



## **White Paper**

# **Untersuchung der Sicherheitsrisiken bei der Verwaltung und Distribution von digitalen Rechten im Online-Handel**

Autor: Alexandra Prilop

Der Inhalt dieses Dokumentes wurde gleichlautend im Tagungsband des 8. Deutschen IT-Sicherheitskongresses des BSI (Bonn, 10. Bis 12. Mai 2005) veröffentlicht.

# Untersuchung der Sicherheitsrisiken bei der Verwaltung und Distribution von digitalen Rechten im Online-Handel

Alexandra Prilop<sup>1</sup>

## Kurzfassung

Mit Hilfe eines allgemeinen Modells für die Verwaltung und Distribution von digitalen Rechten im Online-Handel sollen verschiedene DRM-Systeme erfasst und ihre funktionalen Komponenten beschrieben werden. Die DRM-Verfahren werden in einen allgemeinen Rahmen gestellt und so vergleichbar gemacht. Schwerpunkt der Betrachtung sind die Sicherheitsrisiken solcher Systeme. Es wird sodann diskutiert, wie diese Betrachtung die Grundlage für ein Schutzprofil (nach den „Common Criteria“) für DRM-Systeme bildet und welche Vorteile eine Erstellung und Zertifizierung eines solchen Profils hat. Die Gültigkeit des Modells wird anhand einer Referenzimplementierung veranschaulicht.

## Stichwörter

DRM, Online-Verkaufsplattform, Online-Handel, OMA, MMP, Microsoft WMS, CC - Common Criteria, Schutzprofil.

## 1 Zielsetzung und Einleitung

Bei der Vermarktung von digitalen Inhalten sind die Beteiligten:

- Inhaltseigentümer und Urheber,
- Betreiber von Online-Verkaufsplattformen,
- und Käufer (Endanwender)

an der Wahrung ihrer jeweiligen Anliegen interessiert, die jedoch sehr unterschiedlich sind. Der Endanwender möchte Inhalte möglichst billig, ohne lästige Einschränkungen erwerben und möglichst komfortabel nutzen (z.B. auf vielen Endgeräten). Der Inhaltseigentümer will seine Inhalte vor Missbrauch schützen und seine wirtschaftlichen Interessen wahren. Hier ist die Diskrepanz zwischen der vom Endanwender gewünschten größtmöglichen Freiheit („weak DRM“) und vom Inhaltsanbieter präferierten starker Kontrolle („strong DRM“) offensichtlich (siehe [DRM]). Der Plattformbetreiber hingegen steht zwischen diesen Extremen und ist von der Akzeptanz seiner Plattform bei beiden Seiten abhängig. Gerade der Endanwender wird zur Zeit durch Pressemeldungen über Abmahnungen, neue Gesetze und Schließungen von Tauschbörsen verunsichert. Die angebotenen „legalen“ Verkaufsplattformen und ihre Vorgehensweisen, mit denen die Rechte der Urheber und Inhaltsanbieter geschützt werden sollen, sind sehr unterschiedlich in ihren Ausprägungen, manchmal undurchsichtig und oft sehr restriktiv. Diese Untersuchung erstellt ein Modell für die Verwaltung und Verteilung digitaler Rechte, um so DRM-Verfahren in einen allgemeinen technischen Rahmen zu stellen und vergleichbar zu machen. Schwerpunkt der Betrachtung sind die Sicherheitsrisiken im Online-Handel mit digitalen Rechten und Werten. Risiken betreffen die Integrität (Schutz vor Verfälschung), die Vertraulichkeit (Schutz vor nicht-autorisierter Kenntnisnahme, also dem unberechtigten Zugriff auf die Daten), die Verfügbarkeit (Schutz vor Beeinträchtigung der Funktionalität) und die Unwiderrufbarkeit (Eindeutigkeit des Ursprungs) der sicherheitsrelevanten Daten, die oft auch Werte genannt werden. Weiterhin sind auch Fragen des Datenschutzes bei einer Untersuchung der Sicherheit relevant. Im Folgenden wird zuerst eine Begriffsbestimmung für DRM gegeben, sodann wird ein allgemeines Modell für die DRM-Verfahren definiert und es werden die einzelnen Aspekte erläutert. Daraufhin werden für jeden Aspekt die

---

<sup>1</sup> Alexandra Prilop, media transfer AG, Darmstadt

Sicherheitsrisiken diskutiert. Danach werden diese Arbeiten in den Kontext von „Common Criteria (CC)“ und Schutzprofilen gestellt und erklärt und es wird ein Referenzsystem vorgestellt.

## 2 Was ist DRM? Eine Begriffsbestimmung

Digital Rights Management (DRM) ist ein Sammelbegriff für Technologien, die den Schutz digitaler Daten ermöglichen sollen. Autorisierte Nutzer müssen eine Lizenz erwerben, um geschütztes Material - Dokumente, Musik, Filme - unter Anerkennung der vom urheberrechtlichen Eigentümer festgelegten Nutzungsrechte und -regeln konsumieren zu können.

Aufgabe eines DRM-Systems ist es, die vom Inhaltseigentümer festgelegten Rechte in elektronische Formate abzubilden, einem Inhalt zuzuordnen, zu administrieren (definieren, ändern, löschen) und auf Seiten des Konsumenten durchzusetzen.

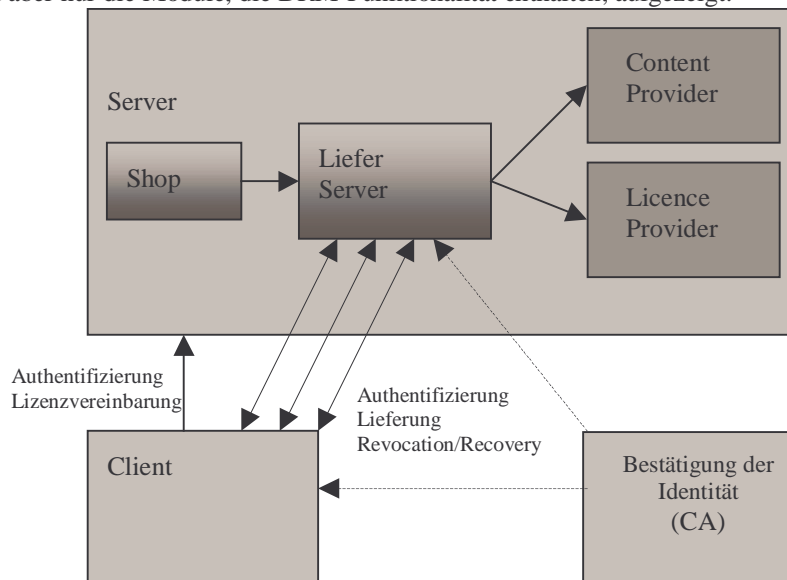
Wichtige Teilaspekte im Online-Handel sind also:

- die Lizenzvereinbarung,
- die Lizenzerstellung,
- die Lieferung von Inhalt und Lizenz,
- die Durchsetzung der Lizenz beim Kunden,
- Wiederherstellung und Widerruf der Lizenz (Recovery und Revocation),
- Authentifizierungsmechanismen für Verkaufsplattform und Käufer.

## 3 DRM im Online-Handel

### 3.1 Überblick

DRM ist eingebunden in eine Infrastruktur zur Vermarktung digitaler Inhalte. Es ist ein Bestandteil einer sogenannten „Online-Verkaufsplattform“. Neben DRM bilden der für den Endanwender sichtbare Shop, Systeme für Benutzerverwaltung, Abrechnung, Inhaltsverwaltung u.ä. die Verkaufsplattform (Server). In der folgenden Abbildung 1 wird ein allgemeines Schema für die Anwendung von DRM-Verfahren im Online-Handel aufgestellt. Bei dem Schema sind aber nur die Module, die DRM-Funktionalität enthalten, aufgezeigt.



**Abbildung 1: Allgemeines Modell von DRM im Online-Handel**

Nach einer gegenseitigen Authentifikation beginnt der Kunde (zumeist über eine Anwendung, dem Client) eine Kommunikation mit dem Server. Dann werden zwischen dem Shop (dem Web-Frontend der Plattform, das der Kunde sieht) und der zugeordneten Anwendung auf Kundenseite (z.B. Browser oder spezifische Clientanwendung) die Lizenzvereinbarungen ausgehandelt. Danach erfolgt die Kommunikation des Clients (bzw. des Endanwenders) direkt oder indirekt mit dem Lieferserver. Der Client kann dabei auf einem mobilen Endgerät, einem PC oder einem anderen von einem Endanwender bedienten Gerät installiert sein. Es folgt eine weitere gegenseitige

Authentifizierung von Client und Lieferserver, z.B. durch Zertifikate einer unabhängigen Instanz (CA<sup>2</sup>). Der Lieferserver wird nun die Daten für die Lieferung aus Inhalt und Lizenz zusammenstellen und dann an den Client liefern. Eine Neulieferung (Recovery) erfolgt im gleichen Schema wie eine Lieferung, wobei eventuell nur die Lizenz geliefert werden muss. Bei der Sperrung einer Lizenz wird der Client identifiziert und sodann die Sperrinformation gesendet (Revocation). Auf Seiten des Clients ist es erforderlich, die erworbenen Rechte (und nur diese) durchzusetzen, sowie erworbene Inhalte und Rechte zu verwalten.

Einige Teilaspekte, z.B. die Bestätigung der Identitäten durch eine dritte unabhängige Instanz (CA) oder die Möglichkeit des Widerrufs einer Lizenz, sind nicht in jedem DRM-System vorhanden. Weiterhin sind die einzelnen Komponenten in unterschiedlichen DRM-Verfahren unterschiedlich ausgeprägt, z.B. kann der Liefervorgang stark variieren. Online-Verkaufsplattformen, die eine hohe Akzeptanz erreichen wollen, werden verschiedene DRM-Verfahren implementieren und den Endanwendern anbieten, damit sie verschiedenen Anforderungen gerecht werden können (Multi-DRM). Eine analoge Vorgehensweise ist auf Client-Seite sinnvoll, um mit möglichst vielen Plattformen interoperabel zu sein.

Die oben beschriebenen Teilschritte werden nun genauer betrachtet.

### 3.2 Lizenzvereinbarungen

Der Bestellvorgang für geschützte Inhalte (Füllen des Warenkorb und Kaufvorgang, sowie der Bezahlvorgang) ist nicht relevant für das DRM-Verfahren. Wichtiger Bestandteil der DRM-Verfahren ist aber die Aushandlung des Lizenzvertrages. In diesem wird festgehalten, welche Rechte nun erworben werden und wie die Inhalte genutzt werden. Sowohl der Client als auch die Verkaufsplattform müssen diese Vereinbarung auswerten können. Hierfür stehen so genannte RELs (Rights Expression Languages) zur Verfügung. Als Beispiel seien hier die beiden XML-basierten Sprachen ODRL (Open Digital Rights Language) und XrML (eXtensible rights Markup Language) erwähnt. ODRL ist ein freier Standard und wird in den Standards für die DRM-Verfahren der OMA (Open Mobile Alliance) verwendet (siehe [OMA]). Die MPEG (Moving Picture Experts Group) verwendet XrML als Beschreibungssprache der digitalen Rechte. Diese REL ist nicht frei, sondern wurde von der Firma ContentGuard lizenziert (siehe [XRML]).

Vorteil einer Lizenzbeschreibung, die mit Hilfe einer dieser standardisierten Beschreibungssprachen gebildet wird, ist, dass sie von vielen Clients oder Plattformen verstanden werden kann und so eine Interoperabilität gewährleistet wird, die eine proprietär formulierte Lizenzvereinbarung nicht bieten kann.

### 3.3 Lizenzerstellung und Lieferung

Unterschiedlichen DRM-Verfahren ist zumeist die folgende Vorgehensweise gemeinsam: die Multi-Media-Daten, die in einem Ursprungsformat vorliegen, werden zusammen mit Metainformationen und Rechten in spezifische DRM-Datenformate „gepackt“.

Weiterhin können den Daten zur Verfolgbarkeit von Urheberrechtsverletzungen sogenannte „Wasserzeichen“ hinzugefügt werden. Es sind Markierungen innerhalb der gelieferten Datei, die nicht entfernt werden können und es ermöglichen, eine Datei genau zu identifizieren. Dieses Verfahren kann genutzt werden, um bei Raubkopien die Besitzer der Originaldateien zu ermitteln (sog. „Ownership Tracking“, siehe hierzu [CHENG]).

In der Regel werden die Multi-Media-Daten ganz oder teilweise verschlüsselt, um unberechtigten Zugriff darauf zu verhindern. Diese Verpackung wird auch häufig als „secure container“ bezeichnet (siehe [GUTH]). An den Kunden werden die „gepackten“ Daten sowie eine „Lizenz“ geliefert. Mit dem Begriff Lizenz umschreibt man eine Kombination aus einem kryptographischen Schlüssel und den dem Kunden zugeordneten Nutzungsrechten, der oben beschriebenen Lizenzvereinbarung. Liegt die Lizenz beim Kunden vor, können die Daten entschlüsselt und gemäß den definierten Rechten genutzt werden.

Grundsätzlich lassen sich zwei Konzepte bei der Auslieferung der Daten und Lizenzinformationen unterscheiden:

- „combined delivery“: Daten und Lizenz sind eine Einheit, die nur zusammen geliefert werden. Das Fraunhofer MMP-Verfahren beispielsweise beruht auf diesem Prinzip.
- „separate delivery“: Daten und Lizenz werden physikalisch getrennt geliefert, gegebenenfalls kann die Lieferung auch zu verschiedenen Zeitpunkten erfolgen. Dieses Vorgehen findet in dem OMA-Protokoll und bei den Verfahren der Microsoft® Windows Media Series® seine Verwendung.

---

<sup>2</sup> CA – Certification Authority

### 3.3.1 Combined Delivery am Beispiel Fraunhofer MMP

Im sog. Multimedia Protection Protocol (MMP) der Fraunhofer Gesellschaft werden aus Contentdaten, Metainformationen und Rechten sogenannte MMP-Dateien erzeugt.

Jede MMP-Datei besteht aus dem Nutzdatenblock und einem MMP-Header. Der Nutzdatenblock enthält die eigentlichen Multimediadaten (Audio / Video) und wird partiell verschlüsselt, um durch die dadurch entstandene deutliche Qualitätseinbuße unberechtigte Nutzung zu verhindern. Die folgende Abbildung 2 illustriert die Struktur einer MMP-Datei.

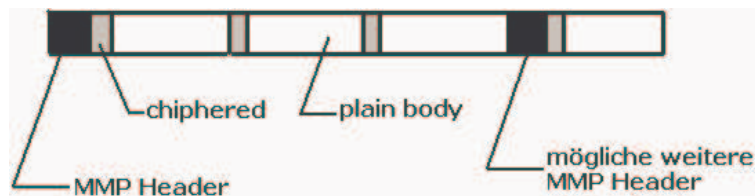


Abbildung 2: Aufbau einer MMP-Datei

Der MMP-Header kann Metadaten und Rechte aufnehmen. Der Nutzdatenblock kann bereits beim Import der Daten in die Verkaufsplattform vorverschlüsselt werden, diese Verschlüsselung ist nicht benutzerspezifisch.

Für jeden Kunden gibt es einen individuellen kryptographischen Schlüssel, der bereits bei der Registrierung des Kunden in einem Shop erzeugt werden kann, und der grob gesprochen als Lizenz fungiert (tatsächlich ist er nur eine von mehreren Komponenten bei der Entschlüsselung der Daten auf Kundenseite).

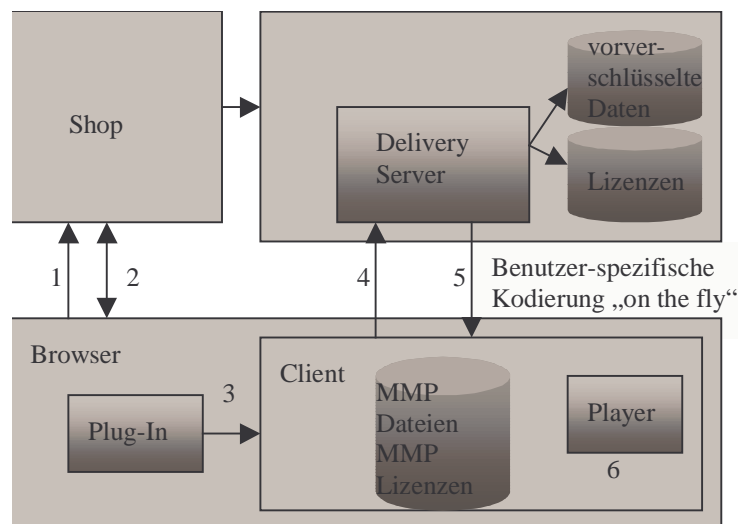


Abbildung 3: Combined Delivery mit MMP

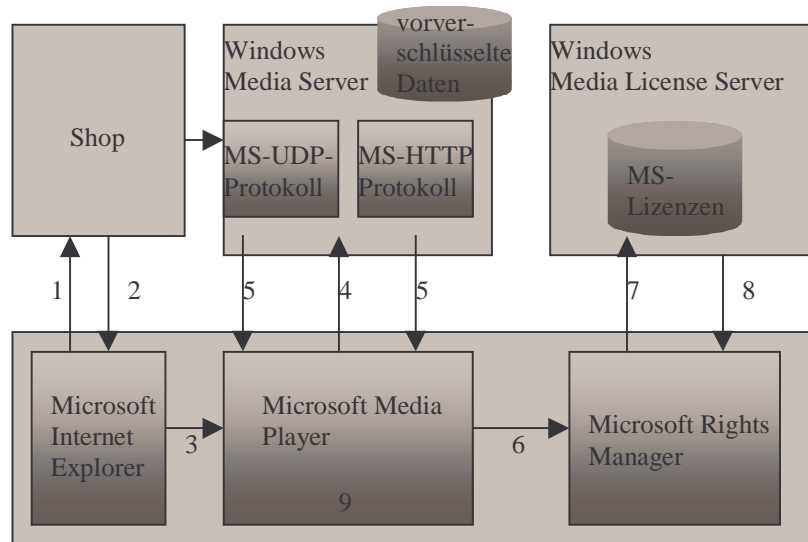
Der Ablauf der Lieferung vollzieht sich bei Combined Delivery in diesen Schritten:

- (1) Kunde wählt Inhalt aus,
- (2) Webserver sendet URL des Delivery Servers zum Browser,
- (3) Browser ruft Client mit dieser URL auf,
- (4) Client ruft Delivery Server mit Content URL,
- (5) Delivery Server verschlüsselt Content „on the fly“ benutzer-spezifisch, liefert Content und Lizenz; Lizenz ist nicht hardware-gebunden,
- (6) Content kann durch einen geeigneten Player abgespielt werden.

### 3.3.2 Separate Delivery am Beispiel der Microsoft® Windows Media Series®

Mit Hilfe des Microsoft® Windows Media® DRM können Dateien für die Microsoft® Windows Media Series® geschützt, geliefert und verwaltet werden. Die Dateien werden zuerst gepackt und verschlüsselt. Ein Link zu dem Lizenzserver wird angefügt. Die Dateien werden im Windows Media Audio (wma) bzw. Windows Media Video

(wmv) Format geliefert. In einem zweiten Schritt wird dann über den angefügten Link die Lizenz geliefert. Dieses zweistufige Konzept mit separater Lieferung von Inhalt und (hardwaregebundener) Lizenz der Microsoft® Windows Media Series® lässt sich schematisch wie folgt darstellen:



**Abbildung 4: Separate Delivery mit Microsoft® Windows Media Series®**

Der Ablauf vollzieht sich in diesen Schritten:

- (1) Kunde wählt Inhalt aus,
- (2) Webserver sendet URL des Media Servers zum Browser,
- (3) Browser ruft Media Player mit dieser URL auf,
- (4) Media Player ruft Media Server mit Content URL,
- (5) Media Server liefert den benutzer-unabhängig verschlüsselten Content über UDP oder HTTP,
- (6) Media Player prüft mittels Rights Manager, ob Lizenz vorliegt,
- (7) Falls nicht, ruft Rights Manager den Lizenzserver,
- (8) Lizenz wird geladen, Lizenz ist hardwaregebunden,
- (9) Content kann abgespielt werden.

### 3.4 Durchsetzung von Lizenzen beim Client

Lizenz und Datenobjekt sowie dessen Kopierschutz sollen eine nicht trennbare Einheit bilden. Um einem Benutzer nur die lizenzierten Rechte zu gewähren, ist eine Clientanwendung erforderlich, bei der die Prozesse des Entschlüsselns und Interpretierens der Daten sehr eng und untrennbar aneinander gekoppelt sein müssen. Die Anwendung entpackt die Inhalte und erlaubt den nach Lizenz möglichen Zugriff auf die Daten (abspielen, kopieren o.ä.). Dies ist das sogenannte „rights enforcement“ (siehe auch [GUTH]).

Weiterhin hat der Client die Aufgabe, erworbene Inhalte und Rechte zu verwalten. Die verwalteten Inhalte mit ihren Rechten müssen vom Client angezeigt werden.

In einigen DRM-Systemen wird von „temper resistant memory“ gesprochen, also muss der Client Sicherheitsvorkehrungen treffen, die es verhindern, die Daten aus der Clientanwendung zu entfernen, gleichzeitig aber erlauben, die Daten im Rahmen der Lizenz zu exportieren.

### 3.5 Recovery und Revocation von Lizenzen

In wieweit in einem DRM-Verfahren überhaupt Möglichkeiten gegeben sind, eine Lizenz zu widerrufen oder eine verlorene Lizenz wieder herzustellen, ist sehr unterschiedlich und nicht allgemein zu behandeln. Für den Anwender und den Provider sind sie aber eminent wichtige Aspekte. Die Möglichkeit der Licence-recovery gibt dem Anwender die Sicherheit, dass er bei Verlust seiner Lizenz (oder auch des Clients, z.B. bei combined delivery) durch den Vorgang seine Inhalte wieder nutzen kann, oder sie sogar auf einen anderen Client übertragen kann (wenn denn seine Nutzungsrechte dies erlauben). Mit Hilfe von Lizenzrevocation können kompromittierte Lizenzen gesperrt werden.

### 3.6 Authentifizierungsmechanismen für Server und Client

Durch eine sichere Authentifizierung kann jede Kommunikationsseite davon ausgehen, dass sie mit den „richtigen“ Partnern redet. Hierbei muss der Kommunikationsteilnehmer einen Beweis der Echtheit seiner Identität erbringen, und die andere Seite muss diesen anerkennen.

Werden z.B. im OMA DRM 1.0 nur rudimentäre Authentifizierungsmechanismen verlangt, ist dies für OMA DRM 2.0 nicht mehr der Fall (siehe [OMA]). Hier soll die Lieferung von Inhalten in ein PKI<sup>3</sup>-basiertes Umfeld gestellt werden. Dies bedeutet, dass sich sowohl der Server vor der Lieferung als auch der Client authentifizieren müssen. In der einfachsten Stufe geschieht dies mit festgelegten Geheimnissen (mutual trust). In einer weiteren Stufe wird dies durch X.509-Zertifikate von CAs erfolgen.

Die Verwendung von PKI-basierten Systemen ermöglicht es weiterhin, diese Verfahren auch zur Sicherung der Kommunikation zu nutzen. Die public/private keys können dann zur zusätzlichen Absicherung durch Verschlüsselung der gesamten Kommunikation benutzt werden. Damit kann man dann auch leicht auf Clientseite Sicherungsmechanismen einbauen, um Kommunikation mit „falschen“ Servern zu verhindern.

## **4 Analyse der Sicherheitsrisiken**

Im Folgenden werden die Sicherheitsrisiken in den einzelnen Schritten des Online-Handels mit DRM untersucht. Es ist zu beachten, dass hier die Sicherheitsrisiken nur aufgewiesen werden, aber noch nicht bewertet werden. Es werden gegebenenfalls Lösungsansätze vorgestellt. Meist ist es nicht möglich, eine vollständige Sicherheit zu erlangen. Es hat sich gezeigt, dass sich fast alle Verfahren unter Einsatz genügend großer Ressourcen umgehen lassen. Wichtig für die Untersuchungen der Sicherheit ist deshalb eine Analyse des Aufwands, der betrieben werden muss, um einen Sicherheitsmechanismus zu umgehen. Dabei muss der Wert der geschützten Information mit dem Aufwand zum „Brechen“ des Schutzes in Relation gestellt werden, um eine Beurteilung des Risikos zu erhalten.

### 4.1 Allgemeine Sicherheitsrisiken

Bei jeglicher Kommunikation zwischen zwei Komponenten muss gewährleistet sein, dass die Nachricht unverfälscht ankommt (Integrität), weiterhin ist insbesondere bei Kommunikation über unsichere Medien (d.h. also über das Internet oder das Mobilfunknetz) die Gefahr des Abhörens gegeben und damit die Vertraulichkeit gefährdet. Es ist sicherzustellen, dass die Unwiderrufbarkeit einer Nachricht gegeben ist, so dass der Sender (und zumeist auch der Sendetermin) eindeutig bestimmt ist, um eine Rechtsverbindlichkeit zu gewährleisten. Für die Kommunikation über unsichere Medien sind die Risiken von Standardverfahren (z.B. SSL) leichter einzuordnen, da sie besser untersucht sind als proprietäre Verfahren.

Innerhalb eines Moduls (z.B. innerhalb des Servers) sind die Risiken bei der Prozesskommunikation gering, aber abhängig von der Art der Implementierung.

Weiterhin muss die Datenhaltung sowohl in den Clients als auch im Server genau betrachtet werden. Hier sind Fragen des Schutzes der Daten vor fremdem Zugriff relevant, sowie die Möglichkeit, Daten nach Verlust wieder herzustellen.

Allgemeine Sicherheitsrisiken für eine konkrete Realisierung einer Online-Plattform verbergen sich auch im Softwareentwicklungsprozess dieser Plattform. Eine genaue Untersuchung dieses Entwicklungsprozesses hilft bei der Beurteilung der Risiken, die durch die Implementierung entstanden sein könnten.

### 4.2 Sicherheitsrisiken bei der Lizenzvereinbarung

Die Lizenzvereinbarung muss im Server unveränderbar und vor dem Zugriff nicht-autorisierter Personen geschützt gespeichert werden. Hier sind Fragen des Verbraucher- und auch des Datenschutzes von Relevanz. Da die Daten personalisiert werden und mit der Lizenzvereinbarung ein Kaufvorgang (und eventuelle Bezahlung) erfolgt, muss die Online-Plattform eine Möglichkeit enthalten, die Kunden zu identifizieren und Benutzerdaten zu erfassen. Aus Sicht der Verbraucher muss es hier klare Aussagen über diese Datenhaltung, die vertrauliche Behandlung und den Schutz der Daten geben.

Die korrekte Umsetzung der schriftlichen Vereinbarung („Worte“, der Kaufvertrag als Text z.B. auf dem Web-Server) in den elektronischen Vertrag (zumeist eine XML-basierte Datei) muss gewährleistet werden. Hier müssen Mechanismen zur Verfügung gestellt werden, mit denen der Kunde diesen Vertrag sowohl während des

---

<sup>3</sup> Public Key Infrastructure

Kaufvorgangs als auch später auf dem Client kontrollieren kann, d.h., es muss eine „sichere und lesbare“ Anzeigemöglichkeit für die mit der Lizenz erworbenen Rechte sowie die dazu gehörigen Inhalte geben.

#### 4.3 Sicherheitsrisiken bei der Lizenzerstellung und Lieferung

Bei der Erstellung der Lieferung (je nach Lieferart sind dies die gepackten Daten und die Lizenz) muss sicher gestellt werden, dass keine Manipulation an den Dateien erfolgen kann bzw. innerhalb der Lizenz und den Daten weitere unerwünschte Daten versteckt an den Kunden übermittelt werden.

Während der Lieferung sind die im Abschnitt „Allgemeine Sicherheitsrisiken“ beschriebenen Punkte bei der Kommunikation von großer Bedeutung. Sowohl die Inhalte als auch die Lizenz, die entweder als eine Einheit oder getrennt geliefert werden, müssen vor Verlust und Manipulation geschützt werden.

#### 4.4 Sicherheitsrisiken bei der Durchsetzung von Lizenzen beim Client

Auf Seiten des Clients ist es erforderlich, die erworbenen Rechte durchzusetzen, sowie erworbene Inhalte und Rechte zu verwalten.

Der Client muss die zumeist verschlüsselt vorliegenden Daten entschlüsseln und je nach Lizenz wiedergeben. Hier besteht die Gefahr, dass die enge Bindung von Inhalt, Lizenz und Verschlüsselung aufgebrochen, und der Inhalt unter Umgehung der erworbenen und in der Regel eingeschränkten Rechte weitergehend genutzt wird. Dazu muss auf die Daten des Clients zugegriffen werden und diese manipuliert werden, deshalb wird z.B. im Standard für das DRM der OMA ein „temper resistant memory“ der Clients verlangt (siehe [OMA]).

Falls ein Zugriff auf die Daten im Client möglich ist, besteht weiterhin das Risiko, dass es möglich ist, ein sogenanntes „Wasserzeichen“, das die Daten eindeutig identifiziert, zu entfernen. Die Güte des verwendeten Wasserzeichen-Verfahrens entscheidet hierbei über den Aufwand, der betrieben werden muss, um das Wasserzeichen zu entfernen.

#### 4.5 Sicherheitsrisiken bei Recovery und Revocation von Lizenzen

Sind Mechanismen für die Wiederbeschaffung von Lizenzen (bzw. auch Inhalten, falls es sich um ein Verfahren mit „combined delivery“ handelt) vorhanden, muss sicher gestellt werden, dass nur der Anwender, der die Lizenz erworben hat, oder eine von ihm autorisierte Person sich diese wiederbeschaffen kann. Dazu muss die Identifikation und Authentifikation des Anwenders korrekt erfolgen (siehe auch Kapitel 4.6). Eine mögliche Attacke durch eine gefälschte Identität eines Angreifers („Impersonating“) ist denkbar.

Genauso müssen die Rechte des Anwenders gewahrt werden, wenn eine Lizenz gesperrt wird. Dieser Prozess darf nur von ihm selber oder von dem Inhaltsanbieter bei Bruch des Geschäftsvertrags angestoßen werden.

#### 4.6 Sicherheitsrisiken bei Authentifizierungsmechanismen

Die Untersuchung von PKI-Verfahren sprengt den Rahmen dieser Ausarbeitung. Hier muss auf bestehende Untersuchungen gängiger Verfahren (siehe z.B. [SCHNEI]) zurückgegriffen werden. Die verwendeten Verschlüsselungsverfahren, wie z.B. der gewählte Hash-Algorithmus und die verwendete Schlüssellänge, sind Indizes für das Sicherheit des Verfahrens. Weitere qualitative Merkmale für ein PKI Verfahren sind die Art der Validierung der Zertifikate (z.B. durch die Verwendung von Sperrlisten (CRLs<sup>4</sup>) oder Online-Protokolle), die Identifikation und Authentifikation des Besitzers sowohl beim Ausstellen der Zertifikate als auch bei ihrer Verwendung. Wichtig ist die Betrachtung, wie die privaten Schlüssel im Client gespeichert werden, so dass sie diesen nicht (ungewollt) verlassen können.

### **5 Ausblick auf Schutzprofile nach den Common Criteria**

Mit Hilfe der Common Criteria werden allgemein anerkannte Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik aufgestellt. Diese Kriterien stellen einen internationalen Standard dar (ISO/IEC 15408). In Deutschland wird die Zertifizierung von IT-Produkten oder IT-Systemen nach den CC vom Bundesamt für Sicherheit in der Informationstechnik (BSI) vorgenommen. Ein erteiltes IT-Sicherheitszertifikat wird im Rahmen internationaler Abkommen von vielen Staaten anerkannt. Neben der Zertifizierung eines einzelnen Produktes kann

---

<sup>4</sup> Certificate Revocation Lists

mit Hilfe der Kriterien auch ein sogenanntes Schutzprofil (PP - Protection Profile) erstellt werden. Mit Hilfe dieses Profils werden die Sicherheitskriterien für die Bewertung einer ganzen Produktpalette festgelegt. Es enthält neben der Verallgemeinerung der Sicherheitsvorgaben und dem Sicherheitskonzept für die Anwendungen eine Aufstellung der Anforderungen an die Funktionalität und die Vertrauenswürdigkeit und enthält einen ausführlichen Erklärungsteil. Schutzprofile werden in einem eigenen Evaluierungsprozess bewertet und zertifiziert (siehe [PP]). Ein solches Profil ergibt die Basis für verschiedene, konkrete Produkte und macht sie vergleichbar. Ein Anwender kann sicher gehen, dass ein Produkt, das sich auf ein zertifiziertes Schutzprofil bezieht und evaluiert wurde, genau diese Kriterien erfüllt. Weiterhin können Produkte schneller und kostengünstiger evaluiert werden, wenn sie auf einem Schutzprofil aufbauen, da der Aufwand der Erstellung der Sicherheitsvorgaben für ein Produkt (die Verfeinerung des Schutzprofils für ein konkretes Produkt) sehr hoch ist. Somit ist ein Schutzprofil sowohl von Vorteil für den Hersteller als auch den Benutzer des Produktes.

Der erste Schritt für die Erstellung eines Profils ist die Erfassung der Sicherheitsrisiken, der Voraussetzungen, sowie der Bedrohungen, die für das untersuchte Sicherheitsproblem. Eine Art Risikoanalyse wird erstellt, bei der Bedrohungen und zu schützende Werte in Relation gesetzt werden.

Durch den allgemeinen Ansatz des Modells ist es möglich, verschiedene DRM-Lösungen zu erfassen und ihre Sicherheitsrisiken zu beschreiben. Die Aussagen der vorherigen Kapitel können somit als Grundlage für die Erstellung eines Profils genutzt werden.

Eine Online-Plattform mit ihren DRM-Komponenten, die diesem Schutzprofil konform die Sicherheitsrisiken abdeckt, bietet ein angemessenes Sicherheitsniveau für alle Beteiligten des Online-Handels. Sowohl der Endanwender, als auch die Inhaltsanbieter und die Plattformbetreiber haben damit ein vergleichbares Qualitätsmerkmal für die Sicherheit der DRM-Komponenten zur Hand. Dies ist für die Bewertung bestehender Systeme (und auch Standards) von Bedeutung, aber auch für die Entwicklung neuer Systeme.

## 6 Anwendung des Modells

Für die Akzeptanz einer Multimedia-Online-Verkaufsplattform bei Kunden und Inhaltsanbietern ist es wichtig, dass die Plattform „multi-DRM“-fähig ist. Das heißt, dass beliebige DRM-Verfahren über sie realisiert werden können. Weiterhin bedeutet es, dass die Plattform so modular gestaltet sein muss, dass erstens die Kommunikation mit den verschiedensten Clients ermöglicht wird, zweitens diese Clients mit Lieferungen bedient werden können und drittens die von den Inhaltsanbietern gewünschten DRM-Verfahren über sie parallel ablaufen können.

Mit Hilfe des in Kapitel 3 vorgestellten allgemeinen Modells ist dies möglich. Es wurde ein System<sup>5</sup> realisiert, welches multi-DRM-fähig ist. Dieses System kann als Referenzimplementierung herangezogen werden.

Zur Zeit unterstützt das System das Fraunhofer MMP-Verfahren, das Verfahren für die Microsoft<sup>®</sup> Windows Media Series<sup>®</sup> sowie das DRM-Verfahren für den OMA-Standard, Version 1.0.

Die Daten, Metadaten und DRM-Informationen der Inhalte werden soweit wie möglich übergreifend in unabhängigen Formaten gespeichert. Damit kann redundante Datenhaltung weitgehend vermieden werden. Die Metadaten können mit Hilfe eines „Content Management Systems“ (CMS) bearbeitet werden. Erst bei der Auslieferung der Daten ist eine verfahrensspezifische „Übersetzung“ der DRM-Informationen und Metadaten erforderlich. Hierbei erfolgt dann auch eine Koppelung mit den Benutzerdaten, um die Personalisierung der Daten vornehmen zu können, soweit es das DRM-Verfahren verlangt. Durch die Personalisierung wird auch die Abrechnung ermöglicht.

Weiterhin wurde ein Multi-DRM-Client entwickelt, der mit der Online-Plattform kommuniziert und dem Benutzer Werkzeuge zur Verwaltung seiner Inhalte an die Hand gibt. Es werden Betriebssysteme und Browser für stationäre und mobile Clients, sowie eine Reihe von Playern und Formaten unterstützt.

## 7 Quellenverzeichnis

CC <http://www.bsi.de/cc/index.htm>

SCHNEI Bruce Schneier, „Angewandte Kryptographie“, Addison-Wesley München, August 1996

CHENG Spencer Cheng, Avini Rambhia, „DRM and Standardization – Can DRM be standardized“, in E.Becker et al. (Eds): Digital Rights Management, LNCS 2770, pp. 162-177, Springer-Verlag Berlin Heidelberg, 2003

<sup>5</sup> BOB, Multimedia Online Plattform, mtG, siehe auch [www.mtg.de](http://www.mtg.de)

- DRM [http://www.witi.cs.uni-magdeburg.de/iti\\_amsl/lehre/04\\_SoSem/drm\\_ps/scripte/Einfuehrung.PDF](http://www.witi.cs.uni-magdeburg.de/iti_amsl/lehre/04_SoSem/drm_ps/scripte/Einfuehrung.PDF)
- GUTH Susanne Guth, „A Sample DRM System“, in E.Becker et al. (Eds): Digital Rights Management, LNCS 2770, pp. 150-161, Springer-Verlag Berlin Heidelberg, 2003
- OMA <http://www.openmobilealliance.org>
- PP <http://www.bsi.de/literat/faltbl/F26SchutzprofileCC.htm>
- XRML <http://www.contentguard.com/xrml.asp>