never'. Derartige Einschränkungen machen aber aus unserer Sicht ohnehin keinen Sinn für ‚Free--to-Air'. Nutzungs-Einschränkungen, welche auf die ‚Authorized Domain' bezogen sind, werden im EBU-Papier zu ‚Free-to-Air' ohnehin als obsolet bezeichnet. Dies sollte also kein Problem für uns sein.

Im Ergebnis sind wir mit unseren Forderungen also sehr nahe bei den Geräte-Herstellern - die Vertreter der Hollywood-Studios dagegen eher isoliert. Andererseits will sich kein Hersteller mit Hollywood anlegen, und so schwelt es oft nur unter der Decke.

Signalisierung der Nutzungs-Rechte für Free-to-Air und eventuelle Sicherung der Signalisierungen:

Für die Definition der Signalisierungen, welche für Free–to-Air als notwendig erachtet werden wurde innerhalb der CPCM System Spezifikation unter 7.2.3. bereits ein Punkt vorgesehen.

Die beiden Signalisierungen sollen in jedem Fall in Klartext übertragen werden, um den Konsumenten über die Nutzungs-Rechte des Inhaltes informieren zu können.

Es besteht jedoch bislang keine Einigkeit darüber, ob es Sinn macht, die Signalisierungen zu schützen. Jean-Pierre Evain und mir erscheint es sinnvoll, eine Sicherung der Nutzungs-Informationen für Free-to-Air gegen Manipulation vorzunehmen. Geschehen könnte dies z.B. mit Hilfe eines so genannten Hashings, wie bereits bei MHP verwendet, wo die Signalisierungen mit einem geheimen Schlüssel vermengt werden, und dadurch vor Manipulation geschützt. Aber auch andere Verfahren, z.B. in Verbindung mit einem Wasserzeichen sind denkbar.

Entgegengehalten wurde uns, dass ein solcher Schutzmechanismus zusätzliche Kosten verursachen, aber keine Vorteile bringen würde, da man in jedem Fall anstatt die Signalisierungen zu manipulieren, sie auch einfach vollständig entfernen könnte, wodurch im Ergebnis ein Inhalt entstehen würde, welcher von einem völlig ungeschützten Inhalt nicht zu unterscheiden wäre, und mit dem man aus technischer Sicht alles machen könnte was man wolle.

Wollte man auch dies verhindern, so müsste man die Signalisierungen z.B. in einem Wasserzeichen im Inhalt unterbringen, welches untrennbar mit ihm verbunden ist, ***und*** man müsste dieses Wasserzeichen in den CPCM-Geräten auswerten. Dies würde sicherlich größere Kosten verursachen, die man für Free-to-Air ja gerade vermeiden will.

Der Grund, warum es dennoch sinnvoll sein könnte, die Signale z.B. mit einem Hashing zu sichern, könnte darin liegen, dass wir aus rechtlicher Sicht einen Vorteil dadurch gewinnen. Durch ein Zusammenwirken von rechtlichen, regulatorischen und technischen Maßnahmen könnte sich vielleicht gerade ein Schutz ergeben, welcher für Free-to-Air Inhalte weit angemessener erscheint, als eine Verschlüsselung, welche den Konsumenten mit plötzlich nicht mehr funktionierenden ‚Legacy'-Geräten verärgern, und auch nicht mit den Auflagen des öffentlich-rechtlichen Rundfunks vereinbar wäre. Und die Alternative, gar keine Möglichkeit zum Schutz vor beliebiger Weiterverbreitung der Inhalte – auch über das Internet vorzusehen – also das andere Ende der Skala wird eventuell einer Zukunft von Free-to-Air ebenfalls nicht gerecht.

Mit einer Sicherung der Signalisierungen z.B. mittels eines Hashings würden wir dem Inhalt zunächst eine ‚Protection' gegen Manipulation der Signalisierungen hinzufügen, und es wäre zu klären, ob nicht bereits durch den bestehenden Europäischen Copyright-Act das Entfernen einer solchen ‚Protection' als illegaler Akt eingestuft würde, und damit rechtlich verfolgbar. Die Sicherung der Signalisierung würde uns damit zwar keinen technischen Schutz gegen das Entfernen der Signalisierungen geben, könnte aber in Zusammenhang mit legislativen oder auch regulativen

Maßnahmen dennoch einen besseren Schutz bewirken, als die Signalisierungen einfach völlig ungeschützt zu übertragen. Schließlich gäbe es dadurch auch eher eine Begründung dafür, dass ein Inhalt überhaupt in den geschützten CPCM-Bereich aufgenommen wird.

Dieser Sachverhalt sollte möglichst von den beteiligten Juristen und Technikern geklärt werden. Die DVB-CPT-Gruppe hat dazu extra ein Papier erstellt (CPT1307r1), welches die verschiedenen Möglichkeiten darstellt und danach fragt, was die Präferenzen der Free-to-Air Broadcaster sind. Das Papier befindet sich im Attachment. (CTA bedeutet übrigens ‘Clear to Air’. Die Unsitte, möglichst viele unerklärliche Kürzel zu verwenden ist den Menschen offenbar einfach nicht auszutreiben)

Weitere Betrachtungen in Zusammenhang mit der Frage sind:

Was soll ein CPCM-Gerät mit einem Free-to-Air-Inhalt anfangen, von dem es glaubt, dass die Nutzungs-Informations-Signale manipuliert wurden?

- Man könnte den Empfang des Inhaltes generell verweigern.
- Man könnte den restriktiveren Fall einer derartigen Signalisierung annehmen. Für ‚No Re-Distribution over the Internet’ würde dies bedeuten, dass der Inhalt nicht mehr über das Internet genutzt oder an jemand anders über das Internet weitergeschickt werden kann. Für ‚Do not CPCM Scramble’ würde es allerdings bedeuten, dass der Inhalt fortan verschlüsselt würde.
- Man könnte die Aufnahme des Inhaltes in den CPCM-Bereich verweigern. Der Inhalt würde dann einem Inhalt ohne jede CPCM-Signalisierung entsprechen.

Die Gefahren eines jeglichen Vorgehens liegen u.a. in der Möglichkeit, dass die TV-Signale auf ihrem Weg zum Sender eventuell versehentlich verändert werden könnten.

Entgegengehalten wurde uns auch, dass jeder beliebige PC dazu in der Lage sei, derartige Signalisierungen mitsamt ihrem Schutz durch ein Hashing zu entfernen, und schon allein deshalb dieser Versuch zu einer Farce entarten würde. Hier ist allerdings zu erwägen, ob sich dies in Zukunft nicht vielleicht ändern wird. Bereits jetzt haben alle namhaften Chip-Hersteller für PCs das eine oder andere Verfahren in Richtung Copy--Protection oder DRM bereits in ihre Chips bis auf Hardware-Ebene integriert. Die Chips befinden sich innerhalb von Geräten sogar bereits seit langer Zeit am Markt. Die Verfahren wurden bis jetzt nur noch nicht freigeschaltet, und sind deshalb nicht aktiv. Ob diese implementierten Verfahren jemals aktiviert werden ist unklar. Zu erkennen ist jedoch, dass die Firmen selbst daran interessiert sind, derartige Methoden aktivieren zu können. Und auch seitens der EU ist eher zu erwarten, dass die Hersteller dazu gedrängt werden, Copy-Protection Maßnahmen für PCs zukünftig vorzusehen. So ist es durchaus denkbar, dass das jetzige Universalinstrument zur Umgehung von IPR – der PC – dies in Zukunft eventuell nicht mehr sein wird. Auch PCs könnten in Zukunft CPCM-kompatibel sein, und ein entsprechendes Logo erhalten, und sie würden dann auch die Free-to-Air Signalisierungen nicht einfach entfernen. Bei der kurzen Lebenszeit von PCs könnte dies sogar weit schneller geschehen als bei CE-Geräten.

Technischer und juristischer Anhang

Verschlüsselungs-Techniken

Die moderne Verschlüsselung von Daten (Video, Audio u.a.) basiert auf einen digitalen bzw. elektronischen Schlüssel. Die Verschlüsselungsverfahren (Algorithmen) benötigen den digitalen Schlüssel als individuellen Bestandteil, der bei der Verschlüsselung und bei der Entschlüsselung vorhanden sein muss. Der digitale Schlüssel ist eine Folge von Zeichen, dessen Länge in Bit angegeben wird. Üblich sind Schlüssellängen mit der Rechen-Basis 2, also z.B. 64, 128, 256 usw. Je länger dieser Schlüssel ist, desto schwieriger ist es, eine verschlüsselte Information zu knacken. Die bekannten Verschlüsselungsverfahren teilen sich in symmetrische, asymmetrische und hybride Verschlüsselungsverfahren auf.

Symmetrische Verschlüsselungsverfahren (Secret-Key-Verfahren)

Symmetrische Verschlüsselungsverfahren arbeiten mit einem einzigen Schlüssel, der bei der Ver- und Entschlüsselung vorhanden sein muss. Die Zeichenfolge der digitalen Schlüssel ist nicht zufällig, sondern entstammt eines besonderen Zweiges der Mathematik, der Polynomdivisionen. Bekannte Verfahren sind Verschlüsselungen mit DES, Triple-DES und AES. Die Daten werden vor der Verschlüsselung in Blöcke mit der Schlüssellänge aufgeteilt. Diese Verfahren sind schnell und bei entsprechend langen Schlüsseln bieten sie auch eine hohe Sicherheit. Der Knackpunkt liegt in der Schlüsselübergabe zwischen zwei oder mehreren Stationen einer verschlüsselten Datenübertragung. Am sichersten ist die Schlüsselübergabe wenn sich zwei Personen persönlich treffen und den Schlüssel austauschen oder der Schlüssel einen anderen Weg geht, z.B. den Postweg.

Asymmetrisches Verschlüsselungsverfahren (Public-Key-Verfahen)

Asymmetrische Verschlüsselungsverfahren arbeiten mit Schlüsselpaaren. Ein Schlüssel ist der öffentliche Schlüssel (Public Key), der andere ist der private Schlüssel (Private Key). Dieses Schlüsselpaar hängt über einen mathematischen Algorithmus eng zusammen. Daten, die mit dem öffentlichen Schlüssel verschlüsselt wurden, können nur noch mit dem privaten Schlüssel entschlüsselt werden.

Der konkrete Anwendungsfall sieht so aus: Will der Sender Daten verschlüsselt an den Empfänger senden, benötigt er den öffentlichen Schlüssel des Empfängers. Mit dem öffentlichen Schlüssel können die Daten verschlüsselt, aber nicht mehr entschlüsselt werden (Einwegverschlüsselung). Nur noch der Besitzer des privaten Schlüssels, also der richtige Empfänger (!) kann die Daten entschlüsseln. Wichtig bei diesem Verfahren ist, dass der private Schlüssel vom Schlüsselbesitzer geheim gehalten wird. Kommt eine fremde Person an den privaten Schlüssel muss sich der Schlüsselbesitzer ein neues Schlüsselpaar besorgen.

Digitale Signatur

Die Digitale Signatur ist mit dem asymmetrischen Verschlüsselungsverfahren verwandt. Die Tatsache, dass der private Schlüssel nur im Besitz des Empfängers ist, erlaubt die Annahme, dass Daten, die mit dem privaten Schlüssel codiert sind, tat-

sächlich vom Schlüsselbesitzer stammen. Ganz ähnlich wie bei der Beglaubigung eines Dokumentes durch einen Notar. Mittels des öffentlichen Schlüssels können die codierten Daten auf ihre digitale Beglaubigung überprüft werden. Dieses umgekehrte Public-Key-Verfahren macht man sich für die Digitale Signatur zu nutze, um festzustellen, ob die erhaltenen Daten tatsächlich vom angegebenen Sender stammen. Vorher muss der Sender die Daten mit seinem privaten Schlüssel codiert haben. Bedeutung hat die digitale Signatur im Bankverkehr über das Internet. Dort gewährleistet sie die Autorisierung des Kunden gegenüber der Bank. Das verwendete Verschlüsselungsprotokoll heißt hier Secure Sockets Layer (SSL).

Hybride Verschlüsselungsverfahren

Hybride Verschlüsselungsverfahren arbeiten mit symmetrischen und asymmetrischen Verfahren um Daten zu verschlüsseln. Damit werden die Schwachpunkte beider Verfahren ausgeglichen. Zunächst wird ein zufällig digitaler Schlüssel generiert. Mit diesem Schlüssel werden die Daten vom Sender symmetrisch verschlüsselt. Dieser Schlüssel wird zum Empfänger zusammen mit den verschlüsselten Inhalten mitgeschickt und dieser kann mit diesem die Daten wieder entschlüsseln. Der mitgesendete Schlüssel selbst wird mit einem asymmetrischen Verschlüsselungsverfahren des Schlüsselpaares verschlüsselt. Mit Hilfe seines privaten Schlüssels kann der Empfänger den eigentlichen Schlüssel entschlüsseln. Danach ist es ihm möglich, mit dem entschlüsselten Schlüssel die eigentlichen Daten zu entschlüsseln.

Die Schlüsselübergabe erfolgt also mit der asymmetrischen Verschlüsselung, die Verschlüsselung selbst mit einer Symmetrischen. Es wird auf ein hinreichend sichere Schlüsselübergabe gebaut.

Alle digitalen Settop-Boxen, die mit der sog. „conditional access" (CA)Technik zum Empfang von verschlüsselten Sendungen ausgestattet sind, arbeiten nach diesem hybriden Verfahren (siehe folgend).

Eine weitere Variante der hybriden Verschlüsselungsverfahren stellt der Kopierschutz nach HDCP dar (siehe Kapitel 6.5 „DRM bei HDTV"). Hierbei wird nicht nur einmal ein digitaler Schlüssel vor der Aussendung generiert, sondern in zeitlich kurzen Abständen, z.B. alle 2 Sekunden. Hierdurch wird es „Hackern" besonders erschwert, sich den privaten Schlüssel anzueignen, da alle bekannten „Knack-Verfahren" rechenintensiv und damit zeitaufwendig sind.

Technische Beschreibung von Conditional Access Verfahren (CA)

CA-Systeme bilden die Schnittstelle zwischen dem verschlüsselten DVB-Datenstrom und der Smartcard des Benutzers (oder Abonnenten). Sinn und Zweck jedes dieser Systeme ist es, ein gültiges Kontrollwort (CW) zu generieren, das den Datenstrom entschlüsselt. Verschlüsselt wird immer mittels des Common Scrambling Algorithm (CSA) gemäß DVB. Übertragen werden müssen also immer zwei verschlüsselte Anteile: das Kontrollwort und das verschlüsselte Fernsehsignal selbst.

Unabhängig vom verwendeten CA-System, muss sich zur Entschlüsselung immer ein eindeutiges CW ergeben. Das ermöglicht unter anderem die Verwendung mehrerer CA-Systeme zur Entschlüsselung ein- und desselben Datenstroms (Simulcrypt). Unter Simulcrypt versteht man die parallele Verwendung zweier Verschlüsselungsnormen

für das CW innerhalb eines mit CSA verschlüsselten Fernsehsignals. Der Schlüssel wird bei Simulcrypt nach zwei verschiedenen Verfahren parallel übertragen. Da der bzw. die übertragenen CW-Schlüssel im Gegensatz zum verschlüsselten Fernsehsignal selbst nur eine geringe Datenmenge darstellt, belastet dies die Kapazität der Übertragung kaum. Mit Simulcrypt sollen Decoder mit unterschiedlichen Entschlüsselungsstandards (unterschiedlichem CAM-Bauteil) ein und dasselbe Fernsehsignal empfangen können, ohne dass eine technische Umrüstung auf das jeweils andere System erfolgen muss. Der Zuschauer erspart sich die Einrichtung von zusätzlicher Empfangselektronik (neues CAM-Bauteil) oder, wie in den meisten Fällen erforderlich, die Anschaffung eines neuen Decoders. Mit Simulcrypt lassen sich also Geräte unterschiedlichen Bautyps (unterschiedlicher technischer Spezifikation) ansprechen.

Der eigentliche Dekodierungsvorgang erfolgt dann per CSA, völlig unabhängig vom verwendeten CA-System. Dieser Aufbau ist nötig, um die Empfangsgeräte (auch Receiver) unabhängig vom eingesetzten CA-System bauen zu können. Das verwendete Verfahren wird dann mittels eines Conditional Access Modules (CAM), eines Bauteils innerhalb des Receivers, eingesetzt. Die etablierte Schnittstelle für CAMs ist das Common Interface. Die Smartcard, die der Kunde von seinem Anbieter erhält, wird dann entweder direkt in das CAM eingeschoben oder in einen Kartenleser, der mit dem CAM in direkter Verbindung steht. Das CAM hat die Form und Baugröße einer PCMCIA-Karte, findet sich aber auch als Software variante oder als fest eingebaute Hardwarelösung.

Zusätzlich zur Information, die sich schon auf der Karte des Kunden befindet, senden alle diese Verfahren noch Steuercodes über den eingehenden Datenstrom. So ist ein eigener Teilbereich (PID) reserviert, mittels dem der Anbieter neue Schlüssel an die Kundenkarten verteilen bzw. Kundenkarten aktivieren oder deaktivieren kann.

Der Common Scrambling Algorithmus (kurz: CSA) ist das Verschlüsselungsverfahren, welches beim Digitalfernsehen DVB verwendet wird um den Videodatenstrom zu verschlüsseln. CSA bedient sich weiterer Verfahren wie DES oder Triple-DES, die den symmetrischen Schlüssel der Spezifikation beschreiben.

CSA wurde über mehrere Jahre geheim gehalten. Einige Hinweise kamen über die Patentschrift ans Licht der Öffentlichkeit, wichtige Details blieben jedoch geheim, zum Beispiel der Aufbau der so genannten S-Boxen. Ohne diese Details war eine freie Implementierung des Algorithmus' nicht möglich. CSA sollte ursprünglich nur in Hardware implementiert werden, womit es unmöglich schien, die nötigen Details durch Reverse Engineering existierender Implementierungen, zum Beispiel Conditional Access Module (kurz: CAM), zu ermitteln.

Im Jahre 2002 erschien ein Programm namens FreeDec, welches den CSA in Software implementierte. Das Programm war nur als binäre Version (auch: Executable) verfügbar. Hacker disassemblierten die Software und ermittelten damit die fehlenden Details. Dadurch wurde es möglich, eine Implementierung von CSA in einer Hochsprache zu verwirklichen.

Seitdem der Algorithmus für CSA vollständig bekannt ist, suchen Kryptoanalytiker nach Schwachstellen des Verfahrens. Wie auch bei anderen Verschlüsselungsverfahren ergibt sich ein Angriffspunkt dadurch, dass Teile des Klartextes als bekannt

oder zumindest als sehr wahrscheinlich anzunehmen sind (zum Beispiel MPEG--Header). Würde man alle möglichen Schlüsselworte mit Hilfe eines Computers durchprobieren, und dieser für jeden Versuch 1 "^is benötigen, würde die Suche über 500.000 Jahre dauern. Durch Annahme bestimmter Klartextbytes lassen sich Rückschlüsse auf den verwendeten Schlüssel ziehen, um die Gesamtanzahl möglicher Schlüssel deutlich zu reduzieren.

Sollte es durch Kryptoanalyse möglich sein, den verwendeten Schlüssel durch Kenntnis der Klartextstruktur zu "erraten", wäre CSA geknackt und würde sämtliche Conditional Access Systeme unbrauchbar machen. Dies ist bis heute nicht der Fall. Man nennt diesen Hack in Hackerkreisen auch den Streamhack.

Technische User Szenarien bei OMA

Mit insgesamt 16 dieser Szenarien soll nun ein Überblick über den Umfang des Standards gegeben werden.

Szenario 1: Inhalte werden auf unterschiedlichen Geräten genutzt
Ein User lädt geschützte Inhalte auf sein z.B. Mobiltelefon. Der User kann nun diesen Inhalt per Bluetooth, Memory Card etc. auf weitere Geräte übertragen. Je nach erworbener Lizenz kann der User diesen Inhalt auf einem oder beiden Geräten (gleichezeitig) benutzen.

Szenario 2: Erwerb von Lizenzen für andere User (Geschenk)
User 1 kann für User 2 Lizenzen bzw. sog. Rechtobjekte für Inhalte erwerben. Dabei ist die Lizenz nur von User 2 benutzbar und von User 1 nicht.

Szenario 3: Wiederherstellung von Lizenzen
Für den Fall, dass Geräte oder z.B. die in Smart Card, Sim Card etc. gespeicherten Identitätscodes zerstört werden, sieht OMA die Wiederherstellung des DRM Content der bereits erworbenen Lizenzen vor. Damit ist aber auch der User als Lizenzinhaber beim Rechteinhaber oder Content Provider gespeichert.

Szenario 4: Backup von DRM Content und Rechteobjekten durch Content Provider
Erneuert ein User sein Gerät, kann er erstmal seinen gespeicherten Content auf diesem neuen Gerät nicht mehr benutzten. Da, wie in Szenario 3 bereits beschrieben, der Content Provider die Lizenzrechte der User gespeichert hat, ist eine Neuerteilung dieser bereits erworbenen Userrechte auf dem neuen Gerät problemlos möglich.

Szenario 5: Urheberschutz - Schutz vor Contentweitergabe
Content kann vor dem Weiterversenden auf andere Geräte geschützt werden (sog. Forward Lock) bzw. die Anzahl wie oft, definiert werden. So kann z.B. ein Photo aus einem Photohandy an einen weiteren User versendet werden, der es aber nur ansehen und nicht mehr weiterleiten oder speichern kann.

Szenario 6: Export von OMA DRM auf andere DRM Systeme
Ist auf einem Gerät ein anderes als ein OMA DRM System installiert, lässt sich der Content mit den Rechten auf dem nicht OMA DRM System wiedergeben bzw. adaptieren. Der Content Provider bestimmt allerdings, ob die Adaption auf dem alternativen DRM System möglich sein soll.

Szenario 7: Content-Pakete
Ein Content kann z.B. aus einem Paket von Musik, Songtext, Bildern, Links, Filmen etc. bestehen. Ein Rechteobjekt kann nun für jeden dieser Paketinhalte verschiedene Rechte bzw. Verwendungszwecke definieren. So kann es beispielsweise sein, dass der Songtext ungeschützt von weiteren Usern kopiert werden darf, der Musiktitel aber nicht. Der Vielfalt und Kombination von Rechtezuweisungen ist damit keine Grenze gesetzt.

Szenario 8: Dauer einer Lizenz
Ein Rechteobjekt kann die Benutzung von Inhalten hinsichtlich ihrer Dauer einschränken. So ist es möglich ein Recht mit Ablaufdatum bis zu einem bestimmten Zeitpunkt zu erteilen und anschließend erlöschen zu lassen, die Benutzung des Contents x-mal gestattet und anschl. verfällt

Szenario 9: Content Zugriff / Abonnement
Anbieter von Content können den Zugriff als Stream oder Downlaod anbieten.
Streaming: Funktionen wie Pause, Neustart etc. werden unterstützt (On Demand Funktionen)
Download: Contents werden von Service Providern heruntergeladen; das Rechteobjekt bestimmt das Rechtehandling

Szenario 10: Multicast Streaming
Verschiedene Multicast Kanäle (z.B. Internet Radio) können selektiert werden, bei denen wiederum die Rechte mittels Rechteobjekte verwaltet wird.

Szenario 11: Rechteobjekt mit „Vorschaufunktion"
Da OMA Inhalt und Zugriffsrecht voneinander trennt, können Inhalte, obwohl noch keine Lizenz erworben, mittels Rechtobjekt zur „Probe" benutzt werden. Dies ermöglicht für die Contenteanbieter ein riesiges Potential an kostengünstiger Werbung.
Folgende Rechtevergaben sind vorstellbar:
Einmaliges benutzen des Inhalts
Inhalt ausschnittsweise (Start-Stopzeit) benutzbar

Szenario 12: Superdistribution
User 2 kann einen Inhalt mittels „local link" von einem User 2 beziehen. Das Rechteobjekt muss beim Rechteinhaber erworben werden. Vor dem Erwerb der Lizenz wird nun im Sinne von User 2 geprüft, ob sein Gerät in der Lage ist, den Inhalt zu verarbeiten bzw. abzuspielen dass sich der Lizenzverleger authentifiziert hat

Szenario 13: Sperren von Kunden (Device Revocation)
Verstößt ein User gegen Lizenvereinbarungen oder tauscht/verbreitet illegal geschützte Inhalte, kann dieser User vom weiteren Bezug von Lizenzen durch den Content Provider ausgeschlossen werden.

Szenario 14: Zuweisung der Useridentität zum Rechteobjekt
Hat ein User zwei Geräte, die er für OMA Inhalte nutzen möchte, so können die Lizenzen so gestaltet werden, dass die Inhalte in beiden Geräten benutzbar werden (im Gerät A oder Gerät B, also nicht gleichzeitig).

Szenario 15: Hackerangriffe
Da OMA DRM möglicherweise ein weit verbreiteter Standart werden könnte, dürfte auch das Interesse von Hackern, diesen Standart zu „knacken", steigen. Der Rechteinhaber kann dann, im Falle, dass Gerät/User als „unsicher" erkannt wurden, diese auf Geräte auf eine „schwarze Liste" setzen und einen weiteren Bezug von Inhalten verhindern.

Szenario 16: Abfrage von Codearten („Cryptografic Strength")
Ein Content Provider hat die Möglichkeit, die Codearten, die ein Gerät des Users unterstützt, abzufragen und danach über die Zuweisung von Rechteobjekten entscheiden.

Im weiteren soll noch auf einen wichtigen Aspekt der Architektur von OMA, nämlich den sog. „Broadcast Domains", die den „authorisized Domains" von DVB entsprechen, eingegangen werden. Die Broadcast Domains lassen sich in zwei Typen einteilen: einer Service Domain und einer Device Domain.
In einer Service Domain kann zwischen den Domain „Mitgliedern" Service und Content ausgetauscht werden - von Terminal X auf Terminal Y. Ein sog. „common group key" ermöglicht den Zugriff auf die Service Schlüssel bzw. die Programm Schlüssel, die zum entschlüsseln des Contents benötigt werden.

Device Domain: der zweite Typ der Broadcast Domain ist die von einer „Authorität", also einem Rechteinhaber, limitierte und beherrschte Ansammlung von Terminals. Diese Terminals in einer Device Domain teilen sich einen gemeinsamen Domänen Schlüssel, der zur Verschlüsselung des SEK („service encrytion key") und PEK („programm encyription key") verwendet wird. Services und Content können unter den Device Domänen Mitgliedern ausgetauscht werden. In dieser Domäne gibt es drei Fälle:

- Gesendeter Content wird in einem Terminal Y gespeichert. Wenn ein Terminal dieser Device Domäne „beitritt", die zu Y gehört, übermittelt Terminal Y den gespeicherten Content. Y benutzt den Domänen Key um die Schlüssel mit dem verschlüsselten Content zu übertragen.
- Ein mit einem Content Provider nicht verbundenes Gerät tritt einer Domäne bei, in der ein verbundenes Gerät vorhanden ist. Das nicht verbundene Gerät benutzt dann das verbundene Gerät über Broadcast Service Funktionen um sich zu registrieren.
- Alle Geräte verfügen über den Domain Key und haben damit Zugriff auf SEK bzw. PEK

Kopierschutz auf Video-DVD

Video-DVDs sind häufig durch mehrere Systeme geschützt, die das illegale Kopieren verhindern sollen: Das analoge Macrovision System erzeugt beim Überspielen der DVD auf VHS ein störendes Flimmern, dunkle Bilder, fehlende Farben etc. Dadurch kann das Programm nicht mehr auf Video-Cassetten überspielt werden. Das

Schutzsignal wird von einem Fernseher nicht erkannt, daher kann das Programm mit klarem Bild betrachtet werden.

Darüber hinaus verwenden viele DVD-Player das Serial Copy Generation Management System (CGMS), das das Kopieren durch eine Veränderung des Videosignals unterbindet.

Zusätzlich sind die meisten DVDs mit dem Content Scrambling System (CSS) verschlüsselt. Die Wiedergabe ist dadurch nur mit einem Dekoder möglich. Dieser Decoder ist in allen DVD-Playern enthalten. Das digitale Kopieren bzw. "Rippen" soll dadurch verhindert werden.

In der Praxis gibt es aber zahlreiche Kopiergeräte, die sowohl CSS als auch CGMS umgehen können.

Ein anderes Verfahren, das die Abspielung auf bestimmte Regionen einschränken sollte, war der „Länder-Code". Dieser, auf der Platte „eingebrannt", war der Vorläufer von den heutigen „modernen" DRM-Verfahren (siehe Abschnitt 4, Klassifizierung der DRM Metadaten). In der Praxis werden die Ländercodes von vielen DVD-Playern heutzutage ignoriert.

Technische Details zu dem DRM von DVB-CPCM

CPCM definiert ein DRM Verfahren, das auf den sog. „Usage Stage Information" (USI) beruht. Dieses definiert vier Fälle:

Content ohne Rechteattribute
- Content mit einmaliger Kopieerlaubnis
- Content ohne Kopiererlaubnis, aber mit Weiterleitung-Erlaubnis Content ohne das Recht zur Kopie

Diese USI kann man als Rechteattribut zur Verwaltung von Kopien betrachten. Der Content kann mit einem Zeitstempel versehen werden, der eine absolute oder relative Zeitangabe enthält, in der der Konsum möglich ist. Damit wird es beispielsweise möglich, einen Film für eine Woche beliebig oft anzusehen. Danach ist eine Betrachtung nicht mehr möglich. Bei der Erstellung von Kopien wird eine CPCM Domäne definiert, die eine lokale und eine geographische Komponente enthält. Die Einschränkungen sind vorwiegend zeitlicher Art, d.h. nur in einem gewissen Zeitraum ist die Bewegung (das „movement") innerhalb der Domäne möglich.

Im Gegensatz zu allen Anderen bisher dem IRT bekannten Verfahren handelt es sich bei diesem um ein relativ kompaktes, welches sich auf die wesentlichen Essenzen eines DRM-Systems beschränkt. Als DVB Verfahren dürfte es Lizenfrei sein oder zumindest für Gerätehersteller zu moderaten Kosten implementierbar.

Auszüge aus den Richtlinien des Europäischen Parlamentes „Zum Schutz des geistigen Eigentums" (2004/48/EG) [9]

(7)Aus den Sondierungen der Kommission zu dieser Frage hat sich ergeben, dass.. weiterhin
zwischen den Mitgliedstaaten große Unterschiede bei den Instrumenten zur Durchsetzung der Rechte des geistigen Eigentums bestehen. So gibt es z. B. beträchtliche Diskrepanzen bei den Durchführungsbestimmungen für einstweilige Maßnahmen, die insbesondere zur Sicherung von Beweismitteln verhängt werden, bei der Berechnung von Schadensersatz oder bei den Durchführungsbestimmungen für Verfahren zur Beendigung von Verstößen gegen Rechte des geistigen Eigentums. In einigen Mitgliedstaaten stehen Maßnahmen, Verfahren und Rechtsbehelfe wie das Auskunftsrecht und der Rückruf rechtsverletzender Ware vom Markt auf Kosten des Verletzers nicht zur Verfügung.

(8)Die Unterschiede zwischen den Regelungen der Mitgliedstaaten hinsichtlich der Instrumente zur Durchsetzung der Rechte des geistigen Eigentums beeinträchtigen das reibungslose Funktionieren des Binnenmarktes und verhindern, dass die bestehenden Rechte des geistigen Eigentums überall in der Gemeinschaft in demselben Grad geschützt sind. Diese Situation wirkt sich nachteilig auf die Freizügigkeit im Binnenmarkt aus und behindert die Entstehung eines Umfelds, das einen gesunden Wettbewerb begünstigt.
(9) Die derzeitigen Unterschiede schwächen außerdem das materielle Recht auf dem Gebiet des geistigen Eigentums und führen zu einer Fragmentierung des Binnenmarktes in diesem Bereich. Dies untergräbt das Vertrauen der Wirtschaft in den Binnenmarkt und bremst somit Investitionen in Innovation und geistige Schöpfungen. Verletzungen von Rechten des geistigen Eigentums stehen immer häufiger in Verbindung mit dem organisierten Verbrechen. Die verstärkte Nutzung des Internet ermöglicht einen sofortigen globalen Vertrieb von Raubkopien. Die wirksame Durchsetzung des materiellen Rechts auf dem Gebiet des geistigen Eigentums bedarf eines gezielten Vorgehens auf Gemeinschaftsebene. Die Angleichung der diesbezüglichen Rechtsvorschriften der Mitgliedstaaten ist somit eine notwendige Voraussetzung für das reibungslose Funktionieren des Binnenmarktes.

(29) Die Industrie sollte sich aktiv am Kampf gegen Produktpiraterie und Nachahmung beteiligen. Die Entwicklung von Verhaltenskodizes in den direkt betroffenen Kreisen ist ein weiteres Mittel zur Ergänzung des Rechtsrahmens. Die Mitgliedstaaten sollten in Zusammenarbeit mit der Kommission die Ausarbeitung von Verhaltenskodizes im Allgemeinen fördern. Die Kontrolle der Herstellung optischer Speicherplatten, vornehmlich mittels eines Identifikationscodes auf Platten, die in der Gemeinschaft gefertigt werden, trägt zur Eindämmung der Verletzung der Rechte geistigen Eigentums in diesem Wirtschaftszweig bei, der in hohem Maß von Produktpiraterie betroffen ist. Diese technischen Schutzmaßnahmen dürfen jedoch nicht zu dem Zweck missbraucht werden, die Märkte gegeneinander abzuschotten und Parallelimporte zu kontrollieren.

Technische Beschreibung von HDCP

Jedes einzelne HDCP-Gerät, egal ob Display oder Fernsehempfangsbox, bekommt über seinen Hersteller ab Werk von einer zentralen Vergabestelle, der Firma Digital Content Protection LLC, einen individuellen Satz von 40 Stück 56 Bit langen Binärzahlen zugeteilt, der nach einer nur ihr bekannten Formel errechnet wird. Diese werden als geheime Schlüssel bezeichnet, und sie müssen vom G e räte h erste ller so

im Gerät platziert werden, dass diese unter keinen Umständen jemals aus dem HDCP Gerät ausgelesen werden können. Wegen Exportbeschränkungen der USA, dürfen von dort nur kryptografische Verfahren exportiert werden, die höchstens 56 Bit lange Schlüssel verwenden. Das DTCP arbeitet im Vergleich dazu mit 160 Bit langen Schlüsseln. Jedes Bit mehr bedeutet eine Verdoppelung der benötigten Zeit beim erraten von Schlüsseln und verringert damit die Unsicherheit. Bei HDCP wird versucht, die Unsicherheit der relativ kurzen Schlüssel durch viele geheime Schlüssel zu verringern.

Jedes HDCP-Gerät bekommt zu den 40 Schlüsseln eine passende - und somit ebenfalls individuelle -nicht geheime Binärzahl mit einer Länge von 40 Bit erteilt, wovon exakt 20 bit den Wert Null und 20 bit den Wert Eins enthalten. Diese Binärzahl wird von der „Digital Content Protection LLC" Key Selection Vektor (KSV) genannt. Die von ihr errechneten Schlüssel haben zusammen mit den KSV numerische Eigenschaften die einen Menschen, der sich nicht ausgiebig mit der Zahlentheorie befasst hat, an Zauberei glauben lassen. Denn die Fernsehempfangsbox kann mit Hilfe des Diplay-KSV und seinen 40 geheimen Schlüsseln einen so genannten Cipherwert errechnen, den nur das Display mit seinen 40 geheimen Schlüsseln und dem Fernsehemfangsbox-KSV rekonstruieren kann. Das HDCP-Verfahren im Display addiert einfach den ersten bis vierzigsten geheimen Schlüssel in Abhängigkeit davon auf, ob das erste bis vierzigste Fernsehemfangsbox-KSV-bit den Wert Eins enthält. Insgesamt werden also 20 Additionen durchgeführt, da ein KSV binär zwanzig Einsen enthält. Der sich für jede Gerätepaarung unterschiedlich ergebene Cipherwert wird sowohl von der Fernsehempfangsbox als auch vom Display für die Ver- bzw. Entschlüsselung der zu schützenden Bild- und Tondaten verwendet. Genau genommen werden nur die ersten 56 bit aus dem Additionsergebnis als Cipherwert verwendet.
Ein Lauscher, der den Datenaustausch zwischen Fernsehempfangsbox und dem Display mithören würde, sollte anhand der KSVs nicht den notwendigen Cipherwert ermitteln können - nicht einmal dann, wenn er selber über einen eigenen Satz von 40 geheimen Schlüsseln verfügen würde, da dieser nicht zum KSV des Displays oder der Fernsehempfangsbox identisch ist. Ob dies wirklich so gut funktioniert, ist schwer zu sagen.

Es gibt ein ähnliches Verfahren zum Schlüsselaustausch, das Kryptografen seit dem Jahr 1976 unter der Bezeichnung Diffie-Hellman-Schlüsselaustausch kennen. HDCP wurde im April 2001 in der Version 1.0 von Firma Intel der Öffentlichkeit vorgestellt. Bereits im Mai 2001 trugen Scott Crosby und vier weitere auf Kryptografie spezialisierte Wissenschaftler im ACM-CCS8 DRM Workshop vor, dass sie eine Kryptoanalyse durchgeführt haben, und zu dem Ergebnissen gekommen waren, dass das HDCP-Verfahren unsicher ist.

Diese Ergebnisse und der Weg dorthin wurden so detailliert präsentiert, dass Scott Crosby im November 2001 wegen der rechtlichen Konsequenzen die sich aus dem Digital Millennium Copyright Act (DMCA siehe 2) ergeben, in einer Selbsterklärung verneinte, jemals wieder eine solche Analyse durchzuführen. Auch hätte er nie eine Analyse durchgeführt, wenn er die rechtlichen Folgen hätte absehen können. Gerade wegen dieser öffentlich gewordenen Analyse besserte Intel mit der Version 1.1 nach, noch bevor Geräte mit HDCP in den Markt gekommen waren. Ob damit alle kritisierten

Schwächen ausgebessert sind, bleibt ungewiss, denn bislang hat noch niemand eine Analyse zu Version 1.1 veröffentlicht.

Der jedem Gerät individuell zugewiesene KSV kann zusätzlich dazu benutzt werden, dass eine Fernsehempfangsbox einigen ausgesuchten Displays keine Bild- und Tondaten über HDCP sendet und diese dunkel bleiben. Damit das auch nach Ausschalten der Geräte einwandfrei funktioniert, werden die betreffenden KSVs in der Fernsehempfangbox in einem nicht flüchtigen Speicher aufbewahrt. Diese so genannte Revoke Liste soll laufend durch Fernsehprogramm begleitende Daten aktualisiert werden. Auf die Revoke Liste sollen laut Spezifikation 1.2 vom Juni 2006 nur KSVs kommen, deren dazugehörige geheime Schlüssel in falsche Hände gelangt sind und missbraucht werden. Ob wirklich nur solche KSVs auf die Revoke Liste kommen, deren Schlüsselsätze missbraucht werden, oder ob nicht in Zukunft durch diesen Mechanismus gezielt die Informationsfreiheit behindert wird, ist eine Gefahr, die nach heutigem Stand unserer Untersuchungen nicht ausgeschlossen werden kann.

Analoge Verschlüsselungsverfahren

Bis zur Einführung des digitalen Fernsehens Mitte der neunziger Jahre beschränkten sich die technischen Möglichkeiten für die Pay-TV Anbieter auf die analoge Verwürfelung von Fernsehzeilen und dem zufälligen zeitlichen Versatz der horizontalen Synchronisation, z.B. mit Verfahren wie „Nagravision". Dieses Verfahren wurde nicht nur bei Fernsehübertragungen, sondern auch auf Videokassetten eingesetzt. Durch dieses Verfahren wurde manch Einer, der eine legal erworbene VHS Kassette mit einem zweiten Videorekorder kopieren wollte, herb enttäuscht. Die Kopie war nicht herstellbar bzw. abspielbar. Natürlich wurden im „Schwarzmarkt" schnell „Gegenmittel" angeboten, meist als Hardware in Form eines Zwischensteckers (auch „Dongle" genannt), den man auf den SCART Eingang steckte. Bereits zu diesem Zeitpunkt ergab sich der bis heute nicht gelöste Konflikt: Recht auf private Kopie versus Verbot illegaler Weitergabe.

Die Haltung von ARD und ZDF zur Grundverschlüsselung

Die deutschen öffentlich rechtlichen Rundfunkanstalten haben sich stets gegen eine Verschlüsselung ausgesprochen. So gaben die ARD und das ZDF gemeinsam am 5.4.2006 eine Pressemeldung heraus, in der eine Verschlüsselung ihres Contents auf den SES ASTRA Satelliten abgelehnt wurde. Eine Woche später gab es eine ähnlich lautende Pressemeldung, was den Inhalt vom kommenden sog. „Handy-TV" angeht. Die Mobilfunkanbieter könnten das Signal von ARD und ZDF ohne zusätzlichen Aufwand einfach weiterleiten. Deshalb sei für die Verbreitung öffentlich-rechtlicher Angebote auch keine "technische Gebühr" zu rechtfertigen. Das Vorgehen würde ja auf eine doppelte Rundfunkgebühr für die Zuschauer hinauslaufen, hieß es.

Anders sieht es beim Österreichischen ORF und der Schweizer SRG/SSR aus, die schon seit geraumer Zeit über Satellit digital verschlüsseln (ORF 1. Programm bzw. SRG/SSR digital). Hier bekommt der Zuschauer zugleich mit der Anmeldung eine Decoderkarte ausgehändigt, die den Empfang ihrer Programme mit speziell dafür ausgerüsteten Settop Boxen erlaubt, eine sog. „Smartcart".

Abkürzungen

BEUC: Bureau Européen des Unions de Consommateurs (Europäische Konsumenten-Organisation)

EBU: European Broadcast Union (Der Europäischen Rundfunkunion gehören 74 zumeist öffentlichrechtliche Rundfunkstationen an, in und außerhalb Europas, darunter die BBC, France Televisions, RAI, sowie ARD und ZDF)

ETSI: European Telecommunications Standards Institute

ICT: information and communication technology

MMG: Melodies & Memories Global, Ltd., Multimedia Firma im asiatischen Markt

NTT: Nippon Telefon & Telegraf, japanisches Gegenstück zur Deutschen Telekom

SMPTE: Society of Motion Picture Television Engineers