

# Datenspuren bei der Nutzung von Digital Rights Management-Systemen (DRM)

Rüdiger Grimm, Stefan Puchta

*DRM-Systeme in aktuellen Shopanwendungen werden in Bezug auf Kundendatenschutz untersucht. Beispielhaft werden die Systeme iTunes von Apple und der Windows Media Rights Manager von Microsoft analysiert. Die Analysestruktur folgt den gesetzlichen Datenschutzprinzipien. Daraus werden Empfehlungen für einen datenschutzfreundlicheren Umgang abgeleitet.<sup>1</sup>*

## 1 Wozu DRM?

Vor der effizienten Digitalisierung von geistigem Eigentum – wie z.B. Musik, Texte, Filme, Bilder – waren Inhalte fest an physikalische Medien gebunden, die nicht ohne Aufwand und Qualitätseinbußen kopiert und übertragen werden können. Das traditionelle Geschäftsmodell mit diesen Gütern war das Geschäft mit den physikalischen Medien. Mit der Digitalisierung, spätestens seit Einführung der Audiokompressionsmethode MP3, funktionieren diese Modelle nicht mehr richtig. Kunden bezahlen nicht für CDs, DVDs oder Bücher, wenn sie den gleichen Inhalt („Content“) in Originalqualität frei im Internet bekommen.

Digitales Rechtemanagement (DRM) versucht den Verlust der physikalischen Bindung zu kompensieren, indem ihre Funktionen die unkontrollierte Vervielfältigung von digitalen Inhalten in den Nutzerendgeräten verhindern. Dazu werden spezifische Nutzungsrechte maschinenlesbar in die Inhaltsdateien einkodiert. Lokale Abspielfunktionen lesen die Rechte und führen sie aus. Auf diese Weise steuern DRM-Mechanismen das Ausführen spezifischer Nutzungsrechte im Nutzerendgerät.

Nutzer können dann nur in der Art und Weise konsumieren, die in den Nutzungsrechten festgelegt ist und für die sie bezahlt haben. Zu Entwicklungen und verschiedenen Funktionsweisen von DRM-Systemen siehe (Rosenblatt et al. 2002) und (Becker 2003).

Auf dem Markt existieren verschiedene DRM-Produkte, z.B. Apples Fairplay als Kernsystem von iTunes, Microsofts Windows Media Rights Manager (WWRM) in vielen verschiedenen Shopsystemen, z.B. in Musicload von T-Online, sowie OpenMG in Sonys Connect-Europe Shop. DRM wird nicht nur für digitale Musik eingesetzt. Für elektronische Text-Dokumente verwendet Adobe zum Beispiel PDF-integrierte DRM-Funktionen zur Unterstützung des E-Book-Formats. Es gibt eine Vielzahl weiterer Systeme am Markt – alle mehr oder weniger inkompatibel zueinander, umständlich

und schwierig zu benutzen. Insbesondere sind sie intransparent im Umgang mit personenbezogenen Daten. Letztendlich werden sie nicht richtig vom Markt akzeptiert, verglichen mit dem möglichen Marktpotenzial.

Das Musicload Infoblatt vom 5.4.2005 (www.musicload.de) schätzt im „Digital Music Report 2004 of the International Federation of the Phonographic Industry (IFPI)“ ca. 200 Millionen legale Musikdownloads, die ungefähr 20% der gesamten Downloads ausmachen: Das bedeutet, dass 80% oder 800 Millionen Downloads in der gleichen Zeit illegal sein müssen. Weiterhin wurde festgestellt, dass die Anzahl legaler Downloads von 2003 bis 2004 gleich geblieben ist. Der Download-Markt von digitaler Musik befindet sich noch weit weg von seinem möglichen Potential.

In unserer Studie (Bizer et al. 2005) stellen wir fest, dass die unkomfortable und umständliche Benutzung von DRM-Systemen einen wesentlichen Grund dafür darstellen. Die Systeme befriedigen nicht die Ansprüche der Nutzer und untergraben das Vertrauen der Kunden, indem sie mit ihren persönlichen Daten falsch oder ohne die erforderliche Sorgfalt umgehen. In diesem Artikel wollen wir speziell auf das Datenschutzproblem existierender DRM-Systeme eingehen.

Zu diesem Zweck analysieren wir im Folgenden einige DRM-Systeme und ihre Shops in Bezug auf ihren Umgang mit den personenbezogenen Daten ihrer Kunden. Die Analyse folgt einer Struktur von Datenschutzprinzipien nach der Europäischen Datenschutzrichtlinie (EU 95/46/EC 2005). Als Beispiele werden Apples iTunes und Microsofts Windows Media im Detail vorgestellt. Daraus werden Empfehlungen für einen besseren Umgang abgeleitet.



Prof. Dr.  
Rüdiger Grimm  
Uni Koblenz

Forschungsthemen:  
IT-Sicherheit,  
E-Commerce,  
Vertrauen.

E-Mail: grimm@uni-koblenz.de



Dipl.-Ing.  
Stefan Puchta

Fraunhofer Institut  
für Digitale Medientechnologie  
Ilmenau Arbeitsgruppe  
„Security for Virtual  
Goods“

E-Mail: Stefan.Puchta@idmt.fraunhofer.de

<sup>1</sup> Der Beitrag geht auf die Studie Privacy4DRM im Auftrag des Bundesministeriums für Bildung und Forschung zurück [Bizer et al. 2005], an der die Autoren mitgewirkt haben.

## 2 Das Datenschutzproblem in DRM

Es gibt drei grundsätzlich verschiedene Vorgehensweisen zum Schutz von Rechten digitaler Güter.

- Der erste Ansatz ist die Verwendung von „harter DRM“, mit dessen Hilfe Rechte mit technischen Mitteln durchgesetzt werden, so dass sich Nutzer nicht illegal verhalten können. Kopierschutztechniken sind die einfachste Form dieser DRM-Systeme.
- Der zweite Ansatz verhindert illegales Verhalten von Nutzern nicht explizit mit technischen Mitteln, personalisiert aber die Nutzung der Produkte, um sie in illegalen Umgebungen identifizieren zu können. Ein Beispiel dieses Verfolgungsansatzes ist das LWDRM-System (Grimm/Aichroth 2004), in dem Nutzer „Fair Usage“-Möglichkeiten erhalten, wenn sie Inhalte digital signieren.
- Der dritte Ansatz benutzt keinerlei Mechanismen zur Durchsetzung von Rechten, sondern belohnt legales Nutzerverhalten. So verwendet beispielsweise das PotatoSystem ([www.potatosystem.de](http://www.potatosystem.de)) ein bestimmtes Provisionsmodell, um Kunden, die für die Nutzung digitaler Güter bezahlen, am Umsatz zu beteiligen.

Sowohl das Verfolgungssystem, als auch das Belohnungsmodell verwenden persönliche Kundendaten, um Nutzer identifizieren zu können. Beide Ansätze müssen also den Datenschutz sehr sorgfältig berücksichtigen. Der erste Ansatz – das „harte DRM“, das Nutzer am illegalen Handeln technisch hindert – sollte strikt produktorientiert ausgelegt sein und ohne eine entsprechende Nutzerreferenz des Inhaltes auskommen. Eben weil technische Funktionen ein richtiges Verhalten durchsetzen, sollten keine weiteren Maßnahmen zur Identifizierung oder Verfolgung gegenüber Nutzern erforderlich sein.

Tatsächlich vertrauen die meisten Shop-systeme aber nur eingeschränkt den eingebauten DRM-Mechanismen zur Rechtedurchsetzung in den Nutzerendgeräten. Sie benutzen sozusagen als eine „zweite Verteidigungslinie“ zusätzliche Verfolgungsmethoden. Sie sammeln weiterhin Daten, um ihre Nutzer zu identifizieren, um ihre Produkte einzelnen Käufern eindeutig zuzuordnen zu können und diese später in illegalen Umgebungen wieder erkennen zu können.

Eine derartige Verwendung personenbezogener Daten in DRM-Systemen wird den Nutzern nicht immer offen gelegt.

## 3 Die Analysestruktur

Wir analysieren die DRM-Systeme anhand der gesetzlichen Datenschutzprinzipien (vgl. Möller 2005). Die Europäische Richtlinie 95/46/EC für Datenschutz bietet ein Modell für den Datenschutz, das weithin akzeptiert ist.

Die Richtlinie definiert „personenbezogene Daten“ als „sämtliche Informationen, die zu einer identifizierten oder identifizierbaren natürlichen Person gehören“. Diese identifizierten oder identifizierbare natürliche Person wird als „Datensubjekt“ bezeichnet (Art. 2). Die Richtlinie schreibt das Speichern, Verarbeiten und Benutzen von personenbezogenen Daten anhand folgender Prinzipien vor:

- Qualität (Art. 6): Die Daten müssen rechtmäßig, angemessen und relevant sein;
- Legitimierung (Art. 7): Persönliche Daten müssen an den Zweck ihrer Verwendung gebunden sein, sie dürfen nur nach Einwilligung des Datensubjekts oder nach gesetzlicher Verpflichtung verwendet werden;
- Zweckbindung (Art. 7): Die personenbezogenen Daten müssen für den Einsatzzweck notwendig sein, z.B. zur Erfüllung eines Vertrags oder einer Dienstleistung;
- Transparenz (Art. 10-12): Nutzer sind über den Umgang des Diensteanbieters mit seinen personenbezogenen Daten in vollem Umfang zu unterrichten;
- Nutzerkontrolle: Nutzer haben das Recht, ihre personenbezogenen Daten einzusehen, zu berichtigen oder löschen zu lassen (Art. 10-12), sowie bestehende Einwilligungen zu widerrufen (Art. 14);
- Vertraulichkeit (Art. 16): Der Anbieter muss die Vertraulichkeit aller personenbezogenen Daten sicherstellen;
- Korrektheit und Sicherheit (Art. 10-12 zum Recht, Daten zu berichtigen, und Art. 17 zu Sicherheit): Der Anbieter muss die Daten gegen Verlust und Beschädigung schützen und ihre Korrektheit sicherstellen;
- Aufsicht/Supervision (Art. 18-19 und 28-30): Vorschriften über eine Aufsichtsbehörde;
- Rechtsmittel, Haftung und Sanktionen (Art. 22-24): Vorschriften über Sanktio-

nen, wenn der Serviceprovider diese Prinzipien nicht einhält.

Ferner dürfe personenbezogene Daten nur dann in ein drittes Land außerhalb der EU transferiert werden, wenn dieser Drittstaat „ein vergleichbares Datenschutzniveau bietet“ (Art. 25). Der „US Safe Harbor“ ist ein solches Abkommen, dem amerikanische Service Provider beitreten können, um ein angepasstes Datenschutzniveau zu garantieren (US Department of Commerce 2005). Die Prinzipien der Europäischen Richtlinie für Datenschutz sind nicht exakt, aber doch ähnlich auf die sieben „Safe Harbor“-Prinzipien übertragbar: „notice, choice, onward transfer, access, security, integrity, and enforcement“.

Natürlich können diese Prinzipien bei jedem Shop, der digitale Waren anbietet, überprüft werden. Internetschops offerieren Datenschutzerklärungen auf ihrer Webseite, z.B. Apple: [www.apple.com/de/legal/privacy/](http://www.apple.com/de/legal/privacy/). Es ist aber sehr schwer herauszufinden, wo genau, an welchem Punkt der Kommunikation zwischen Käufer und Verkäufer und – am allerschwierigsten – für welchen Zweck Daten gesammelt, gespeichert und von den Shopbetreibern verwendet werden, entweder direkt oder unter Zuhilfenahme eines DRM-Systems.

Um herauszufinden, welche Daten an welchem Kommunikationspunkt und an welchem Ort gesammelt und gespeichert werden, können jeder Webshop und jedes beteiligte DRM-System unter den folgenden Gesichtspunkten analysiert werden (Bizer et al. 2005, 2.4-2.5):

- Datenfluss vor Vertragsabschluss: Während der Kaufvorbereitung, während der Nutzerregistrierung und bei der Auswahl eines gewünschten Produktes (Produkt in den Warenkorb);
- Datenfluss zum Zeitpunkt des Vertragsabschlusses: Am Ende der Produktauswahl (Schließen des Warenkorbs), beim Bezahlen und bei der anschließenden Auslieferung des Produktes;
- Datenfluss beim Überprüfen der Nutzungsrechte: Während der ersten Installation einer Software, bei wiederholter Nutzung, bei der Aktualisierung bestimmter Rechte;
- Datenfluss für andere Zwecke: Z.B. zur Verbesserung des Angebots, zum Direktmarketing und für Sicherheitsmethoden (Verschlüsselung);
- Datenfluss durch verborgene Schnittstellen und Verkettung verschiedener Funktionen: Cookies, Pixel Tags (Web Bugs),

das Verbinden von Kundendaten mit Clickstream Daten, z.B. mit IP-Adressen oder Kryptographieschlüsseln.

Darüber hinaus untersuchen wir folgende „Allgemeine Datenspuren“:

- Vom System erzeugt bzw. erhoben: dazu gehören z.B. Informationen, die über das System oder den Browser unabhängig vom Nutzer weitergegeben werden.
- Vom Nutzer erzeugt: dazu werden alle personenbezogenen Informationen gezählt, die der Nutzer bewusst liefert, sowie Daten, die durch das Nutzerverhalten im System anfallen.
- In das Produkt einkodiert: das sind alle personenbezogenen Daten aus den beiden ersten Kategorien, die vom Diensteanbieter in das fertige Produkt einkodiert werden.

## 4 Beispiel Apples iTunes

Apples iTunes ist ein Musikportal mit Online-Shops in über 19 Ländern weltweit. Es bietet mehr als 800 000 Titel aus 28 Genres zum Verkauf an (Stand Januar 2005). Die fünf Major Labels und viele weitere Independent Labels sind bei iTunes mit ihrem Content vertreten. Bis März 2005 zählte iTunes insgesamt über 300 Millionen Downloads, das sind ca. 40 Millionen pro Monat. Neben Musikstücken bietet der iTunes-Shop Videos, Hörbücher, Filmtrailer und Radiostreams an.

Die Anzahl der Kunden ist bisher nicht veröffentlicht. Die Zielgruppe sind junge Menschen, die Musik mögen, die sich oft im Internet bewegen und die bereit sind, für Musik zu zahlen.

Die iTunes-Server stehen in den USA, die Software unterstützt das Format M4P (MPEG-4 protected) und den Codec AAC. Das involvierte DRM-System heißt „Fairplay“ (iTunes Musicstore 2005).

Apples iTunes funktioniert folgendermaßen (siehe Abbildung 1): Der Nutzer interagiert mit dem Shopperserver (Schritt 3 und 5), der den registrierten Content von einem Content Provider speichert und bereitstellt (Schritt 1). Nachdem die iTunes-Clientsoftware installiert wurde (2), kann der Nutzer durch den Shop browsen und entsprechende Stücke zum Kauf auswählen (3). Der Shop wickelt als erstes die Bezahlung der entsprechenden Stücke ab (4), anschließend liefert er die Inhalte an den Nutzer aus (5). Der Nutzer kann nun das Produkt konsumieren (6).

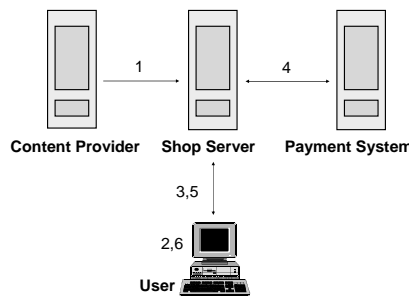


Abb. 1: Das Prozessmodell von Apple iTunes

Der Nutzer kann das Stück zusätzlich auf eine CD brennen und es auf einen Apple iPod transferieren. Er kann es auf bis zu sechs weiteren, vorher am Server registrierten PCs kopieren und abspielen. Wenn er es auf einem siebenten Gerät benutzen möchte, muss er vorher einen der sechs schon angemeldeten PCs am Server wieder abmelden. iTunes Produkte werden vor der Auslieferung mit einem symmetrischen Schlüssel verschlüsselt, der wiederum mit einem öffentlichen Nutzerendgeräteschlüssel asymmetrisch verschlüsselt wird. Das Schlüsselpaar des Nutzerendgerätes wird mittels einer bestimmten Funktion über ausgewählte Hardwareparameter erzeugt. Somit können nur legal angemeldete Geräte den entsprechenden Content entschlüsseln und abspielen (Bizer et al. 2005, Abschnitt 3.1).

## 5 Datenspuren in iTunes

Die Datenschutzanalyse von iTunes folgt der in Abschnitt 3 vorgestellten Struktur.

### 5.1 Anmeldung

Während der Anmeldung muss der Kunde ein Formular ausfüllen, das folgende Pflichtfelder enthält:

- ◆ Name, Adresse, Telefonnummer;
- ◆ E-Mail-Adresse, welche als Apple-ID genutzt wird, und ein Kundenpasswort;
- ◆ Eine persönliche Frage und Antwort, sowie das Geburtsdatum, um später ein verlorenes Passwort wieder herzustellen;
- ◆ Zahlungsinformationen, z.B. Kreditkartennummer und Validierungsdaten.

Optionale Kundendaten sind:

- ◆ Postanschrift zur Auslieferung von Hardware;
- ◆ Fax- und Handynummer;
- ◆ Umsatzsteuernummer.

## 5.2 Während der Kommunikation

Während der Kommunikation werden systemseitig folgende Datenspuren gesammelt:

- ◆ Das vom Kunden benutzte Betriebssystem (Version, Sprache), die iTunessoftwareversion und die IP-Adresse des Kunden aus dem HTTP-Protokoll;
- ◆ Cookies und Session-IDs. Cookies werden genutzt, um herauszufinden, welche Seiten in welcher Reihenfolge wie lange besucht werden; Session-IDs werden genutzt, um zusammengehörige Online-Sitzungen zu organisieren;
- ◆ Device-IDs: um einen PC am Shopperserver zu registrieren, wird aus einem Hash über bestimmte Hardwareparameter eine sogenannte Device-ID erzeugt. Sie wird zusätzlich zum Verschlüsseln des symmetrischen Schlüssels verwendet und stellt somit die Bindung zur entsprechenden Hardware her: dieses ist der Kern des Fairplay DRM-Systems.

## 5.3 Einkodierung in das Produkt durch das Anbietersystem

Dieser Teil des Systems ist dem iTunes-Kunden gegenüber ziemlich undurchsichtig. Durch einen entsprechenden Hexdump (Öffnen des Files in einem Hexeditor) kann man folgende Daten finden:

- ◆ Produkt-ID, vom Shopperserver organisiert und vergeben;
- ◆ Apple-ID, die der tatsächlichen E-Mail-Adresse des Kunden entspricht;
- ◆ Weitere Metadaten über das Produkt (Titel, Genre, Jahr, Album, usw).

Im Regelfall werden die Kunden mangels Information nicht wissen, dass ihre E-Mail-Adresse in das File eingebracht wird und bei einer Weitergabe in dem File verbleibt.

## 5.4 Vor Vertragsschluss

Vor dem Abschluss eines Kaufs muss sich der Kunde bei iTunes registrieren. Zu diesem Zweck muss er das entsprechende Online-Formular ausfüllen (s.o. 5.1). Während der Registrierung werden über ein HTTP-Protokoll noch weitere Systemdaten übertragen (s.o. 5.3). Weitere Daten werden bei der Verwendung von Gutscheinen übermittelt, um eigene iTunes-Accounts aufzufüllen.

## 5.5 Bei Vertragsschluss

Ein registrierter Kunde bringt den Kauf zum Abschluss, indem er sich mit Apple-ID und Passwort einloggt und den Kauf der von ihm ausgewählten Produkte bestätigt. Die Produkte mit dazugehöriger Produkt-ID werden mit der Apple-ID zum Server übermittelt, gespeichert und zum Download vorbereitet. Nach positiver Rückmeldung des Zahlungssystems wird der Download freigegeben und gestartet. Der Downloadstatus wird zusätzlich gespeichert, um erfolglose Downloads wiederholen zu können. Selbst nach erfolgreichem Herunterladen werden alle Kaufinformationen in der Datenbank belassen.

Vor dem Ausliefern des Produktes werden Produkt-ID, Apple-ID und Metadaten in das Stück einkodiert und das File anschließend symmetrisch verschlüsselt.

## 5.6 Überprüfung der Nutzungsrechte

Ein Nutzer-PC muss für das Abspielen von iTunes-Musik am Shopserver angemeldet sein. Beim Anmelden erhält dieser Rechner bestimmte Informationen, um den für den Nutzer verschlüsselten Content entschlüsseln und abspielen zu können.

Ein anderes Gerät, welches nicht am Server registriert ist, wird nicht in der Lage sein, den symmetrischen Contentschlüssel zu entschlüsseln, weil die geheimen und geschützten Funktionen für diesen Vorgang lokale Hardwareparameter benutzen. Dadurch können nur legal angemeldete Nutzer-PCs entsprechende iTunes-Files abspielen (jedenfalls solange das DRM-System nicht umgangen wurde).

## 5.6 Andere Zwecke

Wenn ein (registrierter) Kunde durch den iTunes-Shop surft, werden bestimmte Suchwörter und Produkt-IDs mit IP-Adressen und ggf. mit Apple-IDs verbunden.

Ein weiteres Feature ist der so genannte *iMix*. Er stellt eine persönliche Hitliste von Musiktiteln des Nutzers dar. Der *iMix* wird unter einem selbst gewählten Pseudonym veröffentlicht und kann von anderen Nutzern bewertet werden. Ein iTunes-Kunde kann einen *iMix* anderen Kunden mittels eines Webformulars empfehlen, dabei werden die E-Mail-Adressen des Empfehlenden und des Empfängers eingegeben. Der Empfänger muss dabei kein registrierter iTunes-

Kunde sein. *iMix*, Pseudonyme und E-Mail-Adressen werden von iTunes verknüpft und geben Auskunft über ein bestimmtes Nutzerverhalten.

Eine zusätzliche Anwendungsfunktion ist das *Taschengeldkonto*. Dabei können registrierte iTunes-Nutzer einen monatlichen Betrag auf das Konto eines anderen Nutzers überweisen, der selbst keine Kreditkarte besitzt. Mit dem Einrichten der monatlichen Überweisung kann der Nutzer gleichzeitig einen neuen Account für den Empfänger anlegen. Alle damit verbundenen Daten (E-Mail-Adressen, Geldbeträge und getätigte Käufe) können im iTunes-System verknüpft und ausgewertet werden.

Gutscheine stellen eine zusätzliche Möglichkeit dar, um Geld von einem Nutzer zum anderen zu übermitteln. Dabei werden E-Mail-Adressen (und damit potentielle Apple-IDs) zum Versenden verwendet.

Schließlich bietet iTunes den *Metadaten-service CDDB* von Gracenote zur Identifikation unbekannter Musikstücke an ([www.gracenote.com/music](http://www.gracenote.com/music)). Ein iTunes-Kunde kann diesen umfangreichen Metadaten-Server während einer iTunes-Session anfragen und sich Metadaten schicken lassen. Er kann seinerseits auch entsprechende Metadaten von seinen eigenen Inhalten an diesen Dienst senden. Dieser Dienst ist anonym, so dass Gracenote anfragende Nutzern nicht mit iTunes-Kunden verknüpfen kann.

## 5.7 Verborgene Schnittstellen und Funktionsverketzung

An jedem Punkt der Kommunikation zwischen Client und iTunes-Server stehen sämtliche HTTP-Daten, wie z.B. Clickstreams, IP-Adresse, Sprache, HTTP-Referer („von welcher Seite der Kunde kommt“), Suchanfrage-Wörter, usw. dem Shopserver zu Verfügung und können bei Kenntnis der Apple-ID mit dem Datensubjekt (Kunden) verknüpft werden.

Weitere Informationen über Kundenverhalten kann iTunes über die Verbindung von Apple-ID, *iMix*, verschickte und empfangene Gutscheine und das Einrichten von Taschengeldkonten erfahren. Mittels der Häufigkeit sowie der Art und Weise von Kommunikationsabläufen ist iTunes in der Lage, weiteres Kundenverhalten zu ermitteln und mit realen Kundendaten zu verbinden.

Die E-Mail-Adresse stellt immer eine persönliche Information dar. Selbst wenn

iTunes einige Pseudonymitätskonzepte anbietet, ist eine Verbindung zur E-Mail-Adresse in den meisten Fällen möglich.

Besonders die in die Files eingebrachte E-Mail-Adresse stellt eine einfache Möglichkeit zur direkten Zuordnung des Contents zum Käufer dar.

## 6 Beispiel Microsofts Windows Media Rights Manager

Microsofts Windows Media Rights Manager (WORM) ist ein DRM-System, welches in Musikportale oder E-Commerce-Shops, die kopiergeschützte virtuelle Waren anbieten, integriert werden kann. Die Hauptidee ist die Trennung von verschlüsseltem Content und dazugehöriger Lizenz, die den Entschlüsselungsschlüssel enthält. Inhalte und Lizenzen können von verschiedenen Servern bezogen bzw. gekauft werden. Dabei agiert der Contentserver als so genannter Contentpacker, der Lizenzserver hingegen erstellt, verwaltet und liefert Lizenzen (siehe Microsoft 2005).

Abbildung 2 zeigt den Ablauf des WORM-Systems. Der Contentprovider kodiert die Stücke in ein Microsoftformat (.ASF, .WMA oder .WMV) und schickt sie zum Contentpacker (Schritt 1). Dieser hat zwei Aufgaben: Als erstes generiert er einen Contentschlüssel aus einem vorgegebenen speziellen Anfangswert („seed“) und verschlüsselt damit symmetrisch den Content (2). Danach erstellt er einen Contentheader und signiert ihn (3). Dieser Header beinhaltet eine Schlüssel-ID, den Link zum Lizenzserver (URL) und weitere Informationen. Die Clientsoftware (Windows Media Player oder Internet-Explorer) kommuniziert mit dem Shopserver und lädt entsprechend verschlüsselten Content herunter (4). Dieser Schritt beinhaltet im Hintergrund den Ablauf eines bestimmten Zahlungssystems.

Betrachten wir zum Beispiel das deutsche Musikportal „Musicload“ von T-Online, welches WORM einsetzt. Dieses System benutzt als Backendlösung das ADoRA-System des Digital World Service (DWS) in Zusammenhang mit dem Zahlungssystem T-Pay von T-Online (Musicload 2005, T-Pay 2005). Dem Contentpacker ist es überlassen, die entsprechende Lizenz zum Konsumieren und Abspielen dem Content direkt beizufügen oder nicht (6). Wenn keine Lizenz mitgeliefert wird (5), kontaktiert der Client über den im Con-

tentheader angegebenen Link den Lizenzserver und fordert die Ausstellung einer entsprechend gültigen Lizenz an (5a). Der Lizenzserver generiert diese (5b) und sendet sie an den Client zurück (5c). Mittels dieser Lizenz und des darin enthaltenen Schlüssels kann die Clientsoftware nun das gekaufte Produkt entschlüsseln, die enthaltenen Benutzungsrechte interpretieren und das Stück abspielen (6).

Das Musicload-Portal kann man entweder mit einem Browserprogramm oder mit der seit April 2005 angebotenen MusicManager-Software benutzen. Dabei übernimmt der MusicManager Funktionen sowohl des Windows Media Players als auch des Browsers.

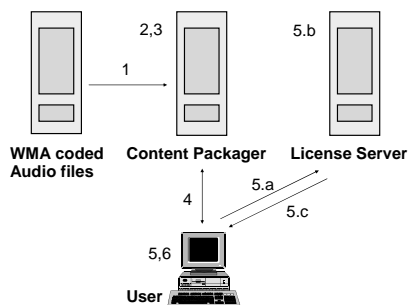


Abb 2: Das Prozessmodell von Windows Media Rights Manager

## 7 Datenspuren in WMRM

Während der Untersuchung des Systems anhand der in Kap. 3 vorgestellten Struktur wurden folgende Datenspuren entdeckt, die von Musicload mit WMRM gesammelt und gespeichert werden. Dabei stellt WMRM die Verfahren zur Verfügung, bestimmt selbst aber nicht, wie die Daten verwertet werden. Microsoft setzt auf flexible Gestaltungsoptionen, um den WMRM-Einsatz in vielen Shopszenarien zu ermöglichen.

### 7.1 Bei der Anmeldung

Während der Anmeldung muss der Kunde ein Formular ausfüllen, das folgende Pflichtfelder enthält:

- ◆ Name, Adresse;
- ◆ E-Mail-Adresse;
- ◆ Bezahlungsinformationen, z.B. Kreditkartennummer und Validierungsdaten; T-Pay-Zugangsdaten;
- ◆ Login und Passwort für den Zugang zu Musicload (Musicload-ID).

## 7.2 Während der Kommunikation

Während der Kommunikation werden systemseitig folgende Datenspuren gesammelt:

- ◆ Das vom Kunden benutzte Betriebssystem (Version, Sprache), die Browserversion und die IP-Adresse des Kunden aus dem HTTP-Protokoll;
- ◆ Cookies: bei Musicload werden Cookies von einer externen Firma (INFOline) gesetzt und analysiert, um Informationen über das Surf- und Einkaufsverhalten von Kunden herauszufinden;
- ◆ Informationen über die installierte Version des Windows Media Player;
- ◆ Es wird weiterhin eine geheime Client-ID (Hardware-ID) über Microsoftkomponenten abgefragt.

## 7.3 Vom Anbietersystem in das Produkt einkodiert

Mithilfe eines entsprechenden Editors wurden folgende Datenspuren gefunden:

- ◆ Produkt-ID, vom Shopperserver organisiert und vergeben;
- ◆ Weitere Metadaten über das Produkt: Titel, Genre, Jahr, Album, usw.

In der Lizenz, die vom WMRM ausgestellt und separat zum Produkt herunter geladen wird, finden sich weitere Informationen wie die Anzahl der erlaubten Exports und Brennvorgänge, Produkt-ID und Lizenz-Server-URL.

### 7.4 Vor Vertragsschluss

Wie auch bei iTunes muss sich der Kunde vor dem Kauf von Musikstücken bei Musicload registrieren. Dabei werden die oben im Abschnitt „Datenspuren bei der Anmeldung“ ermittelten Informationen übertragen. Eine explizite E-Mail-Verifizierung findet nicht statt. Der Nutzer kann einwilligen, ob Daten für Kooperations- und Werbezwecke von T-Online eingesetzt werden dürfen.

### 7.5 Bei Vertragsschluss

Ein registrierter Kunde wählt im Musicload-System Waren aus und hinterlegt sie in einem Warenkorb. Nach Anstoß des Kaufvorgangs kann er sich aus sechs Zahlungsverfahren eines auswählen. Je nach Zahlungssystem sind dann folgende Daten anzugeben:

- ◆ Bezahlung mit Kreditkarte: Kartentyp, Kartennummer, Gültigkeit und Kartenprüfzahl;
- ◆ T-Online Rechnung (für T-Online-Kunden): E-Mail-Adresse und Passwort von T-Online;
- ◆ T-Pay (für T-Com-Kunden): Vor- und Nachname, E-Mail-Adresse, Vorwahl und Telefonnummer, Telekomkundennummer; T-Pay-Nutzername und Passwort;
- ◆ Firstgate click&buy: Vor- und Nachname, Geburtsdatum, E-Mail-Adresse, Passwort, persönliche Frage und Antwort, postalische Anschrift mit Telefonnummer, Daten für Lastschrift oder Kreditkarte;
- ◆ Gutschein: Gutscheincode;
- ◆ HappyDigits: HappyDigits-Kartennummer und PIN.

Bei allen Zahlungsverfahren außer Kreditkarte wird der Nutzer auf die entsprechenden externen Seiten geleitet. Anschließend stellt der Lizenzserver eine Lizenz für den Content aus, die wiederum den Contentschlüssel enthält. Dieser wird mit der vorher vom System erhobenen geheimen Client-ID (Hardware-ID) verschlüsselt. Zusätzlich wird überprüft, ob eine aktuelle Version des Media Players sowie des Internet-Explorers vorliegt.

Vor dem Ausliefern des Produkts werden Produkt-ID, Apple-ID und Metadaten in das Stück einkodiert und das File anschließend symmetrisch verschlüsselt.

## 7.6 Überprüfen der Nutzungsrechte

Ein Nutzer-PC wird vor dem Ausstellen der Lizenz am Shopperserver mit seiner geheimen Client-ID registriert. Die Lizenz ist nur für dieses eine angemeldete Gerät gültig. Wenn Content und Lizenz beim Client zusammenpassen und die Lizenz nicht abgelaufen ist, kann der Inhalt konsumiert werden.

Das Stück kann nach dem Kauf auch offline verwendet und innerhalb von sechs Monaten beliebig oft herunter geladen werden. Die Lizenz hingegen darf insgesamt nur dreimal ausgestellt werden, so ist ein Abspielen auf bis zu drei verschiedenen Rechnern möglich. Wird diese Anzahl überschritten, muss sich der Nutzer an Musicload wenden. Microsoft empfiehlt die Lizenzen regelmäßig zu sichern. Wenn sie gelöscht wird, kann das Stück auf diesem Rechner nicht mehr verwendet werden.

## 7.7 Andere Zwecke

Wenn ein (registrierter) Kunde durch den Musicload-Shop surft, werden bestimmte Suchwörter und Produkt-IDs mit IP-Adressen, Cookies und Nutzerkonten verbunden.

Bereits gekaufte Stücke erscheinen in der Rubrik „Meine Downloads“. Weiterhin kann der Nutzer über „Mein Profil“ sowie „Mein Passwort“ seine Daten einsehen und ändern. Nach Auswählen der Stücke werden diese mittels Cookies in einem Warenkorb gespeichert.

## 7.8 Verborgene Schnittstellen und Funktionsverkettungen

An jedem Punkt der Kommunikation zwischen Client und Musicload-Server stehen sämtliche HTTP-Daten, wie z.B. Clickstreams, IP-Adresse, Sprache, HTTP-Referer („von welcher Seite der Kunde kommt“) und Suchanfrage-Wörter dem Shopserver zur Verfügung und können bei Kenntnis der Logindaten mit dem Daten-subjekt (Kunden) verknüpft werden.

Weitere Möglichkeiten bestehen durch die Verbindung von Musicload-ID und T-Online-ID, wenn man T-Online-Rechnung, T-Pay oder HappyDigits als Zahlungssystem verwendet. Des Weiteren werden Produkt-ID und Metadaten in das fertige Produkt einkodiert. Informationen über die Nutzungsmöglichkeiten werden in die Lizenz-Datei eingebracht.

## 8 Zusammenfassung und Empfehlungen

Um das Gesamtbild zu vervollständigen müssen weitere DRM-Systeme nach der gleichen Struktur analysiert und bewertet werden. Erst dieses Vorgehen erlaubt einen objektiven und transparenten Vergleich der Systeme. In der im Mai 2005 fertiggestellten und im Oktober veröffentlichten Studie (Bizer et al. 2005) werden iTunes, Musicload mit WMRM, Sonys Connect-Europe Shop mit OpenMG und das alternative

Distributionsmodell PotatoSystem untersucht und bewertet. Als Ergebnis können aktuelle DRM-Systeme wie folgt charakterisiert werden:

Sie sammeln mehr personenbezogene Daten als für den Kaufabschluss des vom Kunden gewählten Produktes nötig sind. Es existiert eine nicht geringe Anzahl von verborgenen und geheimen Schnittstellen, sowohl durch das Einbringen von personenbezogenen Daten in den Inhaltscode, als auch durch das Verbinden und Verketteten von Kundenverhaltensdaten und Kundenvertragsdaten.

Einerseits verwenden Online-Shops Informationen über ihre Kunden dazu, einen besseren Service anzubieten, indem sie z.B. Informationen über schon gekaufte oder angesehene Produkte anbieten (Matching-Features). Andererseits ist es nicht notwendig, diese Informationen mit tatsächlichen Kunden und ihrem Verhalten, Vorlieben oder persönlichen Beziehungen zu anderen Nutzern zu verknüpfen.

Verborgene Schnittstellen und im Inhalt versteckte persönliche Daten zeigen, dass Anbieter ihren Kunden nicht vertrauen. Die sogenannte „zweite Verteidigungslinie“ (z.B. durch Watermarking) ermöglicht eine Verfolgung von Kunden, die Produkte illegal weiter vertreiben. Aber mit dem generellen Einbringen von Kundendaten in Produkte werden alle Kunden gleichzeitig verdächtigt. Wenn dies intransparent, das heißt ohne Wissen der Kunden geschieht, verlieren diese umgekehrt das Vertrauen in die Shops, die damit ihr Ansehen bei den Kunden einbüßen.

Wir empfehlen neben dem Prinzip der Datensparsamkeit vor allem den transparenten Umgang mit den persönlichen Daten von Kunden. Wenn Kunden wissen, dass mit ihren Daten verantwortungsbewusst umgegangen wird und wenn sie ihren Vorteil erkennen, dann werden sie ihre korrekten Daten zur Verfügung stellen. Wenn nicht, dürfen die Daten ohnehin nicht verwendet werden.

## Literatur

Becker, E.; Buhse, W.; Günnewig, D.; Rump, N. (2003): Digital Rights Management.

Technological, Economic, Legal and Political Aspects. Springer Lecture Notes 2770, Springer, Berlin etc. 2003.

Bizer, J.; Grimm, R. Will, Andreas; Möller, J.; Puchta, S.; Müller, A.; Müller, M. (2005): Privacy4DRM – Datenschutzverträgliches und nutzungsfreundliches Digital Rights Management. Studie im Auftrag des Bundesministeriums für Bildung und Forschung (BMBF). [www.bmbf.de/pub/privcy4drm\\_studie.pdf](http://www.bmbf.de/pub/privcy4drm_studie.pdf) [download 31.12.2005].

EU (1995): Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. [www.cdt.org/privacy/eudirective/EU\\_Directive\\_.html](http://www.cdt.org/privacy/eudirective/EU_Directive_.html) [download 19 Dec 2005]

Grimm, R., Aichroth, P. (2004): Privacy Protection for Signed Media Files: A Separation-of-Duty Approach to the Lightweight DRM (LWDRM) System. Proc. ACM Multimedia and Security Workshop 2004, Magdeburg, Germany, September 2004.

iTunes Music Store (2005): Überblick über Musikangebot und „Apple Strategie zum Schutz der Persönlichkeitsrechte“ [www.apple.com/de/itunes/music/](http://www.apple.com/de/itunes/music/), [www.apple.com/de/legal/privacy/](http://www.apple.com/de/legal/privacy/) [download 19 Dec 2005]

Microsoft (2005): Resource for developers using Microsoft tools, products, and technologies. [www.msdn.microsoft.com/library/](http://www.msdn.microsoft.com/library/) [download 19 Dec 2005]

Musicload (2005): The Musicload Factsheet of 05.04.2005 ([www.musicload.de](http://www.musicload.de)) with reference to the 2004 Digital Music Report of the International Federation of the Phonographic Industry (IFPI).

Möller (2005): Datenschutzanforderungen an Digital Right Management Systeme (DRM), DuD 2/2006 (in diesem Heft).

Rosenblatt, B.; Trippe, B.; Mooney, S. (2002): Digital Rights Management – Business and Technology. M&T Books, Hungry Minds Inc., New York, 2002, 288 pages.

T-Pay (2005): The payment system of T-Online. [www.t-pay.de](http://www.t-pay.de) [download 19 Dec 2005]

US Department of Commerce (2005): Safe Harbor. [www.export.gov/safeharbor/](http://www.export.gov/safeharbor/) [download 19 Dec 2005].