Jürgen Nützel

Die informatorischen Aspekte virtueller Güter und Waren

Die informatorischen Aspekte virtueller Güter und Waren

Von Jürgen Nützel

Universitätsverlag Ilmenau
2006

Impressum

Bibliographische Information der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Angaben sind im Internet über http://dnb.ddb.de abrufbar.

Diese Arbeit hat der Fakultät für Informatik und Automatisierung 2005 als Habilitationsschrift vorgelegen.

Technische Universität Ilmenau/Universitätsbibliothek
Universitätsverlag Ilmenau
Postfach 10 05 65
98684 Ilmenau
www.tu-ilmenau.de/universitaetsverlag

Herstellung und Auslieferung
Verlagshaus Monsenstein und Vannerdat OHG
Am Hawerkamp 31
48155 Münster
www.mv-verlag.de

ISBN 3-939473-04-9

Danksagung

Die vorliegende Arbeit entstand während meiner Tätigkeit als wissenschaftlicher Assistent am Fachgebiet Rechnerarchitektur des Institutes für Theoretische und Technische Informatik der Technischen Universität Ilmenau. Mit diesem vorangestellten Kapitel möchte ich allen danken, die zum Zustandekommen dieser Arbeit maßgeblich beigetragen haben.

An erster Stelle möchte ich dem Leiter des oben genannten Fachgebietes Prof. Dr.-Ing. habil. Wolfgang Fengler danken. Er hat in mehrfachem Sinne dazu beigetragen, dass diese Arbeit zustande kam. Nach der Verteidigung meiner Dissertation auf dem Gebiet des objektorientierten Entwurfes eingebetteter Systeme [Nützel 99] bot er mir Mitte 1999 die Möglichkeit an, im gleichen Fachgebiet eine Habilitationsschrift zu bearbeiten. Er tolerierte und ermöglichte meine Entscheidung die eingebetteten Systeme wissenschaftlich zu verlassen und mit der Gründung der 4FO AG im Sommer 2000 die Forschung auf das Gebiet der virtuellen Güter zu fokussieren. Er motivierte mich erfolgreich, trotz meiner kommerzieller Bestrebungen nicht die wissenschaftliche Arbeit zu vernachlässigen. Natürlich möchte ich Dr. Bernd Däne – meinem langjährigen Kollegen am Fachgebiet – für die geduldige Beantwortung auch außergewöhnlicher Fragen danken.

Zu besonderem Dank bin ich Prof. Dr. phil.-nat. Rüdiger Grimm verpflichtet. Als Experte auf dem Gebiet von Bezahlsystemen und als Gruppenleiter beim damals noch als Arbeitsgruppe firmierten Fraunhofer IDMT eröffnete er mir ab 2002 völlig neue Möglichkeiten auf den Gebiet der virtuellen Güter. Und dies sowohl in wissenschaftlicher Hinsicht durch gemeinsame Veröffentlichungen, als auch in Hinblick auf die praktische Umsetzung, durch die Zusammenarbeit mit Fraunhofer IDMT. Seine Art und Weise komplexe Sachverhalte zu kommentieren, ermöglichte es mir, vielen Abschnitten der Arbeit die notwendige Schärfe und Klarheit zu verleihen. Die Zusammenarbeit mit Rüdiger brachte nicht nur in der bearbeiteten Thematik interessante Resultate, auch meine prinzipielle Herangehensweise bei der Bearbeitung ähnlicher Fragen konnte dabei an Schärfe gewinnen. Nicht vergessen möchte ich, mich für die Bereitschaft von Prof. Dr. habil. Günther Pernul, sich als kritischer Gesprächspartner für die Arbeit zur Verfügung zu stellen, zu bedanken.

Besonders möchte ich auch den beiden leitenden Mitarbeitern des Fraunhofer IDMT Prof. Karlheinz Brandenburg und Dr. Thomas Sporer danken. Sie erkannten sehr früh, dass die alternativen Ansätze, die in dieser Arbeit behandelt werden, auch zum Patent angemeldet und umgesetzt werden sollten. Auch den Mitarbeitern des Fraunhofer IDMT gilt mein Dank für die fruchtbaren Diskussionen, speziell Patrick Aichroth, Henning Köhler, Stefan Puchta, Matthias Kaufmann und Jens Hasselbach. Der zuletzt genannte wurde von mir auch als Diplomand betreut.

Schließlich möchte ich allen Studenten danken, die im Rahmen der von mir betreuten Hauptseminare, Studien- und Diplomarbeiten zur prototypischen Untermauerung der vorliegenden Arbeit beigetragen haben. Den Auftakt bildeten die beiden Diplomarbeiten von Holger Krauß und Jens Hasselbach. Es folgten die Arbeiten von

Gabriele Frings und Frank Zimmermann, die beide schon in ihrer Studienarbeit wichtige Anteile lieferten. Es folgten Diplomarbeiten von Dirk Behrendt, Oliver Lorenz, Michael Kunze, Jeannine Emer, Tobias Weiß und André Hartmann. Hierbei gilt mein besonderer Dank Oliver Lorenz. Die noch nicht fertig gestellte Arbeit von Mario Kubek bildet den Abschluss. Besonderer Dank gilt auch Kathleen Biedermann, die mit Ihrer Studienarbeit wichtige Fragen aus den durch diese Arbeit tangierten Fachgebieten der Wirtschaftswissenschaften klären konnte.

Nicht vergessen möchte ich die Mitarbeiter der 4FO AG Marko Langbein, Stefan Richter und Frank Zimmermann, ohne die eine praktische Umsetzung der behandelten Konzepte nicht möglich gewesen wäre.

Last but not least will ich an dieser Stelle meiner Familie meinen besonderen Dank aussprechen. Nicht nur weil meine Frau Margit mit mir den Kampf gegen den Fehlerteufel und meine Schachtelsätze aufgenommen hat, sondern weil sie auch in besonders anstrengenden und schwierigen Phasen zu mir und meiner Arbeit gehalten hat. Für sie, meine Tochter Laura und meinen Sohn Sebastian hoffe ich, dass ich nun wieder die Wochenenden für sie frei habe.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1. Kapitel

Einleitung und Motivation

Die informatorischen Aspekte virtueller Güter und Waren umschreiben einen neuartigen Teilbereich der Informatik, der stark interdisziplinär geprägt ist. Im Mittelpunkt dieses Teilbereichs stehen Verfahren und Systeme, die die technischen Voraussetzungen schaffen, dass aus virtuellen Gütern virtuelle Waren werden können. Es geht folglich um die technische Realisierung von bekannten und neuartigen Geschäftsmodelle für virtuelle Waren.

Virtuelle Waren stellen durch ihre Digitalisierbarkeit eine neue Warengruppe mit eigenen Gesetzmäßigkeiten dar. Dadurch, dass die Nutzdaten, welche die virtuellen Waren vollständig verkörpern, unbegrenzt, verlustlos und dazu noch nahezu kostenfrei kopierbar sind, stellen diese Nutzdaten für viele Konsumenten kein seltenes und knappes Gut mehr dar. In den Augen vieler Konsumenten ist der subjektive Wert der Nutzdaten gegenüber Nutzdaten, die an einen physikalischen Datenträger gebunden sind, stark vermindert. Die Absicht diesen Wert wieder zu erhöhen, indem durch technische Maßnahmen wie DRM die Kopierbarkeit der Nutzdaten eingeschränkt wird, verkehrt sich oft ins Gegenteil, denn viele Konsumenten empfinden gerade die verlustlose Kopierbarkeit zwischen unterschiedlichen Endgeräten als den eigentlichen Zusatznutzen.

Der Schwerpunkt der Arbeit trägt dieser Erkenntnis Rechnung und befasst sich der Umsetzung eines alternativen Geschäftsmodells, welches nicht versucht ein direktes Erlösmodell durch Kontroll- und Verhinderungstechniken abzusichern. Es baut dagegen auf ein neuartiges Anreizsystem auf, welches Käufer zu Weiterverkäufern macht.

Die Umsetzung von Geschäftsmodellen für virtuelle Waren erfordert neben der Kenntnis der Verfahren aus der Medien- und angewandten Informatik auch das Verständnis wirtschaftswissenschaftlicher Zusammenhänge. Die vorliegende Arbeit stellt sich dieser interdisziplinären Herausforderung.

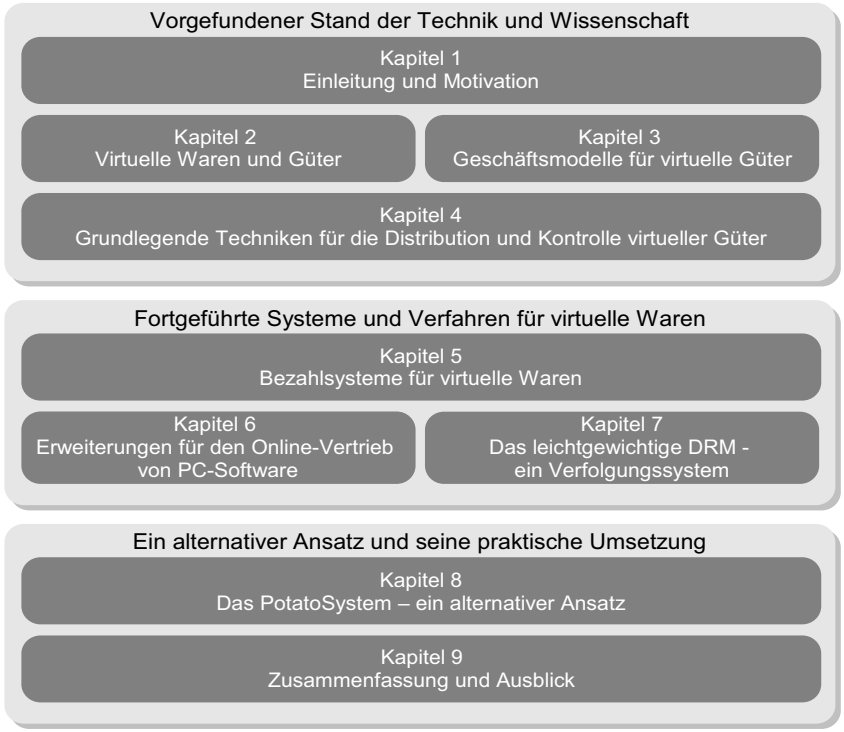
Aufbau und Struktur

Abbildung 1.1 zeigt die Struktur der vorliegenden Arbeit, die sich in drei Hauptblöcke gliedert. Der erste Block, mit den Kapiteln 1 bis 4 befasst sich mit dem vorgefundenen Stand der Technik und Wissenschaft. Nach dem Kapitel 1: „Einleitung und Motivation“ macht das Kapitel 2 den Leser mit virtuellen Gütern und Waren vertraut. Die dortigen Definitionen für virtuelle Güter und Waren verdeutlichen bewusst den Unterschied zu digitalen Gütern. Nicht die Nutzdaten, die die virtuellen Güter repräsentieren können, stehen im Vordergrund, sondern der menschliche Nutzer, der die virtuellen Güter konsumiert, bildet den Kern der Begriffsbildung.

Der Begriff Ware umfasst einen wichtigen Aspekt dieser Arbeit, hier besonders die technische Realisierung von Geschäftsmodellen, bei denen der Konsument der virtu-

elle Ware die Erlösquelle darstellt. Kapitel 3 liefert Grundlagen für wichtige Begriffe und Definitionen aus den Wirtschaftswissenschaften, die nicht zu den Kerngebieten der Informatik gehören, aber für das Verständnis der Arbeit unverzichtbar sind. Die Betonung liegt hier auf den geringen Grenzkosten und der Subjektivität des Gebrauchswerts, wodurch die Preisfindung speziell bei virtuellen Waren erschwert wird.

Abbildung 1.1
Struktur der vorliegenden Arbeit



Anschließend schildert Kapitel 4 ausführlich grundlegende Techniken für die Distribution und Kontrolle virtueller Güter. Die Nutzdaten repräsentieren die virtuellen Güter. Sie können nur mittels spezieller Endgeräte konsumiert werden, die deshalb den Ausgangspunkt der Beschreibung bilden. Neben Verfahren wie Peer-to-Peer-Systeme, die die Verbreitung der Nutzdaten über das Internet auf diese Endgeräte erleichtern, liegt der Schwerpunkt ebenso auf Techniken, die die unkontrollierte Verbreitung verhindern können. Hierzu zählen kryptographische Verfahren und komplexe Systeme, die unter dem Begriff *Digital Rights Management* (DRM) zusammengefasst werden. DRM wird aktuell in der Öffentlichkeit sehr kontrovers diskutiert und bildet einen zentralen Aspekt dieser Arbeit.

Im zweiten Hauptblock (Kapitel 5 bis 7) werden Systeme und Verfahren vorgestellt, die der Autor mitgeprägt hat. Kapitel 5 befasst sich mit Bezahlsystemen, wel-

che auch den Schwerpunkt dieses Blockes bilden. Der Autor leitet das Kapitel bewusst mit dem provozierenden Zitat: „*if you can't bill it, kill it*“ ein. Es verdeutlicht drastisch die Wichtigkeit funktionierender und gleichzeitig vom Nutzer akzeptierter Online-Bezahlsysteme. Denn nur so können direkte Erlöse erzielt werden. Neben dem Stand der Technik dieses Gebietes wird auch das selbst entwickelte Bezahlsystem Paybest erläutert.

Kapitel 6 beschreibt ein für den Online-Vertrieb von PC-Software mit dem Schwerpunkt auf PC-Spiele entwickeltes spezielles Schutzsystem. Die Entwicklung dieses patentierten Systems mit dem Namen Game-Feature-Plattform (GFP) bildete den Auftakt für die Arbeiten des Autors im Bereich der virtuellen Güter. In direkter Folge wurde das Bezahlsystem Paybest entwickelt. Kapitel 7 wird das alternativ zum Kopierschutz entwickelte LWDRM-System vorgestellt, welches die illegale Weitergabe von Kopien durch deren technische Rückverfolgbarkeit begrenzen möchte.

Die GFP und das LWDRM-System stehen in Kontrast zum im dritten Block in Kapitel 8 beschriebenen PotatoSystem. Das PotatoSystem stellt einen vollkommen neuen und eigenständigen Ansatz dar, bei dem für die Umsetzung eines Geschäftsmodells nicht auf technischen Kontroll- oder Verhinderungsmaßnahmen gesetzt wird, sondern primär auf Anreizmechanismen. Kerngedanke des ebenfalls zum Patent angemeldeten PotatoSystems ist es, Käufer zu Weiterverkäufer zu machen, damit diese ein eigenes finanzielles Interesse am legalen Vertrieb der virtuellen Waren entwickeln. Kapitel 8 schildert nicht nur das Grundprinzip, sondern auch das bereits im kommerziellen Einsatz befindliche komplette Client-Server-System des PotatoSystems.

Kapitel 9 schließt diese Arbeit mit einer Zusammenfassung und dem Ausblick auf weitere Forschungen, die ebenso wie das PotatoSystem die Umsetzung alternativer Geschäftsmodelle zum Ziel haben.

2. Kapitel

Virtuelle Waren und Güter

Bevor technische Verfahren und Systeme behandelt werden können, muss zuallererst geklärt werden, was überhaupt *virtuelle* Güter sind, bzw. was der der Autor darunter versteht. Ausgangspunkt der Betrachtung sind die *realen* Güter und Waren. Der Leser wird sehr schnell erkennen, dass die Auswirkungen bzw. Effekte der Digitalisierung eine entscheidende Rolle bei der Virtualität spielen. Oberflächlich könnte man sagen, dass virtuelle Güter digitale Daten sind. Allerdings wird vom Menschen nicht jedes Datenpaket als begehrliches Gut betrachtet. Der Autor macht einen deutlichen Unterschied zwischen den Begriffen digital und virtuell. Der Begriff Information wird hierbei zur Erläuterung herangezogen. Virtuelle Güter können durch digitale Daten, den Nutzdaten, repräsentiert werden. Jedoch sind nicht alle digitale Daten virtuelle Güter.

Ausgehend von grundlegenden Definitionen können weitere Einteilungen und Klassifizierungen vorgenommen werden. Die Basis für diese grundlegenden Definitionen wurden erstmals in [GriNüt 02b] erörtert. Hier wurde ein erster Versuch unternommen, virtuelle Waren bzw. virtuelle Güter zu definieren. Es wurde dabei die Unabhängigkeit virtueller Waren von einer physikalischen Fixierung in den Mittelpunkt gestellt. Der Begriff Ware steht immer dann gegenüber dem Begriff Gut im Vordergrund, wenn Techniken und Verfahren zur Vermarktung virtueller Güter im Fokus stehen.

Bei virtuellen Gütern steht der Mensch als Konsument im Mittelpunkt der Betrachtung. Begriffe wie Konsumierbarkeit, Mehrfachkonsumierbarkeit und Interaktivität können zur Differenzierung herangezogen werden. Der Autor spricht von vollständig virtuellen Gütern und Waren, wenn dieses über ein Endgerät *vollständig* konsumiert werden können. Der gesamte Gebrauchswert erschließt sich dem Nutzer dabei durch diesen Konsumvorgang.

2.1 Was sind virtuelle Waren bzw. virtuelle Güter?

Bevor auf das Virtuelle an den Waren bzw. Gütern eingegangen werden kann, muss zuerst klar gestellt werden, was überhaupt *reale* Waren und Güter sind. Der Begriff Gut lässt sich dabei einfach umschreiben: Ein Gut ist für einen Menschen zu Etwas gut. Es hat einen Gebrauchswert (vgl. auch Kapitel 3.4). Das Englische Wort für Güter lautet *Goods*. Bei der Umschreibung des Wortes werden bereits ökonomischen Aspekte deutlich:

> *possessions which can be moved, not houses, land, etc.; articles for sale; [LangLong 84]*

Dieser noch sehr vage Bezug zur Ökonomie wird beim Begriff Ware noch deutlicher:

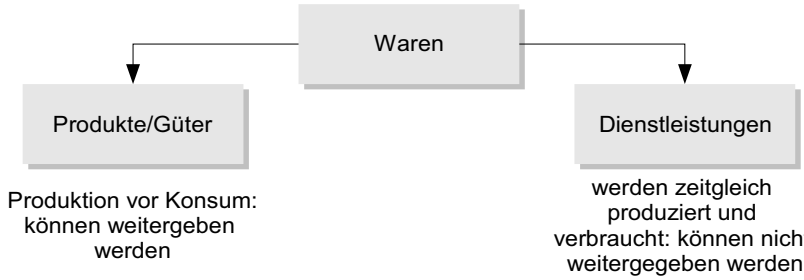
> *„Waren sind Produkte oder Dienstleistungen, die auf einem Markt einen bestimmten Preis erzielen." [Gabler 04]*

Diese Definition unterstreicht, dass es hier nicht nur um Produkte bzw. Güter, sondern auch um Dienstleistungen geht, die zum Zwecke ihrer Kommerzialisierungen existieren.

2.1.1 Produkt oder Dienstleistung?

Reale Produkte können weitergegeben oder aufgebraucht werden. Diese Begriffswelt ist zum Beispiel bei Nahrungsmitteln, Kleidungsstücken, einem Auto oder bei Trinkwasser klar und einsichtig. Bei Dienstleistungen ist dies anders. Eine Dienstleistung ist eine Ware, deren Verbrauch zeitgleich mit ihrer Produktion vonstatten geht [Gabler 04]. Dienstleistungen können nur in Anspruch genommen werden. Indem man sie hat, sind sie schon vergangen. Man kann sie nicht besitzen bzw. weitergeben [GriNüt 02a]. Abbildung 2.1 macht die beiden Ausprägungen von Waren in der Welt realer Waren deutlich.

Abbildung 2.1
Die zwei Ausprägungen von Waren in der „realen" Welt



Im Gegensatz zu Dienstleistungen, kann man reale Produkte bzw. reale Güter auch weitergeben, da sie nicht schon dadurch verbraucht werden, dass man sie hat.

2.1.2 Was bedeutet virtuell?

Durch das Adjektiv *virtuell* wird das Thema der Arbeit abgegrenzt. Es geht explizit nicht um Informatiksysteme für reale Güter bzw. Waren. Die Arbeit beschränkt sich auf die Informatiksysteme, die für die Vermarktung virtueller Waren zum Einsatz kommen.

Was bedeutet nun *virtuell*? Virtuell meint nicht real, nicht körperlich existent, nur ausgedacht. In [GriNüt 02a] wurde ein erster Versuch für eine Definition virtueller Waren vorgenommen:

> *„Eine Ware (Produkt oder Dienstleistung) ist virtuell, wenn sie von ihrem ursprünglichen physikalischen Medium losgelöst ist und an ein anderes Medium derart gebunden ist, dass sie (a) vom Menschen als virtuelles Abbild einer realen Ware erkannt und akzeptiert wird, und dass (b) ihr Konsum allein in der Wahlfreiheit des Konsumenten liegt, d. h. vom Produzenten unabhängig und wiederholbar ist."*

Musik ist ein sehr gutes Beispiel für eine virtuelle Ware. Das physikalische Medium, an das Musik gebunden ist, ist die Luft, und die Bindung geschieht (in diesem Falle flüchtig) durch die Schallwellen in der Luft. Verschiedene andere Medien für Musik, wie eine Schallplatte, eine Kompaktkassette oder eine Audio-CD machen deutlich, dass Musik auch dann hörenswerte Musik bleibt, wenn sie zwischenzeitlich an die unterschiedlichsten Medien gebunden war. Die Definition macht allerdings noch eine zusätzliche Abgrenzung: Der Musikkonsum soll wahlfrei wiederholbar durch den Konsumenten sein. Da diese Einschränkung sehr unscharf ist, soll sie in Folge nicht weiter zur Definition virtueller Waren herangezogen werden.

In der Definition wurde bewusst die virtuelle Ware unabhängig von einer möglichen Digitalisierung definiert. Die Virtualität bezeichnet dabei den grundlegenden Charakter (virtuelle Waren stehen im Gegensatz zu realen Waren) und die digitale Kodierung wird als die primäre Realisierungsform der Virtualität verstanden. Man kann virtuelle Waren aber auch als digitalisierbare oder digital kodierbare Waren bezeichnen:

> *Ein Ware ist virtuell, wenn sie digitalisiert ist oder auf dem Weg zum Konsumenten digitalisiert werden kann, ohne dass sie aus Sicht des Konsumenten dadurch in ihrer Qualität gemindert wird.*

Abbildung 2.2
Virtuelle Waren können digital dargestellt werden

Abbildung 2.2 zeigt schematisch den Schritt der Digitalisierung bzw. Kodierung. Das Ergebnis dieses Schrittes sind die Nutzdaten, die die virtuelle Ware in digitaler Form repräsentieren. Die virtuelle Ware (bspw. Musik) kann digitalisiert werden. Der typische Konsument wird es nicht merken, dass die Musik auf dem Weg an sein Ohr

zwischenzeitlich als digitale Nutzdaten vorlag. Für andere reale Güter wie bspw. Nahrung und Kleidung, kann man sich zur Zeit keine digitale Kodierung vorstellen, deren Ergebnis potentielle Konsumenten zufrieden stellen könnte.

■ Virtuelle Produkte versus virtuelle Dienstleistungen

Im Gegensatz zu den realen Waren ist bei den virtuellen Waren die Aufteilung in Produkt oder Dienstleistung sehr schwer. Musik ist ein gutes Beispiel, um dieses Problem deutlich zum machen. Musik war vor ca. 150 Jahre primär eine Dienstleistung des Musikers am Publikum. Nach der Erfindung des Phonographen [WikiPhono 04] durch Thomas Alva Edison im Jahre 1877 und des Grammophons durch Emile Berliner [LICBerliner 02] im Jahre 1887 wurde sie zu einem medial fixierten (bzw. fixierbaren) Gebrauchsgut. Es folgten hundert Jahre, in der eine „Industrie“ Musik wie eine reale physikalische Ware vertrieb. Dank moderner Kompressionstechniken und des Internets entwickelte sich Musik Ende der Neunziger Jahre des letzten Jahrhunderts wieder zu einer Dienstleistung zurück. Bei dieser neuen Form der Dienstleistung liefert ein Anbieter im Internet die Musik auf Abruf in digitaler Form [NütKau 04]. Virtuelle Waren lassen sich oft nicht eindeutig einer der beiden Kategorien Produkt oder Dienstleistung zuordnen. Prinzipiell könnte alles digital kodierte wie ein reales Produkt weitergegeben werden. Diese Eigenschaft wird aber oft vom Anbieter durch zusätzlich technische Maßnahmen eingeschränkt, um dem Konsumenten virtuelle Waren wie eine Dienstleistung, die man nicht weitergeben kann, anbieten zu können.

■ Virtuelle Güter versus virtuelle Waren

Die Begriffe *virtuelle Güter* und *virtuelle Waren* werden in dieser Arbeit häufig synonym gebraucht. Alle virtuellen Waren sind schließlich auch virtuelle Güter. Wird explizit von virtuellen Waren gesprochen, so soll der kommerzielle Aspekt virtueller Güter unterstrichen werden.

2.2 Information und konsumierbare Nutzdaten

Der Begriff Information kann zusätzlich das thematische Umfeld virtueller Güter beschreiben. Es kann hierüber der Vorgang des Konsumierens (bzw. Kommunizierens) virtueller Güter genauer gefasst werden. Der Konsum eines virtuellen Gutes wird in den Kommunikationswissenschaften auch als Kommunizieren bezeichnet. Allerdings soll auch nicht verschwiegen werden, dass Information ein grundlegender Begriff ist, der je nach Wissenschaftsgebiet unterschiedlich definiert oder interpretiert wird. Nachrichtentechniker definieren Information bspw. wie folgt:

> *Information ist eine zielgerichtete, für den Empfänger verständliche Mitteilung, insbesondere über Werte und Größen [LiBrLe 86 S.379]*

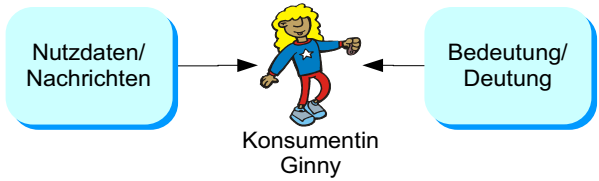
Verschiedene andere Wissenschaftsgebiete neben der Nachrichtentechnik betrachten die Information ebenfalls als ihr Arbeitsgebiet, namentlich die Informatik, die Informationswissenschaft und die Informationsökonomik. Sowohl in der Naturwissenschaft, besonders in der Physik und Biologie, als auch in der Philosophie (Semiotik, Rhetorik, Linguistik) und Sozialwissenschaft (Politik, Publizistik, Kommunikationswis-

senschaft) stellt der Begriff der Information einen wichtigen Untersuchungsgegenstand dar. Ihre Ansätze unterscheiden sich zum Teil erheblich. Erst in jüngster Zeit gibt es Bestrebungen, die einzelnen Ansätze zu verbinden und zu einem allgemeingültigen Informationsbegriff zu verbinden. Von einer vereinheitlichten Theorie der Information kann vorläufig noch nicht gesprochen werden [WikiInfo 04].

Information ist vom Menschen mit Bedeutung versehene Nachricht (vgl. Abbildung 2.3) oder Kenntnis über Sachverhalte. In die gleiche Richtung weist die Definition für Information aus der Norm ISO/IEC 2382-1 [ISO2382]:

> *„Knowledge concerning objects, such as facts, events, things, processes, or ideas, including concepts, that within a certain context has a particular meaning“.*

Abbildung 2.3
Information entsteht aus einer Nachricht erst, wenn die Konsumentin ihr eine Bedeutung zuordnet



Für viele ist Information schlicht die Beseitigung einer Ungewissheit beim Empfänger. Information ist eine vom Menschen gedeutete Nachricht. Der Begriff Information wird bspw. von Peter Rechenberg in [Rechenberg 03] wie folgt beschrieben:

> *„Die Nachricht ist hier etwas Objektives, das durch ein Medium (Draht, elektromagnetische Wellen) unverfälscht oder verfälscht übertragen werden kann, die Information dagegen etwas Subjektives, das erst durch den Empfänger entsteht, indem er der erhaltenen Nachricht eine Bedeutung beilegt.“*

2.2.1 Informationstheorie

Im allgemeinen Sprachgebrauch sowie in einigen Wissenschaften (Semiotik, Informationswissenschaften) wird „Information“ mit „Bedeutung“ oder „übertragenem Wissen“ gleichgesetzt. Eine mehr technische Sichtweise des Begriffes Information stammt aus der Nachrichtentechnik und ist heute von großer praktischer Bedeutung. Die wegweisende Theorie hierzu stammt von Claude Shannon [Shannon 48]. Er betrachtet Information erst einmal völlig unabhängig von jeglicher Bedeutung und Deutung. Ihn interessierten primär die statistischen Aspekte wie die Unterscheidbarkeit von Zuständen. Das unmittelbare Ziel seiner Überlegungen war die optimale technische Übertragung von Information in einem Nachrichtenkanal.

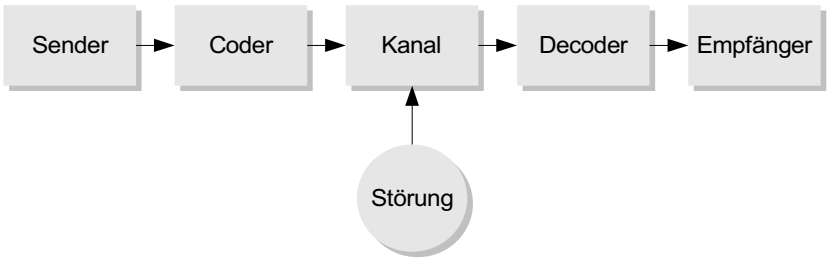
Da virtueller Güter auch unabhängig von ihrer semantischen Deutung durch den Menschen eine effektive technische Repräsentation benötigen, wird im folgenden die Shannon'sche Informationstheorie kurz dargestellt (vgl. auch [Völz 87]). Die binäre Kodierung bzw. Digitalisierung stehen dabei im Mittelpunkt. Was bedeutet aber digitalisieren und kodieren bzw. was bedeutet digital? Und in welchem Zusammenhang steht dazu der Begriff Information?

2.2.1.1 Das Kanalschema

Die Grundfragen, die Claude E. Shannon in den 40er Jahren des 20. Jahrhunderts bearbeitete, stammen aus der technischen Nachrichtenübermittlung. Folgende Fragen, die sich alle um den Nachrichtenkanal drehen, stellten sich dem Forscher damals:

- Wie sieht der kürzeste binäre (digitale) Code aus, um eine gegebene Nachricht über einen ungestörten Kanal zu übertragen?
- Kann man bei einem gestörten Kanal Nachrichten binär so kodieren, dass der Empfänger sie dennoch decodieren kann?
- Wie stark darf dieser Kanal dann höchstens gestört sein, damit die Nachricht noch korrekt decodiert werden kann?

Abbildung 2.4
Kanalschema nach Shannon [Völz 87]



Nach Shannon besteht der Nachrichtenkanal aus fünf Systemen (vgl. Abbildung 2.4): Die vom Sender ausgehenden Signale, die die Nachricht darstellen werden im Coder (bzw. Encoder) so umgewandelt, dass sie dem Übertragungszweck über einen möglicherweise gestörten Kanal optimal angepasst sind. Alle Störungen bis hierher und die im Decoder auftretenden werden als Störquelle dem Kanal zugeordnet. Im Decoder wird die Kodierung wieder rückgängig gemacht. Bei kontinuierlichen Signalen spricht man nicht von Kodierung sondern von Modulation. Der Empfänger erzeugt schließlich wieder das Ursprungssignal bzw. die zu übertragende Nachricht [Völz 87].

Da das gezeigte Kanalschema sehr universell ist, wird es im weiteren Verlauf der Arbeit in abgeänderter Form auch immer wieder erscheinen.

2.2.1.2 Informationsgehalt bzw. Entropie

Als reziprokes Maß der Information gilt in der Informationstheorie von Shannon die Wahrscheinlichkeit ihres Auftretens: Je wahrscheinlicher die Ausprägung (der Inhalt) eines Signals bzw. einer Nachricht, das diese Information ausdrückt, desto geringer ist der Informationsgehalt und umgekehrt.

Hierfür wurde der Begriff der Entropie in [Shannon 48] eingeführt. Die von Shannon eingeführte Entropie bezieht sich nicht auf eine individuelle Nachricht (bspw. ein Satz in deutscher Sprache) sondern auf eine Informationsquelle als Ganzes (bspw.

die deutsche Schriftsprache). Shannon und Weaver haben überhaupt strikt vermieden, individuellen Nachrichten einen numerischen Informationswert zuzuordnen (solche Versuche gab es erst später, allerdings ohne weitere Wirkung) [Grimm 04b]. Über die Definition der Entropie einer Informationsquelle gelangen wir zur optimalen digitalen Kodierung von Information (den Nutzdaten). Nach [Shannon 48] ist die Entropie die maximale Anzahl der Ja-Nein-Entscheidungen, die im zeitlichen Mittel über eine längere Zeit benötigt werden, um ein unbekanntes Signal beim Empfänger zu erkennen und einzuordnen. In der Formel 2.1 ist die Entropie *H* einer gegebenen Informationsquelle *I* über einem Alphabet *Z* definiert, wobei p_j die Wahrscheinlichkeit ist, mit der das j-te Symbol z_j des Alphabets *Z* in einem „typischen" Informationstext der Quelle *I* auftritt. *H* multipliziert mit der Anzahl der Zeichen eines konkreten Informationstexts ergibt dann die mindestens notwendige Anzahl von Bits, die zur Darstellung dieses Texts notwendig sind [WikiEntropie 04]. Deshalb wird die Entropie in Bits/Symbol angegeben.

Formel 2.1

$$Entropie \;=\; H(I) \;=\; -\sum_{j=1}^{|Z|} p_j \cdot \log_2 p_j$$

Wären die Buchstaben in einem Text gleichwahrscheinlich, so hätte jeder Buchstabe einen Informationsgehalt (Entropie) von 4,755 Bit (bei 26 Buchstaben und einem Leerzeichen: 4,755 = $\log_2 27$). Man müsste im Mittel 4,755 Ja-Nein-Fragen stellen, um einen Buchstaben zu bestimmen. Die erste Frage würde dabei jeweils lauten: Liegt der Buchstabe in der ersten Hälfte des Alphabets? Bei deutschen Texten liegt der Mittelwert, da nicht alle Buchstaben gleichwahrscheinlich sind, jedoch nur bei 4,037 Bit (natürlich gilt das analog auch für andere Sprachen). Man würde also besser zuerst fragen: Ist der Buchstabe ein Vokal? Nimmt man noch das Umfeld eines einzelnen Buchstabens hinzu, so sinkt der Entropie-Wert auf ca. 1,6 Bit/Buchstabe (ab ca. 10 Zeichen). Zum Beispiel ist die Wahrscheinlichkeit, dass im Deutschen nach einem S ein C oder ein T folgt sehr hoch. Durch solche statistischen Abhängigkeiten sinkt der Entropiewert der deutschen Schriftsprache ab. Eine optimale Kodierung für deutsche Texte müsste dies berücksichtigen. Umgekehrt weist Shannon mit Recht darauf hin, dass die in den Schrift- und Lautsprachen hohen Redundanzen dazu dienen, Störungen bei der Übermittlung zu überstehen. Eine Rede versteht man eben auch dann noch ganz gut, wenn sie geflüstert wird, und den Sinn eines Textes versteht man, selbst wenn man ihn nur überfliegt. Shannons Theorie zeigt präzise auf, welchen Grad an Redundanz man bei der Kodierung einer Schriftsprache (oder anderer Informationsquellen) einführen muss, damit übermittelte Texte ein gegebenes Störmaß verlustfrei überwinden.

Prinzipiell könnte man die Kodierung noch weiter optimieren. Dies verlangt allerdings, dass Empfänger und Sender sich noch weiter vorab absprechen. Sender und Empfänger könnten sich bspw. auf einen beschränkten Satz von 32 Witzen vorab einigen. Es würde in Folge genügen eine 5 Bit Zahl über den Kanal zuschicken. Der Decoder würde zu dieser Zahl aus einer gespeicherten Tabelle den entsprechenden gespeicherten Witz abrufen.

Ob die übertragene 5 Bit lange Nachricht (5 Bit Nutzdaten) für den menschlichen Empfänger eine verwertbar (konsumierbare) Information bzw. virtuelles Gut verkörpert hängt davon ab, ob die Nachricht korrekt (im Decoder) decodiert bzw. (im Empfänger) gedeutet werden kann.

2.2.2 Bedeutungsgehalt von Information

Shannon hat in seinen Überlegungen sich ausschließlich mit der technischen Frage der optimalen Kodierung von Nachrichten befasst. Der heutige Informationsbegriff geht aber über die Ebene der Kodierung hinaus. Der Begriff der Information wird hierbei gemäß der Semiotik – der Lehre von den Zeichen, Zeichensystemen und Zeichenprozessen – in vier aufeinander aufbauenden Ebenen aufgeteilt (vgl. Tabelle 2.1).

Die Ebenen steigern sich im Hinblick auf den Bedeutungsgehalt der Information von der Kodierungs-Ebene bis hin zur Pragmatik-Ebene. Die Kodierungs-Ebene ist Gegenstand der Nachrichtentechnik, etwa in der Sichtweise von Shannon's. Die Syntax-Ebene behandelt grammatikalische Regeln und repräsentiert die Sichtweise der Theorie der formalen Sprachen [Völz 82]. Auf der semantischen Ebene werden Zeichen Bedeutungen zugeordnet, hiermit beschäftigt sich die Semiotik [Völz 83] (S. 214) in erster Linie. Die Pragmatik bezieht Zeichen und ihre Bedeutungen auf Handlungskontexte und greift dabei auf Konzepte aus den Kognitionswissenschaften zurück [WikiInfo 04].

Tabelle 2.1
Ebenen des Informationsbegriffs

Ebenen
Pragmatik
Semantik
Syntax
Kodierung

Die pragmatische Ebene der Information kommt dem umgangssprachlichen Informationsbegriff am nächsten. Die Aussage, dass es morgen kalt wird, hat echten Informationscharakter für eine Person, die wissen möchte, ob warme Kleidung für den nächsten Tag empfehlenswert ist. Der pragmatische Informationsgehalt ist allerdings gleich Null, wenn der Satz in einer Tageszeitung von vorgestern gelesen wird. Der pragmatische Informationsgehalt einer virtuellen Ware kann mit ihrem Gebrauchswert (vgl. Kapitel 3.4) nahezu gleichgesetzt werden.

2.3 Kategorisierung virtueller Güter

Im Mittelpunkt der vorliegenden Arbeit steht die technische Umsetzung von Geschäftsmodellen, bei denen für den Anbieter der virtuellen Waren primär der Konsument die Erlösquelle (vgl. Kapitel 3.5) darstellt. Um die dabei eingesetzten informatorischen Systeme effektiv gestalten zu können, müssen diese den unterschiedlichen virtuellen Gütern angemessen bzw. angepasst sein. Eine solche Anpassung gelingt nur, wenn eine sinnvolle Kategorisierung virtueller Güter vorliegt.

Das Konsumverhalten und Wertverständnis des Konsumenten (als vorrangige Einnahmequelle) muss bei der Kategorisierung besonders berücksichtigt werden. Der Versuch virtuelle Güter nach den Medientypen wie z. B. Bild, Ton, Text usw. zu kategorisieren, wäre zwar möglich, würde aber eine zu große Vielfalt an Kategorien liefern. Auch technische Parameter wie Datenvolumen oder Datenformat sind nur bedingt geeignet, da das Datenvolumen und das Format der Nutzdaten, die ein virtuelles Gut repräsentieren, stark vom Stand der Technik abhängen.

2.3.1 Mehrfachkonsumierbarkeit

Ein wichtige Hilfe zur Kategorisierung von virtuellen Gütern kann ihre Mehrfachkonsumierbarkeit sein. Bestimmte virtuelle Güter, die nur ein einfaches Informationsbedürfnis befriedigen, wird Ginny sicherlich nur einmal konsumieren wollen. Ein wiederholter Konsum liefert keinen zusätzlich Nutzen, da Ginny bereits beim ersten Konsum die Information erhalten hat. Ein zweiter Konsum liefert für Ginny keinen pragmatischen Informationsgehalt mehr.

Die Mehrfachkonsumierbarkeit ist zwar eng mit dem subjektiven Gebrauchswert (vgl. Kapitel 3.4) virtueller Güter verknüpft, hat aber dagegen den Anspruch ein objektives Maß (in Prozent) für die Möglichkeit mehrfacher Nutzung zu sein.

Formel 2.2

$$Mehrfachkonsumierbarkeit = M(vg) = \frac{I_p(vg) - \Delta I_p(vg)}{I_p(vg)}$$

Die Formel 2.2 beschreibt die Mehrfachkonsumierbarkeit *M(vg)* eines virtuellen Gutes *vg* für eine konkrete Person über den pragmatischen Informationsgehalt $I_p(vg)$ vor dem ersten Konsumvorgang und die Reduktion dieses pragmatischen Informationsgehaltes $\Delta I_p(vg)$ beim ersten abgeschlossenen Konsumvorgang. Die Mehrfachkonsumierbarkeit beträgt 100%, wenn die Reduktion des pragmatischen Informationsgehalt bei diesem Konsumvorgang Null beträgt.

Am rechten Ende der Skala der Mehrfachkonsumierbarkeit (vgl. Abbildung 2.5) stehen virtuelle Güter wie bspw. Musik, deren Konsum mit positiven Gefühle besetzt sind. Ginny könnte sich z. B. beim Konsum eines Musikstücks an die Atmosphäre eines Live-Konzertes erinnern, bei dem sie dieses Stück das erste Mal gehört hat. Für Ginny würde sich der Gebrauchswert dieser Musik, die eine derartige emotionale Komponente enthält, auch bei einem wiederholtem Konsum nicht reduzieren. Das Gegenteil ist sogar möglich ($M(vg) > 1$).

2.3.2 Interaktivität

Interaktivität kann neben der Mehrfachkonsumierbarkeit als weiteres Merkmal zur Kategorisierung virtueller Güter herangezogen werden. Eine virtuelles Gut ohne Interaktivität verlangt von der Konsumentin Ginny keinerlei Aktivität zum Konsum. Musik kann bspw. nahezu passiv konsumiert werden. Etwas mehr Aktivität wird beim Konsum von Texten verlangt. Hier muss Ginny als geringste Form der Interaktivität manuell auf die nächste Textseite wechseln.

Formel 2.3

$$Interaktivität \approx \frac{I_{Eingabe}}{I_{Ausgabe}} = \frac{I_{Eingabe}}{I_{Ausgabe}' + I_{Eingabe}}$$

Mehr Interaktivität findet sich bspw. bei Software-Applikationen, die wiederholt Nutzereingaben erwarten. Ginny kann durch ihre Eingaben am Endgerät den weiteren Konsumvorgang beeinflussen. Ein sehr hohes Maß an Interaktivität findet sich bei Computerspielen und multimedialen Lernprogrammen. Die Interaktivität ist umso höher, je häufiger und schneller sich Nutzereingaben und Gegenreaktionen der Applikation abwechseln.

Die Interaktivität kann qualitativ als das über einen längeren Zeitraum gebildete Verhältnis aus dem pragmatischen Informationsgehalt $I_{Eingabe}$ der Eingaben des Nutzers am Endgerät und des pragmatischen Informationsgehalt der Ausgaben $I_{Ausgabe}$ beschrieben werden (siehe Formel 2.3). $I_{Ausgabe}'$ in der Formel 2.3 ist der untere Grenzwert für $I_{Ausgabe}$, wenn die Eingaben des Nutzer auf ein Minimum zurückgehen. Bei virtuellen Gütern mit maximaler Interaktivität (100%) gibt es folglich keine relevanten Ausgaben ohne relevante Nutzereingaben. Die Interaktivität eines virtuellen Gutes ist minimal (0%), wenn die Ausgabe unabhängig von Nutzereingaben ist.

Abbildung 2.5
Einordnung virtueller Güter

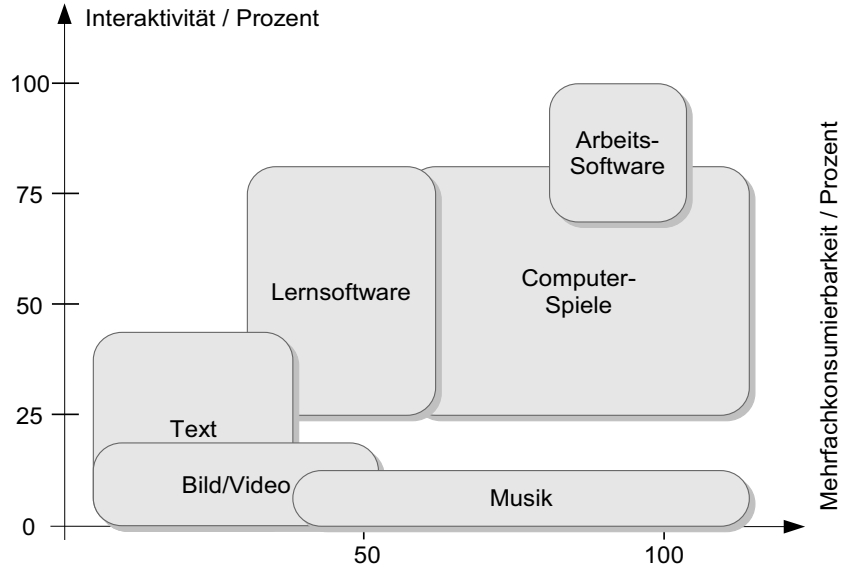


Abbildung 2.5 zeigt die relativ unscharfe Einordnung virtueller Güter nach ihrer Mehrfachkonsumierbarkeit und Interaktivität. Deutlich muss an dieser Stelle betont werden, dass in dieses Schema nicht alle Software-Applikationen eingeordnet werden können. Für maschinennahe, eingebettete Software wie z. B. eine Heizungssteuerung trifft die Einordnung nicht zu, da der Nutzer faktisch nicht mit dem Endgerät interagiert und folglich nur äußerst mittelbar Konsument ist.

2.3.3 Vollständig virtuelle Güter und Waren

Die in dieser Arbeit betrachteten virtuellen Güter können durch den Konsumenten über ein Endgerät ein- oder mehrfach *vollständig* konsumiert werden. Der Konsumvorgang kann hierbei unterschiedlich stark interaktiv sein. Der gesamte Gebrauchswert erschließt sich dem Nutzer durch diesen Konsumvorgang am Endgerät. Die im Weiteren behandelten informatorische Systeme fokussieren sich auf diese vollständig virtuellen Güter.

2.3.4 Berechtigungen, Geld und andere Abgrenzungsbeispiele

Berechtigungen bzw. Zugangsberechtigungen wie bspw. Eintrittskarten oder Zugfahrkarten werden inzwischen auch in digitaler Form über das Internet ausgeliefert.

Für Geld gilt ähnliches. Geld ist zwar keine Berechtigung sondern eine Schuldverschreibung, die allerdings auch als eine Unterart von Berechtigung betrachtet werden kann. Geld kann ebenfalls in digitaler Form als Buchgeld transferiert werden. Digitalisierte Berechtigungen und Geld sind jedoch ein separates Feld, welches einer getrennten Betrachtung im Rahmen einer zukünftigen Arbeit bedarf.

Der Autor hat bewusst sein Arbeitsgebiet nicht auf diese Formen digitalisierbarer „Produkte“ erweitert, da Berechtigungen und Geld zwar in digitaler Form gehandelt und transferiert werden können, diese aber nicht einen direkten Gebrauchswert darstellen, der über ein Endgerät konsumiert werden kann. Sie stellen somit keine vollständigen virtuellen Güter dar. Die in dieser Arbeit nicht behandelten Berechtigungen sind nur Mittel um Zugang zu realen Produkten und Dienstleistungen zu erhalten. Digitale Rechte dagegen, die ausschließlich den Zugang zu virtuellen Waren regeln, sind dagegen Bestandteil der weiteren Abhandlungen (vgl. Kapitel 4.4).

Berechtigungen stellen eine eigene Welt von Gütern dar, die ihren Wert aus anderen Gütern ableiten, und die in großer Variationsbreite auftreten. Sie sind der Welt der verbindlichen Kommunikation, die eine eigene Analyse erfordert, zuzuweisen. Versprechen, Verträge, Geld und Regeln sind dafür Beispiele.

Andere Autoren wie z. B. Röhm und Pernul stellen bei der Definition von *Digital Goods* nicht die Konsumierbarkeit ins Zentrum, sondern nur die Möglichkeit das Eigentum an einem Gut, welches auch real sein kann, elektronisch zu übermitteln: „A digital good is a good, that allows to transfer its ownership rights in an electronic way“ [RoePer 99].

2.4 Information in Beziehung zu Energie und Stoff

Virtuelle Güter stehen im engen Begriff zum Begriff Information. Wie ist nun der Begriff Information in die dem Menschen umgebene gesamte Welt eingebettet. Es existieren zahlreiche Modelle, um diese Welt in Ansätzen zu verstehen. Ein solches Modell, in dem Information eine fundamentale Säule ist, sind die drei Objektklassen (bzw. Kategorien) nach Norbert Wiener [WikiWiener 04]. Die drei Kategorien lauten: Energie, Stoff und Information. Von Wiener stammt die Aussage:

Information is Information nor matter or energy.

Nach verschiedenen Missdeutungen aufgrund falscher Übersetzungen übersetzte Völz in [Völz 91] auf S. 553 diesen Satz wie folgt:

Information ist Information, weder Stoff noch Energie.

Die wichtigen Eigenschaften dieser drei Grundkategorien werden in [Völz 91] ebenfalls auf Seite 553 folgendermaßen beschrieben:

- **Stoff** ist direkt materiell vorhanden; besitzt Masse, Gewicht und Volumen; besteht aus Molekülen, Atomen, Elementarteilchen; existiert fest, flüssig, gasförmig.
- **Energie** besitzt die Fähigkeit, auf Stoffe einzuwirken, sie zu bewegen, verformen, erhitzen, verändern, transportieren, biegen, verdampfen, chemisch umzuwandeln,

zerkleinern usw.; existiert als potentielle Energie innerhalb eines Feldes, z. B. Federspannung, Schwerefeld, elektrisches Feld; entsteht aus Energieträgern durch Wandlung, z.B. chemische Verbrennung von Öl, Gas usw., Kernbrennstoff.

- **Information** ist Objekt von Wechselwirkungen, bei denen stofflich-energetische Aspekte nicht wesentlich sind; enthält einen stofflich-energetischen Träger.

Abbildung 2.6
Die drei Kategorien nach Norbert Wiener [Wiener 65]

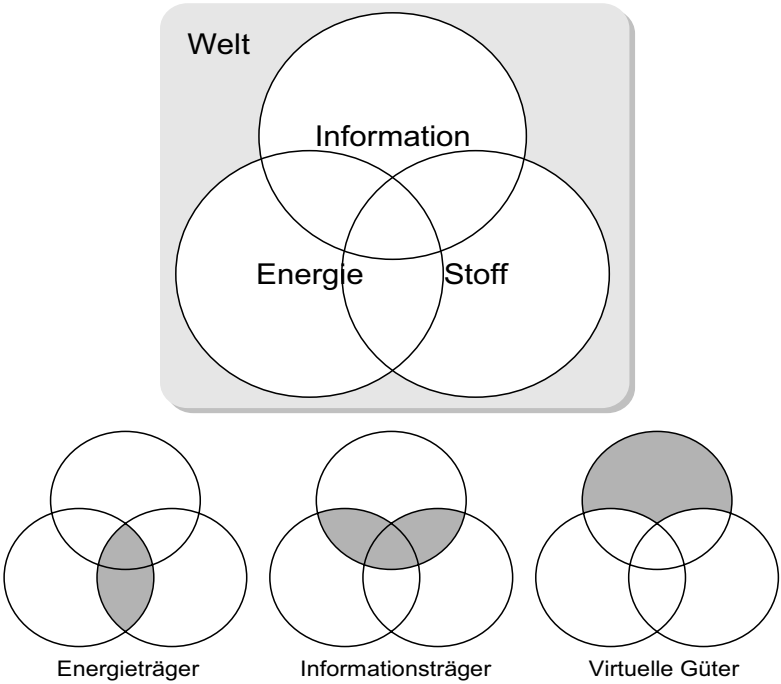


Abbildung 2.6 versucht die Zusammenhänge zwischen den drei Kategorien zu veranschaulichen. Die von Völz nur leicht verändert übernommene Abbildung 2.6 zeigt mögliche Abhängigkeiten und Zusammenhänge zwischen diesen drei Kategorien. Energieträger sind Stoffe, die Energie speichern. Informationsträger speichern oder transportieren dagegen Informationen unter Nutzung von Stoffen und Energie.

Informationsträger

Abbildung 2.6 zeigt deutlich die Bedeutung des Begriffs Informationsträger für die Virtuellen Güter. Danach „bestehen“ virtuelle Güter aus Information, die unabhängig von einem speziellen Informationsträger ist. In der Originaldarstellung von Völz (bzw. Wiener) war allerdings nicht von virtuellen Gütern die Rede. Völz benutzte anstelle

den Begriff *Getragenes* [Völz 91] (S.557). Die damit verbundene abstraktere Bedeutung soll hier allerdings nicht übernommen werden.

Über den Träger der Information lassen sich zwei Varianten von Information unterscheiden. Zum einen gibt es Informationen, die einen bestimmten Träger besitzen. Ohne diesen speziellen Träger, ist die Information für den Empfänger im pragmatischen Sinne wertlos (hier sieht man, welche zentrale Rolle der Begriff Wert einnimmt). Zum anderen gibt es Informationen, die ihren Träger wechseln können, ohne dass aus Sicht des Empfängers Teile der Information verloren gehen.

Ein Beispiel soll diese allerdings sehr unscharfe Trennung verdeutlichen. Kunstwerke wie Gemälde oder Plastiken sind Informationen, die an einen speziellen Träger gebunden sind. Würde man das Gemälde der Mona Lisa von Leonardo da Vinci auf ein anderen Träger übertragen, so würde diese möglicherweise sehr perfekte Kopie nicht den gleichen Wert wie das Original besitzen. Dagegen bleibt bei Musik, die auf dem Weg zu Konsumenten sehr häufig den Träger wechselt, der Nutzen für den Konsumenten erhalten. Allerdings zeigt sich, dass Musik, die an den stofflichen Träger CD gebunden wurde, oft einen höhere Wertschätzung beim Konsumenten erzielt, als Musik, die durch das Internet dieses stofflichen Trägers beraubt wurde. Da menschliche Wertvorstellungen einem zeitlichen und kulturellen Wandel unterliegen, kann es in Zukunft sein, dass der stoffliche Träger bei der Musik keine Rolle mehr spielt.

Die vorliegende Arbeit befasst sich primär mit Information, die unabhängig von ihrem stofflichen Träger ist. Denn die eigentliche ökonomische Revolution für virtuelle Güter besteht darin, dass gewisse Informationen bei Trägerwechsel ihren Wert behalten. Ein Handel der Information (zum Beispiel gespeicherte Musik) ist auf dem Wege des Handels über ihren Träger (zum Beispiel CDs) dann nicht mehr ausreichend zur Realisierung des Gewinns, wenn die Konsumenten den Trägerwechsel zu geringen Kosten selbst übernehmen können (zum Beispiel durch digitale Kopien auf dem Computer). Die Definition einer virtuellen Ware besagt genau dieses, dass sie von ihrem stofflichen Träger unabhängig ist.

3. Kapitel

Geschäftsmodelle für virtuelle Güter

Kern der vorliegenden Arbeit sind Verfahren und Systeme, welche Anbietern die Kommerzialisierung von virtuellen Gütern ermöglichen. Um die Anwendbarkeit bzw. Praktikabilität der unterschiedlichen Systeme und Verfahren bewerten zu können, muss man sich zunächst die verschiedenen möglichen Geschäftsmodelle für virtuelle Güter vor Augen führen. Die bestehenden Geschäftsmodelle aus der Welt der realen Güter sind oft wegen der bereits zuvor beschriebenen besonderen Eigenschaften virtueller Güter nicht ohne weiteres übertragbar.

Bei den verschiedenen Geschäftsmodelltypen mit ihren unterschiedlichen Erlösformen kommt auch die Frage nach dem eigentlichen Wert und damit nach dem richtigen Preis für virtuelle Waren auf. Diese Fragen können nicht alleine aus der betriebswirtschaftlichen Sicht eines einzelnen Anbieters beantwortet werden. Es sollten auch übergeordnete mikroökonomischen Überlegungen aus der Volkswirtschaftslehre [WikiVWL 04] Berücksichtigung finden. Schließlich müssen die eingesetzten Systeme und Verfahren einen längerfristigen Ausgleich zwischen Produzenten und Konsumenten erzielen, bei dem die Konsumenten einerseits kurzfristig die virtuellen Güter in hoher Qualität und Vielfalt beziehen können und andererseits die Produzenten langfristig ein Interesse haben, immer wieder neue virtuelle Güter bereitzustellen.

3.1 Der Begriff des Geschäftsmodells

Technologien und Systeme für den Vertrieb virtueller Güter versuchen in der Regel ganz spezielle Geschäftsmodelle umzusetzen. Um nun geeignete Geschäftsmodelle für virtuelle Güter zu identifizieren, muss zuerst definiert werden, was unter dem Begriff Geschäftsmodell verstanden wird. Als Einstieg in die Thematik dient die in der Betriebswirtschaftslehre etablierte Modelltheorie, wonach ein Modell eine vereinfachte bzw. abstrahierte Darstellung eines realen Systems ist. Ein Geschäftsmodell ist somit eine vereinfachte Darstellung eines Unternehmens, welches wesentliche Bestandteile einer Unternehmung und deren Verknüpfungen abbildet. ([Bieger u.a. 02] S.65f) Das Geschäftsmodell ist somit eine Abstraktion der Funktionsweise eines Geschäftes, die beschreibt, wie ein spezielles Unternehmen am Markt Werte schafft ([Bieger u.a. 02] S.4). [Biedermann 03]

Für die weitere Strukturierung verschiedener Geschäftsmodelle wurde der Ansatz von Timmers ([Timmers 00] S.32) gewählt. Dabei wird ein Geschäftsmodell durch drei Hauptkomponenten charakterisiert:

- Der Architektur von Produkten, Dienstleistungen und Informationsflüssen, welche auch eine Darstellung der beteiligten Wirtschaftsakteure und deren Rollen beinhaltet.
- Den potentiellen Nutzen, den das Unternehmen für die verschiedenen Wirtschaftsakteure bietet.
- Das Erlösmodell, welches aufzeigt, aus welchen Quellen und auf welche Weise sich das Unternehmen finanziert.

3.2 Abgrenzung zu öffentlichen Gütern

In der Volkswirtschaftslehre [WikiVWL 04] werden ökonomische Güter [WikiGut 05] nach der Ausschließbarkeit und Rivalität ihrer Nutzung unterschieden. Die Vier-Felder-Matrix in Tabelle 3.1 zeigt, wie sich daraus vier verschiedene Klassen von Gütern ableiten lassen.

Tabelle 3.1
Rivalität und Ausschließbarkeit der Nutzung virtueller Güter (siehe auch [WikiGut 05])

		Ausschließbarkeit?	
		Ja	Nein
Rivalität?	Ja	Individualgut oder auch privates Gut (z. B. Kleidung, Speiseeis)	Allmendegut oder auch Quasikollektivgut (z. B. Fischbestände der Weltmeere, öffentliche Straßen)
	Nein	Klubkollektivgut oder auch natürliche Ressource (z. B. Kabelfernsehen, Feuerschutz)	Öffentliches Gut oder auch reines Kollektivgut (z. B. frei zugängliches Wissen, Nationale Verteidigung, Rechtsordnung, Währungssystem)

Öffentliche Güter sind im Gegensatz zu privaten Gütern (auch als Individualgüter bezeichnet) durch Nichtrivalität und Nichtausschließbarkeit in der Nutzung gekennzeichnet. Nichtrivalität bedeutet, dass ein Gut von vielen Personen gleichzeitig konsumiert werden kann, ohne dass eine gegenseitige Beeinträchtigung stattfindet. Nichtausschluss liegt vor, wenn potentielle Konsumenten nicht von der Nutzung ausgeschlossen werden können [Heinrich 01] (vgl. Tabelle 3.1 rechts-unten).

Private Güter sind im alltäglichen Leben leichter zu identifizieren (vgl. Beispiele aus Tabelle 3.1). Ein Gebrauchsgegenstand wie bspw. ein Fahrrad ist ein privates Gut. Bei seiner Nutzung besteht zum einen Rivalität, da immer nur eine Person zur gleichen Zeit das Fahrrad nutzen kann. Zum anderen kann man problemlos andere Personen durch ein Schloss von der Nutzung ausschließen. Bei so genannten Allmendegütern dagegen kann man andere Personen nicht von der Nutzung ausschließen. Der Begriff Allmendegüter leitet sich von der Allmendewiese ab. Diese war früher eine Wiese, die von allen Einwohnern eines Dorfes gleichermaßen genutzt werden konnte. Da die Wiesen allerdings in der Fläche begrenzt sind, bleibt Rivalität erhalten.

Bei Maut- und Klubgütern (auch als Klubkollektivgüter bezeichnet) besteht zwar keine Rivalität, man kann aber von ihnen ausgeschlossen werden. Kabelfernsehen ist ein Beispiel hierfür. Der Zugang zum Kabelfernsehen kann leicht über den Zugang zum Kabelanschluss limitiert werden wodurch Ausschließbarkeit ermöglicht wird. Bei öffentlichen Gütern, die in der Regel durch den Staat bereitgestellt werden, existiert weder Rivalität noch Ausschließbarkeit. Straßenbeleuchtung würde bspw. in diese Kategorie fallen.

Die bereits beschriebenen speziellen Eigenschaften virtueller Güter, wie bspw. die einfache Kopierbarkeit bewirken, dass die Produzenten dieser Güter nach und nach die Instrumente verlieren, ihre virtuellen Produkte „zu privatisieren“. Das heißt, ihnen fehlen die Möglichkeiten, Konsumenten von der Nutzung auszuschließen und Rivalität in der Nutzung oder Exklusivität herzustellen, so dass ein Wandel vom privaten zu einem quasi-öffentlichen Gut stattfindet [Buhse 01]. Für die kommerziellen Anbieter virtueller Güter stellt sich nun die Frage, ob durch den Einsatz zusätzlicher technischer Kontrollsysteme dennoch eine nachträgliche „Privatisierung“ mit vertretbarem Aufwand möglich ist, so dass traditionelle Geschäftsmodelle, die sich für private Güter bewährt haben, genutzt werden können.

Sicherlich könnte man virtuelle Güter auch als Klubkollektivgüter betrachten oder sie einfach zu öffentlichen Gütern erklären. Im zweiten Falle würde auf auf jede Form der Kontrolle der Nutzung sowie nutzungsabhängige Abrechnung verzichtet werden. Auf diese Weise bleiben aber nur noch sehr wenige Geschäftsmodelle übrig. Neben einer Entlohnung der Urheber durch Werbeeinnahmen wäre nur noch eine mit einer Steuer vergleichbaren Pauschalabgabe möglich. Diese Abgabe wird oft auch als Kultur-Flatrate [Heise54607] bezeichnet. Für die gerechte Entlohnung müsste zumindest die wirkliche Nutzung der virtuellen Güter gemessen werden. Urheberrechtsgesellschaften wie z. B. die GEMA [GEMA 05] treiben solche Pauschalabgaben in gewissen Umfang schon jetzt analog zu Steuern ein.

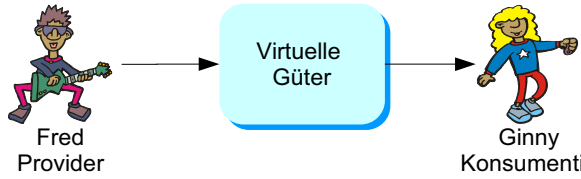
Bei allen Überlegungen zu verschieden Geschäftsmodellen soll in dieser Arbeit nicht das eigentlichen Ziele des Urheberrechts außer Acht gelassen werden. Denn nicht der kurzfristige Profit einzelner Urheber ist das Ziel, sondern der in der Einleitung dieses Kapitels bereits angesprochene längerfristige Ausgleich zwischen den Produzenten und den Konsumenten virtueller Güter [AicHas 03].

3.3 Beteiligte Wirtschaftsakteure

Der Vertrieb virtueller Güter ist ein wirtschaftlicher Prozess, bei dem analog zur Welt der realen Güter verschiedene Wirtschaftsakteure beteiligt sind. Es gibt immer mindestens zwei solcher Akteure: einen Anbieter (engl.: Provider) und einen Konsumenten (engl. Consumer oder Customer) virtueller Güter. Zur leichteren Beschreibung von diversen Anwendungsfällen und Geschäftsmodellen werden an dieser Stelle in Anlehnung an die *Unified Modeling Language* (UML) [UML 04] spezielle stereotype Akteure (*actor*) eingeführt. Krauß (siehe [Krauß 02] S. 35-37) hat hierfür einprägsame Namen und Grafiken gewählt. In der UML sind eine Reihe von Diagrammtypen beschrieben und standardisiert, die sich für die Modellierung von Informationsverarbeitenden Systemen eignen. Jeder stereotype Akteur steht dabei für eine spezielle Rolle, die der Akteur im Umgang mit dem modellieren System einnimmt. Die hier behandelten Systeme dienen dem Vertrieb und Konsum virtueller Güter.

Der stereotype Akteur Fred in der Rolle eines Providers

Abbildung 3.1
Zwei elementare Wirtschaftsakteure und ihre Stereotypen



Ein Provider ist ein Anbieter von virtuellen Gütern, der seine Inhalte (Content, virtuelle Güter) mit Hilfe technischer Systeme vertreiben und verbreiten will. Als Provider kann hierbei der Schöpfer d. h. der Künstler selbst oder aber auch ein beliebiger Rechteinhaber der Güter, wie z. B. ein Musikproduzent oder der Inhaber eines Musikportals oder Musiklabels in Erscheinung treten [Biedermann 03]. Der Stereotyp Fred (vgl. Abbildung 3.1) steht im Folgenden für den Provider.

Die stereotype Akteurin Ginny in der Rolle einer Konsumentin

Dem Provider gegenüber befinden sich die Konsumenten. Sie sind an den virtuellen Gütern des Anbieters (Providers) interessiert. Mit Hilfe technischer Systeme transferieren sie diese Güter auf die für den Konsum notwendigen Endgeräte. Ginny (vgl. Abbildung 3.1) soll im Folgenden eine stereotype Konsumentin darstellen.

Abbildung 3.2
Harry erhält von Ginny virtuelle Güter

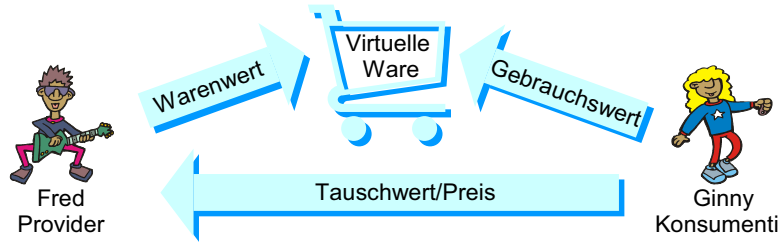
Der stereotype Akteur Harry in der Rolle des Freundes von Ginny

Im weiteren Verlauf dieser Arbeit wird zwischen unterschiedlichen stereotypen Konsumenten differenziert. Harry übernimmt (vgl. Abbildung 3.2) als „Freund“ von Ginny eine besondere Rolle. Harry ist wie Ginny Konsument eines virtuellen Gutes. Er hat dieses virtuelle Gut allerdings nicht vom Provider Fred erhalten, sondern von der Konsumentin Ginny. Hierbei spielt es keine Rolle, ob dieser Transfer mit oder ohne der Zustimmung von Fred erfolgte.

3.4 Der Wert virtueller Güter

Soll ein spezielles Geschäftsmodell für virtuelle Güter erfolgreich sein, muss es die drei verschiedene Wertebegriffe Warenwert, Gebrauchswert und Tauschwert (vgl. Abbildung 3.3) in Einklang bringen und dabei auch das bestehende Wertverständnis der Konsumenten beachten. Menschen bzw. Konsumenten sind mit den Produkten und Dienstleistungen der realen Welt vertraut. Sie haben ein klares Verständnis über den Wert dieser Waren. Der Wert erweist sich im Gebrauch einer Ware („Gebrauchswert“, allein vom Konsumenten bestimmt) und wird über den Tausch mit anderen Waren („Tauschwert“: wird in der Interaktion Anbieter-Konsument bestimmt) bemessen. Die Wirtschaft und ihre Geschäftsmodelle sind auf dieses scheinbar natürliche Wertverständnis fest eingestellt. Nicht nur Marx hat sich damit auseinandergesetzt, was der „eigentliche“ Wert von Waren ist [Marx 62]: Es ist die in einer Ware kondensierte menschliche Arbeit [GriNüt 02a] („Warenwert“: allein vom Anbieter und Produzenten bestimmt).

Abbildung 3.3
Beziehung zwischen Warenwert, Gebrauchswert und Tauschwert



In Abbildung 3.3 wird der Zusammenhang von Warenwert, Gebrauchswert und Tauschwert bzw. Preis deutlich gemacht. Auch wenn das Kapital von Marx [Marx 62] (eine Online-Version findet sich hier [MarxForum 04]) nicht mehr in allen Punkten als zeitgemäß betrachtet werden kann, so ist speziell der Diskurs um den Wertbegriff immer noch hoch aktuell.

Im Folgenden wird die Terminologie an die Begriffswelt virtueller Güter und Waren angepasst. Ein virtuelles Gut enthält menschliche (und vergegenständlichte) Arbeit (= Warenwert oder Wert haben) und muss ein menschliches Bedürfnis befriedigen (sonst ist es kein Gut), also für die Konsumentin nützlich sein (= Gebrauchswert haben). Schließlich muss das virtuelle Gut mit dieser doppelten Eigenschaft für den Austausch, also den Markt oder Verkauf produziert worden sein (damit wird das Gut zur Ware).

3.4.1 Warenwert

Der „eigentliche“ Wert (= Warenwert) im Marx'schen Sinne ist die menschliche Arbeitszeit (inkl. vergegenständlichter Arbeitszeit in Form von Zulieferungen und Maschinen ...). Unter Warenwert verstehen wir den Aufwand, der zur Produktion und Auslieferung der virtuellen Ware nötig war. Der Wert einer bestimmten virtuellen Ware bleibt im Laufe der Zeit nicht unverändert, sondern wechselt mit der zu ihrer Herstellung durchschnittlich notwendigen Arbeitszeit. Letztere verändert sich mit jedem Wechsel der Produktivität.

3.4.2 Gebrauchswert

Der Gebrauchswert einer realen oder virtuellen Ware unterliegt dem subjektiven Urteil des Konsumenten [Gabler 04]. Bei virtuellen Waren kann z. B. die bloße Befriedigung eines Informationsbedürfnisses den Gebrauchswert darstellen. Man spricht hier von der Pragmatik einer Information.

In der realen Welt, gibt es nach Marx Dinge, die einen Gebrauchswert haben, ohne einen Warenwert zu haben (z. B. die Luft). Dieser Fall ist sicherlich nur sehr schwer auf virtuelle Güter übertragbar, da der Konsum virtueller Güter nie ohne technische Hilfsmittel wie z. B. einem Endgerät von statten gehen kann. Dagegen gibt es aber vom Menschen produzierte virtuelle Güter, die keine Waren sind, weil sie nicht für den Austausch (Verkauf) ,sondern z. B. nur für den Eigenbedarf bestimmt sind. Ebenso gibt es virtuelle Güter, die zwar Arbeit enthalten, jedoch nutzlos sind, und somit keinen Wert haben (bei realen Gütern würde man dies z. B. Produktionsausschuss nennen). Wert haben nur Waren, die auch einen Gebrauchswert haben.

3.4.3 Tauschwert

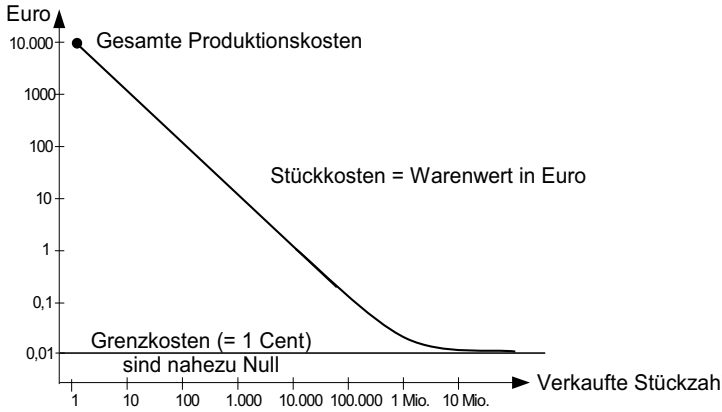
Unter Preis bzw. Tauschwert versteht man das, was der Konsument bereit ist, für die Ware zu bezahlen (zu tauschen). Ein guter Tausch kommt dann zustande, wenn beide Seiten (Käufer und Verkäufer) nach dem Tausch (Kauf) aus ihrer jeweiligen Sicht mehr (Gebrauchswert) haben. Allerdings findet typischerweise in modernen Volkswirtschaften kein Tauschhandel mehr statt. Geld hat die Aufgabe übernommen, Werte zu transferieren. Geld muss allerdings als Tauschmittel eine allgemein gültige, stabile Rechengröße darstellen. Neben der Funktion als Tauschmittel hat es auch die Aufgabe der Wertaufbewahrung und der Wertmessung [WikiGeld 04]. Diese drei Aufgaben kann ein Fünfzig-Euro-Schein, obwohl er selbst keinen Gebrauchswert hat, nur mit Hilfe der Europäischen Zentralbank erbringen.

Bei realen Waren, die nicht digitalisierbar sind, orientiert sich der Preis an den Grenzkosten für ihre Erstellung (vgl. Abbildung 3.4). Die Grenzkosten stellen aus Sicht des Anbieters ein untere Schranke für den Preis dar. Bei virtuellen Waren ist diese Schranke noch viel stärker von der Stückzahl abhängig, was zur Folge hat, dass es Anbieter schwer haben, einen aus ihrer Sicht fairen Preis (deutlich über den Grenzkosten) am Markt durchzusetzen. Der (Gebrauchs-)Wert einer virtuellen Ware (z. B. ein Musikstück), die nicht an einen physikalischen Träger wie z. B. eine Audio-CD gebunden ist, kann sich nur noch schwer an ihrem Warenwert (vgl. Abbildung 3.4) orientieren. Es bleibt nur noch die sehr subjektive Empfindung des Konsumenten aus dem sich ein fairer Tauschwert ableiten lässt.

Bei vernachlässigbaren Reproduktions- und Vertriebskosten fällt der (Waren-)Wert einer einzelnen Kopie, also des individuellen Produktes, proportional mit der Anzahl

verkaufter Exemplare: Auf alle Kunden werden die fixen Produktionskosten umgelegt. Bei einem Musikstück, dessen Produktion einmalig 10.000 € gekostet hat und dessen Vertriebskosten 1 Cent pro digitalisierte Kopie betragen, würde der Warenwert einer von 1.000 verkauften Kopien 10,01 € betragen, eine von 10.000 verkauften Kopien 1,01 € und eine von 100.000 verkauften Kopien 11 Cent (vgl. Abbildung 3.4). Da die Reproduktion und Verteilung virtueller Waren im Internet nahezu kostenlos erfolgen können, trägt dies zusätzlich dazu bei, die klassischen Wertbegriffe der Konsumenten aufzulösen. Diese Eigenschaften von virtuellen Waren in digitalisierter Form verlangen ein Umdenken und Anpassen von aktuellen Geschäftsmodellen [Nützel 03a].

Abbildung 3.4
Die Stückkostendegression bei virtuellen Waren [GriNüt 02a]



3.5 Erlösmodelle und Erlösformen

Die Betrachtung von Erlösmodellen ist bei der Untersuchung von Geschäftsmodellen von zentraler Bedeutung. Erlöse sind der Gegenwert aus der Veräußerung von virtuellen Gütern. Die Erlöse einer Unternehmung bestimmen den Wert und die Nachhaltigkeit eines Geschäftsmodells ([Stähler 02] S. 40ff).

Direkte Erlöse

Die direkten Erlöse eines Anbieter stammen vom Kunden bzw. Konsumenten des virtuellen Gutes. Sie lassen sich in nutzungsunabhängige und nutzungsabhängige direkte Erlöse aufteilen. Bei nutzungsabhängigen Erlösmodellen zahlt der Konsument entweder proportional zu einer Transaktions- bzw. Downloadanzahl, einer Nutzungszeit oder dem Download-Volumen, welches er wirklich in Anspruch nimmt.

Nutzungsunabhängige Erlösmodelle sehen pauschalierte Zahlungen der Nutzer vor. Entweder einmalig für eine Lizenz- oder Abschlussgebühr oder bspw. monatlich wiederkehrend bei einem Abonnement. Beide Formen können natürlich auch kombiniert werden. Der Kunde zahlt dann eine monatliche Grundgebühr, die ihm einen ge-

wissen Umfang an Transaktionen ermöglicht. Über diesen Umfang hinaus wird der Kunde nutzungsabhängig abgerechnet.

■ **Indirekte Erlöse**

Tabelle 3.2
Erlösformen virtueller Güter [Zerdick u.a. 01]

Direkt			Indirekt	
Nutzungsabhängig	Nutzungsunabhängig		via Unternehmen	via Staat
	Einmalig	Regelmäßig wiederkehrend		
Einzeltransaktionen nach Leistungsmenge (Pay-per-use) oder Leistungsdauer (Pay-per-time)	Abschluss-gebühren Lizenz-gebühren Dekoder	Abonnement sonstige Grundgebühren	Werbung, Sponsoring Kommission / Provisionen / Cross-Finanz. Sonstige	Subventionen

Indirekte Erlöse wie bspw. Werbeeinnahmen oder Kommissionen werden von Dritten eingenommen. Dritte können wiederum Unternehmen staatliche oder halbstaatliche Organisationen sein. Staatliche Zuwendungen werden als Subventionen verstanden (vgl. Tabelle 3.2). Zuwendungen von privater Seite kann man als Sponsoring bezeichnen. Die Finanzierung von Opensource-Projekten läuft häufig durch ein solches Sponsoring. Die Office-Lösung OpenOffice [OpenOffice 04] - mit der diese Arbeit erstellt wurde - wird z. B. von der Firma Sun unterstützt, welche das Opensource-Produkt unter dem Namen StarOffice kommerziell vertreibt. Die Möglichkeiten Werbeeinnahmen als Erlösform zu nutzen, sind vielfältig. Neben der bekannten Bannerwerbung können auch innerhalb eines virtuellen Gutes (z.B. ein PC-Spiel, ein Film oder ein Lied) die Produkte eines Werbepartners erscheinen. Dies kann so subtil umgesetzt werden, z. B. als Werbung auf den Autos in einem PC-Rennspiel, dass der Kunde dies nicht als störende Werbung wahrnimmt. Auch der Verkauf von Hardware (z. B. Apple iPods) kann virtuelle Waren quer finanzieren.

3.6 Mögliche Geschäftsmodelltypen

Bevor virtuelle Güter in den Mittelpunkt der Geschäftsmodellbetrachtung gestellt werden, sollen zuerst die generell möglichen Internet-Geschäftsmodelltypen aufgelistet werden.

3.6.1 Business-to-Consumer Geschäftsmodelltypen im Internet

In [WirKle 00] werden vier Business-to-Consumer (B2C) Internet-Geschäftsmodelltypen unterschieden. Die Begriffe Content, Commerce, Context und Connection stehen für diese grundsätzlichen Geschäftsmodelltypen.

- Der mit *Content* bezeichnete Geschäftsmodelltyp umschreibt die Bereitstellung von virtuellen Gütern über das Internet.
- *Commerce* steht für die Unterstützung der Anbahnung, Aushandlung und Abwicklung von Handelstransaktionen (z.B. bei einem Online-Auktionshaus wie eBay).
- *Context* beschreibt die Unterstützung der Konsumenten bei der Suche nach virtuellen Gütern im Internet. Die gelieferten Zusatzinformationen werden aus einem Datenbestand generiert, welcher systematisierte und klassifizierte Verweise auf im Internet verfügbare virtuelle Güter umfasst (z. B. bei Google).
- *Connection* beschreibt die Unterstützung der Kommunikation zwischen privaten Nutzern oder zwischen Endverbrauchern und Unternehmen. Dabei werden die ausgetauschten Nachrichten lediglich den unmittelbar an einem Kommunikationsvorgang beteiligten Partnern bekannt. (Beispiele sind die von E-Mail-, SMS-, Fax- oder Voice-over-IP-Dienste) [Stelzer 04]

Stelzer fügt noch fünf weitere abgeleitete Internet-Geschäftsmodelltypen hinzu:

- *Computing* überschreibt Geschäftsmodelle bei denen der Anbieter Verarbeitungsfunktionen bereitstellt, welche als Reaktion auf nutzerspezifische Anfragen gestartet werden. Computing steht im engen Zusammenhang mit Context und Content. Online-Spiele oder Online-Übersetzungsdienste fallen in diese Kategorie.
- *Community* steht für Dienste, die es zum Ziel haben die Informationssammlung, Publikation und Kommunikation innerhalb einer Nutzergruppe zu unterstützen. Im Unterschied zur Kategorie Connection werden die kommunizierten Inhalte archiviert und publiziert, so dass diese auch von nicht unmittelbar an den Kommunikationsvorgängen beteiligten Akteuren abrufbar sind. Content-Geschäftsmodelle machen sich häufig Community-Dienste zu nutze. Das in Kapitel 8 beschriebene PotatoSystem [Potato 05] mit seinem User-Matching ist ein Beispiel hierfür.
- *Collaborations*-Dienste dienen der Unterstützung der Zusammenarbeit von Team-Mitgliedern mit Hilfe von Link-Sammlungen, Dateiverzeichnissen, einfachen Datenbanken, Chat-Funktionen, Kalender- und Umfragefunktionen. Internet-gestütztes Workgroup-Computing (CSCW) fällt in diese Kategorie.
- *Currency* steht für Geschäftsmodelle, die Zahlungsdienste im Mittelpunkt haben. Content-Geschäftsmodelle, die auf direkten Erlösen aufbauen benötigen solche Zahlungsdienste. Das in Kapitel 5.4 beschriebene Multi-Payment-System Paybest [Paybest 05] verbindet mehrere unterschiedliche Internet-Zahlungsdienstanbieter.
- *Confidence*-Dienste stellen Sicherheitsfunktionen bereit, welche helfen die Integrität, Vertraulichkeit und Verfügbarkeit von sicherheitsrelevanten Elementen zu schützen, sowie die Verbindlichkeit und Authentizität von Kommunikationsvorgängen zu sichern. Das in Kapitel 7 beschriebene LWDRM [LWDRM 04] nutzt digitale Zertifikate, die von einer sog. Certification Authority (CA) ausgegeben werden.

Im Folgenden soll der Schwerpunkt aber nur auf reinen Content-zentrierten Geschäftsmodelle liegen. Geschäftsmodelltypen mit direkten Erlösformen stehen dabei im Mittelpunkt.

3.6.2 Datei-Download

Besitzt ein virtuelles Gut aufgrund hoher Interaktivität oder künstlerischen Inhaltes eine hohe Mehrfachkonsumierbarkeit (siehe Kapitel 2), wie z. B. Standard-Bürosoftware oder Musik, so bietet sich vor dem Konsum ein einmaliger Transfer bzw. Download vom Anbieter (Provider) zum Konsumenten an. Das Geschäftsmodell des Providers ist es hierbei, einen Server im Internet zu betreiben, auf dem für die Konsumenten kostenpflichtig die virtuellen Waren als Dateien zum Download vorgehalten werden. In Kapitel 4 werden die technischen Zusammenhänge im Detail erläutert. Tabelle 3.2 zeigt die unterschiedlichen direkten Erlösformen, die dem Provider zur Auswahl stehen. Der Provider kann sowohl aus nutzungsabhängigen als auch aus nutzungsunabhängigen Erlösformen auswählen.

■ Nutzungsunabhängige Erlöse

Nutzungsunabhängige Erlöse kann der Anbieter durch ein Abonnement, eine Grundgebühr oder eine einmalige Abschlussgebühr erzielen. Die Abschlussgebühr kann z. B. auf den Kaufpreis eines zum Konsum notwendigen Endgerätes aufgeschlagen sein. Der Konsument erhält dann vom Provider Zugang zu einem definierten Leistungsangebot. Dieses Leistungsangebot kann z. B. ein monatlich limitiertes Download-Volumen oder eine bestimmte Transaktionsanzahl umfassen. Bei einer Kombination mit nutzungsabhängigen Gebühren kann die Grundgebühr auch ein monatlicher Mindestumsatz sein.

■ Nutzungsabhängige Erlöse

Problematisch bei nutzungsunabhängigen Erlösmodellen ist, dass neue Konsumenten bspw. nur sehr schwer zum Abschluss eines Abonnement zu gewinnen sind. Sie müssen davon überzeugt werden, dass sie den Dienst dieses Anbieters kontinuierlich und über einen längeren Zeitraum in Anspruch nehmen wollen. Anbietern von Abo-Modelle ist unbedingt empfohlen parallel auch nutzungsunabhängige Modelle für den „Einsteiger“ oder Gelegenheitsnutzer bereitzuhalten. Hier zahlt der Kunde nur für den Download bzw. das Download-Volumen, welches er wirklich in Anspruch nimmt.

Aus Sicht des Anbieters sind allerdings die relativ hohen Verwaltungskosten nachteilig. Jede einzelne Aktivität des Konsumenten muss detailliert abgerechnet werden. Dies kann dazu führen, dass Nutzer, die sehr viele virtuelle Waren kaufen bei diesen Modellen schlecht wegkommen. Um diese Nachteile zu überwinden, empfiehlt sich entweder eine Kombination mit nutzungsunabhängigen Modellen oder der Einsatz von Rabatten.

3.6.3 Online-Konsum und Streaming

Virtuelle Güter, die keine oder nur eine geringe Mehrfachkonsumierbarkeit (d. h. der Gebrauchswert reduziert sich für den einzelnen Konsumenten bereits sehr stark nach dem ersten Konsum) besitzen, werden vom Provider häufig nur zur Online-Nutzung angeboten. Zu diesen virtuellen Gütern zählen z. B. aktuelle Informationen wie eine Fahrplanauskunft oder Videos. Während des gesamten Konsumvorgangs besteht zwischen dem Endgerät des Nutzers und dem Rechner des Anbieters eine

Kommunikationsverbindung. Das Endgerät speichert die Daten der virtuellen Güter bei einem Online-Konsum nicht dauerhaft. Wegen der fehlenden Mehrfachkonsumierbarkeit hat der Nutzer im Regelfall auch keine Verwendung für die gespeicherte Kopie.

Nutzungsunabhängige Erlöse

Für den Online-Konsum können die gleichen nutzungsunabhängigen Erlösmodelle wie beim Datei-Download zum Einsatz kommen. Auch hier empfiehlt es sich Obergrenzen für das Nutzungsvolumen zu definieren.

Nutzungsabhängige Erlöse

Hinter nutzungsabhängigen Erlösmodellen finden sich beim Online-Konsum zeitliche oder Datenvolumen-abhängige Tarife. Sind die dabei einzeln abgerechneten Zeit- bzw. Datenpakete kleiner, so ist die Abrechnung zwar gerechter, auf Anbieterseite entsteht aber mehr Abrechnungsaufwand und auf Konsumentenseite eine höhere Konsumzurückhaltung. Telefongesellschaften umgehen dieses Problem durch Mischtarife, bei denen z. B. erst ab der ersten Minute sekundengenau abgerechnet wird.

Ein weiteres Problem nutzungsabhängiger Erlösmodelle ist das Inkasso. Der Nutzer müsste bei jedem Inhalteanbieter einen Nutzungszähler haben und jeden Anbieter autorisieren, gemäß dieses Zählers Rechnungen zu stellen. Damit der Nutzer nicht eine Vielzahl von Anbietern autorisieren muss, können die Inhalteanbieter ihren Abrechnungen an einen gemeinsamen Dienstleister auslagern. Die Firma Firstgate [Firstgate 04] bietet einen solchen Dienst bspw. für das monatliche Abonnement von Online-Zeitschriften.

3.6.4 Peer-to-peer (P2P) und Superdistribution

In P2P-Systemen erfolgt die technische Verteilung virtueller Güter nicht durch den Originalanbieter (also Fred), sondern durch die Konsumenten selbst. Meisten dieser Systeme arbeiten illegal, da die Verteilung durch die Nutzer ohne Zustimmung der Urheber erfolgt. Werden dagegen die Nutzer unter der Kontrolle des Anbieters als Vertriebsknoten genutzt, so spricht man von Superdistribution. Bei der Superdistribution kann der Empfänger der (typischerweise verschlüsselten) Daten diese erst nutzen, nachdem ein zusätzlicher technischer Vorgang (Bezug einer Lizenz mit Schlüssel) auf dem Endgerät des Empfängers erfolgt. Dieser zusätzliche Schritt unterliegt allerdings der Kontrolle des Anbieters. Bereits 1989 wurde der Begriff Superdistribution geprägt [Mori 89].

Nutzungsabhängige Erlöse

Sollen in einem P2P-System mit oder ohne Superdistribution direkte nutzungsabhängige Erlöse erzielt werden, so geht dies nur durch die Einbeziehung der Nutzer. Krauß [Krauß 02] benennt das Affiliate-Marketing als einen möglichen Ansatz. Hierbei wird der vermittelnde Konsument (z. B. Ginny) belohnt, wenn der neue Konsument (z. B. Harry) eine Bezahltransaktion vornimmt. Für was Harry im Einzelfall bezahlt, kann allerdings sehr unterschiedlich sein. Bei Superdistribution zahlt er bspw.

für die volle Nutzbarkeit der virtuellen Ware. Im PotatoSystems (siehe Kapitel 8) zahlt er für weitere Vergünstigungen und für das Recht, die virtuelle Ware weiter zu vertreiben.

Nutzungsunabhängige Erlöse

Im Jahr 2000 versuchte Bertelsmann das illegale P2P-System Napster [WikiNapster 05]in einen legalen Abo-Dienst umzuwandeln. Dieser Versuch scheiterte nicht nur aus rechtlichen Gründen. Der Autor sieht allerdings für solche Erlösmodelle generell nur sehr geringe Chancen, da dann kein Anreiz mehr besteht, die virtuellen Güter selbst weiter zu verteilen. Der Konsument muss immer bezahlen auch wenn er für viele andere Nutzer die „Arbeit“ macht.

3.6.5 Download mit eingeschränkter Nutzung beim Konsumenten

Mit so genannten DRM (*Digital Rights Management*) Systemen versuchen Anbieter durch zusätzliche technische Maßnahmen (mehr dazu in Kapitel 4) die Nutzung der angebotenen virtuellen Güter zu kontrollieren. Es wird nicht mehr für die Daten, die das virtuelle Gut repräsentieren, Geld verlangt, sondern für separat gehandelte Nutzungsrechte. Auf Basis flexibel definierbarer Nutzungsrechte und der Kontrolltechniken können schließlich nahezu beliebige Geschäftsmodelle realisiert werden. Die dabei gehandelten Rechte, die mittels einer Rechtebeschreibungssprache notiert werden (mehr dazu ebenfalls in Kapitel 4), reichen von dem Recht zur Kopie auf weitere Endgeräte bis hin zum Recht, ein virtuelles Gut nur zeitlich begrenzt zu nutzen. Dieses Nutzungsrecht würde eine Vermietung virtueller Güter möglich machen. Der Konsument soll im Falle von digitaler Musik, sobald er sich erst für ein monatliches Abo entschlossen hat, möglichst alle Songs herunterladen dürfen. Da die Rechte zur Nutzung immer nur einen Monat lang gültig sind, kann der Anbieter bei einer ausbleibenden Zahlung einfach die Rechte für den nächsten Monat zurück halten. Kombiniert der Anbieter DRM-Systeme mit Superdistribution, so kann er sich auch noch die lästige Verteilung großer Datenmengen sparen.

Kritisch muss an dieser Stelle bemerkt werden, dass nicht alles, was technisch machbar, auch wirtschaftlich sinnvoll ist. Am Ende entscheidet doch der zahlende Konsument, ob er solche Systeme akzeptiert. Der anfangs angesprochene Ausgleich zwischen Produzenten und Konsumenten nimmt besonders stark Schaden, wenn Konsumenten, in der Erwartung legal erworbene Musik wie gewohnt frei nutzen zu können, sich für einen Kauf entscheiden und später entgegen dieser Erwartung feststellen müssen, dass dem nicht so ist.

4. Kapitel

Grundlegende Techniken für die Distribution und Kontrolle virtueller Güter

Bevor im weiteren Fortgang der Arbeit auf neue Systeme und Verfahren, an deren Entwicklung der Autor beteiligt war, detailliert eingegangen wird, soll zuerst auf den aktuellen Stand bei den grundlegenden Techniken für die Distribution und Kontrolle vollständiger virtueller Güter Bezug genommen werden. Virtuelle Güter, die nicht vollständig (vgl. Kapitel 2.3.3) über ein Endgerät konsumiert werden können, bleiben hierbei ausgeklammert. Schwerpunkt der Abhandlungen liegt auf Systemen, die das Internet als primäres Bindeglied zwischen Anbieter und Konsument nutzen.

Das Endgerät bildet den Ausgangspunkt der folgenden Beschreibungen. Es wird einerseits für den Konsum der virtuellen Ware benötigt. Zum anderen stellt es technische Möglichkeiten bereit, mit dem Anbieter virtueller Waren über das Internet in Kontakt zutreten. Viele Techniken zur Umsetzung direkter Erlösmodelle für virtuelle Waren bedingen nicht nur spezielle Anbieter-Systeme, sondern auch spezialisierte Endgeräte.

Aufbauend auf den Endgeräten folgt die Beschreibung von Systemen bzw. Techniken, die wie die P2P-Systeme die Verteilung virtueller Güter auf diese Endgeräte zum Ziel haben.

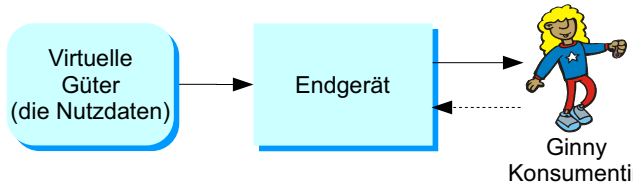
Abschluss bilden schließlich die Techniken, die die Verteilung und Nutzung virtueller Güter z. B. mittels kryptographischer Verfahren wieder einschränken bzw. kontrollieren. Die so genannten *Digital Rights Management* Systeme, die auf dem Endgerät verankert sein müssen fallen in diese Kategorie.

Neben Systemen zur Verteilung und Kontrolle virtueller Waren sind die Bezahlsysteme eine wesentliche Komponente für die Umsetzung direkter Erlösmodelle. Aufgrund der besonderen Bedeutung der Bezahlsysteme dabei, wird diesen ein separates Kapitel (Kapitel 5) gewidmet.

4.1 Das Endgerät

Ginny (unsere stereotype Konsumentin) kann virtuelle Güter, wie sie in dieser Arbeit verstanden werden, nur mit Hilfe eines speziellen technischen Endgerätes konsumieren. Dieses Endgerät in Abbildung 4.1 würde im Kanalschema (vgl. Seite 12) die Rolle des Decoders und eines Teils des Kanals übernehmen. Die vor dem Konsum notwendige Decodierung und Interpretation der Nutzdaten, welche die virtuellen Güter repräsentieren, erfolgt dabei mittels eines speziellen Decoders, der mittels Hard- oder Software realisiert sein kann. Der Kanal wird durch mindestens eine Kommunikationsschnittstelle realisiert, über die die Nutzdaten in das Endgerät gelangen. Über die am Endgerät vorhandenen Mensch-Maschine-Ausgabeschnittstellen wie z. B. eine TFT-Anzeige oder einen Lautsprecher konsumiert Ginny schließlich die virtuellen Güter. Über Mensch-Maschine-Eingabeschnittstellen wie z. B. Tastatur oder Maus kann Ginny mit dem Endgerät interagieren. Diese Interaktion ist fester Bestandteil des Konsumvorgangs virtueller Güter. Vervollständigt werden die meisten Endgeräte durch einen Permanentspeicher, der den wiederholten Konsum mehrfachkonsumierbarer virtueller Waren erst ermöglicht.

Abbildung 4.1
Ginny benötigt ein Endgerät für den Konsum virtueller Güter



Verschiedene Endgeräte nach ihren technischen Fähigkeiten zu klassifizieren ist ein weites Feld. An dieser Stelle soll nur eine sehr grobe Klassifizierung anhand bestimmter Basiskomponenten erfolgen. Prinzipiell haben die betrachteten Endgeräte immer die folgenden Basiskomponenten:

- Kommunikationsschnittstellen für die Verbindung zum Anbieter
- Ein- und Ausgabeschnittstellen für den Konsum der virtuellen Güter
- Permanentspeicher um einen mehrfachen Konsum zu ermöglichen
- Decoder und Steuerung zur Verarbeitung der Nutzdaten und der Nutzereingaben

Die Ausprägung dieser vier Basiskomponenten beeinflusst sehr stark die Art der zur Vermarktung einsetzbaren Systeme.

4.1.1 Kommunikationsschnittstellen

Um ohne physikalische Datenträger den Zugang zu den virtuellen Gütern zu ermöglichen, müssen die Endgeräte mindestens eine bidirektionale digitale Kommunikationsschnittstelle besitzen. Diese Schnittstellen lassen sich in zwei unterschiedliche Ebenen einteilen. Die erste und unterste Ebene ist das physikalische Übertragungsmedium. Im Sieben-Schichten-ISO-OSI-Modell [ISO7498 94] wird diese Ebene als

Schicht-1 bzw. Bitübertragungsschicht (*physical layer*) bezeichnet (in [Tanenbaum 92] findet sich eine ausführliche Darstellung des OSI-Modells). Die Aufgabe der Bitübertragungsschicht ist der Transport eines Bitstroms von einem Gerät zu einem anderen. Die darüber liegenden Ebenen werden durch die unterschiedlichen Protokollschichten gebildet.

Aktuell sind drei physikalische Übertragungsmedien bei Endgeräten im Einsatz: Die elektrische Leitung, die Funkstrecke und das Licht. Die leitungsgebundene Übertragung lässt sich auf drei unterschiedliche Schnittstellen-Typen aufteilen: Der LAN-Anschluss (*local area network*), die Modem-Schnittstelle zum Telefonnetz und die Schnittstellen für diverse Peripheriegeräte. Neben der elektrischen Leitung gewinnt immer mehr die Funkstrecke an Bedeutung. Diese wird durch die fortschreitende Verbreitung mobiler Endgeräte belegt. Hierbei werden Bluetooth-Schnittstellen mehr für den Anschluss von Peripheriegeräten oder zur direkten Verbindung zweier Endgeräte eingesetzt. Wireless LAN (WLAN) dagegen ist der drahtlose Ersatz für drahtgebundene Netzwerkverbindung. Das Mobilfunknetz mit seinen unterschiedlichen Daten-Übertragungstechniken wie CSD (*circuit switched data*), HSCSD (*high speed* CSD) und GPRS (*general packet switched radio system*) liefern im Gegensatz hierzu nur relativ bescheidene Bandbreiten (siehe [Zimmermann 03b]). Erst UMTS (*universal mobile transmission system*) ermöglicht relevante Bandbreiten.

Vor der Einführung von Bluetooth war die optische Übertragung mit IRDA sehr weit verbreitet. In [Zimmermann 03b] werden die unterschiedlichen Übertragungstechniken genauer behandelt. Zimmermann beschreibt hierbei speziell die Übertragungstechniken, die eine direkte Übertragung von Endgerät zu Endgerät ermöglichen. Eine spezielle Erweiterung für das PotatoSystem nutzt diese direkte Verbindung (vgl. Seite 140)

4.1.2 Ein- und Ausgabeschnittstellen

Konsumentin Ginny steuert ihr Endgerät über diverse Eingabeschnittstellen. Eingaben erfolgen einerseits zur Vorbereitung des Konsums als auch beim interaktiven Konsum selbst. Übliche Eingabeschnittstellen an Endgeräten sind Tasten, Dreher, Schieber und Zeigegeräte (wie Maus oder Touchpad), über die am Bildschirm ein Cursor gesteuert werden kann. Speziellere Schnittstellen sind Mikrofone und Kameras.

Die Ausgabeschnittstellen, die ebenso wie die Eingabeschnittstellen entweder im Endgerät integriert sind oder an dieses angeschlossen werden können, ermöglichen erst den eigentlichen Konsum der virtuellen Güter. Sie verwandeln die Nutzdaten in für den Menschen wahrnehmbare Reize. Typischerweise werden die Nutzdaten über Anzeigen in optische Reize und über Lautsprecher in akustische Reize verwandelt. Es gibt Anzeigen in den unterschiedlichsten Formen; von einer einzeln LED bis zu holographischen Displays. Auch Lautsprecher bzw. Kopfhörer existieren in vielfältigen Formen. Bei aktuellen Raumklangsystemen [Iosono 05] werden eine Vielzahl von Lautsprechern vom Endgerät angesteuert. Die Nutzung anderer Sinne des Menschen wie z. B. den Berührungs- oder Geruchssinn werden hingegen noch kaum genutzt.

4.1.3 Permanentspeicher

Sollen virtuelle Güter ohne Verbindung zum Anbieter mehrfach konsumiert werden, müssen die zugrunde liegenden Nutzdaten dauerhaft zwischengespeichert werden

können. Dauerhaft zwischenspeichern meint hier nicht dauerhaft archivieren, sondern dauerhaft im Endgerät speichern, so dass die Daten auch nach dem Ausschalten und wieder Einschalten zur Verfügung stehen.

Die hierzu eingesetzten Permanentspeicher lassen sich nach ihrer Speichertechnologie, Speicherkapazität, Speicherzeiten, Wechselmöglichkeit und Zugriffsmöglichkeiten unterscheiden.

- Da die eingesetzte **Speichertechnologie** fortwährend dem technischen Fortschritt unterworfen ist und für die Vermarktung virtueller Güter primär nicht entscheidend ist, kann die Einteilung kurz gefasst werden. Ein grobe Unterteilung erfolgt in die magneto-optische- und Halbleiter-Technologie. Festplatten sind magnetische Speicher. Die wechselbaren Speicherkarten enthalten in der Regel Halbleiterspeicher.
- Die **Speicherkapazität** bei Festplatten wird in Gigabyte (10^9 Byte) gemessen. Festplatten mit einer Kapazität über einem Terabyte (10^{12} Byte) sind in Kürze keine Besonderheit mehr. Permanentspeicher auf Halbleiterbasis sind über ein Gigabyte noch etwas Besonderes.
- Die **Speicherzeiten** lassen sich in Lese- und Schreibtransferraten und den eigentlichen Zugriffszeiten unterteilen. In der Regel lassen die realisierten Zeit-Parameter keinen Wunsch für den Konsum der meisten virtueller Güter offen. In der Regel sind die verfügbaren Kommunikationsschnittstellen (siehe) mit ihren angeschlossenen Kommunikationsnetzen mit deutlich schlechteren Zeit-Parametern ausgestattet.
- Die **Wechselmöglichkeit** des permanenten Speichers ist für den Vertrieb von virtuellen Gütern von größerer Bedeutung. Hierdurch wird der mehrfache Konsum auf unterschiedlichen Endgeräten möglich.
- Die verschiedenen **Zugriffsmöglichkeiten** (vgl. Tabelle 4.1) für den Konsumenten auf die gespeicherten Nutzdaten sind ebenso bedeutsam wie die Wechselmöglichkeit.

Tabelle 4.1
Zugriffsmöglichkeiten des Konsumenten auf permanent gespeicherte Nutzdaten

Speicherung	Zugriffsmöglichkeiten des Nutzers
im Dateisystem	kopieren, löschen, modifizieren, übertragen und wiedergeben
im unsichtbaren Bereich	Zugriff nur über eine spezielle Steuerung, die Zugriff auf den unsichtbaren Bereich hat
als verschlüsselte Datei im Dateisystem	kopieren, löschen und übertragen der verschlüsselten Datei

Werden die Nutzdaten auf dem Permanentspeicher durch ein dem Nutzer sichtbar gemachtes Dateisystem verwaltet, hat der Nutzer (in der Regel) über die Steuerung (vgl. Kapitel 4.1.4) vollen Zugriff auf die Daten. Der Nutzer kann Dateien kopieren, löschen, auf andere Geräte übertragen und jederzeit über den Decoder (vgl. Kapitel 4.1.4) wiedergeben (konsumieren). Werden die Nutzdaten in einem für den Nutzer unsichtbaren Bereich des Permanentspeichers abgelegt bzw. über ein internes

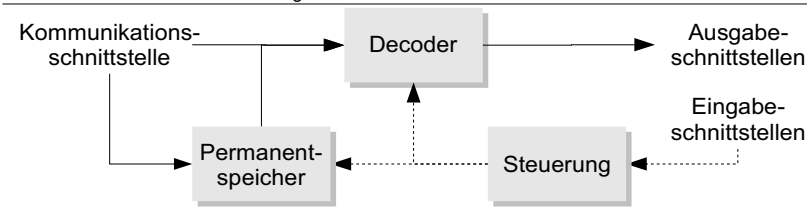
Dateisystem verwaltet, so hat der Nutzer keinen vollen Zugriff. Die Entscheidung über den Konsum bzw. anderer Operationen obliegt der Steuerung des Endgerätes. Ist die Software für die Steuerung unveränderlich, so kann der Hersteller des Endgerätes den Nutzer im Konsum der virtuellen Ware einschränken. In der Regel wird dem Nutzer dadurch das Kopieren unmöglich gemacht.

Bei Endgeräten mit einer für den Nutzer sichtbaren Dateiverwaltung aber ohne einer Möglichkeit Dateien in einem für den Nutzer unsichtbaren Bereichen abzulegen, bleibt nur die verschlüsselte Speicherung der Daten, um den Nutzer im Konsum der virtuellen Güter einzuschränken, bzw. zu kontrollieren. Ist der Nutzer allerdings in der Lage die Software in der Steuerung zu modifizieren oder zu ergänzen, so hat er in der Regel auch Zugriff auf die separat gespeicherten Schlüssel. In Kapitel 4.3.2 wird auf den Kopierschutz auf dem Endgerät genauer eingegangen.

4.1.4 Decoder und Steuerung

Der Decoder bildet neben der Steuerung das zentrale Element im Endgerät. Der Decoder ist eine Hard/Software-Kombination, die die Nutzdaten so aufbereitet (decodiert), dass sie über an den Ausgabeschnittstellen angeschlossene Ausgabegeräte konsumiert werden kann (vgl. Abbildung 4.2).

Abbildung 4.2
Der Daten- und Steuerfluss im Endgerät



Die zu decodierenden Nutzdaten können entweder von außen über die Kommuniktionsschnittstellen (mit den diversen Protokollen) oder von innen über den Permanentspeicher dem Decoder zugeführt werden. Je nach Grad der Interaktivität der virtuellen Güter, hat der Konsument mehr oder weniger Möglichkeit über die Eingabeschnittstellen auf den Ablauf der Decodierung Einfluss zu nehmen.

4.1.4.1 Spezialisierte festprogrammierte Endgeräte

Spezialisierte und festprogrammierte Endgeräte ermöglichen nur die Wiedergabe der vom Gerätehersteller festgelegten Nutzdatenformate. Weder die Steuerung, noch der Decoder des Endgerätes können durch den Anwender umprogrammiert werden. Es können somit auch keinerlei virtuelle Güter mit neueren Formaten wiedergegeben werden. Ein handelsüblicher DVD-Spieler fällt bspw. in diese Kategorie. Ebenso fallen einfache Handys, die nur eine bei der Herstellung des Gerätes festgelegte Art von Klingeltönen, SMS bzw. MMS wiedergeben können, in diese Kategorie.

Aufgrund der fehlenden Möglichkeit der Programmierung bzw. der Unmöglichkeit zusätzlich Software zu laden, können nur begrenzt interaktive Formate wiedergegeben werden. Ein Vorteil dieser festprogrammierten Endgeräte ist allerdings, dass sie

aufgrund ihrer begrenzten Funktionalität sehr kostengünstig hergestellt werden können.

Bestimmte Mobiltelefone, die zwar die Möglichkeit besitzen die Steuerung umzuprogrammieren, fallen zum Teil ebenfalls in diese Gerätekategorie. Diese Geräte besitzen fest in Hardware umgesetzte Decoder für Musikformate wie z. B. MP3 oder AAC (*Advanced Audio Coding*) [Zimmermann 03b].

4.1.4.2 Universelle nutzerprogrammierbare Endgeräte

Durch die Weiterentwicklung von Hard- und Software wachsen spezialisierte Endgeräte und der universelle nutzerprogrammierbare PC immer weiter zusammen. Die Leistungsfähigkeit der Hardware erlaubt inzwischen auch die Produktion von Mobilfunkendgeräten, die sowohl in der Steuerung als auch im Decoder durch den Nutzer umprogrammiert werden können. Diese nutzerseitige Programmierbarkeit hat den Erfolg der so genannten Wintel (*Win*dows und In*tel*) Rechner in den letzten 10 Jahren begründet.

Allerdings zeigt die massenhafte Nutzung dieser Systeme in Verbindung mit einem Zugang zum Internet Schwachstellen des Konzeptes bzw. der Umsetzung auf. Eine nutzerseitige Umprogrammierung erfolgt zunehmend durch ungewollte eingeschleuste Programme, die als Viren und Würmer bezeichnet werden. Die TCG (*Trusted Computing Group*) [WikiTGC 04] versucht daher diese Umprogrammierung generell technisch stärker zu reglementieren. Microsoft hat dieses Konzept zwischenzeitlich unter der Abkürzung NGSCB (Next Generation Secure Computing Base) [WikiNGSCB 04] aufgenommen (siehe auch [Kunze 04] zum NGSCB) und plant mittelfristig das Konzept in seinem Windows-Betriebssystem zu verankern. Kritiker sagen allerdings, dass es reichen würde Fehler und Sicherheitslücken in den bestehenden Windows-Systemen zu schließen. Sie befürchten, dass mit solchen „trusted“ Plattformen der Plattformanbieter (Microsoft) Mittel in die Hand bekommt, den Konsum virtueller Güter gesichert zu kontrollieren.

4.2 Systeme zur Verbreitung virtueller Güter

Das Endgerät ist nur eine Komponente in einem größeren technischen Gesamtsystems zur Umsetzung der in Kapitel 21 ausführlich geschilderten möglichen Geschäftsmodelle. Grundvoraussetzung für die verschiedenen Formen der Vermarktung ist eine Technik, die die effektive Verteilung bzw. Verbreitung virtueller Güter ermöglicht. zeigt einen Überblick über drei unterschiedliche Ansätze hierzu.

Über eine Kommunikationsschnittstelle, die das Endgerät mit dem Internet verbindet, ist der Server des Providers mit dem Endgerät der Konsumentin Ginny temporär oder dauerhaft verbunden. Auf dem Server werden die dort gespeicherten Nutzdaten der angebotenen virtuellen Güter mit einem speziellen Content-Management-System (CMS) [WikiCMS 05] verwaltet.

Konsumentin Ginny hat mit ihrem Endgerät hierbei grundsätzlich zwei verschiedene technische Möglichkeiten: den Datei-Download oder den Online-Konsum.

4.2.1 Datei-Download

Beim Datei-Download transferiert die Konsumentin während einer temporären Verbindung (typischerweise eine Internet-Verbindung) mit dem Server des Anbieters die

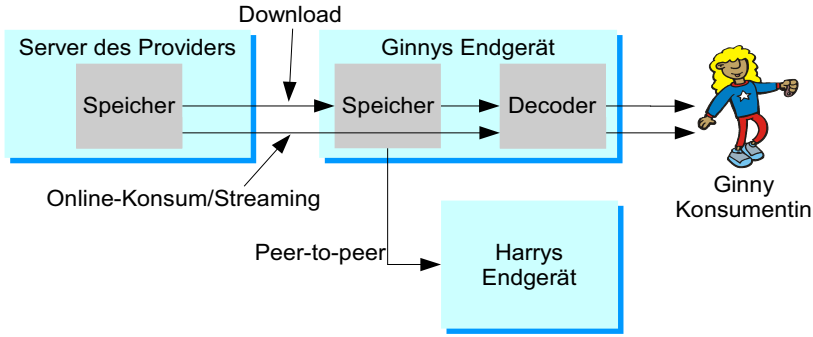
gewünschten Dateien bspw. per FTP oder HTTP in den Permanentspeicher (Festplatte oder Speicherkarte) ihres Endgerätes. Im Anschluss an diesen Download-Vorgang kann sie ohne weitere Verbindung zum Anbieter-Server mit dem Decoder in ihrem Endgerät die virtuelle Ware solange kein DRM (vgl. Kapitel 4.4) beteiligt ist beliebig oft und zeitlich unbegrenzt konsumieren (obere Linien in). In Kapitel 3 wurden bereits hierbei mögliche Erlösformen und bereits übliche Geschäftsmodelle genannt.

Bietet ein Provider sehr viele Dateien an, deren Anzahl und Zusammenstellung sich immer wieder ändert, wird der Einsatz einer speziellen Server-basierten Verwaltungssoftware – einem Content-Management-System – sinnvoll. Diese Systeme erleichtern dem Anbieter die Strukturierung und Aktualisierung der angebotenen virtuellen Güter. Dem Konsumenten erleichtert dies oft die Suche nach speziellen Inhalten.

4.2.2 Online-Konsum und Streaming

Beim Online-Konsum bzw. Streaming von Nutzdaten wird der Zwischenschritt der expliziten Speicherung von Dateien im Permanentspeicher des Endgerätes übersprungen. Die Decodierung der Nutzdaten setzt unmittelbar ein. In der Regel finden sich nach der Decodierung die Nutzdaten nicht mehr auf dem Endgerät. Soll ein erneuter Konsum erfolgen, so muss das Endgerät sich wieder mit den Server des Providers verbinden.

Abbildung 4.3
Das Endgerät als Bestandteil von Systemen zur Verbreitung virtueller Güter



Beim Streaming wird ein kontinuierlicher Nutzdatenstrom (daher auch der Name Streaming) von einzeln decodierbaren Datenpaketen vom Provider bis zum Decoder im Endgerät aufgebaut. Die Datenpakete werden auf dem Endgerät unmittelbar nach ihrem Eintreffen mit zeitlich fest gelegter Rate dekodiert. Häufig puffert der Decoder eine gewissen Anzahl an Paketen, um eine schwankende Kanalkapazität auszugleichen. Typischerweise sind alle Audio- und Videoformate streamingfähig. Bei Live-Ereignissen ist eine Stream die einzig sinnvolle Form der digitalen Übertragung.

Neben Streaming gibt es noch andere Formen des Online-Konsums. So kann man das normale „Surfen“ über Web-Seiten auch als Online-Konsum bezeichnen. Alle

aktuellen Browser zeigen inzwischen eine HTML-Seite schon an, auch wenn noch nicht alle zugehörigen Nutzdaten übertragen wurden.

In Kapitel 3 wurden für den Online-Konsum entsprechende Erlösformen und Geschäftsmodelle benannt. Im Gegensatz zum Download kommt beim hierbei stärker der Service-Aspekt zum tragen. Der Provider erfüllt stärker die Rolle eines Dienstleisters und nicht die eines Händlers oder Lieferanten (vgl. Definition für Dienstleistung in Kapitel 2.1.1).

4.2.3 Peer-to-peer (P2P)

Peer-to-peer (P2P) heißt frei übersetzt „gleich zu gleich“. Der übliche Download-Vorgang bzw. Online-Konsum geht von dezidierten Servern aus, die für viele Client-Endgeräte die gewünschten Nutzdaten bereitstellen. Da die Internet-Transportprotokolle keine solche reine Client-Rolle für die Endgeräte erzwingen, können die Endgeräte auch ganz leicht für andere Endgeräte eine Server-Funktion übernehmen. Netze in denen gleichberechtigte Endgeräte kommunizieren, werden als P2P-Netze bezeichnet.

P2P-Netze können zum Verteilen virtueller Güter an weitere Konsumenten, ohne die Zustimmung des originalen Providers bzw. Rechtsinhabers, genutzt werden, wie Systeme wie KaZaA und andere es demonstrieren. Bspw. von Ginnys auf Harrys Endgerät.

Verschiedene Ansätze, die unter dem Begriff Superdistribution (vgl. Kapitel 3.6.4) zusammengefasst werden können, versuchen die Verbreitungstechnik P2P mit verschiedenen Erlösformen und Geschäftsmodellen zu verbinden.

4.2.3.1 P2P-Modelle

Bei den P2P-Netzwerken lassen sich drei unterschiedliche Modelle identifizieren: Dezentral, zentral und hybrid.

■ Zentrale Systeme

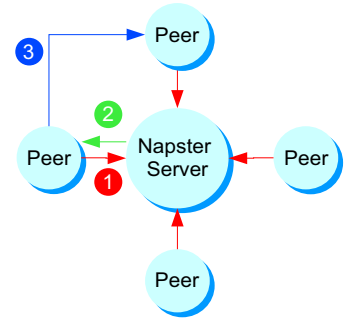
Zentrale P2P-Systeme, die auch assistierte P2P-Systeme genannt werden, bildeten den Ausgangspunkt der P2P-Entwicklung. Sie sind im eigentlichen Sinne keine P2P-Systeme, da sie eine zentrale Komponente besitzen. Dieser zentrale Server indexiert die verbundenen Computer (Peers) und die darauf verfügbaren Dateien. Dieses Verzeichnis dient den anderen Peers als Übersicht über die verfügbaren Ressourcen.

Abbildung 4.4 zeigt wie im ursprünglichen Napster-P2P-System [WikiNapster 05] (inzwischen findet sich unter Napster.com der kommerzielle Musik-Download-Dienst Napster 2.0, der nur noch den Namen mit dem ursprünglichen System gleich hat) die Kommunikation ablief, nachdem die beteiligten Peers ihre freigegebenen Dateien beim zentralen Server bekannt gemacht haben. Bei einer Anfrage (Schritt 1) oder der Suche nach einer bestimmten Datei generiert der Server eine Liste (Schritt 2) mit den Dateien, die dieser Anfrage genügen. Aus dieser Liste wählt sich der anfragende Peer die gewünschte Datei aus und stellt eine direkte Verbindung (Schritt 3) mit dem Rechner her, auf dem sich die Datei befindet. Der zentrale Server ermöglicht zwar eine gute Pflege des Datenbestands, hat aber im Falle von Napster als „single-point-of-failure“ die Abschaltung ermöglicht.

Dezentrale Systeme

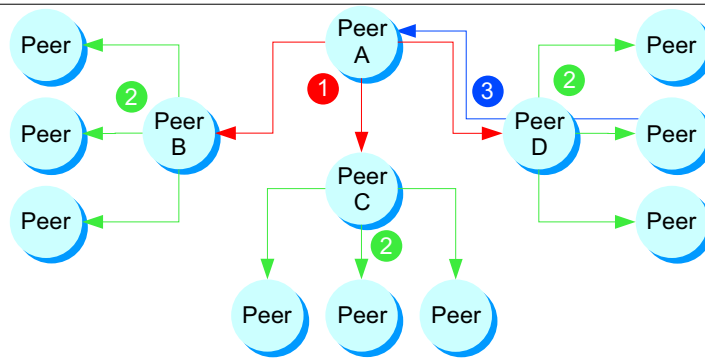
Dezentrale P2P-Systeme sind die eigentlichen P2P-Systeme, bei denen alle Peers mit der gleichen speziellen Steuerungssoftware ausgestattet sind. Diese Software ermöglicht sowohl die Freigabe von Dateien für andere Peers als auch die Suche von Dateien im P2P-Netz. Die Peers fungieren gleichzeitig als Client und Server und werden daher auch als Servants bezeichnet. Jeder Servant kennt eine begrenzte Anzahl von anderen Servants (in Abbildung 4.5 kennt Peer A die Peers B, C und D), die wiederum weitere Servants in deren Umfeld kennen. Hierdurch spannt sich schließlich das gesamte P2P-Netz auf, in dem kein Servant alle anderen Servants kennt.

Abbildung 4.4
Assistiertes Peer-to-Peer



1. Peer stellt Anfrage an Server, der in seiner Datenbank sucht.
2. Server sendet Liste, der bereithaltenden Peers
3. Benutzer fordert die Datei direkt von einem weiteren Peer an.

Abbildung 4.5
Dezentrales Peer-to-Peer



1. A sendet Anfrage an B, C und D
2. B, C und D senden die Anfrage an die ihnen bekannten Peers weiter
3. Wurde die gesuchte Datei gefunden, so wird dies über den gleichen Weg zurück gemeldet. Der Transfer der Datei erfolgt ohne Zwischenstation.

Der Vorteil dieser dezentralen Systeme ist die fehlende zentrale Komponente, wodurch die Robustheit des Netzwerkes gewährleistet wird. Es gibt, anders als beim ursprünglichen Napster, keinen „single-point-of-failure“. Ein Ausfall eines Peers hat nur geringe Auswirkung auf den Rest des Netzes. Ein großer Nachteil hingegen stellt die Anschlussproblematik dar, da sich die Peer-Suche nicht anhand von Inhalten oder der Identität von Anwendern steuern lässt [Biedermann 02]. Peers, die nicht permanent online sind, müssen sich jedes Mal erneut einen Zugang (einen Peer, der online

ist) suchen. Der Kontakt zu diesen Peers wird entweder über bekannte IP-Adressen oder mit Hilfe von Broadcast-Nachrichten hergestellt.

Abbildung 4.5 zeigt, wie die Suche nach einer Datei oder einer anderen Ressource in einem dezentralen P2P-Netzwerk abläuft. Der suchende Peer A gibt (in Schritt 1) die Anfrage nur an die ihm bekannten Peers weiter. Peers, die die Anfrage nicht bedienen können geben im zweiten Schritt die Anfrage an die Ihnen bekannten Peers weiter. Dies geschieht solange bis entweder die Datei gefunden wurde oder eine maximale festgelegte Suchtiefe erreicht wurde. Peers die die gesuchte Datei bereithalten reichen (Schritt 3) Ihre Adresse entlang des Suchpfades zurück zum suchenden Peer. Dieser kann nun die Datei direkt (P2P) transferieren.

Hybride Systeme

Hybride P2P-Systeme verbinden dezentrale und zentrale Techniken. Die Peers können in einer solchen Topologie unterschiedliche Rollen einnehmen. Ist ein Rechner in Bezug auf Performance und Netzanbindung als ein zentraler Server geeignet kann dieser die Rolle eines so genannten *Supernodes* (Bezeichnung aus dem FastTrack-System, vgl. Seite 43) einnehmen.

4.2.3.2 P2P-Technologien

Im folgenden sollen beispielhaft einige bekannte, praktisch umgesetzte, dezentrale bzw. hybride P2P-Technologien angesprochen werden.

Gnutella

Gnutella ist wohl eines der bekanntesten Protokolle für Peer-to-Peer-Systeme. Es wurde 2000 von Justin Frankel veröffentlicht [WikiFrankel 05]. Allerdings musste er dieses Projekt wenig später auf Druck von AOL wieder einstellen. Einer Nutzergemeinschaft gelang es aber das zugrunde liegende Protokoll durch Reverse-Engineering zu ermitteln. Dieses Protokoll existiert momentan in zwei Varianten. Die erste Variante (Version 0.4) basiert auf einem reinen Peer-to-Peer-System. Daher gibt es nur die Peers (Servants) mit denen der Nutzer arbeitet. Allerdings ist diese Aussage nur zum Teil korrekt, denn zum Finden anderer Peers werden schon in der Version 0.4 so genannte GwebCache-Server benutzt. Diese Server werden aber nur beim Starten eines Peers benutzt, damit sich dieser in das Gnutella-Netzwerk eingliedern kann. Es wird ausdrücklich in den Dokumenten unter [Gnutella 05] vor einem zu häufigen benutzen dieser Server gewarnt, da sie sehr hohe Antwortzeiten haben können [Eberhardt 04].

Auf Gnutella basieren viele verschiedenen Clients (bzw. Servants), wie bspw. Gnotella, BearShare, Toadnode, Gnut und Limeware. Abbildung 4.5 skizziert das dezentrale Gnutella-Protokoll. Anfragen werden per Broadcasts mit einem Time-to-Live (TTL) Zähler versehen an andere Peers weitergeleitet. Die Anwendung dieser Broadcasttechnologie gilt als problematisch, da hierbei sehr viele Nachrichten entstehen können. Hierdurch ist die Skalierbarkeit des Systems nicht gewährleistet. Durch den notwendigen Einsatz des TTL-Zählers, der an der Suchanfrage angefügt die Suchtiefe begrenzt, kann nicht mehr garantiert werden, dass wirklich alle Ressourcen im System gefunden werden. Geht man davon aus, dass jeder Peer im Mittel $N_{Mittel}=3$ neue Peers kennt, so werden bei einer einzigen Suche und einer maximalen Such-

tiefe (Hops) von $TTL_{max}=8$ insgesamt 9840 Suchanfragen erzeugt. Bei $N_{Mittel}=10$ sind es schon über 11 Millionen Suchanfragen (vgl. Formel 4.1).

Formel 4.1

$$Nachrichten = \sum^{n=TTL_{max}} N_{Mittel}{}^{n} = \sum^{n=8} 3^{n} = 9840$$

In der Version 0.6 des Gnutella-Protokolls [Gnutella 05] wurden so genannte Ultra-Peers (bzw. Ultra-Nodes) eingeführt. Diese Ultra-Peers müssen bestimmte Voraussetzungen erfüllen. So ist es wichtig, dass sie über eine zuverlässige Netzwerkverbindung und ausreichend Hardware-Ressourcen verfügen. Auf diese Weise wird Gnutella zu einem hybriden P2P-System.

Freenet [Eberhardt 04]

Bei Freenet [Freenet 05] handelt es sich um eine Art verteiltes Dateisystem. Das Freenet-Protokoll ist ebenfalls ein reines dezentrales Peer-to-Peer-System. Freenet kommt im Gegenzug zu Gnutella ohne die problematischen Broadcasts aus. Dies wird durch einen speziellen Routing-Algorithmus ermöglicht. Hierbei werden die gesamten Ressourcen auf einen Index-Raum mit Hilfe einer Hash-Funktion abgebildet. Jeder Peer stellt seine Ressourcen – in erster Linie Festplattenspeicher – zur Verfügung. Dieser Festplattenspeicher wird genutzt um Dateien zu speichern, die zu einem bestimmten Teil des Index-Raumes gehören. Dadurch hat der Nutzer eines solchen Peers aber keine Möglichkeit mehr zu bestimmen welche Ressourcen er auf seinem Rechner verfügbar halten möchte und welche nicht. Ein Nutzer hat nur die Möglichkeit Content anzufragen oder Content hinzuzufügen. Ein Peer spezialisiert sich mit der Zeit auf einen bestimmten Teil des globalen Index-Raumes. Die Entscheidung, auf welchen Teil des Index-Raumes sich ein Peer spezialisiert, wird vom Gesamtsystem getroffen. Die im Freenet eingesetzte zusätzliche Verschlüsselung bietet ein sehr hohes Maß an Anonymität.

Sollte ein Peer auf ein Anfrage nicht antworten können und auch eine Weiterleitung der Anfrage nicht möglich sein, so wird sie an den sendenden Peer zurückgeschickt und dieser sucht nun den Peer mit der nächst kleineren Trefferwahrscheinlichkeit heraus. Durch diesen Algorithmus stellt Freenet einen Tiefensuch-Algorithmus auf einem extrem verteilten und dynamischen System dar (siehe auch [Freenet 05]).

FastTrack

Die FastTrack-Protokoll-Familie mit ihren Clients Morpheus, Grokster, iMesh und KaZaA stellt ein hybrides P2P-System dar. FastTrack basiert auf dem Gnutella-Protokoll und erweitert es um die Instanz der so genannten Supernodes. Bei der FastTrack-Netzwerkstruktur haben viele User-Peers eine Client-Server-Beziehung zu den so genannten Supernodes, welche untereinander ein Gnutella-ähnliches dezentralisiertes Netz bilden. Die Supernode-Funktionalität ist in die Client-Software integriert und jeder Teilnehmer kann, sofern genügend Bandbreite und Rechenleistung vorhanden sind, seinen Computer zu einem Supernode machen.

Supernodes werden je nach Auslastung automatisch und dynamisch ausgewählt und übernehmen die Verwaltung der Suchanfragen der normalen Peers. Die untereinander kommunizierenden Supernodes bilden das eigentliche FastTrack-Netz-

werk. Nach dem Start des Programms erhält der Client vom Server die IPs von den Supernodes bzw. er greift auf die in das Programm fest integrierte Adressliste von Supernodes (bzw. SuperPeers) zu. Dann übermittelt der Peer dem Supernode eine Liste mit seinen angebotenen Dateien. So erstrecken sich die Suchanfragen lediglich auf die Supernodes, die dann die IPs der jeweiligen Peers bereithalten. Der Datentransfer findet dann direkt zwischen den einzelnen Peers statt.

Das ursprüngliche FastTrack-Protokoll ist im Eigentum mehrerer Firmen unter anderem der Sharman Inc., dem Betreiber des KaZaA-Netzwerkes. Daher gibt es auch keine offizielle Dokumentation über dieses Protokoll. Es ist aber gelungen die Kommunikation zwischen dem User-Peer und den Supernodes zu analysieren. Das Ergebnis dieser Untersuchungen kann unter [FastTrack 04] nachgelesen werden.

JXTA

Im Gegensatz zu Gnutella und FastTrack ist JXTA ein offenes Projekt. Ursprünglich wurde es von der Firma Sun entwickelt, inzwischen wird es von der JXTA Community [JXTA 04] verwaltet und weiterentwickelt. JXTA steht für „juxtapose“ was soviel wie „nebeneinander stellen“ heißt. JXTA ist kein P2P-System mit fertigen Clients, es stellt vielmehr die Spezifikation und Architektur für eine allgemein einsetzbare P2P-Plattform mit einheitlichen Schnittstellen und offen gelegten Protokollen bereit. Die Referenz-Implementierung der sechs JXTA-Protokolle ist in Java verfügbar. Eine Implementierung in C++ ist parallel in Arbeit. JXTA spezifiziert ein hybrides P2P-System mit drei verschiedenen Knoten:

- Normale Peers (*Edge Peers*) geben Ressourcen über spezielle XML-Datenstrukturen (den so genannten Advertisements) frei und fragen diese XML-Dokumente auf anderen Peers nach. Die Peers sind in Gruppen organisiert.
- Rendezvous-Peers sind die Supernodes von JXTA. Sie sind für die Bearbeitung von Suchanfragen zuständig. Jeder Peer meldet sich bei mindestens einem Rendezvous-Peer an. Sollte für einen normalen Peer kein Rendezvous-Peer erreichbar sein, so stellt dieser Peer automatisch einen Rendezvous-Peer dar.
- So genannte Relay-Peers ermöglichen normalen Peers, die hinter einer Firewall sind, die Kommunikation mit anderen Peers.

Alle freigegebenen Ressourcen (die Advertisements) werden ab Version 2 von JXTA mit Hilfe des *Shared Resource Distributed Index* (SRDI) auf einen Index-Raum abgebildet. Die Gesamtheit aller Rendezvous-Peers bildet somit eine verteilte und redundante Hash-Tabelle über diesen Index-Raum. Jeder Rendezvous-Peer führt eine Liste mit den benachbarten Rendezvous-Peers mit denen er Teile seiner Freigaben teilt. Sollte ein Rendezvous-Peer eine Anfrage nicht beantworten können, so wird diese an einen anderen Rendezvous-Peer weitergeleitet. Dieses Verfahren soll gegenüber der Version 1 zu einer besseren Skalierbarkeit des Systems führen. Anfragen werde daher nur an Rendezvous-Peers gestellt und auch nur von diesen an andere Rendezvous-Peers weitergeleitet [Eberhardt 04]. Wobei JXTA die Zahl der Hops auf $TTL_{max}=7$ begrenzt und automatisch Kreise vermeidet. Weitere Details finden sich im JXTA 2.3.x: Java Programmer's Guide [JXTAProg 05].

4.3 Verhinderung der Verbreitung und Kontrolle der Nutzung

Nachdem zuvor Systeme beschrieben wurden, die eine Verbreitung virtueller Güter ermöglichen bzw. erleichtern, soll nun der Fokus auf Systeme und Verfahren gelegt werden, die die Verbreitung bzw. Nutzung der Nutzdaten einschränken. Der Provider hat oft ein sehr berechtigtes Interesse daran, dass die Verteilung seiner virtuellen Waren nur unter seiner Kontrolle stattfindet. Den Urhebern virtueller Güter wurde im September 2003 novellierten Urheberrecht [UrhG 03] explizit das alleinige Recht hierfür zugesprochen.

Den Urhebern bzw. den für den Vertrieb beauftragten Anbietern stehen zur Wahrung ihrer Rechte prinzipiell zwei unterschiedliche technische Lösungen bereit. Der Anbieter kann entweder versuchen, die Weiterverbreitung durch technische Maßnahmen direkt zu unterbinden, oder er versucht die illegale Weitergabe zu detektieren, um dann juristisch gegen die illegalen Verbreiter vorzugehen.

4.3.1 Urheberrecht und Urheberschutz

Das Urheberrecht soll einen Ausgleich zwischen den Interessen der Allgemeinheit an der möglichst ungehinderten Nutzung wertvoller Inhalte und den Interessen der Rechteinhaber an Kontrolle und wirtschaftlicher Verwertung schaffen. Das deutsche Urheberrecht [UrhG 03] behält dem Berechtigten vor, über jede Art von Verwertung zu entscheiden und hieran wirtschaftlich teilzuhaben – anders gesagt, steht dem Schöpfer eines Werkes (zunächst – er kann es ja übertragen) das alleinige Verwertungsrecht zu [Kunze 04].

4.3.1.1 Historische Entwicklung

Das Urheberrecht, welches wir heute kennen, ist allerdings kein sehr altes Recht. Kunze beschreibt in [Kunze 04] über die Entwicklung in den letzten ca. 500 Jahren: Vor der Erfindung des Buchdrucks gab es wenig Bedarf sich mit dieser Materie zu befassen. Erst im 18. Jahrhundert wurde eine Theorie vom geistigen Eigentum entwickelt. In einem englischen Gesetz von 1710 wurde erstmals ein ausschließliches Vervielfältigungsrecht des Autors anerkannt (*intellectual property*). Zuvor wurden primär die Rechte der Verleger geschützt.

In den neu gegründeten Vereinigten Staaten von Amerika wurde das geistige Eigentum unter den Schutz der Verfassung von 1788 gestellt. Kurz darauf wurde auch in Frankreich durch zwei Revolutionsgesetze von 1791 und 1793 das „*propriété littéraire et artistique*“ anerkannt. Preußen folgte am 11. Juni 1837 mit dem „Gesetz zum Schutze des Eigenthums an Werken der Wissenschaft und Kunst in Nachdruck und Nachbildung“. Es war das ausführlichste und zugleich modernste Urheberrechtsgesetz seiner Zeit. Noch im selben Jahr beschloss die Bundesversammlung (Deutscher Bund) eine 10-jährige Schutzfrist ab Erscheinen eines Werkes, die 1845 auf 30 Jahre – beginnend mit dem Tode des Urhebers – verlängert wurde. Das Urheberrecht in der Bundesrepublik Deutschland trat vor nunmehr 40 Jahren – am 9. September 1965 – in Kraft.

4.3.1.2 DMCA und die Urheberrechts-Novelle

Die Einführung des Buchdrucks ermöglichte erstmals die größere Vervielfältigung virtueller Güter. Somit wurde ein Urheberrecht überhaupt erst erforderlich. Die Digitalisierung virtueller Güter Ende des letzten Jahrhunderts brachte zusätzlich die Möglichkeit einer massenhaften privaten Kopie und Verteilung. Diese verlangte eine Überarbeitung des Urheberrechts.

1974 wurde als Unterorganisation der UNO die *World Intellectual Property Organization* (WIPO) gegründet. Im Dezember 1996 verabschiedete die WIPO zwei Abkommen: das *WIPO Copyright Treaty* und das *WIPO Performances and Phonograms Treaty*. Die USA waren nun gezwungen, gesetzgeberische Maßnahmen zu treffen, um die beiden WIPO-Abkommen zu erfüllen (was nur zum Teil stimmt, da sie ja diese Abkommen maßgeblich initiiert hatte). Das neue Gesetz, welches am 28. Oktober 1998 einstimmig durch den US Senat angenommen wurde, trägt den Namen *Digital Millenium Copyright Act* (DMCA).

Der DMCA besteht aus fünf Teilen. Der erste Teil ist wohl der umstrittenste Teil. Er erweitert das amerikanische Copyright Gesetz um das Verbot der Umgehung von Kopierschutzmechanismen, sowie das Verbot des Veränderns von *Copyright Management Information* (CMI). Dieser Teil des Gesetzes zeigte in der Praxis bereits entsprechende Probleme, die die Rechte der Konsumenten (nach Meinung der Gegner des DMCA) zu stark einschränken.

Auch die EU hatte die WIPO-Abkommen mit unterzeichnet. Folglich verabschiedete sie am 22. Mai 2001 die *European Union Copyright Directive* (EUCD, vgl. [EUCD 01]), die das Gegenstück zum amerikanischen DMCA darstellt. Am 11. April 2003 macht die Bundesrepublik Deutschland ihr Gesetz EUCD-konform, indem sie die so genannte Urheberrechts-Novelle verabschiedete. Das neue Urheberrechtsgesetz [UrhG 03] trat 5 Monate später, am 13. September 2003 in Kraft.

> *„Wirksame technische Maßnahmen zum Schutz eines nach diesem Gesetz geschützten Werkes oder eines anderen nach diesem Gesetz geschützten Schutzgegenstandes dürfen ohne Zustimmung des Rechtsinhabers nicht umgangen werden, soweit dem Handelnden bekannt ist oder den Umständen nach bekannt sein muss, dass die Umgehung erfolgt, um den Zugang zu einem solchen Werk oder Schutzgegenstand oder deren Nutzung zu ermöglichen.“ (Absatz 1 des neu ins Urheberrechtsgesetz [UrhG 03] aufgenommenen §95a)*

Was ist wirksam? Dies fragen sich gerade Informatiker, denn sie wissen, dass kein Schutz wirklich dauerhaft wirksam ist. Mit dem zweiten Absatz wird den Informatikern aber der Wind aus den Segeln genommen:

> *„ ...Technische Maßnahmen sind wirksam, soweit durch sie die Nutzung eines geschützten Werkes oder eines anderen nach diesem Gesetz geschützten Schutzgegenstandes von dem Rechtsinhaber durch eine Zugangskontrolle, einen Schutzmechanismus wie Verschlüsselung, Verzerrung oder sonstige Umwandlung oder einen Mechanismus zur Kontrolle der Vervielfältigung, die die Erreichung des Schutzziels sicherstellen, unter Kontrolle gehalten wird.“ [UrhG 03]*

Es wird im Gesetz bewusst keine Diskussion um technische Parameter geführt. Wenn die Nutzung vom Rechtsinhaber unter Kontrolle gehalten wird, dann sind die

zugehörigen technischen Maßnahmen wirksam und dürfen (mit im Gesetz definierten Ausnahmen) nicht umgangen werden. Die Kenntnis dieser Ausgangslage ist von entscheidender Bedeutung für die folgenden technischen Beschreibungen.

4.3.2 Kopierschutz auf dem Endgerät

Nach der Klarstellung des rechtlichen Hintergrundes von Verhinderungs- bzw. Schutzsystemen sollen als erstes die Prinzipien für Kopierschutz-Verfahren in den Endgeräten beschrieben werden. Der Kopierschutz für physikalische Datenträger soll hier nicht angesprochen werden. In [Hasselbach 02] kann hierzu mehr gefunden werden, wie bspw. zu Kopierschutzverfahren von Audio-CDs (vgl. auch [Wöhner 05]). Kopieren meint in diesem Kontext den Eins-zu-eins-Transfer (bzw. Versand oder Weiterleitung) eines auf einem Endgerät permanent gespeicherten virtuellen Gutes auf ein zweites Endgerät über eine Kommunikationsverbindung (vgl. den P2P-Transfer in).

In Tabelle 4.1 wurden bereits die zwei grundsätzlichen Techniken für die Verhinderung des Kopiervorgangs angesprochen. Die erste Variante greift überwachend in den Kopiervorgang (Steuerung) des Endgerätes ein. Die zweite Variante nutzt kryptographische Verfahren, um die Dekodierung auf ein spezielles Endgerät zu beschränken.

4.3.2.1 Überwachung des Kopiervorgangs

Die Überwachung des Kopiervorgangs ist technisch sehr einfach auf bestimmten Endgeräten zu realisieren. Folgende Voraussetzungen müssen hierfür bestehen:

- Die Dateien, für die ein Kopierschutz realisiert werden soll, müssen eine zusätzliche Information (Kopierschutzbit) mit sich tragen, die anzeigt, ob das Kopieren erlaubt ist.
- Das Endgerät muss so beschaffen sein, dass jeder angestoßene Kopiervorgang diese spezielle Information (Kopierschutzbit) in der zu kopierenden Datei ausliest und beachtet.

Das von der Firma Sony 1992 vorgestellte MiniDisk-System und DAT (*Digital Audio Tape*) [WikiDAT 04] nutzen das SCMS (*Serial Copy Management System*), welches dem Nutzer nur eine digitale 1:1-Kopie erlauben. Auf der ersten Kopie wird durch das SCMS des MiniDisk- oder DAT-Recoders das Kopierschutzbit gesetzt und bei weiteren Kopierversuchen auch durch die Geräte mit SCMS beachtet. Auch das von der Musikindustrie viel geschmähte MP3-Format enthält ein solches Kopierschutzbit. „Leider“ wurde noch kein PC gefunden, der sich um dieses Bit kümmert. Kritiker des DMCA (vgl. Kapitel 4.3.1.2) brachte dies schon auf die Idee, Microsoft zu verklagen, da die Firma „illegale“ Umgehungsprogramme (z. B. der Befehl *copy* unter MS-DOS) in ihren Betriebssystemen bereithält. Allerdings sind solch leicht zu durchschauenden Einträge in den Dateien auf nutzerprogrammierbaren Systemen (vgl. Kapitel 4.1.4.2) kaum als wirksam anzusehen und werden daher auch vollständig ignoriert.

Im Mobilfunk-Bereich wird eine Variante des Kopierschutzbits als *forward-lock* (OMA DRM 1.0 [OMA1 04]) bezeichnet. Bei Forward-lock wird über zusätzlich angefügte Steuerdaten dem Endgerät signalisiert, dass die Nutzdaten nicht an einen weiteren Nutzer weitergeschickt werden dürfen (siehe auch Kapitel 4.4.4). Die Firma No-

kia hatte bis zur Einführung von OMA DRM 1.0 mit CCL (*Closed Content List*) für ihre Handys eine sehr einfache eigene Lösung: Das mobile Endgerät erlaubt für eine im Endgerät vordefinierte Liste an MIME-Types grundsätzlich das Weiterschicken der Nutzdaten nicht.

4.3.2.2 Digitale Wasserzeichen als versteckter Kanal

So genannte digitale Wasserzeichen [Dittmann 00], [NeKuHe 01] stellen eine Möglichkeit dar, eine Zusatzinformationen direkt mit dem audiovisuellen Inhalt verbunden zu übertragen, ohne dass die Zusatzinformation hörbar bzw. sichtbar wird. Diese auch als „Watermarking" bezeichnete steganographische Technologie bettet die Zusatzinformation in die Nutzdaten (die das eigentliche virtuelle Gut verkörpern) ein, ohne dass dabei das zugrunde liegende Originalformat verändert wird. In diesem Zusammenhang spricht man auch von einem versteckten Kanal für Zusatzinformationen, der keine zusätzliche Infrastruktur benötigt [SiNeSp 03].

Digitale Wasserzeichen-Verfahren zur Einbettung und Extraktion existieren für Bilder, Bewegtbilder und Audiomaterial. Es wird dabei zwischen zerbrechlichen und robusten Wasserzeichen unterschieden. Während zerbrechliche Wasserzeichen Modifikationen an den Nutzdaten aufdecken können, sind robuste Wasserzeichen so beschaffen, dass die eingebrachte Information auch noch bei absichtlichen und unbeabsichtigten Modifikationen ausgelesen werden kann.

Abbildung 4.6
Robuste Wasserzeichen ermöglichen auch nach der Digital-Analog-Wandlung den Kopierschutz

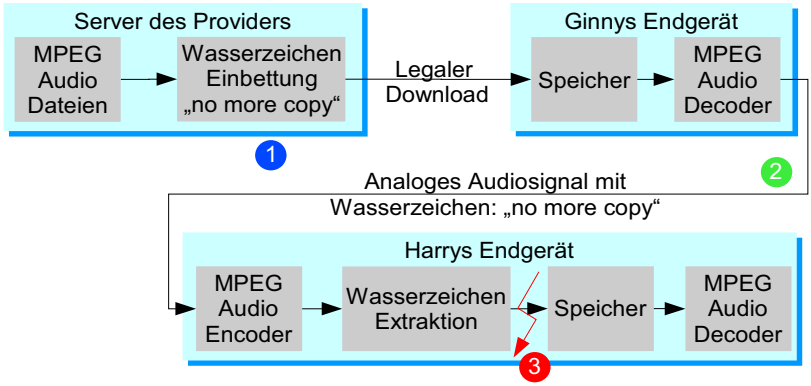


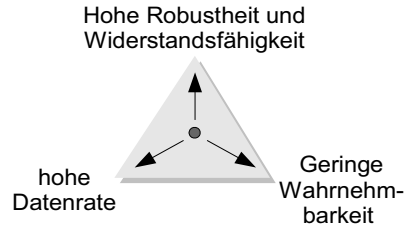
Abbildung 4.6 zeigt eine mögliche Anordnung, die mittels robuster Wasserzeichen illegale Kopien sogar über den Analog-Kanal verhindern soll. Dazu wird bereits auf Anbieterseite ein markantes Wasserzeichen eingebettet (Schritt 1). Der legale digitale Download auf Ginnys Endgerät ist hiervon unberührt. Wird nun über eine analoge Verbindung (Schritt 2) das Audiosignal, in dem das Wasserzeichen immer noch (unhörbar) enthalten ist, auf ein zweites Endgerät zum Zwecke der Kopie übertragen, so wird nach dem Encoder der Wasserzeichen-Extraktor aktiv (Schritt 3). Wird hierbei das markante Wasserzeichen („*no more copy*") detektiert, so wird die Speicherung nicht zugelassen.

Die vorgestellte Anordnung schien alle Piraterie-Probleme der Musik-Industrie zu lösen. Daher wurde im Rahmen der *Secure Digital Music Initiative* (SDMI) im Jahre 1999 [SDMI 04] ein solches Kopierschutz-Wasserzeichen vorgesehen. SDMI schrieb in 2000 einen Wettbewerb (*The SDMI Challenge*) aus, den Wasserzeichen-Schutz (der Firma Verance) zu brechen. Edward Felten [WikiFelten 04] und seinem Team gelang dies zur Überraschung von SDMI sehr durchgreifend. Es wurde ihm allerdings die Publikation untersagt. Das Wasserzeichen der Firma Verance kommt auch bei DVD-Audio zum Einsatz. Abgesehen davon, dass SDMI sich aus verschiedenen Gründen nicht durchgesetzt hat (vgl. [RoTrMo 02] Seite 131-133), ist die Unterbringung des Wasserzeichen-Extraktor im Endgerät des Nutzer als problematisch anzusehen. Der Nutzer kann einerseits den Erfolg seines Versuches das Wasserzeichen durch Manipulation (durch diverse analoge Veränderungen) zu zerstören unmittelbar selbst überprüfen. Andererseits kann der Anbieter später auch nicht mehr auf ein alternatives Wasserzeichen-Verfahren wechseln, da er die Extraktoren in den Endgeräten kaum mehr austauschen kann (vgl. auch Kapitel 4.3.3.3). Als weiteres Problem ist anzusehen, dass gewährleistet werden muss, dass alle Endgeräte mit einem Analogeingang auch einen solchen Wasserzeichen-Extraktor besitzen müssen. Dies ist nur sehr schwer durchzusetzen.

Des Weiteren ist abzusehen, dass für einen sehr sicheren Kopierschutz das Wasserzeichen derart robust (sicher vor erlaubten und unerlaubten Transformationen) eingebettet werden muss, dass eine Beeinflussung der Wiedergabequalität (geringe Wahrnehmbarkeit) nicht mehr ausgeschlossen werden kann.

Beim Einsatz von Wasserzeichen-Verfahren muss je nach Anwendung ein Kompromiss für den Arbeitspunkt zwischen drei widersprüchlichen Parameter gefunden werden (vgl. Abbildung 4.7). Der dritte Parameter ist die Datenrate für den versteckten Kanal.

Abbildung 4.7
Kompromiss beim Arbeitspunkt



Die am Fraunhofer IIS in Erlangen entwickelte Wasserzeichen-Technologie [IIS 05] für PCM-codierte und komprimierte MPEG-Audio-Signale baut auf das dort vorhanden Know-how in der Audio-Kodierung von MP3 und AAC auf. Das IIS-Wasserzeichen-Verfahren, welches durch den Fraunhofer-SpinOff MusicTrace [MusicTrace 05] vermarktet wird, wird allerdings nicht für Anwendungen angeboten, bei der der Endkunde den Extraktor benötigt. Die im Signal eingebrachte Information übersteht auch die Digital-Analog-Wandlung einer Lautsprecher-Mikrofon-Strecke.

Die im Audiosignal zu versteckende Information wird durch ein Spread-Spectrum-Verfahren über den ganzen Frequenzbereich verteilt und zyklisch in das gesamte Musikstück wiederholt eingebettet. Die Kunst ist es das eingebrachte Signal knapp über der Schwelle zuhalten, unterhalb der die Audio-Komprimierung es wieder entfernen würde. Die anfangs nur von den amerikanischen Militärs benutzten Spread-Spectrum-Verfahren gehen auf eine Erfindung der Schauspielerin Hedy Lamarr und des Komponisten George Antheil aus dem Jahre 1942 zurück. Die Details zu dieser Erfindung wurden in [Spread 05] zusammengefasst.

Bei der Wasserzeichen-Einbettung wird ein symmetrischer Schlüssel angewendet, der bei der Extraktion wieder vorliegen muss. Hierdurch ist es möglich auch bei der

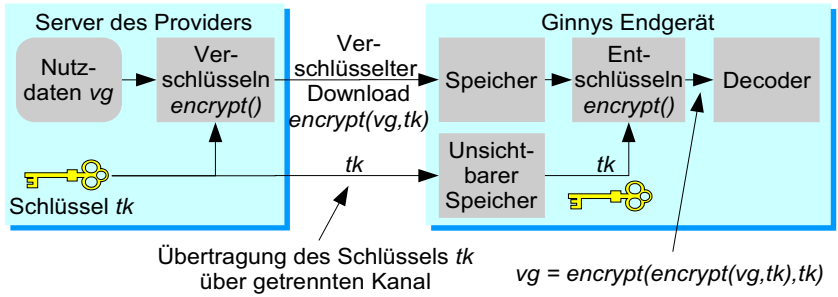
Offenlegung des Verfahrens die Wasserzeichen-Information geheim zuhalten. Im begrenzten Umfang können mehrere Wasserzeichen-Informationen getrennt voneinander nacheinander eingebracht werden.

4.3.2.3 Kryptographische Verfahren

Kann die Datei nicht dem direkten Zugriff des Nutzers entzogen werden, so bleibt nur noch eine Teil- oder Komplettverschlüsselung der Nutzdaten (vgl. Kapitel 4.1.3). Dieser Schritt bringt aber nur dann einen zusätzlichen Schutz vor illegaler Kopie, wenn der zugehörige Schlüssel getrennt und für den Nutzer nicht zugreifbar auf dem Endgerät gespeichert wird. Zur Verschlüsselung von größeren Datenmengen kommen nur symmetrische Algorithmen in Frage. Bei symmetrischen Verschlüsselungsverfahren (Sekret-Key-Kryptographie) wird zur Verschlüsselung und zur Entschlüsselung der gleiche (daher geheime) Schlüssel *tk* (Sitzungsschlüssel oder bei Musikstücken auch *track key* genannt) eingesetzt. Die Algorithmen arbeiten in der Regel blockweise, wobei die Datenblöcke die Länge des Schlüssels haben. Dadurch eignen sich symmetrische Verfahren auch zur kontinuierlichen Verschlüsselung und Entschlüsselung von Nutzdaten-Streams. (Details zu kryptographischen Verfahren in [Wobst 98] und [Raepple 98])

2001 hat der Rijndael-Algorithmus [Rijmen 04] unter dem Namen AES (*Advanced Encryption Standard*) den veralteten DES bzw. Triple-DES-Algorithmus offiziell als Standard abgelöst [FIPS197 01]. AES arbeitet entweder mit Schlüsseln der Länge 128, 192 oder 256 Bit auf Datenblöcken der Länge 128 Bit. AES darf zum aktuellen Zeitpunkt (2005) für den Schutz der Nutzdaten mehr als ausreichend sicher angesehen werden. Hartmann erläutert in seiner Arbeit [Hartmann 04] detailliert die Funktionsweise des Rijndael-Algorithmus.

Abbildung 4.8
Verschlüsselte Übertragung mit geheimen Sitzungsschlüssel (Secret-Key)



zeigt den Einsatz symmetrischer Verschlüsselung für den Kopierschutz auf dem Endgerät des Konsumenten. Hierbei werden die Nutzdaten *vg* auf Anbieterseite verschlüsselt. Die Übertragung und Speicherung der verschlüsselten Nutzdaten (*envg* = *encrypt(vg,tk)*) auf dem Endgerät erfolgt unverändert (vgl. Abbildung 4.3). Die notwendige Übertragung und Speicherung des geheim zuhaltenden Schlüssels *tk* ist allerdings problematisch. Sie muss über einen sicheren nicht abhörbaren Kanal erfolgen. Die Speicherung auf dem Endgerät muss zusätzlich in einem für den Nutzer unsichtbaren Speicher erfolgen. Ist der Permanentspeicher wechselbar (vgl. Kapitel

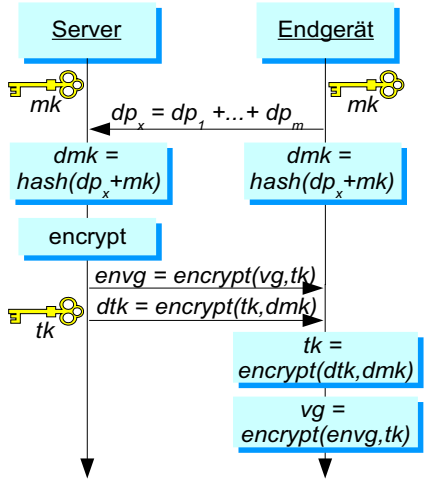
4.1.3) so sollte der Schlüssel in einem separaten Permanentspeicher untergebracht werden, der nicht wechselbar ist.

Sicherung des geheimen Sitzungsschlüssels *tk*

Um den Schlüssel *tk* zu sichern, kann dieser auch ebenfalls verschlüsselt werden. Hierfür stehen verschiedene Verfahren zu Verfügung:

- Symmetrische Verschlüsselung mit einem **Master-Schlüssel *mk***. Es wird nicht mehr *tk* direkt sondern *entk = encrypt(tk,mk)* übertragen. Der Master-Schlüssel ist bspw. direkt in der Entschlüsselungskomponente des Endgerätes abgelegt. Der *mk* darf auf keinen Fall vom Nutzer ausgelesen werden können. Dieser relativ unsichere Ansatz kann verbessert werden, wenn im Endgerät mehrere Master-Schlüssel mk_1 ... mk_n abgelegt werden. Würde mk_1 komprimitiert (offen gelegt) werden, so kann der Anbieter auf mk_2 übergehen.
- Der Master-Schlüssel *mk* wird durch ein oder mehrere **endgerätespezifische Parameter** dp_1 ... dp_m verschlüsselt. Hierdurch wird *tk* als *dtk* endgerätespezifisch verschlüsselt übertragen.

Abbildung 4.9
Sequenz-Diagramm des Schlüsselaustausches



Hierdurch kann *tk* als *dtk* endgerätespezifisch verschlüsselt übertragen werden. Abbildung 4.9 zeigt ein Sequenz-Diagramm mit dem zeitlichen Ablauf des Schlüsselaustausches. Die endgerätespezifischen Parameter können entweder eine vom Hersteller fest eingebrachte individuelle Gerätenummer sein oder eine Sammlung von Kennwerten der typischerweise (speziell bei PCs) variablen Hardware-Ausstattung. Die von Intel 1999 für den Pentium III eingeführte eindeutige Nummer, die *Processor Serial Number* (PSN), konnte sich gegen starke Datenschutz-Bedenken nicht als Standard durchsetzen.

Bei der Produktaktivierung von Microsofts Windows-XP [WikiXP 04] werden unter anderem Informationen über die Grafikkarte, SCSI- und IDE-Adapter, die MAC-Adresse der Netzwerkkarte, den Speicherausbau, den Prozessor, die Festplatte und des CD-ROM-Laufwerks übermittelt. Allerdings werden nicht die Parameter im Klartext übertragen sondern zuvor umcodiert. Für den RAM-Ausbau werden z. B. nur drei Bits übertragen. In [Kunze 04] können weitere Details zur Produktaktivierung gefunden werden.

Wie aus den Geräteparametern der geräteabhängige Master-Schlüssel *dmk* gebildet wird, muss, um das Verfahren sicher zu halten, geheim bleiben. Hier liegt auch die Schwachstelle und der Hauptkritikpunkt des Verfahrens. Ein mögliches Vorgehen ist alle Geräteparameter dp_1 ... dp_m und den geheimen Master-Schlüssel *mk* mit ei-

nem **Standard-Hash-Algorithmus** wie z. B. den MD5 (von Ron Rivest) oder den vom amerikanischen NIST (*National Institute of Standards and Technology*) standardisierte SHA1-Algorithmus zu hashen. Ein Hash-Algorithmus ist eine Einwege-Funktion, die die Aufgabe hat eine beliebig lange Eingangszeichenfolge auf einen Hash-Wert konstanter Länge (bei MD5 128 Bit, bei SHA1 160 Bit) derart abzubilden, dass es sehr unwahrscheinlich ist, dass zwei unterschiedliche Eingangszeichenfolgen den gleichen Hash-Wert ergeben. Ein Hash-Algorithmus gilt als sicher, wenn es nicht trivial (mit überschaubarem Rechenaufwand) möglich ist eine zweite Eingangsfolge zu ermitteln, die den gleichen Hash-Wert liefert.

Ist der Hash-Wert länger als die notwendige Schlüssellänge (128, 192 oder 256 Bit bei AES), wird er gekürzt. Ist der Hash-Wert zu kurz, müssen mehrere Hash-Wert kombiniert werden, die aus unterschiedlichen Teilmengen der Geräteparameter ermittelt wurden.

Vorteil des beschriebenen Verfahrens ist die dabei erzielbare **Gerätebindung** von Nutzdaten. Der gerätespezifische Schlüssel *dtk* kann sogar zusammen mit den verschlüsselten Nutzdaten *envg* übertragen und gespeichert werden, ohne dass diese Kombination auf einem zweiten Endgerät abgespielt werden kann.

- Durch den zusätzlichen Einsatz **asymmetrischer** kryptographischer **Verfahren** (Public-Key-Kryptographie) kann eine weitere Verbesserung der Sicherheit (für den Anbieter) erzielt werden. Im Gegensatz zur symmetrischen Verschlüsselung werden hierbei zur Verschlüsselung *encrypt* und zur Entschlüsselung *decrypt* zwei unterschiedliche Schlüssel eingesetzt. Die beiden Teile dieses Schlüsselpaares werden öffentlicher *pubk* (*public key*) und privater Schlüssel *privk* (*private key*) genannt. Der eine Schlüssel kann nicht mit realistischem Aufwand an Zeit und Speicherplatz aus dem anderen ermittelt werden. Der öffentliche Schlüssel kann in diesem Fall ungeschützt bekannt gegeben werden. Der private Schlüssel muss dagegen geheim gehalten werden. Mit asymmetrischen Verfahren werden wegen Geschwindigkeitsproblemen immer nur kleine Datenblöcke – wie der Schlüssel *tk* – verschlüsselt. Die eigentliche Verschlüsselung der Nutzdaten erfolgt weiterhin symmetrisch. Die Kombination von symmetrischer Verschlüsselung der Nutzdaten und asymmetrisch verschlüsselten Schlüsseln nennt man **hybride Verschlüsselung** (weitere Details zu kryptographischen Verfahren vgl. [Wobst 98] und [Raepple 98]).

Asymmetrische Verfahren beruhen auf mathematisch komplexen Problemen, deren Umkehrung allerdings trivial ist. Beim standardmäßig eingesetzten RSA-Verfahren [RivShaAdl 78] (der Name RSA stammt von seinen Entwicklern Rivest, Shamir und Adleman) ist es die Primfaktorzerlegung großer Zahlen. Die Umkehr der Primfaktorzerlegung ist die triviale Multiplikation. Damit der RSA-Algorithmus ausreichend sicher ist, müssen sehr große Primzahlen (bzw. Pseudoprimzahlen, von denen nicht trivial ermittelt werden kann, dass sie keine Primzahlen sind) eingesetzt werden. Dies führt zu Schlüssellängen (die Mantisse des öffentlichen Schlüssel) von 1024 oder sogar 2048 Bit (eine gute Erläuterung zu RSA findet sich in [Wobst 98], Seite 163). Eine Alternative zur Primfaktorenzerlegung des RSA-Verfahrens sind Verfahren mit digitalem Logarithmus, hierbei besonders effizient im Zahlenraum Elliptischer Kurven ECC (*Elliptic Curve Cryptography*) [WikiECC 04]. Vorteil von Elliptischen Kurven sind die Geschwindigkeit, die wesentlich kürzeren Schlüssel (empfohlene min. Länge 163 Bit) und die Tatsache, dass der gleiche Sicherheitszuwachs, der bei RSA durch eine Verdoppelung der Schlüssellänge erzielt wird, bei ECC nur wenige zusätzliche Schlüsselbits benötigt. Gegenüber dem 2003 geknackten Schlüssel der

Länge 109 Bit benötigt man für einen 163 Bit Schlüssel die 10^8-fache Rechenkapazität [WikiECC 04].

Für den Zweck des Kopierschutzes wird nun jedem Endgerät sein eigenes Schlüsselpaar zugeordnet (*dpubk* und *dprivk*). Hierbei gibt es unterschiedliche Möglichkeiten das Schlüsselpaar in das Endgerät zu bringen, so dass der private Schlüssel nicht durch den Nutzer ausgelesen und kopiert werden kann. Der Idealfall wäre ein spezieller Chip, der das Schlüsselpaar enthält und die kryptographischen Operationen mit diesen Schlüsseln selbst ausführen kann. Der private Schlüssel müsste folglich auch gar nicht auslesbar sein. Seit längerem sind solche Kryptochips in den so genannten Smartcards enthalten, die z. B. für die digitale Signatur eingesetzt werden. Microsoft hat auf Basis der Überlegungen der TCG (*Trusted Computing Group*) [WikiTGC 04], welche primär ein Zusammenschluss von Hardware-Herstellern ist und die TCPA (*Trusted Computing Platform Alliance*) ablöst, eine Betriebssystemerweiterung mit dem Namen NGSCB (*Next Generation Secure Computing Base*) [WikiNGSCB 04] entwickelt. NGSCB – das zuvor Palladium hieß – wird möglicherweise in der nächsten Windows Version *Longhorn* zum Einsatz kommen. Laut Mirkrosoft soll NGSCB mehr Sicherheit für den Anwender bringen. Als Sicherheitsanker dient ein TPM (*Trusted Platform Module*) [WikiTPM 04] genannter Kryptochip (auch Fritz-Chip genannt), der möglicherweise in naher Zukunft auf jedem PC-Board (wie eine fest eingebaute Smartcard) enthalten sein wird. Im TPM werden RSA-Schlüsselpaare der Länge 2048 Bit eingesetzt. Ende 2003 wurden bereits erste Boards und Laptops mit TPM ausgeliefert. Weitere Details zu NGSCB können in [Kunze 04] nachgelesen werden.

So genannte Dongles (die Herkunft des Wortes ist ungeklärt), das sind Geräte in Steckergröße, die typischerweise über USB am PC angeschlossen werden, ermöglichen ebenfalls die sichere Unterbringung eines Kryptochips mit dem zusätzlichen Vorteil der Portabilität. Das Code-Meter-System [BucKüg 04] der Firma Wibu-System AG ist ein solcher Dongle mit einem sicheren Kryptochip, der 128 Bit AES und 224 Bit ECC Schlüssel speichert und verarbeitet.

Natürlich sind bei geringeren Schutzanforderungen auch Software-Lösungen für die sichere Speicherung des privaten Schlüssels denkbar. In Kapitel 6 wird hierzu eine Lösung vorgestellt, bei der *dprivk* mit *dmk* verschlüsselt abgespeichert wird.

Abbildung 4.10
Schlüsselaustausch mit öffentlichem Schlüssel

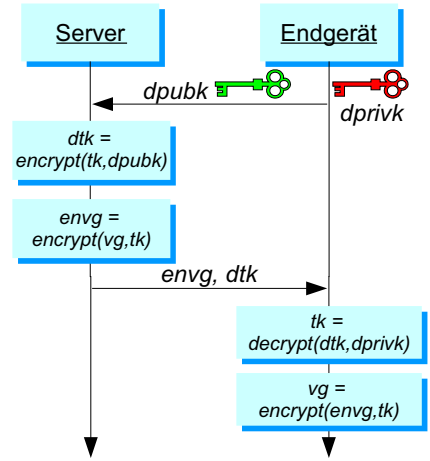


Abbildung 4.10 zeigt das Sequenz-Diagramm mit dem zeitlichen Ablauf des Schlüsselaustausches, wenn ein gerätespezifischer öffentlicher Schlüssel *dpubk* eingesetzt wird. Wurde der öffentliche Schlüssel zufällig ermittelt, kann aus der Kommunikation praktisch keine Information für einen Angriff entnommen werden. Der Anbieter erhält auch keine Informationen über den Aufbau des Endgerätes. Verschlüsselte Nutzdaten *envg* und endgerätespezifisch verschlüsselte Sit-

zungsschlüssel können ohne Sicherheitsbedenken (auch innerhalb *einer* Datei) gespeichert werden.

Bisher wurde noch nicht das Problem der Authentizität des Endgerätes behandelt. In der Abbildung 4.10 kann der Server sich nicht sicher sein, dass *dpubk* wirklich direkt vom Endgerät kommt. Zusätzliche Schlüsselpaare mit denen die Kommunikation signiert werden kann, können das Problem entschärfen. Der Einsatz von digitalen Signaturen wird noch im weiteren Verlauf der Arbeit detailliert zur Sprache kommen.

4.3.3 Verfolgung der Verbreitung

Der Leser kann sich sehr leicht vorstellen, dass ein sicherer Kopierschutz sehr oft im Konflikt mit den Nutzungsgewohnheiten der Konsumenten stehen wird. Speziell dann, wenn die virtuelle Ware durch einen Nutzer auf mehreren unterschiedlichen Endgeräten genutzt werden soll. Bei Musik ist das sicherlich der Regelfall. Daher gibt es einen zweiten Ansatz, der illegalen Verbreitung virtueller Güter technisch entgegen zu wirken. Hierbei setzt man Verfahren ein, die die Nutzdaten derart markieren, dass der Verursacher der illegalen Kopie nachträglich ermittelt werden kann. Dies wird oft als „forensisches" DRM bezeichnet. Bei diesen Verfahren steht Ginny selbst in der Pflicht sich gesetzeskonform zu verhalten.

4.3.3.1 Einfügen von Transaktionsparametern

Tabelle 4.2
Unterschiedliche Formen der Markierung

		Ist die Markierung in den Nutzdaten?	
		Ja	Nein
Sollen auch Dritte auf den Käufer rückschließen können?	Ja	Persönliche Daten in den Nutzdaten „sichtbar"	Persönliche Daten den Nutzdaten angefügt
	Nein	Einsatz unsichtbarer digitaler Wasserzeichen	Angefügte Daten sind nur für den Provider auflösbar

Bei den Transaktionen des Nutzers, die im Einflussbereich des Anbieter erfolgen, besteht die Möglichkeit zusätzliche Informationen tp_x in die Datei einzufügen. Die eingebrachte Information wird vom Provider aus den ihm zur Verfügung stehenden Transaktionsparametern $tp_1 \ldots tp_m$ ausgewählt oder abgeleitet. Diese Parameter verweisen direkt oder mit Hilfe des Providers auf den Käufer der virtuellen Ware. Die Markierung kann für Dritte sichtbar oder unsichtbar ablaufen. Oft ist eine Kombination aus „sichtbarer" und „unsichtbarer" Markierung sinnvoll.

Mit sichtbaren Markierungen ist es möglich den Konsumenten besonders stark von unerwünschten Handlungen abzuhalten. Denn niemand würde ein Buch verleihen, wenn die eigne Kreditkarten-Nummer für alle sichtbar im Buch stehen würde. Wenn die Kreditkarten-Nummer allerdings nicht noch zusätzlich im Buch versteckt ist, könnte man sie sehr leicht entfernen, ohne dabei das Buch zu sehr zu beschädigen.

Markieren beim Erwerb durch den Anbieter

Der Einflussbereich des Anbieters bzw. Providers ist in erster Linie der Server von dem der Nutzer die Nutzdaten per Download bezieht (vgl. Abbildung 4.3). Um die Nutzerin (Ginny) überhaupt später identifizieren zu können, muss sie sich in irgendeiner Form zu erkennen gegeben haben. Dies kann absichtlich erfolgen, indem sich Ginny beim Anbieter (Fred) anmeldet bzw. bezahlt und hierbei verschiedene Angaben (die Transaktionsparameter $tp_1 \ldots tp_m$) macht. Natürlich kann Ginny auch unbewusst Daten hinterlassen, wie bspw die IP-Adresse und den Browser-Typ. Im Weiteren soll aber nicht auf Verfahren eingegangen werden, die den Nutzer ohne sein Wissen ausspionieren.

Markierung der Kopie bei der Weitergabe

In Abbildung 4.3 wurde neben dem direkten Download von Provider zum Konsumenten auch der P2P-Transfer gezeigt. Auch bei dieser Form der Kopie besteht prinzipiell die Möglichkeit Transaktionsparameter einzufügen. Dazu muss allerdings der Anbieter seinen Einflussbereich auf das Endgerät des Nutzers erweitert haben. Diese kann bspw. durch eine anbieterspezifische Anwendung erfolgen, die neben dem Konsum der virtuellen Güter auch deren kontrollierte Weitergabe ermöglicht.

Ist das Endgerät nutzerprogrammierbar (vgl. Kapitel 4.1.4.2), so ist die Einbringung der Parameter auf dem Endgerät immer auch angreifbar und daher nur begrenzt sicher. Allerdings entlastet es auch den Server des Anbieters.

Nutzbare Transaktionsparamter

- Hat der Nutzer einen eindeutigen Login-Namen beim Anbieter, so kann dieser **Name bzw. Alias** (bspw. „Ginny“) als Transaktionsparameter eingefügt werden. Auf diese Weise können auch Dritte auf den Käufer rückschließen.
- Alternativ können auch **persönliche Kundendaten**, wie Namen, Adresse, Kreditkarten-Nummer oder E-Mail-Adresse eingefügt werden. Diese Vorgehensweise ist allerdings aus datenschutzrechtlichen Gründen sehr bedenklich. Gesetzliche Vorschriften (Gesetz über den Datenschutz bei Telediensten [TDDSG 97]) untersagen dies ohne die Zustimmung des Kunden.
- Die Einfügung einer eindeutigen **Kundennummer** erfüllt die gleiche Aufgabe, ohne dabei die Kundin Ginny zu kompromittieren. Allerdings nur solange Dritte nicht wissen, wer hinter einer Kundennummer steht.
- Eine zufällige und einmalige **Transaktionsnummer** kann nur noch mit Hilfe des Anbieters aufgelöst werden. Die hat den Vorteil, dass die möglicherweise zeitaufwendige Einbringung der Transaktionsnummer in die Nutzdaten bereits vorab erfolgen kann.

Wird eine personalisierte Markierung für Dritte „sichtbar“ in eine Datei eingebracht, so ergeben sich zusätzliche Anforderungen, die beachtet werden müssen:

- Die **Vertraulichkeit** der eingebrachten Information ist je nach Anwendungsfall unterschiedlich wichtig. Soll Dritten nicht die Möglichkeit gegeben werden, von der eingebrachten Information auf eine reale Person rückzuschließen, so ist es möglich die eingebrachte Information zu verschlüsseln.

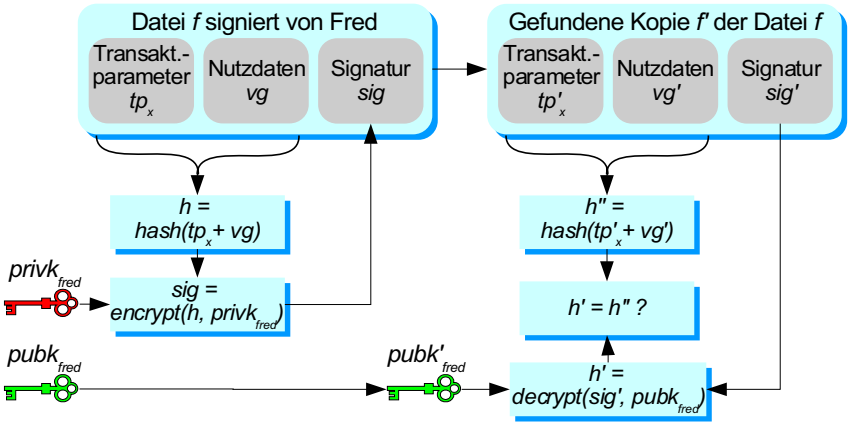
- Die **Integrität** bzw. die Verlässlichkeit der eingebrachten Informationen ist von großer Wichtigkeit. Es darf nicht möglich sein, dass die eingebrachten Parameter unbemerkt verfälscht werden können. Ebenso darf es auch nicht möglich sein, dass die Parameter mit den Parametern einer anderen Transaktion, die mit einem anderem Nutzer und einer anderen virtuellen Ware lief, ausgetauscht werden.
- Eng mit der Integrität verknüpft ist die Forderung nach der **Authentizität** der eingebrachten Parameter. Es muss sichergestellt sein, dass der Urheber der Markierung (typischerweise der Anbieter) eindeutig zugeordnet werden kann.
- Durch eine allgemeine **Nachweisbarkeit** wird gewährleistet, dass auch Dritte die Integrität und Authentizität der eingebrachten Parameter verifizieren können.

4.3.3.2 Digitale Signatur zur Sicherung von Integrität und Authentizität

Durch den Einsatz der auf der Public-Key-Kryptographie (asymmetrische Verschlüsselung, vgl. Seite 52ff) aufbauenden digitalen Signatur [WikiSignatur 04] besteht die technische Möglichkeit, die Integrität, Authentizität und Nachweisbarkeit von durch den Provider verteilten Daten zu gewährleisten.

Bei der digitalen Signatur wird ein Hashwert *h* über die zu signierenden Daten *d* errechnet. Dieser Hashwert $h = hash(d)$ wird mit dem privaten Schlüssel $privk_{fred}$ des Unterzeichners (z. B. Fred) chiffriert. Die dabei entstandene Signatur $sig = encrypt(h, privk_{fred})$ wird an die Daten *d* angefügt.

Abbildung 4.11
Verifikation der Integrität und Authentizität von angefügten Transaktionsparametern



Soll nun die Integrität und die Authentizität der (legal oder illegal) erlangten Daten *d'* überprüft werden, so kann mit dem öffentlichen Schlüssel von Fred $pubk_{fred}$ der Hashwert *h'* nach der Entschlüsselung wieder ermittelt werden $h' = decrypt(sig', pubk_{fred})$. Wenn jetzt der aus den empfangenen Daten berechnete Hashwert $h'' = hash(d')$ gleich *h''* ist, dann kann man sicher sein, dass empfangenen Daten *d'* unver-

ändert sind (nur Fred könnte sie verändern) und vom Besitzer des privaten Schlüssel $privk_{fred}$ signiert wurden.

Die linke Seite der Abbildung 4.11 zeigt den Ablauf wie der Anbieter Fred seine angeboten virtuellen Güter, mit den Nutzdaten *vg*, zusammen mit den eingebrachten kundenspezifischen Transaktionsparametern tp_x signiert. Die gezeigte Signatur über die Verschlüsselung eines Hash-Wertes ist der bei RSA angewendete Weg. Die schließlich verteilte Datei $f = tp_x + vg + sig$ besteht aus der resultierenden Signatur *sig*, dem Transaktionsparameter tp_x und den Nutzdaten *vg*.

Wird ein Kopie *f'* dieser Datei an einem an einer vom Anbieter nicht gewünschten Stelle gefunden, so kann nun auch durch Dritte die Integrität und Authentizität sowohl der Nutzdaten als auch des Transaktionsparameters tp_x verifiziert werden. Die rechte Seite der Abbildung 4.11 zeigt diesen Prozess unter Nutzung des öffentlichen Schlüssel von Fred $pubk'_{fred}$. Bei der Verifikation muss allerdings auch sichergestellt werden, dass der benutzte öffentliche Schlüssel wirklich von Fred ist und dass Fred auch vertrauenswürdig ist. Dies kann durch Zertifikate (vgl. Kapitel 4.3.3.4) sichergestellt werden. Ist dies sichergestellt, so können folgende Manipulationen aufgedeckt bzw. nicht aufgedeckt werden:

- Die **Veränderung des Transaktionsparameter** tp'_x wird festgestellt, da sich ebenfalls der berechenbare Hashwert *h''* ändert, ohne dass sich gleichzeitig auch der in der Signatur enthaltene Hashwert *h'* ändert.
- Auch die **Veränderung der Nutzdaten** wird durch den gleichen Mechanismus festgestellt.

Natürlich kann nicht verhindert werden, dass die Transaktionsparameter entdeckt und komplett gelöscht werden. Solange die Nutzdaten danach noch decodierbar bleiben, kann auf diese Weise eine nutzbare illegale Kopie immer noch anonym erfolgen. Um das zu verhindern, muss der Transaktionsparameter mit steganografischen Verfahren wie der Wasserzeichen-Technologie in den Nutzdaten versteckt werden.

4.3.3.3 Einsatz von Wasserzeichen-Steganografie

In Kapitel 4.3.2.2 wurden Wasserzeichen bereits eingeführt. Dort hatten sie die Aufgabe auf dem Endgerät einen Kopierschutz zu realisieren. An dieser Stelle kommen die Wasserzeichen das zweite Mal als steganographische Technologie zur Sprache. Im Gegensatz zum Kopierschutz muss bei der Nachverfolgung illegaler Kopien das Wasserzeichen nicht auf dem Endgerät extrahiert werden. Es genügt völlig die Wasserzeichen der gefundenen Dateien auf einem speziellen Rechner, der den normalen Nutzern nicht zugänglich ist, zu extrahieren. Dies hat mehrere Vorteile:

- Ein potentieller Angreifer, der das Wasserzeichen mit den Transaktionsparametern zerstören will, hat keine Möglichkeit, den Erfolg seines Angriffs zu überprüfen, da er nicht über eine Testmöglichkeit verfügt.
- Da der Detektor nicht in den Endgeräten enthalten ist, kann der Wasserzeichen-Algorithmus jederzeit verändert oder angepasst werden. Es müssen keine Updates beim Endkunden durchgeführt werden.

Die Firma MusicTrace [MusicTrace 05], eine Ausgründung des Fraunhofer IIS in Erlangen, hat es sich zur Aufgabe gemacht mittels der Fraunhofer-Wasserzeichen-Technologie [IIS 05] Musik, die ein Wasserzeichen enthält, im Internet wieder aufzu-

finden. Der Musik-Download-Dienst von Medion [Medion 05] fügt in die verkauften MP3-Dateien Transaktionsparameter mittels der Wasserzeichen-Technologie *ActivatedAudio* der Firma Activated Content ein.

Ein spezielles Problem von Transaktionswasserzeichen ist allerdings, dass sehr leicht sich beliebig viele Varianten der gleichen Nutzdaten mit unterschiedlichen Wasserzeichen (legal) beschaffen lassen. Werden all diese Varianten gemittelt, so kann es je nach Verfahren sein, dass sich das Wasserzeichen irgendwann heraus mittelt. Dieser Angriff wird in der Literatur [Dittmann 00] als *Collusion Attack* bzw. Koalitionsattacke bezeichnet.

4.3.3.4 Zertifikate, Zertifizierung und PGP

Wie kann bspw. die Konsumentin Ginny sicher sein, dass der öffentliche Schlüssel $pubk'_{fred}$ in Abbildung 4.11 wirklich eine Kopie des öffentlichen Schlüssels $pubk_{fred}$ des Anbieters Fred ist? Fred könnte entweder selbst unehrlich sein oder auf dem Übertragungsweg hat ein Angreifer seinen eigenen öffentlichen Schlüssel untergeschoben, nachdem dieser zuvor mit seinem privaten Schlüssel die Signatur ausgetauscht hatte. Für die Lösung dieser Fragen existieren zwei technische Ansätze.

■ PGP

PGP [WikiPGP 05] steht für *pretty good privacy* und wurde 1986 von Phil Zimmermann initiiert [Zimmermann 95]. In PGP kann jeder Nutzer selbst sein Schlüsselpaar erstellen. Das Vertrauen in die Zuordnung der Schlüsselpaare zu einer Person wird durch gegenseitige Beglaubigungen realisiert. Nutzer, die sich gegenseitig vertrauen, signieren gegenseitig ihre öffentlichen Schlüssel. Kann Fred Ginny einen öffentlichen Schlüssel präsentieren, der von sehr vielen anderen Personen unterzeichnet ist, denen Ginny auch vertraut, so kann Ginny dem Schlüssel von Fred ebenfalls vertrauen.

■ Zertifikats-basierte Systeme nach X.509

In Zertifikats-basierten Systemen erhält jeder Benutzer sein Schlüsselpaar von einer vertrauenswürdigen zentralen Instanz, einer *Certification Authority* (CA) ausgestellt. Das Schlüsselpaar (bzw. nur der öffentliche Schlüssel) ist hierbei Bestandteil eines so genannten digitalen Zertifikates, welches die Identität des Schlüsselbesitzers beschreibt. Jedes Zertifikat ist von der ausgebenden Stelle (CA) beglaubigt d.h. digital signiert, die ihrerseits wieder von einer höheren Stelle (CA) beglaubigt sein kann. Das Vertrauenssystem ist streng hierarchisch. Den gemeinsamen Vertrauensanker bildet das Wurzel-Zertifikat (*Root Certificate*) der Wurzel-CA.

Ein Zertifikat verknüpft den öffentlichen Teils eines Schlüsselpaares mit Daten des Inhabers und einer Zertifizierungsstelle (CA), sowie mit weiteren Spezifikationen wie Version, Gültigkeitsdauer, Verwendungszweck und Fingerprint. Der ITU-Standard X.509v3 (nach RFC3280 [RFC3280 02]) beschreibt den Aufbau der Zertifikate. Der PKCS#7 (*Public-Key Cryptography Standard*) der RSA Laboratories [RSALabs 05] wird für den Austausch des öffentlichen Schlüssels genutzt. PKCS#12 enthält zusätzlich den kennwortgeschützten privaten Schlüssel [WikiSignatur 04].

4.4 Digital Rights Management (DRM)

Im Kapitel 2 wurden bereits die entscheidenden Unterschiede von realen und virtuelle Gütern deutlich gemacht. Im Kapitel 3 wurden mögliche Erlösmodelle vorgestellt. Das grundsätzliche Problem, dass eine digitale Kopie einer virtuellen Ware von ihrem Original nicht zu unterscheiden ist, macht es unmöglich, Geschäfts- und Erlösmodelle aus der Welt der realen Güter eins-zu-eins auf die virtuellen Güter zu übertragen. Der Nutzer kann sehr leicht die Rolle des Anbieters übernehmen. Er kann die Nutzdaten ohne Zustimmung des ursprünglichen Providers weiterverteilen.

Es wurden bereits einige Basistechniken in Kapitel 4.3 vorgestellt, mit deren Hilfe der Provider die Weiterverteilung entweder ganz verhindern oder zumindest nachverfolgen kann. Allerdings geben sich die Anbieter mit diesen wenig flexiblen Möglichkeiten nicht zufrieden. Man suchte nach Lösungen, die es ermöglichen, dem Nutzer sehr feingranular das wiederzugeben, was man ihm durch den eingebrachten Kopierschutz weggenommen hat.

Die als *Digital Rights Management* (DRM) bezeichneten Systeme ermöglichen dem Anbieter über eine in einer Lizenz-Datei eingebrachte Rechtedefinition dem Nutzer nur bestimmte Operationen mit der virtuellen Ware zu erlauben. Die Festlegung dessen, was geht bzw. nicht geht, erfolgt über Maschinen-interpretierbare Rechtebeschreibungssprachen, den *Rights Expression Languages* (REL) (siehe Kapitel 4.4.3).

4.4.1 Definitionen

Was allgemein unter einem DRM verstanden wird, wird von verschiedenen Instanzen bzw. Personen unterschiedlich gesehen. Microsoft hatte bis einschließlich zur Version 9 von Windows Media eine sehr technikzentrierte Sichtweise auf das Thema DRM. Verschiedene Stellen im Web ordnen das folgende Zitat Microsoft zu. Auf den aktuellen Seiten von Microsoft [WMRM 05] ist es allerdings inzwischen nicht mehr zu finden.

> *„DRM is a system that encrypts digital media content and limits access to only those people who have acquired a proper license to play the content. That is, DRM is a technology that enables the secure distribution, promotion, and sale of digital media content on the Internet.“*

Renato Iannella, dessen Firma IPR Systems [IPRSys 05] die ODRL (*Open Digital Rights Language*) [W3CODRL 02], [ODRL 05] entwickelt hat, unterscheidet zwischen dem DRM der ersten Generation, welches sich nur um illegale Kopien kümmerte und dem DRM der 2. Generation:

> *„The second-generation of DRM covers the description, identification, trading, protection, monitoring and tracking of all forms of rights usages over both tangible and intangible assets including management of rights holders relationships. Additionally, it is important to note that DRM is the "digital management of rights" and not the "management of digital rights". That is, DRM manages all rights, not only the rights applicable to permissions over digital content. [Iannella 01]“*

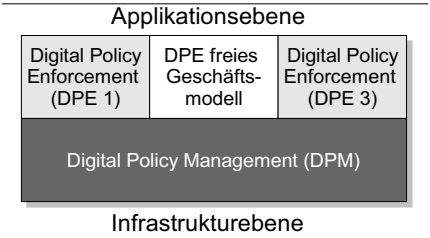
Hier wird deutlich, dass DRM ein extrem komplexes Thema ist, welches nicht nur die technische Fragestellung betrifft. Niels Rump bezeichnet DRM als einen dreibeinigen Hocker mit den Beinen Recht (*Law*), Technologie (*Technology*) und Geschäft (*Business*). Im gleichen Vortrag [Rump 04] teilt er DRM in zwei Blöcke bzw, Ebenen:

- Das **Digital Policy Management (DPM)** übernimmt die Verwaltung der Rechte für eine virtuelle Ware.
- Das **Digital Policy Enforcement (DPE)** setzt die definierten Rechte technisch durch.

DPM bildet die Basis auf dem applikationsabhängig unterschiedliche DPE aufsetzen. Es sind auch Anwendungen bzw. Geschäftsmodelle wie das PotatoSystem (vgl. Kapitel 8) denkbar, bei denen auf ein DPE verzichtet werden kann (vgl. Abbildung 4.16).

Rüdiger Grimm dagegen demaskiert mit seiner DRM-Definition die eigentlichen Wünsche der Content-Provider, die sich hinter DRM verstecken:

Abbildung 4.12
DRM besteht aus zwei Blöcken



> *„Unter „Digital Rights Management (DRM)“ versteht man Verfahren, die helfen Rechte an digitalen Waren so zu schützen, wie wir das von den an physische Medien gebundenen intellektuellen Erzeugnissen her gewöhnt sind. Kopie und Weitergabe sollen an die Regeln des Rechteinhabers, also der Warenanbieter (Content Provider) gebunden sein. [Grimm 04a]“*

DRM soll (mindestens) die von den realen Waren her gewohnten Geschäftsmodelle auf die virtuellen Waren ausdehnen, ohne dabei die spezifischen Eigenschaften von diesen beachten zu müssen.

4.4.2 Referenz-System

In [RoTrMo 02] wird ein DRM-Referenz-System beschrieben (vgl. Abbildung 4.8), welches sehr gut die den meisten DRM-Systemen zugrunde liegende Architektur beschreibt. Die drei Komponenten der dort beschriebenen DRM-Referenz-Architektur sind auf mehrere Bereiche verteilt. Sie befinden sich zum einen auf der Seite der Anbieter und zum anderen auf der Seite der Konsumenten. Eine dritte Seite könnte ein spezieller DRM-Service-Provider sein, falls der Anbieter dies nicht gleichzeitig miterledigt.

Der Server des Providers besteht aus drei Komponenten: einer Datenbank bzw. einem Repository mit den Nutzdaten, dem DRM-Packer und einer Produkt-Info-Datenbank. Das Nutzdaten-Repository ist entweder an ein komplettes DRM-System angeschlossen oder über eine Schnittstelle mit einem Content-Management-System (CMS) verbunden. In der Nutzdaten-Info-Datenbank werden zusätzliche Informationen über die virtuellen Waren, die Metadaten, gespeichert. Dies könnten zum Beispiel die Preise oder zusätzliche Beschreibungen sein.

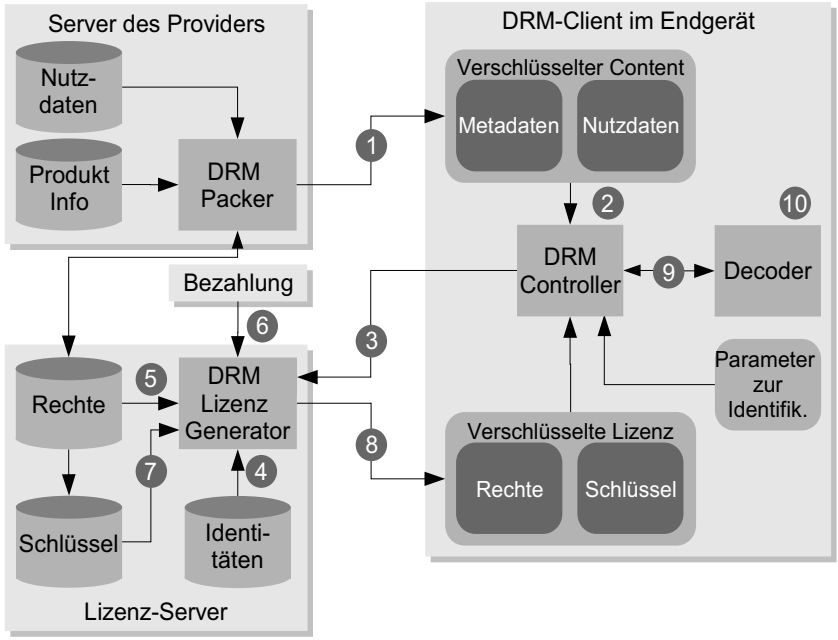
Jedes auf Verschlüsselung (vgl.) basierende DRM-System (bzw. DPE) enthält eine Funktion zum Vorbereiten der Nutzdaten für den Vertrieb. Diese Funktion wird

als DRM-Packer oder Content-Packer bezeichnet. Der Packer erledigt seine Aufgabe entweder bevor die Nutzdaten ins Repository gelangen oder on-the-fly vor dem Abruf durch den Konsumenten. Ein Content-Paket beinhaltet einerseits die verschlüsselten Nutzdaten selbst, andererseits die Metadaten, wie zum Beispiel einen Content-Identifier (ID) und die Adresse des Lizenz-Servers.

Rechte und Lizenzen

Ein wichtiger Bestandteil des DRM-Modells sind die Rechte. Solche Rechte können zum Beispiel abspielen, drucken, lesen, kopieren, speichern oder wiederverwenden sein. Um eine individuelle Verteilung der Rechte für unterschiedliche Benutzer zu gewährleisten, werden die Rechte nicht an den Inhalt gebunden, sondern als getrennte Lizenzen vergeben. Eine Lizenz bezieht sich auf einen bestimmten Nutzer oder ein Endgerät, welche die Rechte ausüben will, der Identifikation des Inhaltes und der genauen Spezifikation der Rechte. Eine DRM-Lizenz ist vergleichbar mit einen Flugticket. Dieses wird für einen bestimmten Flug zu einer bestimmten Uhrzeit gebucht und ist nur für diese gebuchte Uhrzeit und Strecke und auch nur für die Person gültig, die ihn auch gebucht hat.

Abbildung 4.13
Referenz-Modell für DRM-Systeme (nach [RoTrMo 02])



Die Verwaltung der Lizenzen erfolgt durch den Lizenz-Server. Durch den DRM-Packer des Content-Servers des Providers werden die Rechte erstellt und an den Li-

zenz-Server verschickt. Außerdem kreiert der DRM-Packer eine Reihe von Schlüsseln, die den Benutzer identifizieren und den Inhalt entschlüsseln. Schlüssel und Rechte werden in unterschiedlichen Datenbanken auf dem Lizenz-Server gehalten. Eine weitere Datenbank auf dem Lizenz-Server enthält die Identitäten. Das sind zusätzliche Informationen über den Benutzer. Die vierte Komponente des Lizenz-Servers ist der DRM-Lizenz-Generator, der die Lizenzen erstellt und dabei auf die anderen drei Datenbanken zurückgreift.

DRM-Client

Der DRM-Client ist der Teil des DRM-Systems, der sich im Endgerät des Konsumenten befindet. Der DRM-Client besteht aus einem DRM-Controller, einer Anwendung zur Wiedergabe der Nutzdaten (Decoder) und einem Mechanismus zur Benutzer-Identifikation bzw. Endgeräte-Identifikation. Der DRM-Controller kann als unabhängige Software vorliegen, in die Hardware oder in den Decoder integriert sein. Er nimmt die Anfrage des Benutzers entgegen, der seine Nutzungsrechte an einem Content-Paket geltend machen will, sammelt die Benutzer-Informationen und erhält die Lizenzen vom Lizenz-Server. Weiterhin übernimmt er die Aufgabe der Entschlüsselung des Inhaltes und gibt diesen für den Decoder frei.

Ablauf

Zuerst (Schritt 1 in Abbildung 4.8) lädt sich der Nutzer die Nutzdaten in verschlüsselter Form vom Server des Anbieter auf sein Endgerät. Der Versuch die Nutzdaten zu öffnen aktiviert (im Schritt 2) den DRM-Controller, der daraufhin alle für eine Lizenz nötigen Informationen sammelt. Dazu gehört der Content-Identifier und Parameter über die entweder der Nutzer oder das Endgerät identifiziert werden können (vgl. Seite 51). Als nächstes schickt (in Schritt 3) der DRM-Controller diese Informationen an den Lizenz-Server. Der Lizenz-Generator verifiziert (in Schritt 4) die Identität des Nutzers bzw. des Endgerätes. In Schritt 5 werden die Nutzungsrechte für die jeweiligen Nutzdaten aus der Datenbank geladen. In Schritt 6 kann je nach Festlegung eine Finanztransaktion erfolgen. Der Lizenz-Generator erstellt darauf die Lizenz, die die Rechte, Benutzerinformationen und den passenden Schlüssel (*track key*) enthält (Schritt 7). Die Lizenz mit dem Sitzungsschlüssel selbst kann nochmals verschlüsselt sein. Die Lizenz wird (in Schritt 8) dem Nutzer zugeschickt. Der DRM-Controller entschlüsselt schließlich die Nutzdaten und gibt ihn an den Decoder (in Schritt 9) weiter. Der Nutzer kann in Schritt 10 schließlich die virtuelle Ware konsumieren.

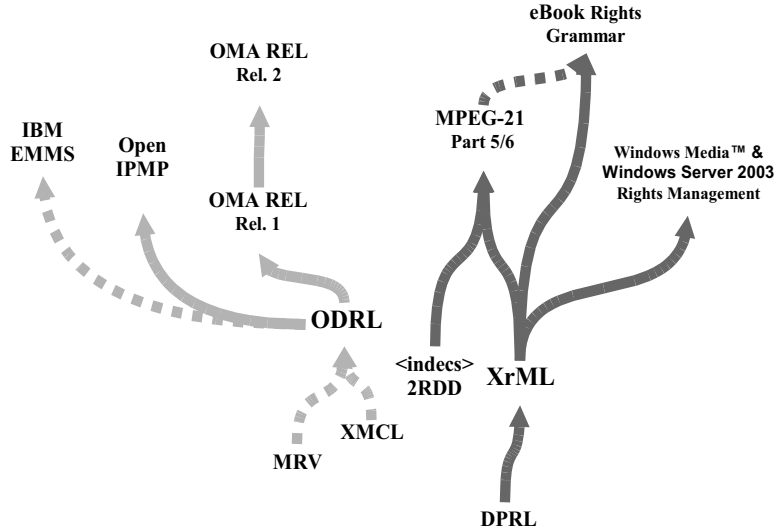
4.4.3 Rights Expression Languages (REL)

Damit Anbieter virtueller Waren unterschiedliche Geschäftsmodelle unter Einsatz von DRM-Techniken realisieren, müssen sie die damit verbundenen unterschiedlichen Rechte (siehe Seite 61) mittels einer Lizenz dem Konsumenten zukommen lassen. Da die dabei gewährten Rechte immer eine Einschränkung der tatsächlichen technischen Möglichkeiten darstellen, müssen diese Rechte von einem DRM-Controller technisch durchgesetzt werden. Dies erfordert, dass die in der Lizenz übermittelten Rechtebeschreibung vom DRM-Controller vollautomatisch interpretiert werden kann. Neben den Rechten, die den Konsumenten gewährt werden, gibt es auch rechtliche Vereinbarungen, ohne dass Konsumenten beteiligt sind. Plattenlabels ge-

währen bspw. Online-Händlern das Recht, bestimme Musikstücke in digitaler Form mit bestimmten Nutzungsrechten innerhalb eines definierten Territoriums zu verkaufen. In diesem Fall müssen die gewährten Rechte nicht technisch durchgesetzt werden. Es reicht, wenn sie unmissverständlich notiert sind.

Für die maschinenlesbare Notation der gewährten Nutzungsrechte haben sich so genannte Rechtebeschreibungssprachen (*Rights Expression Languages*, REL) auf Basis von XML etabliert. Alternative Ansätze nutzen als syntaktische und semantische Basis Programmiersprachen wie Lisp oder Prolog [ChCoEtHaLa 03].

Abbildung 4.14
Ein Stammbaum der Rechtebeschreibungssprachen aus [ScTaWo 04]



Bisher (2005) gibt es keinen durchgesetzten Standard für Rechtebeschreibungssprachen (REL), der eine Interoperabilität von gewährten Nutzungsrechten ermöglicht. In [ScTaWo 04] findet sich Abbildung 4.14, die den „Stammbau" der RELs zeigt. In der Mitte sind die Sprachen angeordnet, die sehr universell und applikationsunabhängig angelegt sind. Am Rand finden sich die Sprachen, die für konkrete Applikationen konzipiert wurden. Der linke Ast wird durch ODRL (*Open Digital Rights Language*) [ODRL 05] gebildet. ODRL ist eine offene Standardisierungsinitiative, welche z. B. von Nokia unterstützt wird. Sie hat das Ziel, eine freie REL verfügbar zu machen. Über ODRL Profile wurde die REL der *Open Mobile Alliance* (OMA) [OMA 05] definiert.

MPEG-21

Ausdrücke, die mit einer XML-basierten REL notiert werden, sind erst dann eindeutig interpretierbar, wenn sie ein definiertes Vokabular besitzen. Für jedes Schlüsselwort aus diesem Vokabular muss eine definierte Semantik festgelegt sein. Der Standard MPEG-21 [MPEG21 04] trägt dieser Notwendigkeit Rechnung und definiert in Teil 5

nicht nur eine XML-basierte REL, sondern auch in Teil 6 ein *Rights Data Dictionary* (RDD).

Die MPEG-21 REL beruht auf der XrML (*eXtensible rights Markup Language*) [XRML 05], welche in Konkurrenz zur ODRL steht. XrML beruht ihrerseits auf der von Xerox PARC 1996 entwickelten *Digital Property Rights Language* DPRL. XrML bildet die Basis für die REL von Microsoft. [ScTaWo 04]

In Teil 5 von MPEG-21 sind vier Kernelemente festgelegt, die in jedem mit der REL notiertem Recht (*Grant* = *Permission* + *Condition* + *Principle* + *Resource*) vorkommen:

- *Permission:* beschreibt die Nutzung an einem *Digital Item*, die ein Nutzer einem anderen Nutzer bietet.
- *Condition:* beschreibt eine Bedingung, die der erste User einen zweiten User für die Nutzung seiner *Digital Items* auferlegt.
- *Principle:* identifiziert einen User, dem ein Nutzungsrecht (*Grant*) gewährt wird.
- *Resource*: beschreibt exakt das *Digital Item* oder ein Teil dessen, für welches die *Permission* gelten soll.

In Teil 6 wird das MPEG-21 RDD standardisiert. Dort sind unter anderem 14 grundlegende Rechteverben definiert. Neben den Verben *play* und *print* findet sich dort auch das Verb *adapt*, welches für die Notation von Kopierrechten eingesetzt wird [Rump 04]. Nach dem Verständnis von MPEG-21 kann es keine echte Kopie von den in Teil 2 definierten *Digital Items* gegeben, sondern lediglich eine Adaption dieser. Selbst wenn die Nutzdaten (der *Digital Items*) bei der Kopie unverändert bleiben, so wurde doch mindestens deren Speicherort adaptiert. Diese Beispiel macht deutlich, wie komplex und haarspalterisch die Formulierung von Nutzungsrechten verstanden werden kann. Es bleibt abzuwarten, ob sich hierbei das MPEG-Konsortium durchsetzen kann. Möglicherweise sind einfachere Lösungen auf Basis von ODRL (vgl. Abbildung 4.15) erfolgversprechender.

4.4.4 Open Mobile Alliance (OMA) DRM

Die *Open Mobile Alliance* (OMA) [OMA 05] ist eine Interessenvertretung von Firmen und Organisationen, die sich mit der Weiterentwicklung von Diensten auf Basis der Mobilfunknetze befassen. OMA hat unter anderem auch einen Standard für DRM verabschiedet, der in der Version 1.0 seit 2004 im praktischen Einsatz ist. OMA DRM 1.0 [OMA1 04] definiert eine Rechtebeschreibungssprache auf der Basis von ODRL 1.1 und unterstützt drei verschiedene Schutzmechanismen (DPE):

- *Forward-lock*: Hierbei werden die Nutzdaten beim Anbieter in eine *DRM Message* verpackt. Diese DRM-Nachricht kann als Datei mit der Endung .dm zum Download auf das Endgerät angeboten werden. Der syntaktische Aufbau der Nachricht folgt den RFC-Empfehlungen ([RFC2045 96], [RFC2046 96] und [RFC2047 96]) für multifunktionale E-Mail-Anhänge (MIME). Bei forward-lock ist in der DRM-Nachricht nur ein Nutzdaten-Paket und kein Rechteobjekt enthalten. Das Fehlen der Rechtebeschreibung, wird vom OMA-Endgerät per Definition als Aufforderung zur Unterbindung der Weitergabe interpretiert. Es ist einem, vom Endgerät zu beachtendem Kopierschutzbit (vgl. Seite 47) gleichzusetzen. Der MIME-Type der unabhängig von der Endung eine OMA-DRM-Nachrichten kennzeichnet lautet:

```
Content-type: application/vnd.oma.drm.message
```

- *Combined delivery*: Hierbei gilt das bereits für Forward-lock gesagte, mit dem Unterschied, dass zusätzlich in der DRM-Nachricht eine Rechtebeschreibung enthalten sein muss. Die dabei eingesetzte REL ist ODRL 1.1. Abbildung 4.15 zeigt ein Beispiel [NokiaDRM 04]. Der MIME-Type der Rechtebeschreibung in OMA-DRM-Nachrichten lautet:

```
Content-type: application/vnd.oma.drm.rights+xml
```

- *Separate delivery*: Diese DRM-Methode, die auch Superdistribution ermöglicht, kommt dem DRM-Referenz-System aus Kapitel 4.4.2 am nächsten. Die Nutzdaten werden hierbei getrennt von der Lizenz auf das Endgerät übertragen. Für die mit AES [FIPS197 01] symmetrisch verschlüsselten Nutzdaten definiert OMA ein eigenes Format, das *DRM Content Format* (Endung .dcf). Für die getrennte Übertragung der Rechtebeschreibung, die auch den Schlüssel enthält, werden von OMA entweder WAP-Push- oder SMS-Dienste vorgeschlagen. Für diesen Fall wird die Rechtebeschreibung binär umkodiert, um ihre Größe zu minimieren. Der MIME-Type für binär codiert Rechtebeschreibungen lautet:

```
Content-type: application/vnd.oma.drm.rights+wbxml
```

Abbildung 4.15
Beispiel für eine XML Rechtebeschreibung innerhalb einer OMA-DRM-Nachricht

```
<o-ex:rights
   xmlns:o-ex="http://odrl.net/1.1/ODRL-EX"
   xmlns:o-dd="http://odrl.net/1.1/ODRL-DD"
   xmlns:ds="http://www.w3.org/2000/09/xmldsig#/">
  <o-ex:context>
   <o-dd:version>1.0</o-dd:version>
  </o-ex:context>
  <o-ex:agreement>
   <o-ex:asset>
    <o-ex:context>
     <o-dd:uid>cid:20141-9729@http://contentpro.com</o-dd:uid>
    </o-ex:context>
    <ds:KeyInfo>
     <ds:KeyValue>PkerZ9f5g0a37UC2u/G+QA==</ds:KeyValue>
    </ds:KeyInfo>
   </o-ex:asset>
   <o-ex:permission>
    <o-dd:display>
     <o-ex:constraint>
      <o-dd:count>3</o-dd:count>
     </o-ex:constraint>
    </o-dd:display>
   </o-ex:permission>
  </o-ex:agreement>
</o-ex:rights>
```

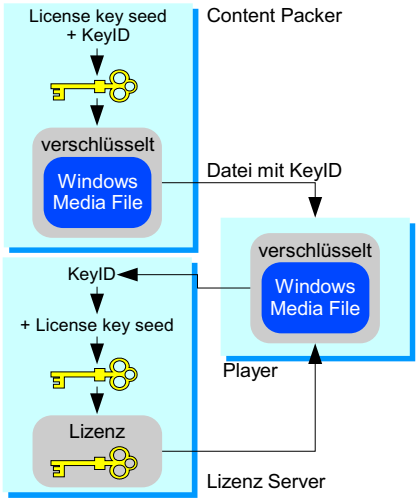
OMA DRM 1.0 bietet für schnelllebigen Content, wie z. B. Logos oder einfache Java-Spiele, einen ausreichenden Schutz. Da die mobilen Endgeräte immer leistungsfähiger werden und inzwischen auch durch die Nutzer umprogrammierbar (vgl. Seite 38) sind, sind sowohl Schutzfunktionen als auch die Möglichkeiten zur Umsetzung weiterer Geschäftsmodelle vielen Anbietern von höherwertigen virtuellen Waren wie z. B. Musik nicht mehr ausreichend. Es fehlt neben einer gesicherten Ende-zu-Ende-Übertragung der Rechteobjekte eine Reihe weiterer Funktionen, die Systeme aus dem PC-Bereich (wie z.B. der *Windows Media Rights Manager*) bereits seit längeren besitzen. OMA DRM 2.0 [OMA2 06], welches kurz vor der Verabschiedung steht, soll diese Lücken von OMA DRM 1.0 schließen.

4.4.5 Windows Media Rights Manager

Der *Windows Media Rights Manager* (WMRM) in Version 9 von der Firma Microsoft ist die am weitesten verbreitete Umsetzung des DRM-Referenz-Systems (vgl. Kapitel 4.4.2). Durch die Integration des DRM-Clients in den Windows-Media-Player (Version 9), der zur Standardausstattung von Windows-XP zählt, fällt das Problem für die Provider weg, eine spezielle Software auf dem Endgerät (Windows-PC) des Nutzers zu installieren. Aktuell (2005) liegt der WMRM in der Version 10 [WMRM 05] vor. Die Version 10 ermöglicht es, zeitlich limitiert Nutzungsrechte auch auf speziellen portablen Endgeräten zu realisieren. Der Musik-Download-Dienst Napster nutzt diese Funktionalität seit Anfang 2005, um ein Abonnement für die Nutzung aller (über 1 Millionen) Songs ihren Kunden anzubieten. Der Kunde kann alle Napster-Songs DRM-geschützt herunterladen und solange auf seinem tragbaren Endgerät anhören, wie er die monatliche Abo-Gebühr bezahlt.

Content Packer

Abbildung 4.16
Generierung des symmetrischen Schlüssels



Das Rechtesystem von Microsoft ist zwingend an die Audio- und Videoformate WMA (*Windows Media Audio*), WMV (*Windows Media Video*) und ASF von Microsoft gebunden. Auf dem Content Packer des Anbieters werden die Mediendaten symmetrisch verschlüsselt (vgl. DRM Packer in Abbildung 4.8). Der hierfür eingesetzte Schlüssel wird aus der *KeyID* und dem *License key seed* nach einem nicht publizierten Verfahren berechnet. Im Interesse der Sicherheit des gesamten DRM-Systems sollte dieses Verfahren auch nicht bekannt werden. Die *KeyID* wird vom Content-Packer festgelegt und in den unverschlüsselten Header der geschützten Datei eingebracht. Zusätzlich wird im Header die URL eines Lizenz-Servers (*Microsoft Media License Service*) und eine Prüfsumme über den benutzten Schlüssel eingetragen. Ein eindeutige ContentID und weitere applikationsabhängige Attribute (wie bspw. *UserNumber*) sind optional. Der gesamte Header wird mit dem privaten Server-Schlüssel signiert.

Lizenz-Server und Media-Player

Damit der Player die Datei abspielen kann, muss eine gültige Lizenz vorliegen. Der Windows-Media-Player fordert die Lizenz von dem Lizenz-Server an, der im Header eingetragen ist. Dabei wird mit dem übermittelten Header auch die KeyID übertragen. Aus der KeyID und dem nur dem Content-Packer und dem zugehörigen Lizenz-Server bekannten *License key seed* kann der benötigte symmetrische Schlüssel ge-

bildet werden. Dieser Schlüssel wird dann als Teil der Lizenz dem Client übermittelt, womit die Datei abgespielt werden kann. Bestandteil der Lizenz sind auch die vom Lizenz-Server eingefügten Rechte. Insgesamt können über 20 verschiedene Rechte gesetzt werden, darunter bspw. Abspielzähler und Abspielzeiträume, CD-Brennzähler, Verhalten bei Veränderungen der Computer-Zeit und Regeln, die den Transfer zu tragbaren Endgeräten betreffen.

Die Art und Weise der Speicherung der Lizenzen auf dem Windows-PC fällt wieder in das Gebiet der Geheimnisse, die Microsoft bewahren muss, wenn das System sicher bleiben soll. Lizenzen können grundsätzlich nicht von einem PC auf einen anderen übertragen werden. Die verschlüsselten Mediendateien können natürlich kopiert werden. Wird die Datei auf einem weiteren PC mit dem Windows-Media-Player geöffnet, so fordert dieser erneut eine Lizenz an. Der Lizenz-Server muss anhand der übermittelten Header-Daten entscheiden, ob er eine neue Lizenz ausstellt.

Der Lizenz-Server kann den Nutzer auffordern sich einzuloggen oder anderweitig zu authentifizieren. Soll bspw. verhindert werden, dass eine anonym ausgegebene Preview-Lizenz (bspw. nur dreimal Anhören) erneut an den gleichen Rechner ausgeben wird, so kann das durch Speicherung der IP-Adresse erfolgen. Da Nutzer oft wechselnde IP-Adresse haben, kann alternativ durch Setzen und Vergleichen eines Internet-Explorer-Cookies festgestellt werden, ob die Vorhör-Lizenz bereits an einen Rechner ausgeben wurde. Natürlich kann ein solches Cookie nicht mehr abgefragt werden, wenn der Nutzer diese im Internet-Explorer manuell gelöscht hat. Andere Varianten einen PC automatisch zu identifizieren bestehen in Windows Media Rights Manager Version 9 nicht, jedenfalls wurden sie dem Autor nicht bekannt.

4.4.6 Bewertung und zukünftige Entwicklungen

Der Apple iTunes Music Store (iTMS) hat ab Mitte 2003 gezeigt, dass der Einsatz von DRM-Systemen der 2. Generation kommerziell erfolgreich sein kann. Ob dieser Erfolg, der im Vergleich zum normalen CD-Verkauf noch sehr bescheiden ist, wegen oder trotz DRM möglich war, ist umstritten. Der Erfolg des iTMS ist zu einem Großteil den geringen Restriktionen dieses DRM-Modells zu verdanken. Das beim iTMS eingesetzte Fairplay DRM-System wurde allerdings schon mehrfach erfolgreich attackiert (vgl. [Hartmann 04] Seite 30). Sicher ist, dass das Schutzbedürfnis gerade der großen Plattenfirmen derzeit den Einsatz von möglichst sicheren DRM-Systemen erzwingt. Ohne DRM erhält kein Online-Händler die Erlaubnis die Musik dieser Firmen zu verkaufen.

Der Autor erwartet daher, dass die Bedeutung von DRM mindesten in den nächsten Jahren noch zunehmen wird. Allerdings hat DRM natürlich auch für die Anbieter Nachteile. Zum einen sind zusätzliche technische Aufwendungen notwendig. Die zusätzliche Technik macht die Vertriebssysteme der Anbieter und die Endgeräte der Konsumenten aufwendiger und teurer. Derzeit sind die verschiedenen DRM-Systeme alles Insellösungen. Musik, die mit WMRM geschützt ist, kann nicht auf OMA-Endgeräten abgespielt werden. Der Autor ist der Meinung, dass dies das Wachstum der Online-Musik-Branche aktuell noch nicht behindert. Ist das Volumen in einigen Jahren größer, werden diese Inkompatibilitäten, wie seiner Zeit die zwischen den drei unterschiedlichen Videorecorder-Systemen (VHS, Betamax und Video 2000), das weitere Wachstum behindern. Es wird schließlich zu einem Verdrängungswettbewerb kommen, bei dem entweder ein DRM-System übrig bleibt, oder DRM in der jetzigen Form wird an Bedeutung verlieren, da Konsumenten nicht für die Verhinderung von Nutzung zahlen wollen, sondern für die Ermöglichung von Nutzung.

Der Autor will nicht behaupten, dass ein gewisser technischer Kopierschutz sinnvoll ist, allerdings stellt er in Frage, ob sich solche DRM-Systeme durchsetzen können, die den Nutzer wie im Fall von WMRM und Napster 2.0 nie mehr aus ihrer Kontrolle entlassen? Bei Software, die primär auf einem Endgerät einmal installiert wird und dann nicht mehr transferiert wird, kann Kopierschutz ohne große Nachteile eingesetzt werden (vgl. Kapitel 6). Bei Musik, die vom Kunden über lange Zeit auf den unterschiedlichsten Endgeräten genutzt wird, kann Kopierschutz maximal bei kostenlos verteiltem Werbe-Content akzeptiert werden.

Eine weiterer Aspekt neben der mangelnden Akzeptanz durch den Kunden wird ebenfalls oft ignoriert: Welche Folgen hat es, wenn sich eine proprietäre firmenspezifische DRM-Lösung, wie WMRM am Markt durchsetzt? Wer könnte dann noch Microsoft Konkurrenz machen? Microsoft hätte dann alle Mittel in der Hand, sein Quasi-Monopol aus dem PC-Bereich auf alle anderen Endgerätetypen (wie Handys oder Festplatten-Receiver) auszudehnen. Dies kann nicht im Sinne des Wettbewerbs sein.

5. Kapitel

Bezahlsysteme für virtuelle Waren

In diesem Kapitel stehen Bezahlsysteme für virtuelle Waren im Mittelpunkt. Ein oft vernachlässigter Aspekt virtueller Güter ist deren Bezahlung durch den Konsumenten. Gegenüber einer Bezahlung realer Güter existieren bei der Bezahlung virtueller Waren zusätzliche Anforderungen.

Der Spruch „*if you can't bill it, kill it*“ wird häufig von der Firma Firstgate ins Feld geführt und verdeutlicht die Wichtigkeit einer funktionierenden Bezahlmöglichkeit. Die im Folgenden abgehandelten Bezahlsysteme sind daher eine besonders wichtige Teilkomponente bei den informatorischen Systemen für den Vertrieb virtueller Waren. Sie sind entscheidend bei der Realisierung direkter Erlösmodelle. Diese Geschäftsmodelle scheitern zu Zeiten von Breitband-Internet-Zugängen nicht mehr an dem Transfer der Nutzdaten vom Anbieter zum Konsumenten. Der Bezahlvorgang durch den Konsumenten ist der eigentliche Schwachpunkt.

Unterschiedliche Bezahlmethoden werden durch verschiedene am Markt agierende Unternehmen in ihren Bezahlsystemen angeboten. Das vom Autor mitentwickelte Bezahlsystem Paybest bietet mehrere dieser Systeme unter einer einheitlichen Schnittstelle Anbietern von virtuellen Waren an. Eine offengelegte Web-Service-Schnittstelle soll die Integration von Bezahlsystemen in spezialisierte Client-Anwendungen vereinfachen.

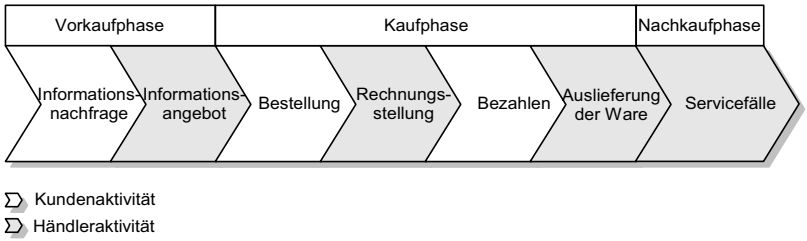
5.1 Anforderungen an ein Bezahlsystem für virtuelle Waren

Virtuelle Güter werden erst zu virtuellen Waren, wenn sie auf einem Markt angeboten und durch den Konsumenten für einen Preis erworben werden können. Da in der vorliegenden Arbeit Systeme für direkte Erlösmodelle (vgl. Kapitel 3.5) im Vordergrund stehen, ist folglich auch das Bezahlen der virtuellen Ware durch den Konsumenten von zentraler Bedeutung.

5.1.1 Bezahlen, eine Stufe im Verkaufsprozess

Unabhängig davon, ob es sich um virtuelle oder reale Waren handelt, ist das Bezahlen ein entscheidender Schritt im Verkaufsprozess. Abbildung 5.1 zeigt schematisch diesen Prozess, der sich in drei Hauptphasen unterteilt. In der *Vorkaufphase* müssen sich Anbieter und Konsument finden. Der Käufer sucht nach einem Händler, der die gewünschte Ware anbietet. Um entscheiden zu können, welches Angebot am besten geeignet ist, liefert der Anbieter ausführliche Informationen über Art, Umfang und Qualität der angebotenen Waren. Wenn sich der Käufer für ein Angebot entschieden hat, beginnt die eigentliche *Kaufphase*. Dort ordnen sich auch die Bezahlsysteme ein.

Abbildung 5.1
Der Verkaufsprozess [Lorenz 04]



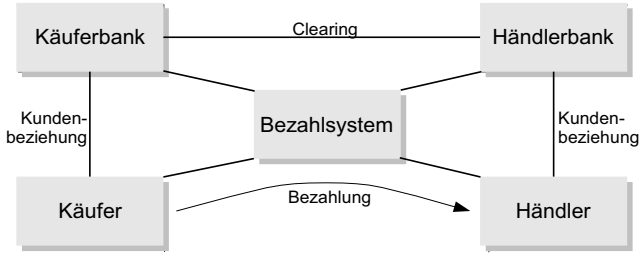
Der Kunde bekundet gegenüber dem Händler sein Kaufinteresse und erhält darauf eine Rechnung. Er wählt eine Zahlungsart aus und autorisiert die Zahlung. Um die Sicherheit zu erhöhen, wird im Interesse des Kunden an dieser Stelle unter Umständen bewusst ein Medienbruch eingefügt, um bspw. die Autorisierung über einen getrennten (sicheren) Kanal durchzuführen. Nachdem die Zahlung veranlasst wurde, kann der Händler mit der Auslieferung der Ware beginnen. Die Bezahlung kann bei physischen Waren allerdings auch nach der Auslieferung erfolgen. Die letzte Hauptphase ist die *Nachkaufphase*. Sie ist optional und umfasst unter anderem produktbezogene Dienstleistungen, wie Reklamationen oder Support. [Lorenz 04]

5.1.2 Weitere Akteure

In Kapitel 24 wurden bereits einige Wirtschaftsakteure eingeführt. Neben dem Anbieter und dem Konsumenten bzw. Händler und Käufer sind weitere Akteure bei der Bezahlung beteiligt.

Denkt man sich in Abbildung 5.2 erst einmal das Bezahlsystem in der Mitte weg, so zeigt es den Fall, wie er z. B. bei Lastschrift oder Rechnung vorkommt. Zwischen Käufer und Händler soll eine Zahlung stattfinden. Diese wird nicht direkt geleistet. Zur Abwicklung beauftragen Käufer und Händler ihre Banken. Durch ein separates Bankennetzwerk, welches Käuferbank und Händlerbank verbindet, wird die Zahlung verrechnet (*Clearing*).

Abbildung 5.2
Akteure, die bei einer Bezahlung beteiligt sind (aus [Lorenz 04] auf Basis von [Weber 98])



Bei Zahlung per Rechnung würde der Käufer die Käuferbank beauftragen, von seinem Konto das Geld auf das Händlerkonto bei der Händlerbank überweisen. Nachdem Händler- und Käuferbank miteinander abgerechnet haben, kann das Geld dem Händlerkonto gutgeschrieben werden. Der Zahlungseingang wird dem Händler mit dem Kontoauszug mitgeteilt. [Lorenz 04]

5.1.3 Das Bezahlsystem als Vermittler und Dienstleister

Bei Zahlungen im Internet – besonders wenn es um virtuelle Waren geht – übernimmt das in der Mitte in Abbildung 5.2 eingezeichnete und dazwischen geschaltete Bezahlsystem die Funktion eines spezialisierten Vermittlers und Dienstleisters. Im Folgenden werden die wichtigsten Gründe aufgelistet, warum es für Händler und Käufer sinnvoll ist, eine solche zusätzliche Instanz zuzulassen.

■ Der Wunsch der Händler die Transaktionskosten zu senken

Laut [KetStr 02] (S. 178) lohnt sich eine einzelne Abrechnung erst ab einem Betrag von 3,83 EUR (= ehemals 7,50 DM). Da der Preis für virtuelle Waren wie bspw. Musikstücke typischerweise darunter liegt, hat der Anbieter, wenn er den Verkauf einzelner Songs zulassen will, zwei Optionen: Entweder die Kleinstbeträge getrennt für jeden Kunden selbst aufsummieren, bis ein relevanter Betrag sich ergibt, oder dies einem zwischengeschalteten Dienstleister zu überlassen.

■ Zusätzliche Abrechnungsmodelle

Neben der Akkumulierung von Einzeltransaktionen, kann ein Bezahlsystem dem Händler und Käufer auch neue Abrechnungsmodelle (z. B. Abonnement) als Dienstleistung anbieten. Bezahlsysteme können sich auf Abrechnungsmodelle spezialisie-

ren, die besonders bei virtuellen Waren einen Zusatznutzen für Händler und Käufer darstellen (siehe Kapitel 5.2.4).

Reduzierung des technischen Aufwands beim Händler

Händler müssen unterschiedliche Abrechnungsmethoden (siehe Kapitel 5.2.1) anbieten, wenn sie die unterschiedlichen Bezahlwünsche ihrer Kunden befriedigen wollen. Überträgt der Händler dies nicht einem externen Dienstleister, muss er selbst einen sehr großen organisatorischen und damit finanziellen Aufwand betreiben, um alle Abrechnungsmethoden selbst in sein Shop-System zu integrieren. Dies lohnt sich finanziell nur für sehr große Händler.

Der Mangel am gegenseitigen Vertrauen und Datenschutzüberlegungen

Ist das Bezahlsystem durch die Masse zufriedener Nutzer bereits als vertrauenswürdig eingestuft, so können auch unbekannte Händler hiervon profitieren. Bezahlsysteme können für den Fall, dass der Kunde dem Händler keine Kontodaten anvertrauen möchte, eine teilweise Anonymisierung des Käufers (gegenüber diesen Händlern) als Dienstleistung anbieten. Die zur Abrechnung benötigten Kontoinformationen werden nicht an den Händler weitergeleitet. Käufer können gegenüber unbekannten Händlern teilweise anonym bleiben (siehe Kapitel 5.2.5).

Darüber hinaus können Bezahlsysteme zusätzliche Dienstleistungen, wie z. B. eine Bonitätsprüfung oder eine bedingte Versicherung des Risikos eines Zahlungsausfalls, dem Händler anbieten.

5.1.4 Der rechtliche Rahmen

Nutzt bspw. ein Händler ein Bezahlsystem, welches in einem anderen EU-Mitgliedstaat seinen Sitz hat, so kann es über den rechtlichen Rahmen Unsicherheit geben. Der Händler hat keine Gewissheit, welche rechtlichen Bestimmung bspw. bei der Insolvenz eines Bezahlsystems greifen. Dies machte es unter anderem notwendig, dass auf europäischer Ebene durch das EU-Parlament neue rechtliche Rahmenbedingungen geschaffen wurden. Die beiden folgenden Richtlinien bilden die Basis für die Gesetzgebung in Deutschland und den anderen Mitgliedsstaaten.

Richtlinie 2000/31/EG [EU31 00]

Die „E-Commerce-Richtlinie“ bildet den groben Rahmen für den elektronischen Geschäftsverkehr innerhalb des Binnenmarktes. Sie soll den freien Verkehr von Waren und Dienstleistungen innerhalb der EU durch eine Harmonisierung der nationalen Regelungen ermöglichen. Ebenso sollen Rechtssicherheit für den Anbieter und Schutz des Konsumenten erreicht werden.

Kernpunkte der Richtlinie ist das so genannte Herkunftslandprinzip. Es besagt, dass das Angebot eines Anbieters unter die jeweilige Rechtsprechung des Landes fällt, in dem dieser seine Niederlassung hat. Der Standort des Servers spielt dabei keine Rolle. Für die Besteuerung und das Urheberrecht gilt dieses Prinzip allerdings nicht.

■ **Richtlinie 2000/46/EG [EU46 00]**

In dieser Richtlinie werden die Rechts- und Verwaltungsvorschriften der Mitgliedsstaaten über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeiten von E-Geld-Instituten koordiniert und harmonisiert. Die Ausgabe und Verwaltung von elektronischem Geld (Geldkarten- und Netzgeldgeschäft) zählt zu den Bankgeschäften und wird von Kreditinstituten durchgeführt (Artikel 2 Absatz 1). In Deutschland wird diese Richtlinie durch das Kreditwesengesetz (KWG) [KWG 04] realisiert [Müller 04].

Für den Betrieb eines solchen Bankgeschäftes bedarf es der besonderen Genehmigung durch die Bundesanstalt für Finanzdienstleistungsaufsicht [BaFin 04]. Eine solche Genehmigung wird nur gewährt, wenn eine Reihe von Anforderungen erfüllt sind. So wird beispielsweise ein Anfangskapital von 1 Mio. Euro verlangt, die Leitung des Institutes muss fachlich geeignet sowie zuverlässig sein und der Geschäftsplan wird auf Tragfähigkeit untersucht.

Da nicht jedes Bezahlsystem zwangsläufig Bankgeschäfte im Sinne der E-Geld-Richtlinie durchführt, ist es wichtig die Definition von E-Geld genauer zu betrachten. Folgende Begriffsbestimmung findet sich im [KWG 04] (§1 Absatz 14):

> *„Elektronisches Geld sind Werteinheiten in Form einer Forderung gegen die ausgebende Stelle, die*
> *1. auf elektronischen Datenträgern gespeichert sind,*
> *2. gegen Entgegennahme eines Geldbetrags ausgegeben werden und*
> *3. von Dritten als Zahlungsmittel angenommen werden, ohne gesetzliches Zahlungsmittel zu sein.“*

Unter E-Geld fallen somit Systeme, auf denen der Kunde über ein vorausbezahltes Guthabenkonto verfügt und dieses Guthaben bei einem Dritten einlösen kann. Wenn die ausgebende Stelle die einzige Stelle ist, bei der dieses Guthaben eingelöst werden kann, so handelt es sich nicht um E-Geld. Bisher ist es nicht geklärt in wieweit Bonuspunkte, die der Kunde bei unterschiedlichen Händlern in Waren oder Dienstleistungen einlösen kann, zum E-Geld gehören.

5.2 Klassifizierung

Um die unterschiedlichen existierenden Bezahlsysteme einordnen zu können, wird eine Klassifizierung benötigt. Elektronische Bezahlsysteme, die sich für die Abrechnung virtueller Waren eignen, können nach unterschiedlichen Kriterien klassifiziert werden.

5.2.1 Abrechnungsmethode

Das Bezahlsystem bzw. der Händler kann über eine Auswahl von alternativen Methoden mit dem Käufer abrechnen. Diese Abrechnungsmethoden unterscheiden sich in der Art und Weise, wie der Käufer schließlich die Forderung begleicht.

- **Vorkasse/Überweisung**: Bevor der Händler die virtuelle Ware ausliefert, muss der Käufer den vollen Betrag überweisen. Dieses Verfahren bietet dem Händler maximale Sicherheit, da der Kunde eine Überweisung nur mit großer Mühe stornieren kann. Der Käufer muss allerdings die Banklaufzeiten von mindestens ei-

nem Tag abwarten, bevor er die Ware geliefert bekommt. Bei einer Online-Überweisung kann die Banklaufzeit verkürzt werden.

- **Rechnung**: Der Käufer zahlt erst nach Erhalt der Ware. Dieses Verfahren bildet das Gegenstück zur Vorkasse und bietet maximale Sicherheit für den Käufer. Für Händler hingegen bedeutet es einen hohen Verwaltungsaufwand und die Unsicherheit, wirklich die Zahlung zu erhalten. Bei der Abrechnung von virtuellen Waren über ein Bezahlsystem wird diese Abrechnungsmethode nicht eingesetzt.
- **Lastschrift**: Der Käufer autorisiert den Händler bzw. das Bezahlsystem (meist durch Übermittlung der Bankverbindung), den festgelegten Rechnungsbetrag vom Käuferkonto abzubuchen. Aus Sicht des Verbraucherschutzes bietet eine Lastschrift eine ähnliche Sicherheit wie eine Rechnung, da sie vom Käufer 6 Wochen nach dem Kauf ohne Angaben von Gründen storniert werden kann. Daher besteht keine Zahlungsgarantie für den Händler. Sie gehört allerdings zu den kostengünstigsten Abrechnungsmethoden. Abhängig vom Abbuchungszeitpunkt (sofort oder nach einer Frist) gehört die Lastschrift zu den Pay-Now oder Pay-Later-Verfahren.
- **Kreditkarte**: Bei Kreditkartenzahlungen teilt der Käufer dem Händler bzw. dem Bezahlsystem seine Kreditkartendaten (Nummer und Gültigkeitsdauer) mit, die von diesem zur Abrechnung mit dem zwischengeschalteten Kreditkartenunternehmen benutzt werden. Dieses Verfahren bietet keine Zahlungsgarantie, da ohne Unterschrift keine wirkliche Zahlungsverpflichtung für den Karteninhaber besteht. Die Kreditkartennummer ist auch nicht als ein Geheimnis zwischen Käufer und Kartengesellschaft einzustufen, das den berechtigten Karteninhaber nach außen authentifiziert, da sie auf allen Abrechnungsbelegen gedruckt wird. Dieses Problem wurde durch die Einführung der dreistelligen Kartenprüfnummer entschärft. Diese Prüfnummer erscheint auf keinem Beleg und wird bei einem Kauf zusätzlich zu den normalen Kartendaten angegeben.
- **Kreditkarte mit SET**: SET (*Secure Electronic Transaction*, vgl. [KetStr 02] S. 215ff) ist eine Weiterentwicklung der Kreditkartenzahlung speziell für das Internet. SET bringt zwar für den Empfänger der Zahlung durch den Einsatz von digitalen Signaturen (vgl. Seite 56) eine Zahlungsgarantie, muss allerdings aufgrund des hohen technischen Aufwands und der mangelnden Akzeptanz inzwischen als gescheitert betrachtet werden.
- **Kreditkarte mit 3D-Secure**: Der Standard 3D-Secure (vgl. [KetStr 02] S. 219ff) wurde von Visa entwickelt und wird unter der Bezeichnung *Verified by Visa* vermarktet. MasterCard unterstützt den Standard unter dem Namen *MasterCard SecureCode*. Das Verfahren erweitert die einfache Kreditkartenzahlung um eine Autorisierung z.B. durch Passwortangabe. Der Händler erhält eine Zahlungsgarantie. [Lorenz 04]
- **Inkasso/Billing**: Hiermit wird keine Abrechnungsmethode bezeichnet, sondern nur der Vorgang, bei dem mehrere kleinere Forderungen nicht sofort abgerechnet werden, sondern erst nachdem ein gewisser Betrag zusammengekommen ist. Auf diese Weise fallen die hohen Fixkosten einer Lastschrift oder Kreditkartenzahlung nicht mehr ins Gewicht.
- **Inkasso per Telefon bzw. Handy**: Hier wird der Rechnungsbetrag über die Telefonrechnung des Konsumenten beglichen. Entweder über den Anruf einer Mehrwertnummer oder das Senden einer SMS-Nachricht (sog. Premium-SMS) an eine spezielle Mobilfunknummer. Es fallen nicht nur die normalen Verbindungskosten

an, sondern darüber hinaus zusätzliche Entgelte, die die jeweilige Telefongesellschaft an den Anbieter weiterleitet. Entweder löst der Rechner über eine spezielle Software (Dialer) diesen Anruf selbsttätig aus oder der Kunde ruft manuell an. Oft werden hierbei spezielle Einmalcodes angesagt, die der Kunde zur Autorisierung einer Transaktion dann benutzen muss. Bei einer SMS löst bspw. ein bestimmter einzugebender Text eine Aktion aus. Mit dieser SMS wird auch die Handy-Nummer des Kunden übermittelt, an die der Anbieter entweder das virtuelle Gut direkt sendet oder es wird eine SMS mit einem Einmalcode zurückgeschickt. Weitere SMS-Bezahlmethoden werden in Kapitel 5.3.5 beschrieben.

- **Online-Überweisung**: Um die Zahlung zu autorisieren, wird der Kunde z. B. durch ein Java-Applet auf ein Banken-Gateway weitergeleitet. Dort führt er die Überweisung auf das Händlerkonto direkt per Eingabe von PIN und TAN durch. Der Händler erhält eine Zahlungsgarantie. Allerdings ist dieses Bezahlverfahren nur mit Kunden möglich, die über ein Online-Konto verfügen.
- **Freischaltkarten**: Vor dem eigentlichen Kauf von virtuellen Waren muss der Kunde zuerst eine «Rubbelkarte» (Scratchcard) erwerben. Mit der auf dieser Karte freizurubbelnden Buchstaben-Ziffern-Kombination erhält der Käufer Zugriff auf ein anonymes Konto, dessen Stand gleich dem Kaufpreis der Freischaltkarte ist. Durch Eingabe dieser Buchstaben-Ziffern-Kombination autorisiert der Käufer Zahlungen. Dieses Verfahren ist von den Prepaid-Handys her bekannt. Die Freischaltkarte ist nahezu die einzige Möglichkeit, virtuelle Waren vollständig anonym zu bezahlen.
- **Geldkarte**: Auf den meisten EC-Karten befindet sich der Chip für die Geldkartenfunktion. Prinzipiell könnte man mit der Geldkarte auch Zahlungen am heimischen PC durchführen. Dazu benötigt der Käufer allerdings einen relativ teuren Klasse-3-Kartenleser mit Display und Tastatur. Vor einer Zahlung muss der Käufer den Chip auf der Karte an einem Bankterminal aufladen. Dieses Guthaben kann dann für die Begleichung von Rechnungen eingesetzt werden. Technisch wäre eine vollständig anonyme Zahlung möglich. Allerdings haben sich die Banken gegen die Ausgabe von namenlosen (weißen) Karten ausgespochen.

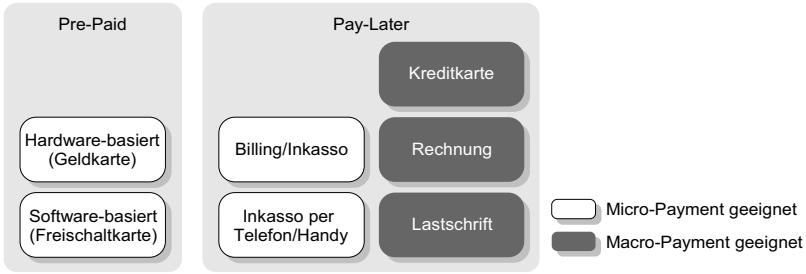
Eine andere Form der Klassifikation von Bezahlsystemen erfolgte durch Angelika Zobel [Zobel 02]. In Ihrer Diplomarbeit beschreibt sie die Methode der Nutzwertanalyse, bei der 128 Kriterien strukturiert und ausgewertet wurden.

5.2.2 Zeitpunkt des Zahlungsübergangs

Der Zeitpunkt des eigentlichen Zahlungsübergangs ist ebenfalls ein wichtiges Unterscheidungsmerkmal von Bezahlsystemen bzw. Bezahlmethoden. Gemeint ist der Zeitpunkt an dem der Rechnungsbetrag dem Käufer nicht mehr zur Verfügung steht.

- **Pre-Paid**: Der Käufer muss bereits vor der Kaufphase (vgl. Abbildung 5.1) einen bestimmten Geldbetrag aufwenden. In Abbildung 5.3 unterscheidet Lorenz zwischen Hardware- und Software-Lösungen, z. B. Geldkarte bzw. Freischaltkarten (Scratchcard).
- **Pay-Now**: Zum Zeitpunkt der Auslieferung der virtuellen Ware wird Zug-um-Zug die Ware gegen eine Zahlung herausgegeben. In [KetStr 02] (S. 32) werden Nachnahme, bedingte Lastschrift und bestimmte mobile Bezahlsysteme als Pay-now-Bezahlmethoden eingeordnet.

Abbildung 5.3
Klassifizierung von Bezahlsystemen und ihre Abrechnungsmethoden [Lorenz 04]



- **Pay-Later**: Hier wird der Geldbetrag für die virtuelle Ware erst nach Auslieferung fällig. Die meisten Bezahlsysteme, die auf Bezahlmethoden wie Kreditkarte, Rechnung oder Lastschrift aufbauen, sind Pay-Later-Systeme.

5.2.3 Transaktionshöhe

Eine Klassifizierung nach der typischen Höhe der Zahlung ist eine sehr unscharfe Einteilung. In der Regel werden drei Klassen unterschieden:

- **Micro-Payment**: Hier werden Rechnungsbeträge bis ca. 1 Euro einsortiert. Virtuelle Waren bewegen sich häufig in dieser Größenordnung. Diejenigen Abrechnungsmethoden, die sich für Micro-Payment eigenen, sind in Abbildung 5.3 hellblau hinterlegt.
- **Small-Payment**: Mittlere Rechnungsbeträge bis ca. 10 Euro lassen sich in dieser Kategorie zusammenfassen. Anbieter virtueller Waren sind bestrebt solche Beträge abzurechnen, da Micro-Payment oft zu teuer ist. Small-Payment wird oft auch noch zu Micro-Payment gerechnet.
- **Macro-Payment**: In diese Kategorie fallen Rechnungsbeträge über 10 Euro. Für solche Beträge benötigt man nicht zwingend spezielle Bezahlsysteme, die einzelne Kleinsttransaktionen zusammenfassen. Die klassische Kreditkartenzahlung oder Überweisung zählt zu den Macro-Payments.

5.2.4 Abrechnungsmodelle

Auf virtuelle Waren fokussierte Bezahlsystem können speziell für diese Warengruppe Abrechnungsmodelle anbieten.

- **Pay-per-Use**: Der Nutzer zahlt für die Nutzung des Dienstes wie zum Beispiel für einen Download oder eine Datenbankabfrage eine einmalige Gebühr. Dieses Abrechnungsmodell wird z. B. bei Musik-Downloads von den meisten Käufern bevorzugt [LeiStr 03].
- **Pay-per-Time**: Der abgerechnete Betrag ergibt sich aus der tatsächlichen Nutzungsdauer.

- **Abonnement**: Dem Kunden wird zyklisch (z. B. monatlich) ein fester Betrag in Rechnung gestellt, für den er Zugang zum Content eines Anbieters erhält. Handelt es sich um Zugang zu Dienstleistungen, die unbeschränkt in Abspruch genommen werden können, spricht man auch von *Flatrate*.
- **Paket**: Der Nutzer kauft vorab ein definiertes Kontingent an virtuellen Waren, das sukzessive aufgebraucht werden kann.

5.2.5 Grad der Anonymität des Käufers

Der Grad der Anonymität des Käufers beim Bezahlvorgang kann zusätzlich zur Unterscheidung der Bezahlsysteme dienen. Anonymität ist gegeben, wenn der Käufer keine persönlichen Daten, wie bspw. den Namen oder die Adresse preisgeben muss. Vier Stufen der Anonymität lassen sich unterscheiden:

- **Keinerlei Anonymität** liegt vor, wenn der Käufer beim Anbieter persönliche Daten hinterlassen muss.
- **Anonymität gegenüber dem Anbieter** der Ware liegt vor, wenn der Käufer nur beim Bezahlsystem persönliche Daten hinterlassen muss und das Bezahlsystem diese gegenüber dem Händler geheim hält.
- **Pseudoanonymität** besteht, wenn zusätzlicher (erhöhter) Aufwand nötig ist, um die Identität des Käufers zu ermitteln. Z. B. bei Bezahlsystemen, die über die Telefonrechnung das Inkasso abwickeln (0190er bzw. 0900er Nummern). Auch die Geldkarte mit ihrer *Separation-of-Duty*-Pseudonymität ließe sich hier einordnen.
- **Vollständige Anonymität** besteht nur bei Bargeld. Wenn man von der Übermittlung der Identität über die IP-Adresse absieht, ermöglichen bar vorausbezahlte Freischaltkarten diese vollständige Anonymität auch beim Kauf virtueller Waren im Internet. Die elektronische Münzen des ecash-Systems würden dies ebenfalls ermöglichen. Allerdings konnten sich ecash nicht am Markt durchsetzen.

5.2.6 Weitere Unterscheidungsmerkmale

Der Autor hat sich bewusste gegen eine spezielle Strukturierungsmethode für Bezahlsysteme für seine Betrachtungen entschieden. Der sehr schnelllebige Markt bei Bezahlsystemen lässt solche umfassenden Strukturierungsansätze oft sehr kurzlebig erscheinen. Dennoch gibt es immer wieder erfolgversprechende Ansätze [Zobel 02]. Die folgenden zwei weiteren Unterscheidungsmerkmale zeigen exemplarisch die Vielfalt auf diesem Gebiet.

Art der Autorisierung

Der Käufer kann eine Zahlung für den Händler mit unterschiedlichen Methoden autorisieren. Die **Kenntnis** der Abrechnungsdaten des Käufers durch den Händler ist die schwächste Form der Autorisierung. Die Autorisierung über ein **Passwort** – ein gemeinsames Geheimnis zwischen Käufer und Händler – ist ein übliches Verfahren. Eine höhere Sicherheit für den Käufer bieten Einmal-Passwörter, wie es z. B. TANs (Transaktionnummern) sind.

Mit dem **Handy** bzw. einer **SMS** lässt sich eine Zahlung über einen sicheren Kanal autorisieren. Man geht in diesem Fall davon aus, dass der Käufer mit dem Besitzer des Handys identisch ist. Ist dies nicht so, liegt Missbrauch vor, den der Besitzer des Handys zu verantworten hat.

Bei längerfristigen Verträgen (Abo) und höherpreisigen Gütern kann auch noch eine manuelle **Unterschrift** benutzt werden. Die elektronische Version der Unterschrift ist die **digitale Signatur** (vgl. Seite 56). Dabei wird jede Transaktion digital signiert, wodurch die Authentizität gewährleistet werden kann. Allerdings ist der Aufwand beim Käufer sehr hoch.

Kosten

Die Kosten eines Bezahlsystems sind ein wichtiges Unterscheidungsmerkmal. Man muss zwischen den zusätzlichen Kosten für den Käufer und den Kosten für den Händler unterscheiden. In der Regel werden dem Käufer keinerlei zusätzliche Kosten zugemutet. Es sei denn, er benötigt, wie bei der Geldkarte, einen zusätzlichen Kartenleser. Der Händler muss mit **Monatsgebühren**, festen **Transaktionsgebühren** und prozentualen **Abschlägen** rechnen. Diese Transaktionsgebühren und Abschläge können mit dem Rechnungsbetrag und dem monatlichen Volumen des Händlers variieren.

Bei virtuellen Waren sind jedoch nicht nur die Händlerkonditionen entscheidend. Es ist vielmehr oft die Akzeptanz bei nationalen oder internationalen Käufern, warum sich derzeit ein Händler für ein spezielles System entscheidet. Auch die technischen Komponenten, wie eine elegante Content-Verwaltung, eine einfache Integration oder z. B. die Möglichkeit Abonnements abzurechnen, sind weitere wichtige Entscheidungskriterien.

5.3 Ausgewählte Bezahlsysteme

Nachdem in Kapitel 5.2.1 die unterschiedlichen möglichen Abrechnungsmethoden aufgezeigt wurden, wird nun eine Auswahl von konkreten Bezahlsystemen beschrieben. Die ausgewählten Systeme erheben keinen Anspruch auf Vollständigkeit. Der Fokus liegt vielmehr auf den Systemen, die in das selbstentwickelte Multipayment-System Paybest [Paybest 05] integriert wurden, weil die Systeme einerseits bei Käufern bereits angenommen waren und ihre Integration mit überschaubaren technischen und finanziellen Aufwand möglich war. Eine aktuelle Beschreibung der beschriebenen Systeme findet sich in [Nützel 04]. Eine detailliertere aber ältere Beschreibung findet sich in [Nützel 02].

5.3.1 Kontenbasierte Systeme mit Peer-to-Peer-Zahlfunktion

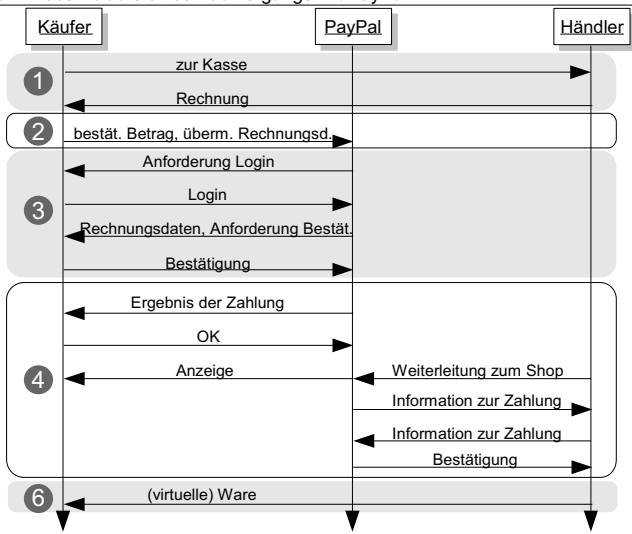
PayPal

PayPal [Paypal 04] ist ein amerikanischer Finanzdienstleister, der seit 2003 zum amerikanischen Internet-Auktionshaus eBay gehört. PayPal hatte bereits bei der Ausweitung seines Dienstes auf Zahlungen in Euro (Ende 2002) über 30 Millionen registrierte Nutzer weltweit. PayPal (Europe) Ltd. ist als E-Geld-Institut von der Fi-

nancial Services Authority (FSA) in Großbritannien autorisiert und wird von dieser gemäß EU-Richtlinie 2000/46/EG [EU46 00] reguliert.

Um mit PayPal bezahlen zu können, benötigt man seit Anfang 2004 nicht mehr unbedingt eine Kreditkarte. Zahlungen mittels Überweisung sind seitdem auch möglich. Da PayPal kein Lastschriftverfahren anbietet, sind Zahlungen per Überweisung auf ein PayPal-Konto nur beschränkt für Echtzeitzahlungen geeignet. Bei der ersten Zahlung mit PayPal muss der Kunde sich registrieren. Dabei wird ein Online-Konto bei PayPal für den Kunden eingerichtet. Weitere Zahlungen erfolgen über dieses Konto durch Login (E-Mail-Adresse und Passwort). [Nützel 04]

Abbildung 5.4
Sequenzdiagramm des Ablaufs eines Kaufvorgangs mit PayPal



Mit diesem PayPal-Account können auch Zahlungen anderer PayPal-Nutzer für dieses Konto entgegen genommen werden (Peer-to-Peer-Zahlung). Dies hat besonders beim Verkauf von Waren über eBay Bedeutung. Möchte man eine solche Peer-to-Peer-Zahlung innerhalb von PayPal durchführen, so muss man nur die E-Mail-Adresse des Zahlungsempfängers wissen. Im PayPal-System gibt man dann diese Adresse, den Betrag und einen Betreff ein und löst per Maus-Klick die Transaktion aus. Der Empfänger wird von PayPal daraufhin per E-Mail über den Eingang einer Zahlung informiert und aufgefordert diese durch anklicken eines Bestätigungslinks anzunehmen. Spätestens jetzt muss der Empfänger sich bei PayPal registrieren, um die Zahlung anzunehmen.

Zur automatischen Bezahlungsabwicklung bietet PayPal dem Händler, der bspw. virtuelle Waren anbietet, eine Reihe von Möglichkeiten an. Die erste Variante ist der so genannte *Buy Now Button*, der sich für einzelne Waren eignet. Eine einfache Möglichkeit, einen kompletten Online-Shop zu erstellen, bietet der *PayPal Shopping Cart*. Der Käufer kann mehrere Artikel einem Warenkorb hinzufügen und anschließend diesen über PayPal bezahlen. Zusätzlich wird dem Händler ein Abonnement-

System zur Abrechnung wiederkehrender Zahlungen angeboten. Selbst Spenden können über PayPal abgewickelt werden. [Lorenz 04]

Für eine elegante Kopplung eines Online-Shops mit PayPal bietet sich die so genannte IPN (*Instant Payment Notification*) an. Nach einer erfolgten Bezahlung sendet PayPal eine Bestätigung mit Einzelheiten der Transaktion an den Anbieter-Server.

Das Sequenz-Diagramm aus Abbildung 5.4 zeigt den Ablauf einer Zahlung unter Nutzung der IPN. Der Ablauf eines Verkaufsvorgangs wurde von Lorenz [Lorenz 04] allgemein in 6 Schritte unterteilt, wobei die Schritte 4 bis 6 nicht bei jedem Bezahlsystem enthalten sind:

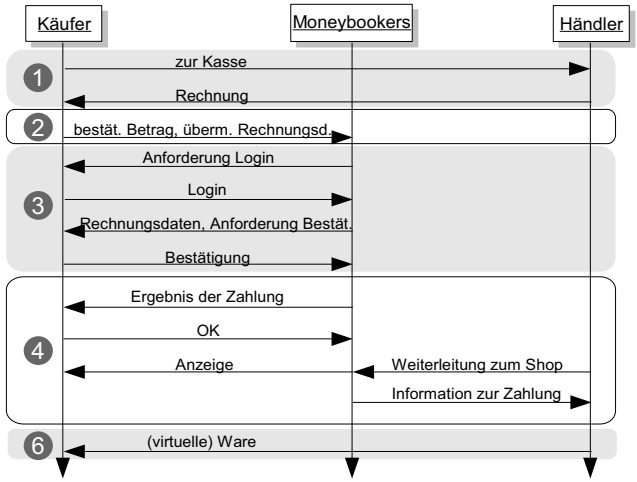
- Schritt 1: Der Käufer erhält an der virtuellen Kasse eine Rechnung.
- Schritt 2: Der Käufer wählt eine Zahlungsart aus und bestätigt gleichzeitig damit den Kauf. Der Käufer wird darauf zum eigentlichen Bezahlsystem weitergeleitet, das vom Händler die notwendigen Rechnungsdaten zur Zahlungsabwicklung bekommt. Der Händler kann die Zahlung sofort verbuchen lassen, oder aber den Betrag erst reservieren lassen, um ihn später auf einmal oder mehrmals in Teilbeträgen abzubuchen. Auf diese Weise erlaubt das Bezahlsystem Kontingente oder eine zeitlich getaktete Abrechnung.
- Schritt 3: Das Bezahlsystem präsentiert dem Käufer eine Zusammenfassung der Zahlung, die vom Käufer schließlich autorisiert wird.
- Schritt 4: Käufer und Händler werden über den Erfolg der Zahlung bzw. Reservierung informiert.
- Schritt 5: Falls die Zahlung im zweiten Schritt nur reserviert wurde, kann der Händler nun die Abbuchung des Gesamt- bzw. eines Teilbetrages veranlassen.
- Schritt 6: Die Ware wird an den Käufer ausgeliefert.

Moneybookers

Moneybookers Ltd. [Mbookers 05] ist eine Tochterfirma der in London ansässigen Gesellschaft Gatcombe Park Ventures Limited. Moneybookers versteht sich als direkter Konkurrent zu PayPal und funktioniert ähnlich [Nützel 04]. Es gibt ein Online-Konto auf das der Kunde Beträge einzahlen und anschließend zum Bezahlen verwenden kann. Ein P2P-Geldtransfer ist analog zu PayPal ebenfalls möglich. Damit Kunden, die noch keinen Moneybookers-Account besitzen, ebenfalls online bezahlen können, kann die Zahlung per Kreditkarte oder Lastschrift abgewickelt werden. Moneybookers bot Lastschrift lange vor PayPal an. In Gegensatz zu PayPal bietet Moneybookers dem Händler eine Zahlungsgarantie. Allerdings sind für Auszahlungen auf ein normales Bankkonto höhere Gebühren (1,80 Euro) als bei PayPal (1 Euro) zu entrichten.

Für den Händler steht für die Abrechnung ein umfangreicheres System namens *Merchant Gateway* zur Verfügung. Es erlaubt die Integration von Moneybookers in einen Online-Shop. Abbildung 5.5 zeigt das Sequenzdiagramm für die Kommunikation mit Moneybookers. In Schritt 4 ist der Ablauf gegenüber PayPal (vgl. Abbildung 5.4) unterschiedlich.

Abbildung 5.5
Sequenzdiagramm des Ablaufs eines Kaufvorgangs mit Moneybookers



Anypay

Das Anypay System [Anypay 05] der Firma Globyte Internet GmbH aus Deutschland ist ein weiteres kontobasiertes Bezahlsystem, welches ebenfalls P2P-Zahlungen anbietet und damit wie PayPal und Moneybookers ein E-Geld-Institut ist.

WEB.Cents

Der E-Mail-Dienstleister WEB.DE [WEBDE 05] bietet seit September 2003 seinen internen kontenbasierten Abrechnungsdienst (WEB.Cent) auch für externe Anbieter an. Um mit WEB.Cent virtuelle Waren kaufen zu können, muss der Kunde auf ein spezielles Konto per Lastschrift, Überweisung oder Kreditkarte einzahlen. Bei der Lastschrift unterscheidet WEB.Cent zwischen temporären und voll verfügbaren „Cents“. Nachdem der Kunde die Lastschrift an WEB.Cent in Auftrag gegeben hat, verfügt er bis zum Zahlungseingang lediglich über temporäre „Cents“. Diese kann er nur eingeschränkt für Zahlungen verwenden. WEB.Cent-Nutzer können untereinander (P2P) auch Geld zwischen ihren Online-Konten transferieren. Es wird lediglich die E-Mail-Adresse und die Postleitzahl des Zahlungsempfänger benötigt. Im Anschluss an die Zahlung erhalten Sender und Empfänger eine Bestätigung per E-Mail. [Lorenz 04]

5.3.2 Inkasso/Billing-Systeme

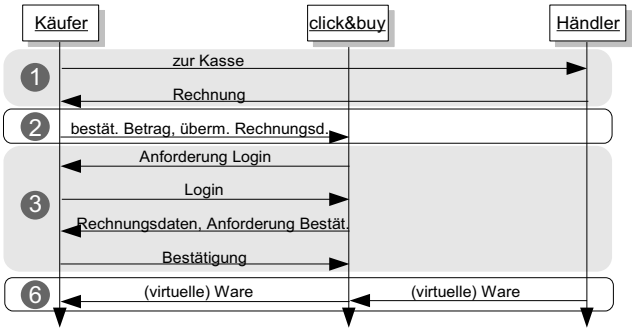
FIRSTGATEs click&buy

Die Januar 2000 gegründete FIRSTGATE Internet AG [Firstgate 04] ist mit ihrem click&buy System in Deutschland zum Marktführer bei Bezahlsystemen für virtuelle

Güter geworden. Im Unterschied zu den kontenbasierten Systemen ist click&buy ein Inkasso/Billing-System, welches auf virtuelle Waren beschränkt ist. Die einzelnen Rechnungsbeträge werden gesammelt und am Monatsende per Lastschrift abgebucht bzw. der Kreditkarte belastet und an die jeweiligen Händler überwiesen.

FIRSTGATE bietet seinen Händlern ein eigenes Content-Management-System, welches speziell den Verkauf virtueller Waren für die Anbieter sehr einfach gestaltet. Das System kümmert sich um die Auslieferung der Ware, die auf den Servern der Händler gehostet (bereitgehalten) wird. Der Händler muss zuvor seine virtuellen Waren bei Firstgate registrieren. Es können einzelne Dateien oder komplette Verzeichnisse zusammen mit einer Beschreibung und Tarifierung angegeben werden. Als Ergebnis erhält der Anbieter einen so genannten *Premium Link*, den er auf seiner Website veröffentlichen kann. Wird ein solcher Link angeklickt, so wird der Kunde zu Firstgate weitergeleitet. Nach erfolgter Bezahlung (Schritt 3 in Abbildung 5.6) lädt Firstgate die Ware transparent vom Händler-Server und gibt sie an den Kunden weiter (Schritt 6). [Lorenz 04]

Abbildung 5.6
Sequenzdiagramm des Ablaufs eines Kaufvorgangs mit click&buy



Neben einer flexiblen Tarifierung können auch Benutzergruppen eingerichtet werden, für die spezielle Konditionen gelten. Dies macht es möglich, bspw. Stammkunden Rabatte einzuräumen. Zusätzlich ist es, ähnlich zu Moneybookers und Paypal, möglich eine Server-to-Server-basierte Bezahlungsabwicklung zu nutzen. Dieser Dienst wird allerdings nur auf Anfrage manuell eingerichtet.

Paybox

Das Paybox-System ist ein lastschriftbasiertes Inkasso-Verfahren, bei dem, im Unterschied zu click&buy, der Käufer die Autorisierung der Zahlung und somit die Abbuchung von seinem Bankkonto mittels Handy durchführt. Paybox zielt nicht primär auf die Abrechnung virtueller Waren, sondern auch auf klassische Produkte und Dienstleistungen (z. B. Zahlung von Taxi-Fahrten). In den Jahren 2000 und 2001 war Paybox ein ernstzunehmender Konkurrent von click&buy. Ende 2002 musste die Paybox.net AG allerdings den Betrieb einstellen. Anfang 2004 hat die niederländische Firma Moxmo den Betrieb des Paybox-Systems wieder aufgenommen. Im September 2004 kam auch für Moxmo das Aus. Aktuell (2005) betreibt in Österreich die

paybox austria AG [PayboxAT 05], die zu 100% im Besitz der mobilkom austria AG & Co KG ist, den Paybox-Dienst.

Bei der Paybox-Anmeldung gibt der Kunde neben seinen Kontodaten auch seine Mobilfunknummer an. Zur Datensicherheit kann auch ein Alias-Name vereinbart werden. Zusätzlich legt er noch einen 4-stelligen Paybox-PIN fest. Entscheidet sich ein Kunde auf der Webseite eines Händlers für Paybox, so wird er vom Händler aufgefordert, seine Mobilfunknummer oder den Alias-Namen einzugeben. Der Server des Händlers leitet im Hintergrund die Mobilfunknummer (bzw. Alias) an den Paybox-Server weiter. Bei dieser Weiterleitung werden zusätzliche Parameter wie Preis und Händler-Kennung übermittelt. Darauf erfolgt ein (Mobilfunk-)Rückruf durch das Paybox-System. Der Kunde bekommt von Paybox den Anbieter und Preis akustisch mitgeteilt. Ist der Käufer mit den Zahlungsdaten einverstanden, so gibt er am Handy seine 4-stellige Paybox-PIN ein. Paybox betrachtet diese Aktion als Legitimation, den entsprechenden Betrag vom Bankkonto des Kunden abzubuchen, und dem Händler zu überweisen.

Das Paybox-System gilt durch die Autorisierung über das vom Internet getrennte GSM-Netz als relativ sicher. Damit ein Angreifer illegale Einkäufe tätigen kann, müsste er neben der Paybox-PIN auch noch das Handy eines Paybox-Nutzers in seine Gewalt bringen. Allerdings ist der Rückruf über das GSM-Netz relativ teuer. Deshalb eignet sich die Paybox-Methode nicht für Micro-Payments unter einem Euro (vgl. Kapitel 5.2.3).

5.3.3 Freischaltkarten

paysafecard

Die paysafecard (vgl. auch das entsprechende Kapitel in [KetStr 02]) war 2000 in Europa die erste Prepaid-Freischaltkarte für Zahlungen im Internet. Die Karte wurde anfangs nur in Österreich und etwas später in Deutschland und Slowenien angeboten. Das Prinzip ist analog den Prepaid-Karten für Mobiltelefone. Der Kunde kauft (z. B. an einer Tankstelle) für 25 , 50 oder 100 Euro eine paysafecard. Es gibt für Jugendliche auch die <18 paysafecard. Sie kostet 25 bzw. 50 Euro und ist nur auf jugendfreien Internet-Seiten gültig. Mit diesem Kauf hat der Kunde völlig anonym ein entsprechendes Guthaben für den Kauf virtueller Waren angelegt. Auf der Rückseite der scheckkartengroßen Karte findet man nach dem Freirubbeln einen 16-stelliger PIN-Code. Dieser PIN-Code kann sich auch auf einem Ausdruck aus einem elektronischen Händlersystem (Kassenbons, Automatenausdrucke) befinden [Nützel 02]. Wählt der Kunde bei einem Händler die Bezahlmethode paysafecard aus, so leitet der Händler den Käufer zusammen mit Preis und Produktdaten an den Payment-Server von paysafecard weiter. Der Kunde gibt nun den PIN-Code von der Karte ein. Der vom Händler übermittelte Betrag wird von dem Online-Kartenkonto abgebucht. Nach erfolgreicher Bezahlung wird der Kunde wieder zum Händler-Server zurückgeführt.

In Österreich hat sich die Karte einen gewissen Marktanteil speziell bei Sportwetten schaffen können. In Deutschland allerdings konnte sich die paysafecard nie richtig etablieren. Als sich 2002 abzeichnete, dass sich Abrechnungsplattformen wie click&buy durchsetzen werden, versuchte die paysafecard Wertkarten AG [Paysafe 05] eine entsprechende Plattform mit dem Namen paysafekey zu vermarkten. Auch dies nur mit wenig Erfolg.

MicroMoney und T-Pay

MicroMoney [MicroMoney 05] ist ein Konkurrenz-System der Telekom-Tochter DeTeCardService zur paysafecard. Es ist einerseits ein eigenständiges Bezahlsystem, andererseits ist es ein Baustein des Ende 2002 eingeführten Bezahlsystems T-Pay [TPay 05]. Neben MicroMoney enthält T-Pay die Abrechnung über Lastschrift und Kreditkarte, sowie als Besonderheit die Abrechnung über die Telefonrechnung. Die Beträge, die der Kunde über diese Methode abrechnen lässt, werden kumuliert und mit der nächsten Telekom-Telefonrechnung fällig [Lorenz 04].

Die Freischaltkarte MicroMoney kann in jedem T-Punkt-Laden oder in größeren Postfilialen erworben werden. Der Wert einer Karte beträgt 15 Euro. Der Kunde kann damit Waren ab 10 Cents erwerben.

5.3.4 Online-Überweisung

Die Firma Pago bietet über ein temporäres signiertes Java-Applet die direkte Online-Überweisung über das PIN/TAN-Verfahren an [Pago 05]. Händler, die diese Online-Überweisung anbieten, leiten ihre Kunden mit den Rechnungsdaten zum Pago-Server. Dort wird der Kunde aufgefordert, seine Kontonummer und die Bankleitzahl in ein Web-Formular einzugeben. Danach lädt Pago ein spezielles Java-Applet auf den Käuferrechner. Das Applet, welches die weitere Abwicklung übernimmt, ist bereits mit den Konto- und Rechnungsdaten (Preis, Produkt und Händlerkonto) initialisiert.

Nach Eingabe der Homebanking-PIN und der Bestätigung, dass das Ergebnis der Überweisung dem Händler mitgeteilt wird, öffnet sich im Applet ein bereits ausgefülltes Überweisungsformular (siehe Abbildung 5.7). Wird eine gültige TAN eingegeben, kontaktiert das Applet (also der Käuferrechner) direkt die Käuferbank. Nach erfolgreicher Annahme der Überweisung liefert das Applet die Erfolgsmeldung. Diese Status-Meldung wird auch dem Pago-Server mitgeteilt, der daraufhin den Server des Händlers informiert. Im Anschluss kann der Händler die Ware ausliefern. Ein- bis zwei Tage später hat der Händler auch das Geld auf seinem Konto.

Abbildung 5.7
Applet für die Online-Überweisung [Pago 05]

Schließt der Nutzer das Applet, wird es automatisch von seinem Rechner gelöscht. Es bleiben keinerlei Transaktionsdaten auf dem Rechner zurück. Das Problem bei diesem Verfahren ist allerdings, dass der Käufer nicht wirklich sicher sein kann, dass das Applet die Daten nicht an eine „falsche“ Stelle übermittelt.

5.3.5 SMS-Bezahlmethoden

Bezahlmethoden auf der Basis von SMS-Nachrichten (*Short Message Services*) lassen sich in zwei unterschiedliche Ansätze aufteilen:

Premium-Rate-SMS

Eine Premium-Rate-SMS oder auch Premium-SMS ist das SMS-Gegenstück zum Anruf einer 0190/0900-Telefonnummer (vgl. Seite 87). Wird eine SMS-Nachricht an eine fünfstellige Kurznummer verschickt, so wird diese SMS dem Handy-Nutzer mit einem festgelegten Betrag zwischen 0,19 bis 3,00 Euro in Rechnung gestellt. Der Nachteil gegenüber den 0190/0900-Telefonnummern für den Kunden besteht darin, dass er an der Kurznummer nicht den Preis erkennen kann.

Es spielt bei der Premium-SMS keine Rolle, bei welchem Mobilfunkanbieter der Handy-Nutzer Kunde ist. Durch die Integration einer Mitteilung innerhalb der SMS-Nachricht können verschiedenen Anbieter und Angebote über die gleiche Kurznummer verarbeitet bzw. individuelle Angebote abgerechnet werden. Über eine weitere SMS, die an den Handy-Nutzer zurückgesendet wird, wird die bezahlte virtuelle Ware zugänglich gemacht. Bspw. indem der Kunde in dieser Rück-SMS ein Code zur Eingabe auf einer speziellen Web- oder WAP-Seite erhält.

Nachteilig für Händler ist die sehr geringe Ausschüttung beim Premium-SMS-Diensten. Oft bleiben dem Händler nicht einmal 55% des abgerechneten Betrages.

Inkasso über die Mobilfunk-Rechnung

Viele Mobilfunk-Netzbetreiber bieten ihre eigenen Abrechnungssysteme, mit denen sie normalerweise nur die Gesprächsminuten und die SMS ihrer Kunden abrechnen, inzwischen auch anderen Anbietern als Inkasso-System an. Vodafone z. B. hat mit m-pay [MPay 05] ein solches System 2003 auf den Markt gebracht. Dort muss der Käufer zur Autorisierung einer Belastung seiner Mobilfunkrechnung beim Anbieter (von z. B. virtuellen Waren) seine Mobilfunk-Nummer angeben (vgl. Paybox auf Seite 82). Der Anbieter veranlasst nun m-pay, dem Käufer eine SMS zu senden, in der ein Code enthalten ist. Wird dieser Code bei m-pay eingegeben, so wird damit Vodafone autorisiert, den Betrag (maximal 10 Euro) über die nächste Mobilfunkrechnung zu belasten. Zeitgleich wird der Anbieter über die erfolgreiche Zahlung informiert, so dass er die virtuelle Ware ausliefern kann.

Dienstleister wie z. B. die Firma bruNet GmbH erweitern mit ihrem System allpay [AllPay 05] das m-pay-System um die Abrechnungssysteme weiterer Mobilfunkbetreiber.

5.4 Multipayment-Systeme anhand von Paybest

Die Vielzahl an Bezahlsystemen, die meist auch eine Registrierung der Kunden erfordern, macht es für Anbieter von virtuellen Waren notwendig, mehrere Bezahlsysteme parallel anzubieten. Denn ein Käufer, der sich bereits bei PayPal angemeldet hat, hat möglicherweise kein Interesse daran, sich zusätzlich bspw. bei Firstgate anzumelden, nur weil der Anbieter click&buy und nicht PayPal anbietet. Das parallele Angebot mehrerer Bezahlsysteme muss der Anbieter normalerweise allerdings mit einem mehrfachen Integrations- und Wartungsaufwand erkaufen. Folglich ist es sinnvoll, ein Meta- bzw. Multipayment-System einzubinden, welches unter einer Integrationsschnittstelle mehrere Bezahlsysteme in das Anbieter-System integriert. Idealerweise sollte ein Anbieter, der ein Multipayment-System nutzt, nur mit dem Betreiber dieses Systems einen Vertrag schließen müssen und nicht mit den allen Betreibern der Teilsysteme.

Das vom Autor und der 4FO AG [4FO 05] entwickelte Paybest [Paybest 05] ist ein solches Multipayment-System. Paybest bietet aktuell (2005) neben der Zahlung über PayPal, Moneybookers, click&buy, paysafecard, MicroMoney auch ein selbstentwickeltes Telefon-basisiertes Gutscheinsystem an.

5.4.1 Das Gutscheinsystem von Paybest

Ende 2000 entstand für die 4FO AG die Notwendig für die in Entwicklung befindliche Game-Feature-Plattform (GFP, vgl. Kapitel 6) eine funktionierende Bezahlmöglichkeit bereitzustellen, die es auch Minderjährigen ermöglicht, virtuelle Waren spontan ohne Registrierung zu bezahlen. Deshalb wurde auf der Basis eines kostenpflichtigen Telefonanrufes ein Gutscheinsystem entwickelt. Anfang 2001 ging die GFP mit dieser Bezahlmethode in den Probebetrieb. Im September 2001 wurde dieser Dienst unter dem Namen Paybest – unabhängig von der GFP – angeboten. In [Nützel 02] ist diese Entwicklung der 4FO AG detailliert beschrieben. Im Rahmen von [JanLan 02] wurde eine Sicherheitsanalyse durch das DFKI in Saarbrücken durchgeführt. Außerhalb Deutschlands fand die Technik in [Centano 02] Beachtung.

■ Gutscheine einlösen

Aus der Sicht eines Käufers stellt sich der Bezahlvorgang wir folgt dar: Nachdem der Käufer bei einem Händler die Paybest-Gutschein-Bezahlmethode ausgewählt hat, so öffnet der Payment-Server ein neues Fenster. Dort wird der Käufer aufgefordert, eine gültige 8-stellige Gutscheinnummer (z. B. TTME1MK8) einzugeben. Dieser Vorgang ist mit dem Freischaltkarten (vgl. Seite 83) vergleichbar. Für jede gültige Gutscheinnummer wird auf dem Paybest-Server ein anonymes Verrechnungskonto mit einem Startwert von 2,50 Euro bereitgehalten. Aus Sicherheitsgründen sind die Gutscheinnummern nicht selbst auf dem Payment-Server gespeichert. Es wird lediglich das Ergebnis einer Hash-Funktion gespeichert. Dies ist ausreichend, um die Nummer auf Gültigkeit zu überprüfen.

Die Eingabe einer gültigen Gutscheinnummer erlaubt dem Nutzer, Zahlungen in entsprechender Höhe durchzuführen. Die Gutscheinnummer muss aber nicht in einer einzelnen Transaktion verbraucht werden. Auch können mehrere Gutscheinnummern kombiniert werden, um höhere Beträge zu begleichen. Um die Länge der Nummern auf acht Stellen beschränken zu können, ohne dabei an Sicherheit einzubüßen, verlieren die Nummern 65 Tage nach der letzten Nutzung ihre Gültigkeit [Nützel 04].

■ Verteilung von Gutscheinnummern

Auf einem vom Internet nicht erreichbaren Computer werden neue Gutscheinnummern mit einem Zufallsgenerator blockweise erstellt. Bereits erzeugte Nummern werden auf diesem Rechner im Klartext gespeichert, um Dubletten sehr schnell zu erkennen. Jeder Gutscheinnummer wird zwecks der Verwaltung der anonymen Online-Konten eine fortlaufende Ziffer zugeordnet.

Man könnte nun diese Gutscheinnummern auch auf Freischaltkarten drucken und gegen Bargeld verkaufen. Paybest verteilt diese Gutscheinnummer allerdings ausschließlich per kostenpflichtiger Telefonansage. Damit ein Händler die Integration des Paybest-Servers testen kann, werden nichtverrechnende Gutscheinnummern,

die auf diesen Händler beschränkt sind, ausgegeben. In [Centano 02] wird erläutert warum es sich bei den Paybest-Gutscheinnummern im Gegensatz zu den Freischaltkarten nicht um eine E-Geld-Institut nach [EU46 00] handelt. Die entscheidende Bedeutung spielt hier die Art der Abrechnung des Telefonanrufes durch die Telefongesellschaft.

Abbildung 5.8
Upload und Ansage der Gutscheinnummern

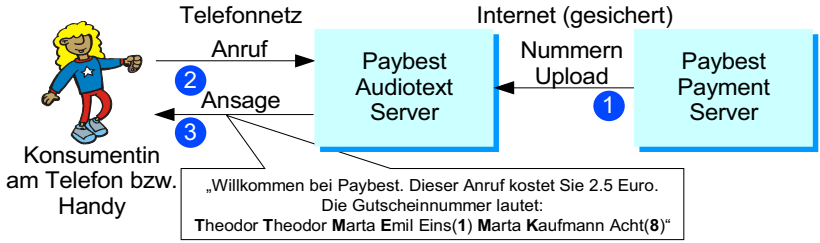


Abbildung 5.8 zeigt die beiden zentralen Server des Paybest-Systems. Der Audiotext-Server ist für die kostenpflichtige Ausgabe (Ansage) der Gutscheinnummern verantwortlich. Der eigentliche Payment-Server, der die Online-Konten mit den Nummern in Verbindung bringt, liefert die Nummern blockweise (ca. 1000 Nummern pro Transfer) beim Audiotext-Server ab (Schritt 1: Nummern Upload). Der Rechner auf dem die Nummern zuvor erzeugt wurden, ist nicht gezeigt. Der Audiotext-Server ist über das Internet und das Telefonnetz erreichbar.

Die Konsumentin in Abbildung 5.8 gelangt an eine Gutscheinnummer, indem sie die Telefonnummer 0900-1-729237 (0900-1-PAYBEST) anruft (Schritt 2: Anruf). Nutzern, die nicht aus dem Netz der Deutschen Telekom anrufen können oder wollen, steht alternativ eine 0190-8-Nummer zur Verfügung. Diese Nummer ist von den meisten Mobiltelefonen aus erreichbar. Der Anruf dieser beiden Nummern kostet dem Nutzer über seine Telefonrechnung 1,86Euro/min. Die gesamte Anrufdauer wurde auf eine Minute und 21 Sekunden festgelegt. Folglich kostet der Anruf exakt 2,50 Euro. Vor der kostenpflichtigen Ansage ist noch eine für den Anrufer kostenlose kurze Gebührenansage vom Netzbetreiber vorgeschaltet. Der Nutzer wird auch aufgefordert nicht vorzeitig aufzulegen, sondern abzuwarten, bis der Audiotext-Server die Verbindung automatisch nach 81 Sekunden trennt. Der Nutzer hört dann während der nächsten 81 Sekunden eine automatische Ansage (Schritt 3), die ihm dreimal hintereinander eine 8-stellige Gutscheinnummer bestehend aus Buchstaben und Ziffern mitteilt (vgl. Sprechblase in Abbildung 5.8). Sollte ein Nutzer dennoch vorher auflegen (z. B. weil er glaubt, dadurch Geld zu sparen), so wird der Payment-Server diese Nummer nicht annehmen, obwohl hierfür ein Online-Konto existiert. Deshalb wird beim Versuch, eine bisher nicht benutzte Gutscheinnummer am Payment-Server einzulösen, die Audiotext-Plattform im Hintergrund vom Payment-Server abgefragt, ob die jeweilige Gutscheinnummer korrekt angesagt wurde. Wurde die Nummer noch nicht bzw. unvollständig angesagt, so wird dies dem Payment-Server entsprechend zurückgemeldet. In [JanLan 02] wurde die formale Analyse dieses Protokolls vorgestellt.

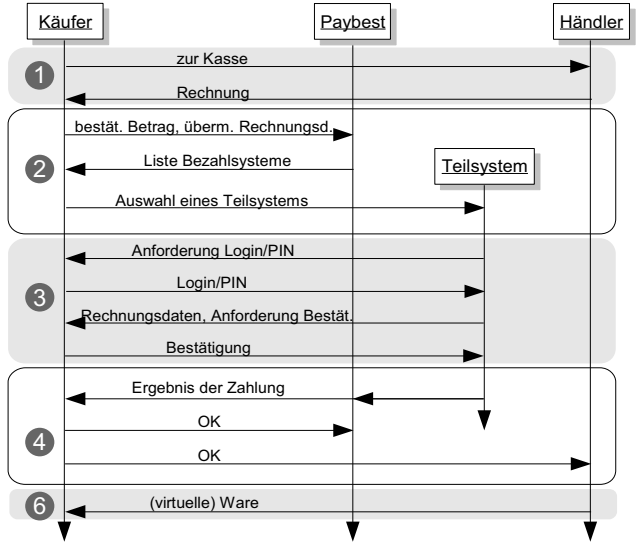
5.4.2 Zwei Varianten der Integration von Paybest

In [PaybestTech 04] beschreibt die 4FO AG zwei unterschiedliche Methoden das Paybest-System in ein Händler-System einzubinden.

■ Kopplung über HTTP-POST-Parameter

Die erste Integrationsvariante ist zwar für den Anbieter virtueller Waren aufwendiger, bietet aber weit mehr Freiheiten bei der Gestaltung von unterschiedlichen Erlösmodellen (vgl. Kapitel 3.5). Die Kommunikation des Paybest-Servers mit dem Rechner des Kunden und dem Rechner des Händlers unterteilt sich in drei Abschnitte:

Abbildung 5.9
Sequenzdiagramm des Ablaufs eines Kaufvorgangs mit Paybest



Der Händler präsentiert in Schritt 1 von Abbildung 5.9 dem Käufer eine Webseite mit den Rechnungsdaten. Diese Seite enthält einen Link, der auf den Paybest-Server weist und eine Reihe von POST-Parametern enthält. Der wichtigste Parameter ist der Preis (in Cent inkl. gesetzlicher Mehrwertsteuer). Damit dieser und alle weiteren Parameter nicht auf dem Weg dorthin verfälscht werden können, wird ein zusätzlicher Hash-Wert (Schritt 2) hinzugefügt.

Der in Tabelle 5.1 gezeigte Hash-Wert wird mit der MD5-Funktion, die in allen Server-Sprachen (bspw. auch php) verfügbar ist, berechnet. Dazu werden alle Parameter (ohne den Hash-Wert) und der erste geheime Paybest-Händler-Schlüssel (*Paybest-Key1*) zu einem String verkettet, der schließlich den Operanden für die MD5-Hash-Funktion liefert.

Nachdem Paybest die Parameter und den Hash geprüft hat, erscheint das Paybest-Bezahlfenster. Der Kunde wird aufgefordert, eines der aufgelisteten Teilsysteme auszuwählen. Darauf werden die in dem Link enthaltenen Rechnungsdaten an

Tabelle 5.1
Post-Parameter, die der Händler an Paybest leitet

POST-Parameter	Erläuterung
price	Preis in Cent inkl. gesetzlicher Mehrwertsteuer
customerId	Kunden/Händler-Nummer
shopId	Paybest-Shop-Nummer des Händlers (in der Regel 1)
target	Name des Zielfensters für die Antwort von Paybest
sessionId	Kennung für die Session-Verwaltung des Händlers. Wird von Paybest protokolliert.
shopUrl	Mit der Händler-Domain verknüpft die URL, die Paybest aufruft.
products	(Datei-)Name der virtuellen Ware. Wird protokolliert.
hash	MD5-Hash über alle übertragenen Parameter und den ersten geheimen Paybest-Händler-Schlüssel (*Paybest-Key1*).

das jeweilige Teilsystem übermittelt. Der Schritt 3 aus Abbildung 5.9 verläuft jetzt ohne Mitwirkung von Paybest (mit Ausnahme beim Gutscheinsystem).

In Schritt 4 wird dem Käufer und Händler die erfolgte Zahlung signalisiert. Paybest liefert hierzu eine Webseite aus, die einen Link zum Server des Händlers (*shopUrl* in Tabelle 5.1) enthält. Über diesen Link wird, mit dem Kundenrechner als Zwischenstation, dem Händler der Status der Zahlung mitgeteilt. Der Link enthält, die in Tabelle 5.2 aufgeführten Parameter.

Tabelle 5.2
Post-Parameter, die Paybest an den Händler zurücksendet

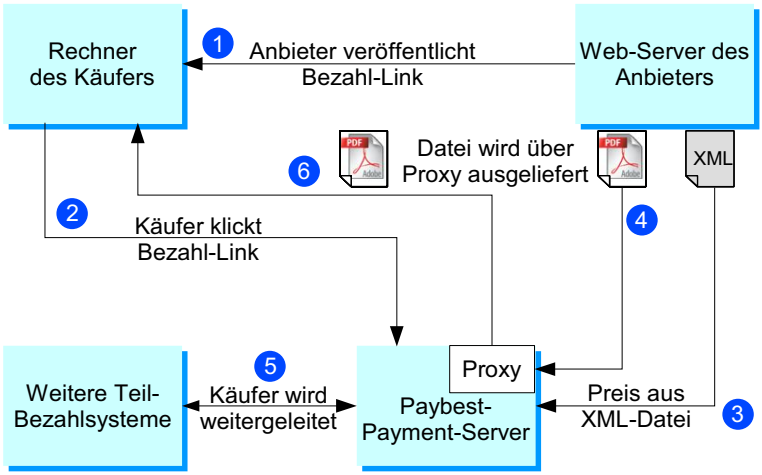
POST-Parameter	Erläuterung
sessionId	Hier wird die Information, die mit dem ersten Posting an Paybest übermittelt wurde wieder zurückgesendet. Sie dient zur Session-Verwaltung des Händlers.
products	(Datei-)Name der virtuellen Ware. Der Händler kann hieraus bspw. einen Download-Link ableiten.
units	Bleibt anderen Anwendungen vorbehalten
result	Steht eine 1 im Parameter, so verlief die Bezahlung erfolgreich. Bei ungleich 1 war der Bezahlvorgang nicht erfolgreich.
hash	MD5-Hash über alle übertragenen Parameter und dem zweiten geheimen Paybest-Händler-Schlüssel (*Paybest-Key2*).

In Schritt 6 wertet der Händler diese Parameter aus. Aus Sicherheitsgründen sollte auf jeden Fall auch der Hash-Parameter mittels des zweiten geheimen Paybest-Händler-Schlüssels (*Paybest-Key2*) überprüft werden. Beide Schlüssel erhält der Händler auf seinem Admin-Bereich bei Paybest. Der Hash deckt auf, falls bspw. der result-Parameter durch den Käufer manipuliert wurde. Bei korrekten Hash und *result=1* war der Bezahlvorgang erfolgreich und der Händler kann die virtuelle Ware ausliefern. Die Parameter *sessionId* und *products* ermöglichen die Zuordnung des Bezahlvorgangs beim Händler.

Kopplung über den Paybest-Proxy

Die Kopplung über POST-Parameter hat den Nachteil, dass der Anbieter selbst für die Umsetzung einfacher Download-Geschäftsmodelle Programmierkenntnisse benötigt. Möglicherweise hat der Anbieter auch gar nicht die Möglichkeit, spezielle Programme (bspw. in php) auf seinem Server zu installieren. Die Einbindung des Paybest-Payment-Servers als zwischengeschalteter Download-Proxy (vgl. Abbildung 5.10) vereinfacht die Integration des Bezahlsystems sehr stark, da so für Pay-per-Download-Geschäftsmodelle auf eine Server-Programmierung auf Seiten des Anbieters komplett verzichtet werden kann.

Abbildung 5.10
Paybest mit Download-Proxy



Beispiel: Möchte der Anbieter ein PDF-Textdokument für 50 Cent zum Download anbieten, laufen in der Vorbereitung durch den Anbieter und beim Download durch den Käufer folgende in Abbildung 5.10 dargestellten Schritte ab:

- Vor Schritt 1: Der Anbieter legt die zu verkaufende Datei in einem zusätzlichen Verzeichnis auf seinem Web-Server ab. Durch Einspielen einer speziellen .htaccess-Datei (vgl. [PaybestTech 04]) kann der Web-Zugriff vom Paybest-Server auf dieses Verzeichnis begrenzt werden. Parallel dazu legt der Anbieter eine einfach aufgebaute XML-Datei ab. In dieser Datei steht der vom Anbieter festgelegte Preis, der von Paybest eingefordert werden soll. (weitere Details zum Aufbau dieser XML-Datei finden sich in [PaybestTech 04])
- Schritt 1: Der Anbieter veröffentlicht auf seinem Web-Server einen Bezahl-Link. Der Link führt auf den Paybest-Server und enthält mehrere GET-Parameter. Die Parameter kennzeichnen den Anbieter und die entsprechende XML-Datei bzw. die zum Verkauf angebotene Datei.

- Schritt 2: Ein Käufer öffnet den Bezahl-Link und transferiert damit die angefügten Parameter zum Payment-Server.
- Schritt 3: Mit den transferierten Parametern und Angaben aus der Anbieter-Datenbank des Paybest-Systems lässt sich die URL zur passenden XML-Datei ermitteln. Die Preis-Information wird aus der XML-Datei ausgelesen.
- Schritt 4: Aus den Parametern bzw. der XML-Datei lässt sich auch die URL zur angebotenen Datei ermitteln. Befindet sich diese Datei noch nicht im Proxy, so wird sie nun in den Proxy kopiert.
- Schritt 5: Dem Käufer wird eine Auswahlseite für die verschiedenen Teilsysteme präsentiert. Je nach Auswahl wird der Käufer weitergeleitet. Paybest wartet, bis das jeweilige Teilsystem die erfolgreiche Zahlung zurückmeldet.
- Schritt 6: Paybest ermöglicht (aus dem Proxy) dem Käufer den Download der bezahlten Datei.

Das Prinzip des Verkaufs virtueller Güter über einen zwischengeschalteten Proxy-Servers ist keine Erfindung des Autors und der 4FO AG. Um für den Anbieter den Verkauf einfach zu gestalten, entstanden zuerst Bezahlsysteme (z. B. NET900 [LeiStr 03], Seite 40), die die Dateien komplett und ausschließlich auf ihren eigenen Servern vorhalten. Als die FIRSTGATE AG dies erstmalig kommerziell erfolgreich in eine Proxy-Lösung verwandelte, entstand diese vermutlich aus einem Wettbewerbsverbot, das dem FIRSTGATE-Gründer Norbert Stangl vom Internet-Hoster Strato Medien AG auferlegt wurde, als er seine Strato-Anteile verkaufte. Norbert Stangl hatte die Strato AG 1997 gegründet. Die Strato AG wollte sicher gehen, dass Herr Stangl mit seiner neuen Firma kein konkurrierendes Hosting anbietet. Inzwischen ist das Proxy-Prinzip ein akzeptiertes Verfahren, das neben Paybest auch WEB.Cent (vgl. Seite 81) und das in Kapitel 8 beschriebene PotatoSystem nutzt.

5.4.3 Ein Web-Service für Paybest

Aus den Überlegungen eine einheitliche Schnittstelle für mehrere Bezahlsysteme den Händlern anzubieten, entstand der Entschluss, technologisch noch einen Schritt weiter zu gehen. Die Web-Service-Technologie bot sich als Basis an. Ziel der von Oliver Lorenz prototypisch in [Lorenz 04] umgesetzten Überlegungen ist es, einen Web-Service zu spezifizieren und zu entwerfen, der so allgemein gehalten ist, dass mit ihm für verschiedenste Bezahlsysteme Bezahltransaktionen durchgeführt werden können. Im Fokus dieses Web-Services stehen nicht virtuelle Waren, die über einen Standard-Browser konsumiert werden, sondern Content, der zu seiner Nutzung eine spezielle Software-Komponente benötigt, die auf dem Endgerät installiert wird. Denn nur aus diesen Software-Komponenten wäre ein Web-Service ansteuerbar.

Was ist ein Web-Service?

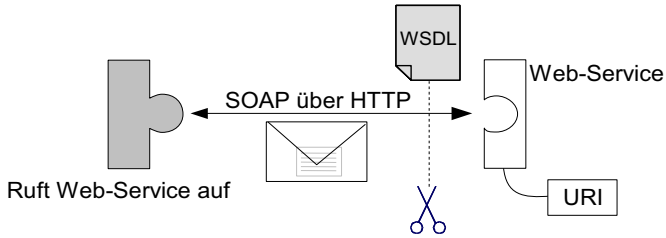
Bevor die speziellen Aufgaben eines Bezahl-Web-Services besprochen werden können, muss erläutert werden, was im Allgemeinen ein Web-Service ist.

Gabriele Frings nennt in ihrer Diplomarbeit [Frings 03] in Anlehnung an das W3C-Konsortium [W3C 02] folgende Kennzeichen für einen Web-Service:

- ein **Software-System**, das eindeutig durch eine URI (*Uniform Resource Identifier*, z.B. URL) identifizierbar ist
- öffentliche **Schnittstellen**, die klar durch XML definiert und beschrieben sind
- eine **Beschreibung**, die für andere Software-Systeme zugänglich ist
- andere Systeme können mit dem Web-Service **interagieren** (wie in der Schnittstellen-Beschreibung festgelegt)
- die Kommunikation erfolgt über ein Nachrichten-Format auf XML-Basis
- zur Übertragung werden **Internet-Protokolle** genutzt, z. B. HTTP, FTP, ...

Zur einheitlichen und maschinenlesbaren Beschreibung der Schnittstellen dient die auf XML aufbauende *Web Service Description Language* (WSDL). Zur Interaktion mit anderen Systemen kommt das *Simple Object Access Protocol* (SOAP), welches Nachrichten und Protokolle festlegt, zum Einsatz (vgl. Abbildung 5.11).

Abbildung 5.11
Bestandteile eines Web-Services



Um Web-Services öffentlich bekannt zu machen, wurde eine Art «Gelbe Seiten» für Web-Services definiert. Diese Verzeichnisdienste bauen auf UDDI (*Universal Description, Discovery and Integration*) auf.

WSDL-Beschreibungen der Web-Services können inzwischen von sehr vielen Software-Entwicklungswerkzeugen automatisch verarbeitet werden, um einerseits Web-Services zu nutzen und andererseits Web-Services zu erstellen. Dirk Behrendt beschreibt in seiner Diplomarbeit [Behrendt 03] die Vielfalt der vorhandenen Werkzeuge.

Zusammenspiel der Web-Services

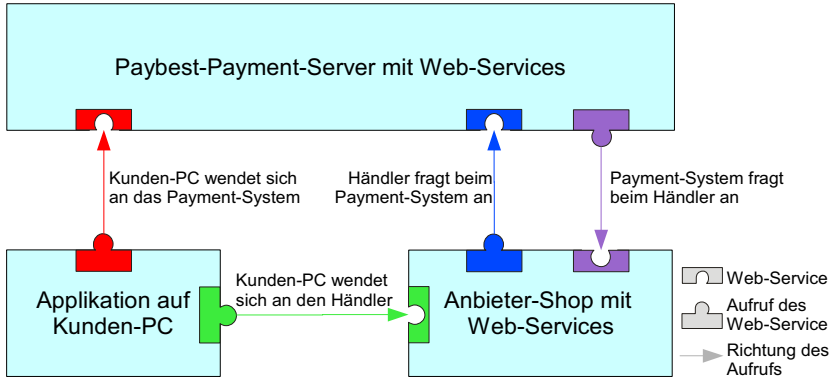
Abbildung 5.12 zeigt das Zusammenspiel der insgesamt vier Web-Services von Paybest. Bestimmte Nachrichtenabfolgen sind den Möglichkeiten aktueller Web-Service-Implementierungen geschuldet. Web-Services unterstützen aktuell keine asynchrone Kommunikation. Der Aufruf eines Web-Services ist einem entfernten Prozeduraufruf an einen Server gleichzusetzen. Eine Nachricht, die der Server an die Client-Applikation senden möchte, muss zuvor von der Applikation explizit angefordert werden.

Bei der prototypischen Umsetzung der Kopplung von Client-Applikation und den beiden beteiligten Servern mir ihren Web-Services standen mehrere Möglichkeiten zur Auswahl. Lorenz entschied sich in [Lorenz 04] nach der Diskussion verschiedener Varianten schließlich für die nun hier dargestellte Vorgehensweise. Abbildung

5.13 zeigt den Ablauf einer Bezahlung in einem Sequenzdiagramm mit den beteiligten Operationen. Die ausgetauschten Nachrichten sind von 1 bis 9 und von i bis iv durchnummeriert. Die Nachrichten i bis iv wurden gegenüber einer vereinfachten Version zusätzlich aufgenommen.

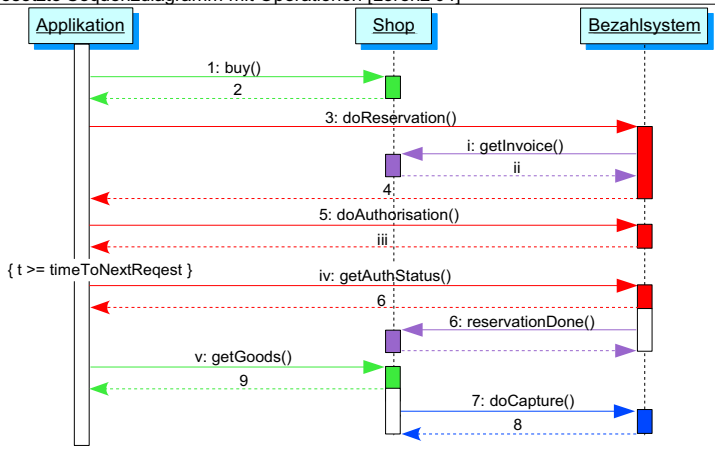
- Web-Service-Aufruf mit den Nachrichten 1 und 2: Der Kunde wählt eine virtuelle Ware in seiner Applikation aus und übermittelt seinen Kaufwunsch über die Applikation mit der Nachricht 1 (*buy*) dem Shop-System des Händlers mit. Der Shop antwortet auf diesen Web-Service-Aufruf mit der Nachricht 2 und liefert damit die Rechnung und eine Auswahl der angebotenen Bezahlmöglichkeiten.

Abbildung 5.12
Zusammenspiel der verschiedenen Web-Services



- Web-Service-Aufruf mit den Nachrichten 3 und 4: Der Kunde akzeptiert die Rechnung und wählt eine bestimmte Bezahlmöglichkeit aus. Die Applikation überträgt mit der Nachricht 3 diesen Zahlungswunsch inklusive Shoprechnung, Kunden- und Händlerkennung an das Bezahlsystem. Das Bezahlsystem prüft, ob die Zahlung möglich ist, und fordert mit Antwort-Nachricht 4 eine explizite Autorisierung an. Zusätzlich können hierbei zusätzliche Informationen (bspw. spezifische Hilfetexte) an den Kunden übermittelt werden.
- Web-Service-Aufruf mit den Nachrichten i und ii: Nachdem das Bezahlsystem die Rechnungsdaten von der Applikation erhalten hat, holt es sich zusätzlich vom Shop die gleichen Rechnungsdaten und vergleicht die beiden Rechnungen. So wird sichergestellt, dass zwei übereinstimmende Willenserklärungen vorliegen. Ein Nebeneffekt ist außerdem, dass keine ungültigen Rechnungen bezahlt werden können. Das Bezahlsystem nimmt die Rolle eines unbeteiligten Dritten ein, es muss allerdings sowohl vom Shop als auch vom Kunden als solcher akzeptiert werden. [Lorenz 04]
- Web-Service-Aufruf mit den Nachrichten 5 und iii: Die Applikation liefert mit der Nachricht 5 dem Bezahlsystem die Autorisierungsdaten des Kunden, z. B. in Form eines Passwortes. Das Bezahlsystem antwortet mit der Nachricht iii. Dies ist der kritischste Zeitpunkt der Kommunikation. Der Kunde muss der Applikation vertrau-

Abbildung 5.13
Umgesetzte Sequenzdiagramm mit Operationen [Lorenz 04]



en, dass sie die Autorisierungsdaten in verschlüsselter Form nur an das Bezahlsystem übermittelt.

- Web-Service-Aufruf mit den Nachrichten iv und 6: Die Autorisierung kann im Extremfall mehrere Minuten dauern. In dieser Zeit wird beispielsweise ein Hintergrundsystem befragt, ob die Kreditkarte gesperrt ist. Um zu verhindern, dass ein Timeout während der Web-Service-Kommunikation auftritt, wurde in den Ablauf ein Polling integriert. In der Antwort-Nachricht iii erhält die Applikation die Zeit (*timeToNextRequest* in Abbildung 5.13) mitgeteilt, die das Bezahlsystem voraussichtlich für die Bearbeitung der Autorisierung benötigt und nach deren Ablauf die Applikation erneut mit der Nachricht iv den Status der Bearbeitung nachfragen soll. Das Bezahlsystem bucht den Rechnungsbetrag noch nicht endgültig, sondern reserviert diesen für den Shop einen gewissen Zeitraum lang. Bis zur endgültigen Buchung, die der Shop einleiten muss, bleibt diese schwebend. Der Shop wird mittels Web-Service-Aufruf (Nachricht 6 *reservationDone*) direkt über den Erfolg der Reservierung informiert. Die Applikation erhält die Erfolgsmeldung als Antwort auf die Nachricht iv. Mit dieser Erfolgsmeldung wird eine Quittung über die Reservierung übermittelt.
- Web-Service-Aufruf mit den Nachrichten v und 9: Mit dem Web-Service-Aufruf v fordert die Applikation mit den in der Nachricht 2 erhaltenen Rechnungsdaten schließlich die virtuelle Ware vom Shop an. Die Antwort 9 liefert entweder die virtuelle Ware direkt oder einen temporären Link, über den diese bezogen werden kann.
- Web-Service-Aufruf mit den Nachrichten 7 und 8: Der Shop sendet nach erfolgreicher Auslieferung die finale Buchungsanforderung (Nachricht 7) an das Bezahlsystem. Diese Nachricht enthält Daten wie die Buchungsnummer und den Betrag. Das Bezahlsystem bucht den angegebenen Betrag vom Kundenkonto ab. Zur Bestätigung wird an den Shop eine Buchungsbestätigung (Nachricht 8) gesendet. Danach ist der Bezahlvorgang abgeschlossen.

5.4.4 Bewertung des Web-Services-Ansatzes

Ziel vieler Bezahlsystem-Betreiber ist es, auch beim Endkunden die eigene Marke bekannt zu machen. Speziell Anbieter, bei denen der Kunde sich registrieren muss, erhoffen sich hierdurch eine höhere Kundenbindung und damit auch bei den Shops bessere Akzeptanz. Denn je größer der Kundenstamm eines Bezahlsystem ist, desto attraktiver ist das Bezahlsystem für einen Händler. Die Konditionen geraten deshalb oft noch bei den Transaktionskosten in den Hintergrund. Da sich der Markt für virtuelle Güter auch im Jahre 2005 noch in den Kinderschuhen befindet und sich viele Content-Eigner noch gar nicht für den bezahlten Download entschlossen haben, findet noch kaum ein Verdrängungswettbewerb zwischen unterschiedlichen Bezahlsystemen statt. Die Bezahlsysteme können es sich noch erlauben durch proprietäre Techniken und den sich dadurch ergebenen Lock-in-Effekten ihre Kunden (die Händler) dauerhaft an sich zu binden und das Wechseln zur Konkurrenz zu erschweren. Daher gibt es aktuell auch kein Bedürfnis von Seiten der Bezahlsysteme sich auf eine einheitliche Web-Service-Schnittstelle zu einigen. Bezahlsysteme verstehen sich in der Regel auch als Internet-Portal, welches nicht über die „Hintertür“ eines Web-Services angesteuert werden will.

Das Bedürfnis die eigene Marke stärker in der Client-Applikation sichtbar zu machen, könnte dadurch unterstützt werden, dass das Bezahlsystem z. B. in der Nachricht 4 auch HTML-Code transferiert, der durch die Client-Applikation mittels einer eingebetteten Browser-Komponente (vgl. Seite 104) sichtbar gemacht wird. Da die Bezahlfunktion aus Sicht der Kundenfreundlichkeit am besten immer in der Client-Applikation ablaufen sollte, die der Nutzer auch zum Konsum der virtuellen Ware benötigt (das ist bei HTML-Seiten der Standard-Browser), bleibt die Web-Service-Schnittstelle für Paybest (und die anderen Bezahlsysteme) auf spezielle Client-Applikationen wie bspw. Musik- und Video-Player mit integrierten DRM-Client beschränkt. Die Integration in einen Standard-Browser ist realistisch betrachtet kaum durchsetzbar.

6. Kapitel

Erweiterungen für den Online-Vertrieb von PC-Software

Die Erfindung und Entwicklung der so genannten Game-Feature-Plattform (GFP) [Nützel 01] stellte Ende 1999 für den Autor den Ausgangspunkt für seine Forschung im Bereich der virtuellen Güter dar. Die GFP startete als eine Business-Plan-Idee, die schließlich im Jahre 2000 zur Gründung des Start-Ups 4FriendsOnly.com Internet Technologies AG (4FO AG) [4FO 05] durch den Autor führte. Arbeiten zur GFP initiierten auch die Entwicklung und Forschung im Bereich der Bezahlsysteme.

Bei der GFP handelt es sich um ein *Digital Policy Enforcement* (DPE) System (vgl. Seite 60) für interaktive Software, die auf dem Endgerät (typischerweise einem Windows-PC) installiert wird. Die GFP greift die Shareware-Idee [WikiSWare 05] auf und stellt ein technisches System bereit, mit dem das Geschäftsmodell Pay-per-Feature umgesetzt werden kann.

Die GFP ist ein Client-Server-System, bei dem ein spezieller Client in die vermarktete Software integriert wird. Dieser verbindet sich über das Internet mit dem Server, um client-spezifisch verschlüsselte Datenpakete oder Aktivierungsinformationen automatisch herunterzuladen.

Das für die GFP Ende 2000 angemeldete Patent [NüBöStSc 00] wurde Ende 2002 erteilt, weil es eine neuartige Funktionalität realisiert, die große unverschlüsselte Datenpakete auf der Client-Seite gegen eine ungewollte Nutzung schützen kann. Der Schutz erfolgt dadurch, dass kleinere aber notwendige Teile dieser Pakete fehlen und nur verschlüsselt vom Server bezogen werden können. Natürlich können die Nutzdaten auch komplett verschlüsselt vom Server geladen werden.

In [Kunze 04] wurde die GFP schließlich so überarbeitet, dass die kryptographische Server-Komponente über einen Web-Service (vgl. Seite 91) angesprochen werden kann. Des Weiteren wurde die Funktionalität der GFP auf eine Freischaltung bzw. Aktivierung beschränkt. Dem Kunden wird somit ermöglicht, eine kostenlose aber in ihrer Funktionalität eingeschränkte PC-Anwendung aus der Anwendung heraus zu einer Vollversion freizuschalten.

6.1 Online-Vertrieb von PC-Spielen und anderer PC-Software

Interaktive virtuelle Güter (vgl. Kapitel 2.3.2) wie z. B. Computerspiele oder andere Software, die auf dem Endgerät des Nutzers installiert werden, existieren schon deutlich länger als das kommerziell verfügbare Internet. Folglich haben sich für Software bereits eine Reihe von unterschiedlichen Vertriebsformen (mit direkten Erlösmodellen) herausgebildet, auf die im Internet-Zeitalter aufgebaut wurde. Inzwischen sind die Anbieter nicht mehr darauf angewiesen, ihre Software auf physischen Datenträgern im traditionellen Handel anzubieten. Allerdings bauen besonders große Anbieter (bspw. Sony oder Nintendo) gerade im Bereich von Unterhaltungs-Software immer noch mit Erfolg auf dieses traditionelle Modell. Für kleinere Anbieter ist der Online-Vertriebskanal die bessere weil kostengünstigere Lösung. Was kann nun als Ausgangslage für den Online-Vertrieb genutzt werden und was sollte ergänzt bzw. geändert werden? Ebenfalls muss man sich fragen, welcher Schutz gegen illegale Verbreitung nötig und möglich ist.

6.1.1 Freeware oder Opensource

Freeware ist Software, die der Autor völlig kostenlos abgibt. Typischerweise behält hierbei der Autor den Quelltext für sich. Bei Opensource ist dies völlig anders, auch wenn viele Personen häufig fälschlicherweise *freie* Software mit Opensource gleichsetzen. Die *Open Source Initiative* hat hierzu die *Open Source Definition* (OSD) [OSD 04] mit zehn Bedingungen veröffentlicht. Die OSD legt fest, ob eine Software-Nutzungsbedingung unter den Begriff Opensource eingeordnet werden kann. Sie geht zurück auf die *Debian Free Software Guidelines* [WikiDFSG 05] von Bruce Perens. Die wichtigsten Punkte betreffen die kostenlose Weitergabe und den Zwang, den Quellcode ebenfalls zugänglich zu machen. Der Grundgedanke dabei ist es, dass jeder Entwickler sich aus einem Pool von Teillösungen bedienen kann, wenn er seinerseits bereit ist, seine Leistungen diesem Pool zur Verfügung zu stellen.

Opensource hat sich bislang bei PC-Spielen nicht durchsetzen können. Möglicherweise liegt es daran, dass die Entwicklungskosten von PC-Spielen nicht nur die Kosten der Programmierung enthalten. Oft ist der künstlerische Entwurfsaufwand für Grafik und Sound deutlich höher.

6.1.2 Shareware als Ausgangslage für den Online-Vertrieb

Shareware (von engl. "*to share*": etwas gemeinsam nutzen) bezeichnet eine Vertriebsform für Software, bei der diese vor dem Kauf getestet werden kann. Damit betrachten Autoren von Shareware, im Gegensatz zu Freeware- oder Opensource-Autoren den Nutzer der Software als potentielle direkte Erlösquelle. In dem Wort Shareware steckt schon die Idee von der Superdistribution (vgl. Kapitel 3.6.4), bei der die Nutzer ermuntert werden, die virtuelle Ware weiterzuverteilen.

In der klassischen Variante räumt der Autor der Software dem Nutzer eine zeitlich limitierte Nutzungsdauer (von bspw. 30 Tagen) ein. Danach soll der Nutzer für die Software entweder eine Registierungsgebühr bezahlen oder die Software nicht mehr benutzen. In den 80er Jahren nutzten Jim Knopf mit der Datenbank *PC-File* und Andrew Fluegelman mit *PC-Talk* als erste die Shareware-Idee. Den Begriff Shareware prägte allerdings erst kurz danach Bob Wallace mit der Textverarbeitung *PC-Write* [WikiSWare 05].

Diese ursprüngliche Form von Shareware ist allerdings inzwischen unüblich geworden, da die Nutzer häufig doch nicht so gutmütig wie erhofft sind. Häufig wird der Nutzer explizit im Programm durch so genannte Nagscreens (Nörgelbildschirme) aufgefordert sich zu registrieren. In Abbildung 6.1 ist der Nagscreen des Packers WinZip zu sehen (Die Winzip-Entwickler mögen dem Autor die lange Testzeit von 309 Tagen nachsehen). Nach der Registrierung ist der Nagscreen nicht mehr zu sehen

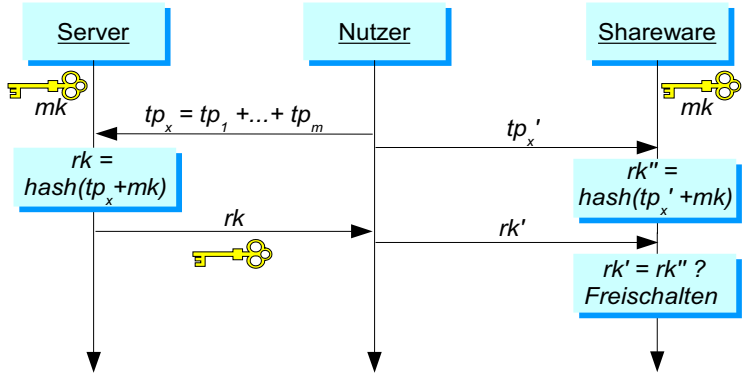
Abbildung 6.1
"Nagscreen" des Shareware-Packers Winzip

Es gibt weitere Formen, wie der Nutzer für eine Registrierung belohnt werden kann. Eine Shareware-Version ist bspw. nicht voll funktionsfähig. Nach der Registrierung und Bezahlung erhält der Nutzer die Vollversion zum Download.

Von Kritikern wird dies allerdings nicht als Shareware im strengen Sinne akzeptiert. Sie nennen diese nur teilweise funktionierende Software Demo-Software oder noch abweisender *Crippleware*.

Nach der Registrierung und Bezahlung auf der Web-Seite des Shareware-Autors erhält der Nutzer einen Login-Namen und einen Registrierungsschlüssel *rk* zugeteilt.

Abbildung 6.2
Sequenz-Diagramm des Registrierungsvorgangs



Der Schlüssel wird nach einem geheim zu haltenden Verfahren (bzw. nach einem bekannten Verfahren mit einem geheimen Master-Schlüssel *mk*) aus dem Login-Namen (oder anderen kundenspezifischen Transaktionsparametern tp_x) gebildet. Abbildung 6.2 zeigt wie mittels eines Hash-Algorithmus' (vgl. Seite 52) der Schlüssel aus dem Master-Schlüssel und dem Login-Namen gebildet wird. Der Schlüssel und der Login-Name müssen durch den Nutzer in das Programm eingegeben werden. Nach

der Eingabe verschwindet schließlich der lästige Nagscreen, wenn das Programm ebenfalls aus dem Login-Namen den eingegebenen Schlüssel *rk'* bilden kann.

Alternativ zur einfachen Abschaltung des Nagscreens kann die Eingabe eines Registrierungsschlüssels aus einer Demo-Version bzw aus der Crippleware auch direkt die Vollversion machen.

6.1.3 Grundprobleme des Shareware-Konzepts

Das Web-Portal share*it! [Shareit 05] bietet für Shareware-Autoren die Abwicklung der Nutzerregistrierung, der Bezahlung und Schlüsselgenerierung als Dienst an. Dieser Dienst zeigt sich sehr flexibel und unterstützt nahezu alle Formen des Shareware-Vertriebs. Der Autor kann auch einen eigenen Schlüsselgenerierungsalgorithmus bereitstellen. Die Grundprobleme des Shareware-Konzepts sind auch mit diesem Dienst nicht beseitigt.

- **Umständliche Registrierung**: Der Weg vom Nagscreen, der den Nutzer zur Registrierung auffordert, bis zur Nutzung der Vollversion ist zu lang. Nur sehr begeisterte und versierte Nutzer folgen diesem Weg. Gelegenheitsnutzer fallen oft als Erlösquelle aus.
- **Geringer Anreiz**: Der Anreiz eine Registrierungsgebühr zu entrichten, nur damit der Nagscreen verschwindet ist zu gering. Shareware, die nach der Registrierung mehr bietet ist hier im Vorteil.
- **Mangelnder Schutz**: Die Registrierung entsprechend Abbildung 6.2 ist zwar sicher genug für den Gelegenheits-Hacker. Es muss aber nicht betont werden, dass ein Profi-Hacker unter Hinzunahme eines Debuggers die Registrierung umgehen kann indem er entweder den Master-Schlüssel aus dem Programm ausließt oder die Stelle findet und modifiziert, an der die Freischaltung geprüft wird. Diese aufwendigen Angriffe sind unnötig, wenn ein legaler Nutzer seinen Login-Namen und den Registrierungsschlüssel öffentlich zugänglich macht. Noch schlimmer ist es, wenn ein Hacker, der den Master-Schlüssel aus der Shareware ausgelesen hat, ein Programm verbreitet, welches gültige Registrierungsschlüssel erzeugt.

6.2 Erweitertes Konzept für den Online-Vertrieb

Die Erweiterung des Shareware-Konzeptes für den Online-Vertrieb muss mindestens eine engere Kopplung der Client-Software mit dem Registrierungsserver und einen verbesserter Schutz gegen eine illegale Weitergabe bieten. Darüber hinaus sind Online-Update und Ergänzungen wünschenswert.

6.2.1 Pay-per-Feature

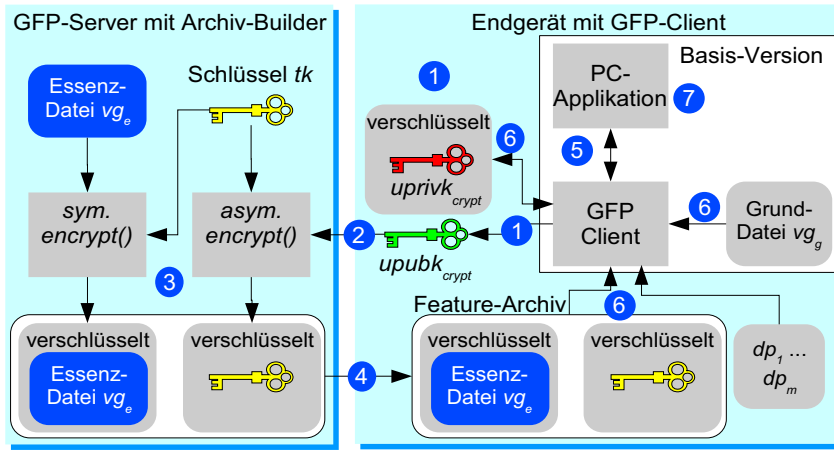
Bei der Entwicklung der so genannten Game-Feature-Plattform (GFP) [Nützel 01] stand nicht die simple Freischaltung bzw. Aktivierung einer Vollversion im Vordergrund. Grundlage der Entwicklung war das Pay-per-Feature-Modell. Hierbei erhält der Nutzer eine kostenlose Basis-Version per Download oder CDROM, die er nach seinem eigenen Wünschen Schritt-für-Schritt um weitere Features (bei Spielen sind das bspw. zusätzliche Levels, Karten, Hintergrundmusik, Fahrzeuge oder Charaktere) erweitern kann. Da solche Features typischerweise keinen Programmcode son-

dern Nutzdaten enthalten, die erst durch die Anwendung (Spiel) decodiert werden, lag der Gedanke nahe, diese Nutzdaten analog zu einem DRM-System (vgl. Kapitel 4.4) verschlüsselt zum Download anzubieten und diese erst kurz vor ihrer Verwendung (Decodierung) durch die Applikation im Arbeitsspeicher zu entschlüsseln. Prinzipiell ließe sich dieses Vorgehen auch auf Programmcode erweitern. Allerdings müssten dann bei der Entschlüsselung viel stärker die Spezifika des jeweiligen Betriebssystems berücksichtigt werden.

Das spezielle an der GFP ist die Möglichkeit, nur kleinere aber wichtige Teile der Feature-Nutzdaten zu verschlüsseln. Diese in [NüBöStSc 00] als Essenz-Datei bezeichneten Nutzdaten vg_e ergänzen die in der Basis-Version enthaltene Grund-Datei vg_g zur kompletten Feature-Datei.

Abbildung 6.3 zeigt wie der GFP-Client (eine Komponente, die in der Basis-Version integriert ist) die Feature-Datei (in den Schritten 5 bis 7) aus der Essenz-Datei und der Grund-Datei für die Applikation rekonstruiert. Das Feature-Archiv, welches die ganz oder teilweise verschlüsselte Essenz-Datei enthält, wurde zuvor (in Schritt 4) vom GFP-Server heruntergeladen. Im Unterschied zum DRM-Referenz-System (vgl. Kapitel 4.4.2) ist das Archiv hybrid (vgl. Seite 52) verschlüsselt und enthält somit bereits den Sitzungsschlüssel *tk*. Dieser ist aber noch zusätzlich mit dem öffentlichen RSA-Schlüssel $upubk_{crypt}$ verschlüsselt. Der öffentliche Schlüssel wurde bereits in Schritt 2 vom Endgerät an den Server übertragen. Auf Seite 53 wurde bereits das bei der GFP eingesetzte Verfahren für den Schlüsselaustausch (mit dem Schlüsselpaar *dpubk* und *dprivk*) beschrieben.

Abbildung 6.3
Zusammenspiel von Server und Endgerät



Schritt 6 startet, wenn die Applikation in Schritt 5 eine Feature-Datei öffnet. Es wird zuerst der symmetrisch verschlüsselte private RSA-Schlüssel $uprivk_{crypt}$ geladen und mit Hilfe der endgerätespezifischen Parametern dp_1 ... dp_m entschlüsselt. Dies ermöglicht erst die Entschlüsselung des hybrid verschlüsselten Feature-Archivs. Schritt 6 ist abgeschlossen, wenn der GFP-Client Grund-Datei und Essenz-Datei im Ar-

beitsspeicher zusammengeführt hat. Die eigentliche Decodierung bzw. Verarbeitung der Nutzdaten erfolgt schließlich in Schritt 7 innerhalb der PC-Applikation.

Motivation für die Aufteilung der Nutzdaten in eine Essenz- und eine Grund-Datei ist das Superdistributions-Szenario (vgl. Kapitel 3.6.4). Die Grund-Datei, die den Großteil der benötigten Feature-Nutzdaten darstellt, wird zusammen mit der Basis-Version der Applikation auf einer CDROM oder DVD (als Heftbeilage) oder über ein P2P-System kostenlos verteilt. Die Features können allerdings erst dann genutzt werden, wenn die Grund-Datei um die fehlenden Essenz-Daten ergänzt wird. Die Struktur des Archivs, mit der die Essenz-Daten verschlüsselt übertragen werden, unterstützt die Möglichkeit, die Essenz-Daten an einer beliebigen Stelle aus den Nutzdaten zu entnehmen. Damit ergeben sich die folgenden Fälle:

- Es gibt keine Grund-Datei, die zusammen mit der Basis-Version der Applikation verteilt wird. Vom Server gelieferte Archive enthalten die kompletten Nutzdaten für ein Feature.
- Die Essenz-Datei bildet den Anfang der Nutzdaten. Die Grund-Datei wird im Arbeitsspeicher an die entschlüsselten Essenz-Daten angefügt. Dies ist der übliche Fall, da oft vorangestellte Header-Daten benötigt werden, um die eigentlichen Nutzdaten erst sinnvoll decodieren zu können. Ein Beispiel ist die Farbtabelle einer GIF-Datei.
- Die Essenz-Datei wird an einer definierten Stelle (oder auch am Ende) in die Grund-Datei eingefügt.

Um Rechenzeit sowohl auf Server- als auch auf Client-Seite zu sparen, besteht die Möglichkeit nur ausgewählte Teile der Essenz-Datei in Schritt 3 zu verschlüsseln. Dies ist besonders dann relevant, wenn das ganze Feature vom Server geliefert wird. Zusätzlich kann auf dem Server die Rechenzeit reduziert werden, wenn die Essenz-Daten vorab mit einem – dann aber für alle Nutzer gleichen – Sitzungsschlüssel *tk* verschlüsselt werden. Dies ist das übliche Vorgehen beim Einsatz von DRM-Systemen, wie dem von Microsoft [WMRM 05].

6.2.2 Bindung an das Endgerät

Den Schutz vor illegaler Weitergabe der bezahlten Registrierungsschlüssel lässt sich durch die Integration von endgerätespezifischen Parametern in den Registrierungsprozess bewerkstelligen. Hochpreisige Software wie z. B. CAD-Software wird seit vielen Jahren auf diese Weise an ein einzelnes Endgerät gebunden.

Im Falle von Shareware würde im Registrierungsdialog (das ist ein schöneres Wort für Nagscreen) dem Nutzer ein Registrierungscode *rc* angezeigt werden. Der Code *rc* wird nach Formel 6.1 innerhalb der Client-Software aus endgerätespezifischen Parametern $dp_1 \ldots dp_m$ (siehe Seite 51 zu möglichen Hardware-Parametern) und einer Zufallszahl *rand* gebildet.

Formel 6.1

$$rc = hash(dp_1 + dp_2 + \ldots + dp_m + rand)$$

Der Nutzer übermittelt diesen Code an den Registrierungs-Server, der im Unterschied zu Abbildung 6.2 diesen Code anstelle von tp_x in die Hash-Funktion einfügt, um den endgerätespezifischen Registrierungsschlüssel *rk* zu bilden. Die Zufallszahl

rand sorgt dafür, dass der Registrierungsschlüssel *rk* selbst bei einer Neuinstallation auf dem gleichen Endgerät nicht noch einmal benutzt werden kann.

Einsatz asymmetrischer Kryptographie

Der Einsatz asymmetrischer kryptographischer Verfahren (z. B. RSA) hat den Vorteil, dass keinerlei endgerätespezifische Parameter (dp_1 ... dp_m) zwischen Client und Server ausgetauscht werden müssen. Dieses Verfahren wurde bereits auf Seite 53 beschrieben. Anstelle der Parameter, die die Interna des Endgerätes an den Server „verraten", wird in Schritt 2 (vgl. Abbildung 6.3) der öffentliche Teil eines zufällig in Schritt 1 erstellten RSA-Schlüssel-Paares übertragen.

In der ursprünglichen GFP-Idee sollte das Schlüsselpaar aus einer Smartcard benutzt werden. Smartcards gewährleisten, dass die auf ihr gespeicherten privaten Schlüssel nicht ausgelesen werden können. Da Smartcards sich entgegen den Vorhersagen der Experten auch 2005 noch nicht verbreitet haben und nur sehr wenige Laptops serienmäßig mit einem Kartenleser ausgestattet sind, wurde das weniger sichere dafür aber kostengünstigere Konzept einer „virtuellen Smartcard" verfolgt.

Beim ersten Start erzeugt der GFP-Client (Schritt 1 in Abbildung 6.3) der PC-Applikation zwei applikationsspezifsche 1024 Bit lange RSA-Schlüsselpaare. Der $upubk_{crypt}$ (*User Crypt Public Key*) und der $uprivk_{crypt}$ (*User Crypt Private Key*) werden für das Verschlüsseln und Entschlüsseln von symmetrischen Sitzungsschlüsseln *tk* benutzt. Der $uprivk_{sign}$ (*User Sign Private Key*) und der $upubk_{sign}$ (*User Sign Public Key*) werden für das Signieren und Prüfen von Signaturen benutzt (*User* ist hier etwas verwirrend, gemeint ist das Endgerät des Users). Die Signatur der zwischen Client und Server ausgetauschten Daten und die dabei eingesetzten Schlüssel wurden aus Gründen der Übersichtlichkeit nicht in die Abbildung 6.3 aufgenommen.

Zwei Schlüsselpaare deshalb, um RSA-spezifische Angriffe zu verhindern. In [Wobst 98] (S.166 und S.264) wird beschrieben, wie ein Angreifer, der einen mit dem öffentlichen Schlüssel verschlüsselten Sitzungsschlüssel abfängt und diesen nach einer Modifikation dem GFP-Client zum Signieren unterschiebt und dann aus den Signierten Daten den Sitzungsschlüssel errechnen kann. Das kann dadurch verhindert werden, dass für das Signieren von Nachrichten und das Verschlüsseln von Sitzungsschlüsseln getrennte Schlüsselpaare benutzt werden.

Die beiden privaten Schlüssel $uprivk_{crypt}$ und $uprivk_{sign}$ werden, bevor sie in Schritt 1 lokal abgespeichert werden, nochmals symmetrisch verschlüsselt. Der Schlüssel hierfür wird aus endgerätespezifischen Parametern dp_1 ... dp_m nach einem geheim zu haltenden Verfahren bzw. geheimen Master-Schlüssel im GFP-Client gebildet (vgl. Seite 51). Damit können die symmetrisch verschlüsselten privaten RSA-Schlüssel nur auf denjenigen Endgeräten entschlüsselt und genutzt werden, die die gleiche Konfiguration besitzen. Da es jedoch selten zwei gleich aufgebaute und gleich konfigurierte PCs gibt, kann dieser Schutz als ausreichend sicher angesehen werden.

6.3 Umsetzung der GFP

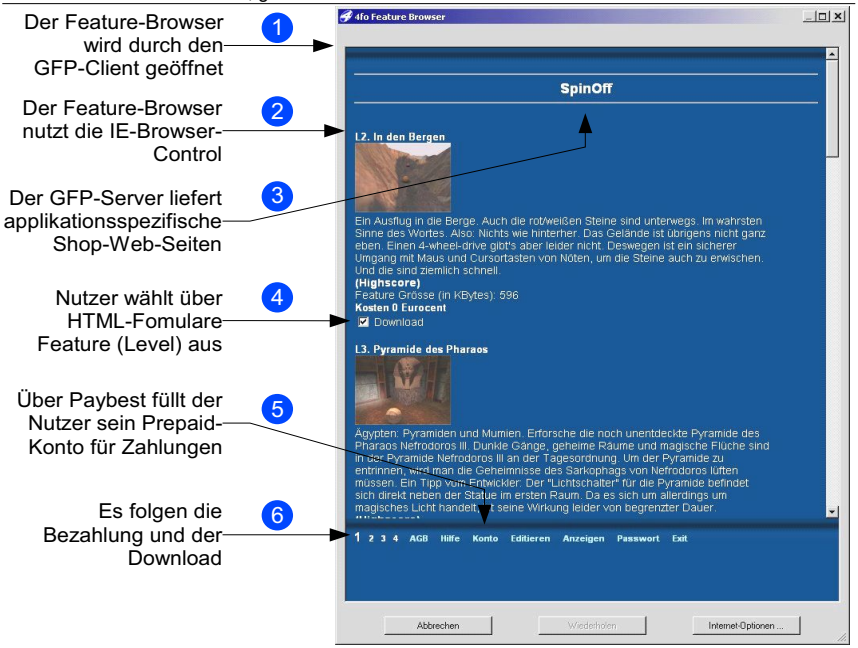
Die erste Umsetzung der GFP-Technik erfolgte durch die 4FO AG. Der dabei entstandene monolitische GFP-Server enthält nicht nur eine Funktionalität zur Erstellung der Download-Archive, sondern ein komplettes Datenbank-gestütztes System zur Verwaltung der angebotenen Features, der Nutzer und ihrer Registrierungs- bzw. Kauftransaktionen. Auf die Beschreibung dieses Transaktionsverwaltungssystems wird zu Gunsten der Beschreibung des PotatoSystems in Kapitel 8 verzichtet.

6.3.1 GFP-Client-DLL

Der GFP-Client wurde spezifisch für Windows-Betriebssysteme als DLL (*Dynamic Link Library*) umgesetzt. Dies ermöglicht eine flexible Integration in die meisten PC-Applikationen. Damit Applikationsentwickler diese DLL integrieren können, wurde die API dieser DLL dokumentiert. Die API kapselt vollständig die Kommunikation mit dem GFP-Server. Der Entwickler hat Funktionen, um die Präsenz eines Features auf dem Client zu testen, das Feature zu öffnen und durch den GFP-Client im Arbeitsspeicher entschlüsseln zu lassen. Wird über die API ein Feature angefordert, welches sich noch nicht auf dem Endgerät befindet, so nimmt die DLL automatisch Kontakt mit dem GFP-Server auf.

Die Übermittlung der beiden öffentlichen RSA-Schlüssel und der Download der Feature-Archive erfolgen automatisch durch den GFP-Client. Der im CFP-Client integrierte Feature-Browser (siehe Schritt 1 in Abbildung 6.4) übernimmt diese Aufgabe unter Verwendung des Internet-Explorer-Controls (Schritt 2). Das Internet-Explorer-Control ist auf jedem Windows-System standardmäßig vorhanden. Mit dieser Browser-Komponente können spezialisierte Applikationen erstellt werden, die HTML-Seiten zur Anzeige nutzen und über das Internet Daten austauschen.

Abbildung 6.4
HTML-Seite vom GFP-Server, geöffnet im Feature-Browser des GFP-Clients



Der Einsatz einer Browser-Komponente ermöglicht es die Nutzerregistrierung, die Feature-Auswahl und die Bezahlung komplett über serverseitig erzeugte HTML-Formulare abzuwickeln. Über POST-Parameter, die an den Server übermittelt werden,

weiß der GFP-Server, dass er in Schritt 3 nur die Features der jeweiligen Applikation anzeigen darf. In Schritt 4 wählt der Nutzer die gewünschten Features aus. Vor der Zahlung muss der Nutzer in Schritt 5 seinen Prepaid-Account auf dem GFP-Server mit Paybest (vgl. Kapitel 5.4) auffüllen. In Schritt 6 kann der Nutzer schließlich die restlichen interaktiven Aktionen bis zum Start des Download durchführen. Sollen diese Schritte einmal im Design verändert werden, so ist keine Modifikation der Client-Applikation notwendig.

Neben der Möglichkeit den Kaufvorgang Client-unabhängig zu gestalten, bringt der Einsatz eines Browsers auch Probleme mit sich. Eine Browser-Komponente ist nicht dazu geeignet, den Download und die Installation der Feature-Archive so automatisch abzuwickeln, dass die Applikation (in der der GFP-Client integriert ist) sofort danach mit den neuen Features fortsetzen kann. Um dies dennoch möglich zu machen, musste auf der Client-Seite zusätzlich eine (selbstentwickelte) ActiveX-Komponente eingesetzt werden. Diese neben der GFP-Client-DLL zweite zu installierende DLL kann aus einer HTML-Seite heraus durch den Internet-Explorer gestartet werden. Auf diese Weise wird das Feature-Archiv vom GFP-Server entgegengenommen, auf Konsistenz geprüft, auf dem Endgerät gespeichert und dem Server als erfolgreich gespeichert zurückgemeldet (vgl. Abbildung 6.5).

6.3.2 Aktivierung und Freischaltung

Der einfachste Einsatzfall der GFP-Technik ist die Freischaltung einer Basis-Version zu einer Vollversion. In diesem Fall dient der Applikation alleine schon die Entschlüsselbarkeit der Essenz-Datei als Signal, um die volle Funktionalität freizugeben. Diese binäre Aussage, die vom GFP-Client an die Applikation gemeldet wird, kann allerdings leicht durch Manipulation übergangen werden. Ein höheres Maß an Sicherheit wird erzielt, wenn in der Essenz-Datei Informationen enthalten sind, die von der Applikation auch wirklich benötigt werden.

6.3.3 Ergänzungen und Updates

Ziel der GFP ist es, den Anbietern bzw. Entwicklern ein System bereitzustellen, mit dem diese auch Features anbieten können, die zum Zeitpunkt der Fertigstellung der Basis-Version noch nicht verfügbar sein müssen.

Das mit der GFP-Technik vertriebene PC-Spiel *SpinOff* [SpinOff 02] ist ein Beispiel dafür. *SpinOff* ist die 3D-Umsetzung eines Kugelspiels, bei dem man mit der Maus eine virtuelle Landschaft neigt und die Kugel dadurch beschleunigt oder abbremst. Ziel des Spiels ist es, diese Kugel vorbei an diversen Hinternissen in möglichst kurzer Zeit in das Ziel zu bringen. In der kostenlos verteilten Basis-Version des Spiels sind zwei Level (virtuelle 3D-Landschaften) enthalten. Weitere Level, die der Entwickler nach und nach, später auch einige Spieler, auf dem GFP-Server bereitstellten, können direkt aus dem Spiel heraus bezogen werden (vgl. Abbildung 6.4). Die Essenz-Daten sind in diesem Fall die kompletten Level-Dateien.

Abbildung 6.4 zeigt das Content-Management-System des GFP-Servers, wie es dem Nutzer über den Feature-Browser die verfügbaren Level anzeigt. Das erste zusätzliche Level „In den Bergen“ wird dem Nutzer bewusst kostenlos angeboten, damit dieser auf diesem Weg den gesamten Anmeldungs- und Download-Prozess ohne ein finanzielles Risiko testen kann.

Die GFP-Technik ermöglicht es auch, bereits vorhandene Dateien aus der Basis-Version vom GFP-Server aus überschreiben zu lassen. Etwas komplizierter ist es für

die ausführbaren Dateien der Applikation. Diese (EXEs oder DLLs) können nicht ersetzt werden, während sie vom Betriebssystem geladen sind. Die neuen Programm-Dateien müssen durch den GFP-Client unter einem temporären Namen gespeichert werden. Danach wird die Applikation automatisch beendet und eine spezielle *Update.exe* gestartet. Diese Hilfsapplikation übernimmt das Umkopieren der ausführbaren Dateien und startet sofort danach die aktualisierte Applikation erneut.

6.4 Ergänzungen und mögliche Erweiterungen

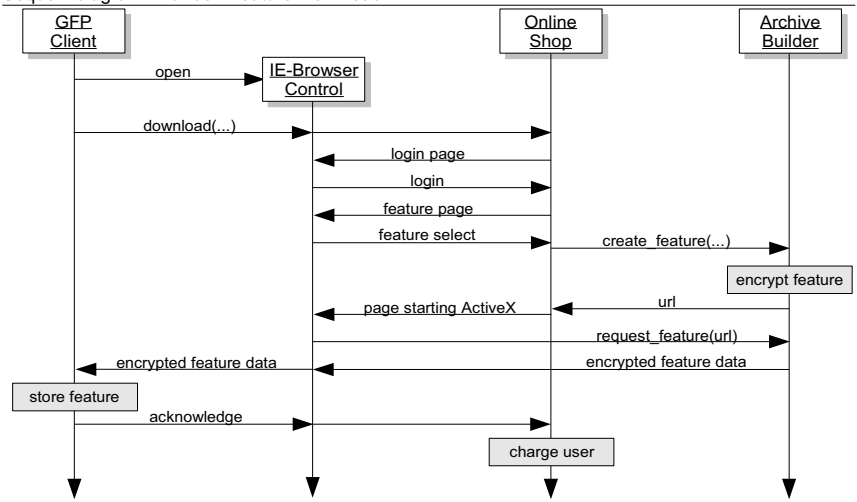
Die umgesetzte GFP-Technik erfüllte bereits 2002 die zu Beginn der Entwicklung aufgestellten Anforderungen. Allerdings zeigten sich zwei grundlegende Mängel:

- Der GFP-Server ist monolitisch aufgebaut. Die in der GFP-Technik innovativen neuen Teile, wie die Erstellung der verschlüsselten Feature-Archive, kann nicht als separate Funktionalität Interessenten angeboten werden.
- Die Integration des GFP-Clients in eine PC-Applikation muss vor Abschluss der Entwicklung erfolgen. Selbst einfache Szenarien, wie die Freischaltung, verlangen zusätzliche Modifikationen an der PC-Applikation.

6.4.1 Ausgliederung der Archiv-Erstellung als Web-Service

Größere und mittlere Software-Anbieter betreiben sehr häufig eigene Online-Shop-Systeme. Es ist also sinnvoll, nur die kryptographischen Teile der GFP-Technik über eine Web-Service-Schnittstelle (vgl. Kapitel 5.4.3) bereitzustellen. Michael Kunze lieferte in seiner Diplomarbeit [Kunze 04] wesentliche Teile für die Kapselung der Archiv-Generierung (*Archive Builder*).

Abbildung 6.5
Sequenzdiagramm für den Feature-Download



Das in Abbildung 6.5 gezeigte Szenario findet statt, wenn der GFP-Client von der Applikation aufgefordert wird, ein Feature zu entschlüsseln, welches sich noch nicht auf dem Endgerät befindet. Der GFP-Client nutzt das Browser-Control, um eine Kennung für die Applikation, eine Kennung für das gewünschte Feature und den öffentlichen Schlüssel $upubk_{crypt}$ (*User Crypt Public Key*) an den Online-Shop zu übertragen. Der Shop liefert die Login-Seite und danach die Feature-Auswahl-Seite (vgl. Abbildung 6.4). In der Auswahl-Liste ist das vom Client angeforderte Feature bereits ausgewählt. Der Nutzer hat dann die Möglichkeit, weitere Features auszuwählen. Wenn der Online-Kontostand des eingeloggten Nutzers ausreichend ist, ruft der Online-Shop den Web-Service (*create_feature*) auf. Als Parameter werden neben der Applikationskennung und dem öffentlichen Schlüssel auch eine Liste der angeforderten Features übertragen.

Da die unverschlüsselten Essenz-Daten beim Online-Shop liegen, werden die URLs auf diese Nutzdaten vom Online-Shop an den Web-Service übertragen. Der Archive-Builder lädt darauf vom Shop-Server die Nutzdaten, um die Verschlüsselung durchzuführen. Das Verzeichnis in dem die unverschlüsselten Daten liegen ist im Zugriff auf den Archive-Builder beschränkt. Das erstellte Feature-Archiv wird unter einer temporären Adresse gespeichert. Die URL für dieses Archiv, in dem mehrere Features zusammengefasst sein können, bildet den Rückgabewert des Web-Service-Aufrufes.

Der Online-Shop erstellt daraufhin eine Download-Seite in der die auf dem Endgerät installierte ActiveX-Komponente verlinkt ist. Als Parameter erhält das ActiveX-Control die URL. Der Download wird gestartet. Nach erfolgreichem Download wird das Feature-Archiv auf dem Endgerät gespeichert. Der Erfolg wird dem Online-Shop signalisiert. Nun zieht der Online-Shop dem Nutzer den Kaufpreis endgültig von seinem Prepaid-Account ab. Alle sicherheitskritischen Nachrichten und das Feature-Archiv werden zusätzlich signiert.

6.4.2 Automatische Integration des GFP-Clients

Bei Applikationen, die im Rahmen einer Zweitvermarktung lange nach ihrer Fertigstellung online verkauft werden sollen, ist es in der Regel nicht mehr möglich, den Quellcode zu verändern. Um dennoch die GFP-Technik einsetzen zu können, muss eine Patch-Applikation bereitgestellt werden, mit der der GFP-Client in eine fertig übersetzte PC-Applikation im PE-Format (*Win32 Portable Executable File Format,* siehe [Pietrek 02]) integriert werden kann. Diese Patch-Applikation führt an der PC-Applikation die folgenden Modifikationen automatisiert durch:

- Die EXE wird mit Ausnahme des Headers verschlüsselt. Der eingesetzte symmetrische Schlüssel lautet *ck*. Die im Header gespeicherte Startadresse lautet *sa*.
- An die verschlüsselte EXE wird zusätzlicher Code angefügt. Die Startadresse dieses Codes lautet danach *ea*.
- Im Header wird die alte Adresse *sa* durch *ea* ersetzt. Wird die modifizierte EXE gestartet, wird zuerst der angefügte Code ausgeführt.
- Es wird für den Online-Shop eine Essenz-Datei erstellt, die *ck* und *sa* enthält.

Der angefügte Code enthält einen Aufruf des GFP-Clients, um *ck* und *sa* aus einem Feature-Archiv zu laden. Mit *ck* wird der Original-Code entschlüsselt. Nach der Entschlüsselung wird an der Adresse *sa* die Abarbeitung fortgesetzt.

Mit der beschriebenen Methode, die sich auch Autoren von Viren zunutze machen, wird nahezu jede Windows-EXE zu einer Applikation, die erst läuft, wenn eine Freischaltung mit der GFP-Technik erfolgt ist.

6.4.3 Redundante Hardware-Bindung

Für die GFP-Technik wird für die Entschlüsselung der Essenz-Daten der private Schlüssel $uprivk_{crypt}$ benötigt. Dieser RSA-Schlüssel ist zusätzlich symmetrisch verschlüsselt auf dem Endgerät gespeichert. Der symmetrische Schlüssel wird aus den *m* endgerätespezifischen Parametern $dp_1 \ldots dp_m$ gebildet (vgl. Seite 103).

Damit der private Schlüssel auch dann noch genutzt werden kann, wenn einer der *m* Parameter bei einer Veränderung der Konfiguration verloren gegangen ist, muss der private Schlüssel *m*-mal *zusätzlich* redundant unterschiedlich verschlüsselt (jeweils ein anderer der *m* Parameter ist nicht bei der Bildung des symmetrischen Schlüssels beteiligt) abgespeichert werden.

Kann der mit allen *m* Parametern verschlüsselte RSA-Schlüssel nicht mehr entschlüsselt werden, dann hat sich mindestens einer der *m* Parameter verändert. Stellt der GFP-Client dies fest, beginnt er damit, die *m* anderen, die nur mit *m*-1 Parametern verschlüsselt sind, nacheinander zu testen, solange bis ein gültiger RSA-Schlüssel gefunden wird.

Sobald eine Entschlüsselung scheitert, muss dies dem Nutzer auf jeden Fall signalisiert werden. Eine automatische Neuverschlüsselung scheidet aus, da auf diesem Weg nacheinander alle Parameter verändert werden können.

Der Aufwand wächst beträchtlich an, wenn sich zwei Parameter gleichzeitig ändern dürfen.

6.4.4 Weitere Verbesserungen und Ergänzungen

Für weitere wünschenswerte Verbesserungen und Erweiterungen der GFP-Technik liegen dem Autor keine fertigen Lösungen vor. Nichtsdestotrotz sollen diese Ansätze nicht ungenannt bleiben. Produktbeschreibungen anderer Systeme wie z. B. dem HASP der Firma Aladdin [HASP 05] ist zu entnehmen, dass solche Lösungen bereits bestehen.

■ Zeitliche Beschränkungen

Ein Problem der automatischen Integration des GFP-Clients in Kapitel 6.4.2 ist, dass ohne Freischaltung von der Original-Applikation nichts zu sehen ist. Ein Testen vor dem Kauf ist nicht mehr möglich. Dies wäre durch eine zeitlich begrenzte Aussetzung der Verschlüsselung lösbar. Nach der Installation kann der Nutzer die Applikation ohne Limitierung eine gewisse Zeit nutzen. Nach Ablauf dieser Test-Periode ist die Applikation erst nach der Freischaltung wieder nutzbar.

Um diese Forderung umzusetzen, muss die Applikation Merker oder Zähler auf dem Endgerät verwalten, die der Nutzer nicht mehr löschen kann. Das ist nur eingeschränkt manipulationssicher umsetzbar.

- **Einsatz einer Rechtebeschreibungssprache**

Soll die durch das Feature-Archiv erfolgte Freischaltung mit zusätzlichen Bedingungen verknüpft werden, bietet es sich an, diese Bedingungen in einer Rechtebeschreibung (vgl. Kapitel 4.4.3) im Feature-Archiv abzulegen. In diesem Fall müsste die Rechtebeschreibung im GFP-Client ausgewertet werden. Ein Anwendungsbeispiel wäre die zeitliche Limitierung einer Freischaltung.

- **Erhöhung der Sicherheit durch *Code Obfuscation***

Auf einem Windows-PC kann Hackern das Innenleben des GFP-Clients auf Dauer nicht geheim gehalten werden. So genanntes *Code Obfuscation* (obfuscate – verwirren, verdunkeln) [WikiObfus 05] kann ihnen allerdings das Reverse Engineering der internen Abläufe erschweren.

7. Kapitel

Das leichtgewichtige DRM - ein Verfolgungssystem

Unter Leitung der beiden Fraunhofer-Institute IIS in Erlangen und IDMT in Ilmenau entstand das Konzept für das so genannte *Light Weight Digital Rights Management* System (kurz LWDRM) [LWDRM 04] [NeBrSi 02], an dessen Umsetzung der Autor mitbeteiligt war. Die Leichtgewichtigkeit dieses Konzeptes, die auch den Namen motivierte, findet sich in dem gegenüber traditionellen DRM-Systemen geringeren technischen Aufwand zur Umsetzung von Endgeräte-Interoperabilität bei gleichzeitiger Verhinderung von Urheberrechtsverletzungen.

Der LWDRM-Ansatz überträgt die Verantwortung zum legalen Umgang mit den virtuellen Waren auf den Nutzer. Es wird dem Nutzer eine technisch unbeschränkte Kopierbarkeit ermöglicht, wenn er sich im Gegenzug dazu bereit erklärt, seine Kopien individuell zu markieren. Diese Markierung macht es möglich, dass eine Kopie, die außerhalb des erlaubten privaten Umfeldes des Nutzers gefundenen wird, auf ihn als Ursprung zurückgeführt werden kann.

In der ursprünglichen LWDRM-Idee wurde die nutzerspezifische Markierung mittels Signatur und Verschlüsselung realisiert. Die zusätzliche mit der Signatur verbundene Verschlüsselung machte allerdings die Kompatibilität mit dem unmarkierten Format zunichte. Inzwischen (Anfang 2005) zeigt sich, dass für die ursprünglich geplante Nutzung für Privatnutzer im Download-Geschäft von LWDRM möglicherweise nur noch das als zweite Verteidigungslinie geplante Wasserzeichen übrig bleiben wird.

Das erweiterte Format mit Signatur und Verschlüsselung wird Speziallanwendungen im B2B-Umfeld zur Kommunikation und Authentifizierung von Nutzerrechten vorbehalten bleiben.

7.1 Motivation für ein anderes DRM

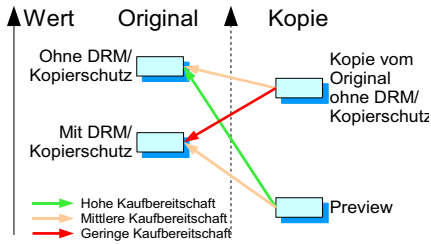
Digital Rights Management (DRM) besteht nach [Rump 04] aus einem *Digital Policy Management* (DPM) und einem darauf aufsetzenden *Digital Policy Enforcement* (DPE) (vgl. Seite 60), welches die in dem DPM vereinbarten Regeln (Policies) durchsetzt. Üblicherweise verbindet man mit dem Begriff DRM ein DPE in Form eines Kopierschutzes auf dem Endgerät (vgl. Kapitel 4.3.2). Auf Basis dieses Kopierschutzes werden dem Nutzer durch das DPE wieder bestimmte Nutzungsrechte *zurückgegeben*. Diese Nutzungsrechte werden strickt auf dem Endgerät des Nutzers durchgesetzt. Die Motivation der Anbieter solcher restriktiver Techniken ist sicherlich, die illegale Verbreitung der virtuellen Waren durch den Konsumenten zu unterbinden. Natürlich möchten manche Anbieter auch neuartige Erlösmodelle realisieren, die einen höheren Profit versprechen (vgl. Seite 32).

Problematisch bei dieser Form des DPE ist die hohe technische Komplexität, wenn es darum geht Interoperabilität zu gewährleisten. Derzeit wird dieser Aufwand noch gescheut (bzw. bewusst in Kauf genommen); was Inkompatibilitäten zwischen unterschiedlichen Endgeräten nach sich zieht. Gescheiterte Ansätze wie bspw. SDMI (vgl. Seite 49) belegen diese Schwierigkeiten. Es gibt allerdings immer wieder auch Ansätze, aktuell DMP (*Digital Media Project*) [DMP 05], DRM interoperabel zu machen. Auch das DRM des OMA-Konsortium (vgl. Kapitel 4.4.4) hat gute Chancen, bei den Marktteilnehmern breite Zustimmung zu finden.

Bei herkömmlichen DRM-Systemen ist es technisch sehr aufwändig, zu erkennen, ob ein Transfer auf ein tragbares Endgerät legal oder illegal ist. Ist es das Endgerät des Nutzers, der bereits für den Song bezahlt hat, ist die Kopie legal. Ist es das Portable eines fremden Nutzers, so ist die Kopie illegal. Um dem Problem der fehlenden Unterscheidbarkeit zu entgehen, wird oft ein Kompromiss eingegangen, indem eine definierte Anzahl von Transfers pro Nutzungslizenz erlaubt werden (vgl. Kapitel 4.4). Der legale Nutzer der diese Anzahl, während seiner privaten Nutzung, dennoch erreicht, betrachtet diese Limitierung allerdings als technischen Mangel. Er fragt sich, warum er bei legaler Nutzung größere Einschränkungen hat, als Nutzer illegaler Kopien, die keiner DRM-Kontrolle unterliegen.

Aichroth und Hasselbach beschreiben dieses Problem der umgekehrten Anreize [AicHas 03] (vgl. Abbildung 7.1). Sie zeigen auf, dass Besitzer einer illegalen Kopie natürlich wenig Anreiz haben ein Original zu kaufen. Dieser Anreiz ist noch viel geringer, wenn das Original durch DRM in seiner Funktionalität eingeschränkt ist. Zur Lösung schlagen sie das Konzept der *Previews* vor. *Previews* sind im Wert (über die Länge oder Qualität) verminderte Kopien der Originale. [Hartmann 04], [AiPuHa 04]

Abbildung 7.1
Probleme mit Kaufbereitschaft [Hartmann 04]



7.1.1 Der alternative Ansatz

Möchte man nicht ganz auf ein DPE verzichten, so bietet sich ein alternativer Ansatz an, bei dem das Kopieren nicht technisch verhindert wird. Es wird vielmehr die an il-

legaler Stelle gefundene Kopie nachträglich (forensisch) bis zum Verursacher zurückverfolgt (vgl. Kapitel 4.3.3). Der Grundgedanke dahinter ist die Überlegung, dass man nicht die ehrlichen Nutzer mit Kopierschutz und anderen Nutzungseinschränken bestrafen sollte, sondern nur die, die sich wirklich illegal verhalten: „*Keep the honest people honest*".

Das illegale Verhalten wird nicht technisch verhindert bzw. erschwert, sondern es wird verfolgbar gemacht. Eine in Diskussionen und Vorträgen der LWDRM-Entwickler häufig verwendete Analogie ist die der roten Ampeln im Straßenverkehr. Eine rote Ampel verhindert auch nicht die Durchfahrt. Die Autofahrer wissen aber, dass das Ignorieren eines Rotlichts verfolgt werden kann.

Vom Standpunkt der Umsetzung benötigt die Einführung forensischen DPE auf der Seite der tragbaren Endgeräte keine Nachrüstung. Es muss dem Nutzer nur mitgeteilt werden, dass illegale Kopien zurückverfolgt werden können. Die Einführung von Ampeln 1918 in New York und 1924 in Berlin machte in den bereits vorhandenen Fahrzeugen ebenfalls keine Änderung der Technik notwendig. Es mussten lediglich die Nutzer der Fahrzeuge instruiert werden. Natürlich bedarf es des Systems der Kraftfahrzeugkennzeichen, welches anonymes Fahren unmöglich macht.

Ein besonders nutzerfreundliches DRM-System würde dem Käufer virtueller Waren die Verfolgbarkeit nicht zwingend vorschreiben, sondern es als Alternative anbieten. Es würde dem Käufer die Wahl zwischen Kopierschutz mit gewissen Nutzungseinschränkungen und der völligen technischen Freiheit in der Nutzung bei gleichzeitiger Option der Verfolgbarkeit belassen. Somit hätte der Nutzer die Möglichkeit auch beim Kauf von Musik anonym zu bleiben.

DPE mit Kopierschutz könnte man mit Busfahren vergleichen. Man kommt hierbei auch von A nach B. Allerdings hat man dabei nicht mehr die Freiheit, einen Umweg zu fahren. Im Gegensatz dazu kann man natürlich auch nicht mehr die Straßenverkehrordnung verletzen und muss sich im Bus auch nicht ausweisen.

7.2 Erweiterung herkömmlicher DRM-Systeme durch LWDRM

Im Zentrum des LWDRM-Systems steht das Endgerät (vgl. Abbildung 7.2), welches einen DRM-Client besitzt, der wie bereits beim Referenz-System erläutert (vgl. Kapitel 4.4.2) verschlüsselte Nutzdaten und Lizenzen verwaltet. Darüber hinaus ist dieser DRM-Client für den LWDRM-spezifischen Signaturvorgang um eine Wasserzeicheneinbettung und ein Signatur-Modul erweitert. Bei diesem Signaturvorgang werden die Nutzdaten, soweit es die Lizenzen erlauben, entschlüsselt, so dass sie auf ein portables Endgerät ohne DRM-Client übertragen werden können.

7.2.1 DRM-Controller

Vorbedingung für die Signatur sind die in Schritt 1 (siehe Abbildung 7.2) vom Anbieter-Server gelieferten verschlüsselten Nutzdaten, die nur durch den DRM-Controller (vgl. Kapitel 4.4.2) bei Vorhandensein einer gültigen Lizenz entschlüsselt werden können. Eine unverschlüsselte Speicherung ist im Referenz-System nicht vorgesehen. Das Konzept des leichtgewichtigen DRM dagegen sieht explizit vor, dem Konsumenten zu erlauben, die Nutzdaten unverschlüsselt zu speichern, wenn er im Gegenzug dafür bereit ist, digital zu unterschreiben.

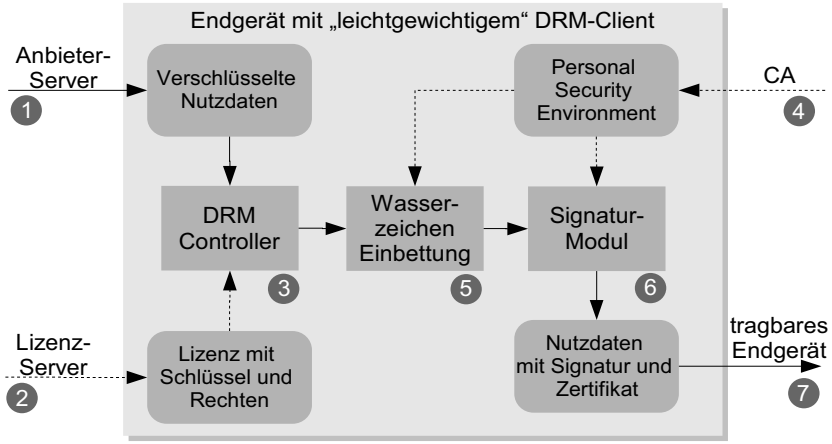
Damit auf die Nutzdaten zugegriffen werden kann, muss zuvor vom Lizenz-Server eine gültige Lizenz (in Schritt 2) angefordert worden sein. Mit dieser Lizenz kann der DRM-Controller in Schritt 3 die Entschlüsselung vornehmen. Nach Schritt 3 könnte

bereits die Wiedergabe über eine Ausgabeschnittstelle erfolgen. Ob die weiteren Schritte (4 bis 7) ablaufen können, hängt auch davon ab, ob in der in Schritt 3 geöffneten Rechtebeschreibung (Bestandteil der Lizenz) der Signaturvorgang als Nutzungsrecht notiert ist.

7.2.2 Zertifikat und Personal Security Environment

Das LWDRM-System unterscheidet sich primär vom DRM-Referenz-System aus Kapitel 4.4.2 durch den clientseitigen Einsatz der digitalen Signatur. Der dazu notwendige private RSA-Schlüssel muss der Nutzer sich zusammen mit dem ebenfalls notwendigen Zertifikat (vgl. Kapitel 4.3.3.4) in Schritt 4 von einer *Certification Authority* (CA) ausstellen lassen. Das Zertifikat wird zusammen mit dem privaten Schlüssel in der sogenannten *Personal Security Environment* (PSE) auf dem Endgerät gespeichert. Ein PSE kann ein in einer Smartcard eingebetteter Crypto-Chip, ein fest im Endgerät eingebauter Crypto-Chip (z. B. das *Trusted Platform Module* von Seite 52) oder eine passwortgeschützte PKCS#12-Datei [RSALabs 05] sein.

Abbildung 7.2
Ablauf beim leichtgewichtigen DRM im Endgerät



Das Zertifikat enthält neben dem öffentlichen Schlüssel nutzerspezifische Daten. Neben einer E-Mail-Adresse können der Name, die Adresse und weitere persönliche Daten enthalten sein. Diese Daten und der öffentliche Schlüssel wurden von der ausgebenden CA signiert. Die CA muss sich zuvor durch geeignete Maßnahmen vergewissert haben, dass die Nutzerdaten auch korrekt sind. Sind die Anforderungen an das Zertifikat sehr hoch, kann die CA auch verlangen, dass der Nutzer persönlich mit seinem Personalausweis erscheinen muss.

■ Pseudonyme Zertifikate und Gewaltenteilung

Da das Zertifikat in Schritt 6 an die Nutzdaten angefügt wird, würden die darin enthaltenen persönlichen Daten die Privatheit (*privacy*) des Nutzers unnötig stark verlet-

zen. Um eine Gewaltenteilung (*seperation of duty*) bei der Rückverfolgung illegaler Kopien zu gewährleisten, darf in der Datei keine Information einhalten sein, mit der eine beliebige Person die Rückverfolgung durchführen kann. Eine mögliche Lösung für diese Problem stellen pseudonyme Zertifikate dar. In diesen Zertifikaten ist nur ein Pseudonym enthalten, mit dem nur die ausstellende CA auf den Nutzer rückschließen kann. Damit erhält die CA eine bedeutsame und verantwortliche Stellung bei der Identifikation sich illegal verhaltender Nutzer (vgl. auch [GriAic 04]).

7.2.3 Wasserzeichen als zweite Verteidigungslinie

Die Signatur und das Zertifikat haben zwar den Vorteil, dass jeder – auch der Unterzeichner selbst – sofort erkennen kann, dass die Nutzdaten individuell markiert sind. Allerdings kann die Markierung auch leicht wieder entfernt werden. Um für diesen Fall eine zweite Verteidigungslinie zu besitzen, wird vor der Signatur in Schritt 5 ein Wasserzeichen in die Nutzdaten eingebettet. Bei den eingebetteten Daten handelt es sich um das Pseudonym aus dem Zertifikat. In Kapitel 4.3.2.2 wurde die dabei einsetzbare Wasserzeichentechnologie bereits als versteckter Informationskanal eingeführt. Ebenso wurde in Kapitel 4.3.3.3 das Verstecken von Transaktionsparameter mittels Wasserzeichen als etablierte Technologie bereits vorgestellt.

Die aktuell eingesetzten Wasserzeichenverfahren lassen ein Auslesen der eingebetteten Information für Dritte bewusst nicht zu. Zum einen sind die Extraktionsverfahren nicht öffentlich zugänglich. Zum anderen erfolgt bei der Einbettung noch eine zusätzliche Verschlüsselung. Dies ermöglicht es, dass verschiedene Firmen, die die gleiche Wasserzeichentechnologie einsetzen, nicht gegenseitig ihre Wasserzeichen auslesen können.

7.2.4 Signatur

Nachdem in Schritt 5 die unverschlüsselten Nutzdaten um ein Wasserzeichen angereichert wurden, erfolgt in Schritt 6 die eigentliche Signatur der Nutzdaten. Damit Dritte die Signatur, die mit dem privaten Schlüssel durchgeführt wurde verifizieren können, wird das Zertifikat mit dem öffentlichen Schlüssel den Nutzdaten beigefügt.

Der Konsument tritt durch diese Signatur quasi an die Stelle eines Herausgebers (vgl. Fred in Kapitel 4.3.3.2), der sein Werk signiert, um anderen nachzuweisen, dass er der Urheber ist. Der Konsument wird in diesem Fall natürlich nicht wirklich zum Herausgeber. Er ist aber Verursacher der Entschlüsselung, und damit verantwortlich für eine mögliche illegale Verbreitung. Das leichtgewichtige DRM verlagert die Verantwortung für ein legales Verhalten vom Anbieter auf den Nutzer.

■ Umgekehrte Interessenlage

Der entscheidende Unterschied zur digitalen Signatur aus Kapitel 4.3.3.2 ist, dass der signierende Konsument typischerweise kein Interesse hat, dass die Urheberschaft seiner Entschlüsselung für Dritte nachweisbar wird. Dieses Interesse haben nur die Instanzen, die illegale Kopien zurückverfolgen wollen.

Diese gegenüber der normalen digitalen Signatur umgedrehte Interessenlage macht das Signatur-Modul sowie die Wasserzeicheneinbettung in ähnlicher Weise zu einer sicherheitskritischen Komponente wie den DRM-Controller. Das Signatur-

Modul und die Wasserzeicheneinbettung dürfen nicht durch den Nutzer umprogrammiert werden können.

7.3 Abschließende Wertung

Bei den Arbeiten am leichtgewichtigen DRM hat sich herausgestellt, dass es leider nicht wirklich technologisch leichtgewichtig ist. Es sind lediglich die reinen Abspielendgeräte leichtgewichtig. Das Endgerät, auf dem die Signatur durch geführt wird (vgl. Abbildung 7.2) ist allerdings sogar deutlich komplexer als ein Endgerät mit „schwergewichtigem“ DRM. Auch auf Server-Seite werden mit der CA-Infrastruktur, die Pseudonyme verwalten muss, zusätzliche Komponenten benötigt.

Signcryption versus Kompatibilität

Im Mittelpunkt der Entwicklungen zu LWDRM [NeBrSi 02], [GriNüt 02c], [SiNeSp 03] stand die auch zum Patent eingereichte Idee [BrNeKuSiSp 02] der kombinierten Anwendung von Signatur und Verschlüsselung. Mit der Signatur wird zwar die Identität des Käufers mit der Datei verbunden, aber die zusätzliche Verschlüsselung sorgt dafür, dass die Signatur bei der Wiedergabe nicht ignoriert oder einfach abgeschnitten werden kann. Die Signatur sowie die Verschlüsselung der Nutzdaten erfolgen mit dem privaten Schlüssel des Nutzers. Der zur Entschlüsselung notwendige öffentliche Schlüssel ist im beigefügten Zertifikat enthalten. Daher muss das Zertifikat ausgewertet werden, um die Nutzdaten wiederzugeben. In [Zheng 97] wurde für diese ursprünglich sequentielle Anwendung der Signatur und Verschlüsselung ein effektiver Kombinationsalgorithmus, der Signcryption genannt wird, entwickelt.

Wenn man Vorteile (die Signatur kann nicht ignoriert werden) und Nachteile (das Format kann nicht mehr auf bestehenden Endgeräten abgespielt werden) der zusätzlichen Verschlüsselung gegeneinander abwägt, kommt man (der Autor) zum Schluss, dass sich ein „leichtgewichtiges“ DRM gegenüber einem „harten“ DRM nur dann durchsetzen kann, wenn die Kompatibilität mit bestehenden Endgeräten besser ist. Daher darf die Signatur und das Zertifikat die Nutzdaten nur im Rahmen der bestehenden Standards (bei LWDRM MPEG-1 oder MPEG-4) verändern. In [Hartmann 04] wurde eine Signatur für AAC (MPEG-4) umgesetzt.

Diese pragmatische Einschätzung, dass eine zusätzliche Verschlüsselung sich am Markt nicht durchsetzen würde, motivierte den Autor schließlich in der Darstellung das Gewicht auf die unverschlüsselte Variante des leichtgewichtigen DRM zu legen.

Legales File Sharing und B2B-Anwendungen

In [NütGri 03] wird gezeigt, wie man die nutzerseitige Signatur der Nutzdaten auch im Interesse des Nutzers anwenden kann. Das im Folgenden vorgestellte Anreizmodell des PotatoSystems ist ein Beispiel dafür, dass eine Personalisierung von Nutzdaten auch zum Nutzen des Konsumenten eingesetzt werden kann. Diese für den Nutzer positive Markierung muss daher auch nicht vor der Entfernung geschützt werden. Es reicht, wenn sie nicht gefälscht werden kann.

Ebenso sind bei B2B-Anwendungen, bei denen bspw. der Autor eines Werkes seine Urheberschaft in der Datei verankern möchte lohnende Anwendungsfelder, bei denen die Interessenlage (vgl. Seite 115) nicht mehr umgekehrt ist.

8. Kapitel

Das PotatoSystem – ein alternativer Ansatz

Das so genannte PotatoSystem® – der Name ist dem Erfindungsort gewidmet – ist nicht wie das LWDRM-System (vgl. Kapitel 7) nur ein technologisches Verfahren, sondern ein komplettes System für den Vertrieb virtueller Waren. Das PotatoSystem, welches nicht auf spezielle Dateiformate beschränkt ist, verfolgt einen vom klassischen DRM (vgl. Kapitel 4.4) und LWDRM abweichenden durch den Autor mitentwickelten Ansatz. Das PotatoSystem bietet weder eine Technologie, die es dem Anbieter wie beim LWDRM ermöglicht, eine illegale Weitergabe zu erkennen, noch ist es eine technische Vorrichtung, die es wie bei der GFP (vgl. Kapitel 6) ermöglichen würde, eine Weitergabe zu verhindern.

Das PotatoSystem verfolgt einen anderen Weg. Es versucht durch finanzielle Anreize, die Nutzer zum legalen Umgang mit virtuellen Gütern zu motivieren. Die zentrale Idee hinter dem System besagt, dass Käufer die eine virtuelle Ware gekauft haben, neben der virtuelle Ware auch das Weiterverkaufrecht für diese Ware erhalten.

Die Grundidee, die aus den Überlegungen zur Superdistribution und P2P entstammt, wurde durch die 4FO AG und das Fraunhofer IDMT als Client-Server-System umgesetzt. Mit Abschluss der vorliegenden Arbeit (Mai 2005) konnten bereits die allermeisten wünschenswerten Funktionen und Ergänzungen umgesetzt werden. Die Hauptfunktionen sind auch bereits kommerziell in der Anwendung. Eine Reihe weiterer Ergänzungen konnten allerdings noch nicht praktisch erprobt werden.

8.1 Ausgangslage für einen alternativen Ansatz

Die Ideen für das im Folgenden vorgestellte Konzept bzw. Verfahren entstammt Überlegungen, die sich mit dem Sinn und Zweck von DRM-Systemen befassen. Urheberrechtsverletzungen von Musikkonsumenten und die Gegenmaßnahmen der Musikindustrie bildeten den Ausgangspunkt der Diskussion.

8.1.1 Konflikt durch DRM-Systeme

Das unlizenzierte Weitergeben bzw. Veröffentlichen virtueller Waren bspw. über P2P-Netzwerke (vgl. Kapitel 4.2.3) wie KaZaA oder ähnliche Systeme untergräbt die traditionellen direkten Erlösmodelle (vgl. Kapitel 3.5) der Medienindustrie. Im Falle der Musikindustrie stellt sich sogar die Frage, ob es in Zukunft überhaupt noch eine Produktion geben wird, wenn diese nicht mehr in der Lage ist, Autoren, Komponisten und Interpreten zu bezahlen, da ihre Produkte keinen Marktwert mehr haben.

Als Gegenmaßnahme versuchen die Anbieter virtueller Waren die unkontrollierte Verbreitung zu verhindern. Dabei geraden sie allerdings in ein Dilemma: Sie wollen einerseits legalen Käufern die virtuellen Waren zugänglich machen, d. h. die zugehörigen Nutzdaten auf deren Endgeräte überspielen und damit in deren Einflussbereich übergeben. Andererseits möchten die Anbieter die Nutzdaten den Konsumenten nur eingeschränkt zur Verfügung stellen. Die Nutzer verzichten allerdings häufig darauf, sich derart einschränken zu lassen. [GriNüt 02a]

Die Musikindustrie reagiert auf diese Umgehungsreaktion der Konsumenten mit der Einführung eines Sicherheitskonzeptes, welches die Nutzer zum Gebrauch von Abspielgeräten zwingt, in denen die Verwendung der Nutzdaten technisch stärker kontrolliert wird. In den Kapiteln 4, 6 und 7 werden eine Reihe von solchen technischen Verfahren (DPE - *Digital Policy Enforcement*) beschrieben, die diese Kontrolle direkt oder indirekt ermöglichen.

Da die Nutzer es viele Jahre gewohnt waren, Musik und andere virtuelle Waren ungehindert zu kopieren, und sei es nur zum privaten Gebrauch, bringt die Einführung von strikten DPEs eine hohes Konfliktpotential in die Beziehung zwischen Anbieter und Konsument. Viele Nutzer sehen sich zu Unrecht kriminalisiert. Misstrauen ist allerdings auch für das Geschäftsmodell der Anbieter keine solide Basis.

8.1.2 Konfliktlösung

Strebt man eine Konfliktlösung an, kann verallgemeinert angenommen werden, dass der Nutzer virtueller Waren sich, wie von Spranger postuliert, als *homo oeconomicus* verhält: *„Der ökonomische Mensch im allgemeinsten Sinne ist also derjenige, der in allen Lebensbeziehungen den Nützlichkeitswert voranstellt. Alles wird für ihn zu Mitteln der Lebenserhaltung, des naturhaften Kampfes ums Dasein und der angenehmen Lebensgestaltung.“* ([Spranger 22])

Man kann also davon ausgehen, dass der Konsument versucht, möglichst viel im Tausch gegen möglichst wenig zu bekommen. Es ergeben sich daraus für die Anbieter mehrere mögliche Ansätze den zuvor beschriebenen Konflikt zu lösen:

Einsatz von DRM und nutzungsunabhängige Erlösmodelle

Im Kapitel 7.1 wurde bereits dargelegt, dass der Gebrauchswert der Nutzdaten aus Sicht vieler Konsumenten sinkt, wenn diese durch DRM (bzw. strikte DPE) in ihrer Nutzung eingeschränkt sind. Der Anbieter kann diesen Nachteil ausgleichen indem er bspw. für Nutzer, die relativ viele virtuelle Waren konsumieren möchten, nutzungsunabhängige Erlösmodelle anbietet. Hierbei erhält der Konsument gegen ein monatliches Entgelt (Abonnement) Zugriff auf das gesamte Angebot des Händlers (vgl. Kapitel 3.5). Diesen kurzfristigen Vorteil erkauft sich der Nutzer allerdings durch den Nachteil, dass nach dem Kündigen des Abonnements der Zugriff auf die Nutzdaten nicht mehr möglich ist. Der Windows-Media Rights Manager in der Version 10 (vgl. Kapitel 4.4.5) ermöglicht bspw. der Firma Napster dieses Geschäftsmodell.

DRM in Kombination mit zusätzlichem Service und Mehrwert

Möchte der Anbieter nutzungsabhängige Erlösmodelle wie Pay-per-Track in Kombination mit DRM anbieten, so kann er nur im geringen Maße über den Preis den Kunden für sein Angebot gewinnen. Er muss den Verlust an Gebrauchswert, der durch DRM entsteht, über zusätzliche Dienste und andere ergänzenden Leistungen ausgleichen. Die Firma Apple geht mit dem iTunes Musicstore diesen Weg. Neben einem reichhaltigen Angebot und einer sehr komfortablen Nutzerführung gewinnt Apple seine Nutzer primär über seine populären tragbaren Endgeräte (iPod). Der Apple iPod [iPod 05] ermöglicht eine mobile Form des Musikkonsums, der bei der Einführung des iPods noch ohne Konkurrenz war.

Verzicht auf DRM

Natürlich sind Nutzdaten in Standardformaten ohne DRM für den Konsumenten am attraktivsten. Es gibt dann keine Probleme, wenn der Nutzer diese legal erworbenen Nutzdaten auf eine anderes Endgerät übertragen will. Der Nutzer könnte sich allerdings vor dem Kauf ungeschützter Nutzdaten fragen, warum er für diese bezahlen soll, wenn er dieselben Inhalte über andere Kanäle auch kostenlos bekommen kann (vgl. Free-Rider- bzw. Trittbrettfahrer-Problem [WikiFreeRider 05] und öffentliche Güter in Kapitel 3.2). Hier muss jedoch bemerkt werden, dass DRM nicht sicher verhindern kann, dass Kopien ohne DRM kostenlos verteilt werden. Es reicht ein Hacker, der den DRM-Schutz umgeht und die ungeschützte Datei über illegale P2P-Systeme verbreitet. Bei dem aktuellen Stand der PC-Technik findet sich dieser eine Hacker immer. Meistens muss der DRM-Schutz nicht einmal technisch umgangen werden, da viele Systeme (z. B. der Windows Media Rights Manager, vgl. Kapitel 4.4.5) einen Export auf ungeschützte Audio-CDs erlauben.

Ohne DRM mit zusätzlichen Service und Mehrwert

Das Free-Rider-Problem kann mit zusätzlichen Diensten und Mehrwert exklusiv für registrierte Käufer angegangen werden. Wenn allerdings die Konsumenten kein Interesse an den zusätzlichen Diensten haben, wird dieser Ansatz scheitern. Wenn der Anbieter nicht primär neue und wenig verbreitete virtuelle Waren anbietet, so muss er auf die Attraktivität der zusätzlichen Dienste vertrauen. Oft sind die zusätzlichen Dienste an ein Netzwerk (bspw. eine Nutzer-Community) gebunden, an dem nur registrierte, bezahlende Nutzer teilnehmen können.

8.2 Käufer zu Händlern machen

Die Netzwerke und Communities, welche die Konsumenten virtueller Güter bisher am meisten begeistert haben, sind die illegalen P2P-Netzwerke. Je mehr Nutzer in diesen Netzwerken Inhalte öffentlich zugänglich machen, umso attraktiver werden diese für die teilnehmenden Nutzer (Netzwerkeffekt).

Diese P2P-Systeme zu legalisieren, und damit den Rechteinhabern Erlöse zu ermöglichen, ist realistisch betrachtet mit üblichen Erlösmodellen kaum möglich. Wer für den Download eines Songs nutzungsabhängig bezahlt, kann verlangen, dass dieser vom Server des Anbieters zuverlässig bereit gestellt wird. Für den Zugang zu P2P-Systemen eine monatliche Pauschalgebühr zu erheben wäre denkbar. Aber warum soll man für einen Dienst auch noch bezahlen, bei dem man für andere den eigenen Rechner laufen lassen muss? Die Konsumenten gleichzeitig als Mitarbeiter und als Erlösquelle zu nutzen, widerspricht sich. Diesen Widerspruch können allerdings Systeme beseitigen, die neuartige Geschäftsmodelle umsetzen, bei denen der Nutzer für seine erfolgreiche vertriebliche Mitarbeit belohnt wird. Diese Geschäftsmodelle müssen nicht auf P2P-Netzwerke beschränkt bleiben. Auch bewährte Client-Server-Architekturen können von der Peer-to-Peer-Vermittlung profitieren. Diese Form der Verkaufsförderung durch die Belohnung eines empfehlenden oder vermittelten Nutzers, wird Affiliated-Marketing genannt (vgl. [Krauß 02] Seite 18 und [Emer 04]). Im Unterschied zur Bannerwerbung bei der schon der Klick auf das Banner einen Erlös liefert, wird bei Affiliated-Marketing der Werbende nur dann entlohnt, wenn die Werbung wirklich zu einem Kauf führt.

Der Kaufanreiz für virtuelle Güter ohne DRM lässt sich nun dadurch erhöhen, dass nur registrierte Käufer das Recht zum Mitverdienst erhalten. Dieses Prinzip ist zwar auch **mit** DRM umsetzbar, allerdings gelangt man auf diese Weise wieder in die beschriebene Konfliktsituation. Dies ist in diesem Fall möglicherweise besonders fatal, weil man doch gerade die Nutzer für die Position des Anbieters gewinnen möchte und daher besonders daran interessiert ist, dass die Interessen der Käufer mit denen der Anbieter übereinstimmen. Der Anbieter erreicht sein Ziel nur dann, wenn möglichste viele Käufer, im eigenen und im Interesse des Anbieters handelnd, erfolgreiche Weiterverkäufer werden.

8.2.1 Die Grundidee des PotatoSystems

In [GriNüt 02a] und [GriNüt 02b] wurde die Grundidee des PotatoSystems nach erfolgter Patentanmeldung [SpGrNüLa 02] erstmals publiziert: *Nutzer, die für eine virtuelle Ware bezahlen, erhalten vom Anbieter das Recht die virtuelle Ware weiterzuverkaufen und dabei mitzuverdienen.*

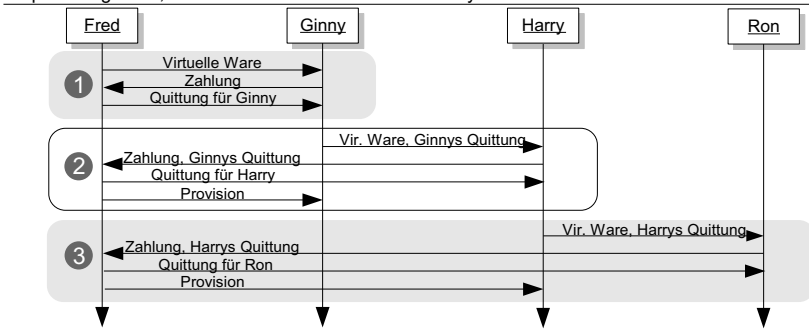
Abbildung 8.1 zeigt ein Szenario mit drei Käufern (Ginny, Harry und Ron) und einem Anbieter (Fred).

- In Schritt 1 erhält Ginny die virtuelle Ware vom Erst- oder Originalanbieter (Fred). In der Grundidee ist es prinzipiell egal, über welche Wege die Nutzdaten zum Käufer kommen. Der Käufer muss nur wissen, an welchen Anbieter er sich für die Zahlung wenden muss. Die Zahlung wird vom Anbieter durch eine Quittung bestätigt. In der Quittung werden die virtuelle Ware und der Käufer (in diesem Fall Ginny) belegt.
- In Schritt 2 gelangt die virtuelle Ware in Verbindung mit der Quittung von Ginny zu Harry. Ginny überzeugt Harry, diese beim Anbieter zu bezahlen. Bei der Bezah-

lung legt Harry Ginnys Quittung vor. Ist die Quittung gültig, erhält Harry eine neue Quittung und Ginny erhält einen Teil des Kaufpreise als Provision gutgeschrieben bzw. ausgezahlt.

- Schritt 3 zeigt schließlich, wie Harry es Ginny gleich tut und einen weiteren neuen Käufer (Ron) für die virtuelle Ware gewinnt.

Abbildung 8.1
Sequenzdiagramm, welches die Grundidee des PotatoSystems beschreibt



Die Kette kann beliebig fortgesetzt werden bzw. sich zu einem Baum ausweiten. Für jeden Weiterverkauf wird einen neue gültige Quittung erstellt, mit der der Käufer zum provisionsberechtigten Weiterverkäufer wird. Genau genommen kann beim PotatoSystem nicht von *Weiter*verkaufen gesprochen werden, da die Ware nur als Kopie vom Weiterverkäufer weiterverteilt wird. In diesem Sinne kann Ginny (und jeder weitere Kunde in der Weiterverkaufskette) seine virtuelle Ware beliebig oft (in Kopie) weiterverkaufen. Jede Kopie ist so gut wie ihr Original.

8.2.2 Die Quittung wird mit den Nutzdaten verbunden

Tabelle 8.1
Parameter in der XML-Registrierungsquittung (CREATOR.XML)

Parameter-Name	Erläuterung
createdate	Datum ersten Bereitstellung der Datei (den Nutzdaten)
url	Adresse des zentralen Accounting-Servers
author	Informationen zum Urheber der Datei
price	Preis und Provisionsmodell der Datei
file	Weitere Metadaten zur Datei

Bei der Grundidee des PotatoSystems liegt der Fokus nicht auf der Verteilung der Nutzdaten, sondern auf der Behandlung der Quittungen. Diese werden von einer zentralen Stelle (im Weiteren als Accounting-Server bezeichnet) ausgegeben. Der Accounting-Server nimmt auch die Zahlungen entgegen und verteilt die Provisionen.

In [GriNüt 02b] wird ein Konzept beschrieben, bei dem eine für jeden Nutzer überprüfbare Quittung zusammen mit der Nutzdaten verteilt wird. Diese Quittung besteht

aus mehreren XML-Dateien, die durch den Accounting-Server digital signiert wurden. Eine erste XML-Datei (*CREATOR.XML*, vgl. Tabelle 8.1) wird bei der Registrierung einer virtuellen Ware am Accounting-Server angefügt. Bei jeder Bezahlung eine weitere XML-Datei (*REDIST01.XML*, *REDIST02.XML* usw., vgl. Tabelle 8.2). Je nachdem, ob man dem potentiellen Käufer, die ganze Weiterverkaufskette (von Käufer Ginny bis Käufer Ron) mitteilen will oder ob nur das Ende der Kette mit dem letzten oder den *n* letzten Käufern sichtbar sein soll, sind unterschiedlich viele XML-Dateien angehängt.

Tabelle 8.2
Parameter in der XML-Kaufquittung (REDISTxx.XML)

Parameter-Name	Erläuterung
paydate	Datum der Bezahlung
generation	Stufe in der Weiterverkaufskette
url	Adresse des zentralen Accounting-Servers
actualredister	Angaben zum Käufer

Um die Nutzdaten und die XML-Quittungen sowie die Signaturen gemeinsam in einer Datei zu transportieren, bietet sich das JAR-Format (Java-Archive) an. Alternativ könnte man auf das bei OMA (vgl. Kapitel 4.4.4) verwendete MIME-Format zurückgreifen. Das JAR-Archive dient der Paketierung von Bibliotheken und Anwendungen in Java. Eine JAR-Datei ist ein ZIP-Archiv mit einer genau festgelegten Verzeichnisstruktur.

Abbildung 8.2
Verknüpfung von Nutzdaten, Quittungen und Signaturen in einer JAR-Datei

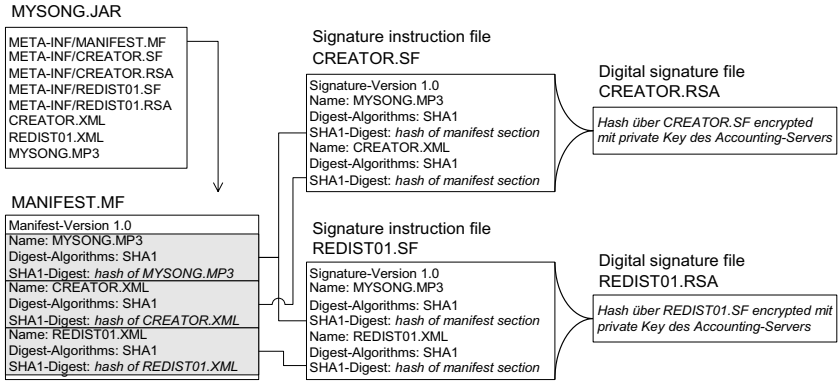


Abbildung 8.2 zeigt den Aufbau eines JAR-ähnlichen Archivs mit dem Namen *MYSONG.JAR*. Wie alle JAR-Dateien, enthält dieses Archiv ein Unterverzeichnis *META-INF*, in dem sich die Datei *MANIFEST.MF* befindet. Hier werden alle Dateien zusammen mit ihrem Hash-Wert aufgelistet. Im Beispiel befinden sich die Nutzdaten (*MYSONG.MP3*) und zwei Quittungen (*CREATOR.XML* und *REDIST01.XML*) im Archiv.

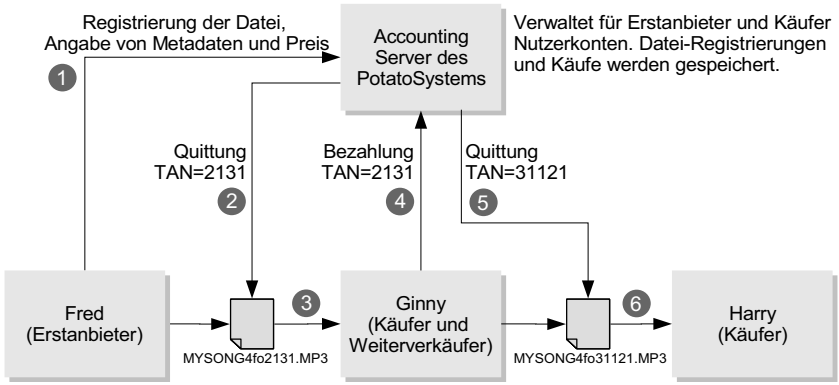
Die Definition des JAR-Formates [JAR 04] umfasst auch die Möglichkeit, digitale Signaturen beizufügen. Eine Signatur wird im Verzeichnis META-INF gespeichert. Die *Signature Instruction Files* (*CREATOR.SF* und *REDIST01.SF* in Abbildung 8.2) geben an, über welche Dateien die Signaturen erfolgten. Die eigentlichen Signaturen finden sich in den Dateien *CREATOR.RSA* und *REDIST01.RSA*. Die Signatur erfolgt, indem der Hash über die SF-Dateien mit dem privaten Schlüssel (RSA in diesem Fall) des Unterzeichners (Accounting-Server) verschlüsselt wird.

Vorteil des gezeigten Ansatzes ist es, dass potentielle Käufer, die die Nutzdaten in einem JAR-Archive erhalten, die enthaltene Quittung vor der Zahlung selbst ohne Online-Verbindung verifizieren können. Die enthaltenen XML-Dateien ermöglichen es, dem potentiellen Käufer offline Informationen über den Verkäufer und die Provisionen zukommen zulassen.

8.2.3 Transaktionsnummern (TAN) als Quittungsersatz

Da der Accounting-Server auch Kopien der ausgegebenen Quittungen speichert, ist es nicht zwingend notwendig, den kompletten Inhalt der Quittungen zusammen mit den Nutzdaten zu versenden. Es genügt eine Referenz auf die am Server gespeicherte Quittung. In [GriNüt 02d] wird das Konzept der Transaktionsnummern (TAN) eingeführt. Die TAN ist für den zentralen Accounting-Server eine eindeutige Referenz auf einen Kaufvorgang oder eine Dateiregistrierung. Der Accounting-Server vergibt diese systemweit eindeutigen Nummern für eine Content-Registrierung und einen Content-Kauf. Zu jeder TAN kann der Accounting-Server feststellen, welche Nutzdaten durch welchen Anbieter im System registriert wurden bzw. welche Nutzdaten durch welchen Käufer erworben wurden.

Abbildung 8.3
Transaktionsnummern (TAN) als Quittung für Registrierung und Kauf



Damit die TAN die Funktion der Quittung aus Abbildung 8.2 erfüllen kann, muss sie zusammen mit den jeweiligen Nutzdaten transferiert werden können. Liegen die Nutzdaten in unterschiedlichen Formaten vor, gibt es nur eingeschränkte Möglichkeiten, die TAN mit den Nutzdaten zu verknüpfen, ohne das Format der Nutzdaten da-

bei zu verändern. In [GriNüt 02d] und [Krauß 02] wurde als Kompromiss die Änderung der Dateinamen vorgeschlagen.

Abbildung 8.3 zeigt, wie Fred (der im PotatoSystem als Erstanbieter bezeichnet wird, vgl Seite 128), der die entsprechenden Verwertungsrechte an der Datei *MY-SONG.MP3* besitzen muss, in Schritt 1 die Datei beim Accounting-Server (AS) registriert. Dabei übermittelt er diverse Metadaten (bei Musik gehört bspw. der Name des Interpreten und der Titel dazu), den gewünschten Preis und einen Hash (bspw. SHA-1) über die Datei. Der AS speichert die übermittelten Daten und quittiert dies in Schritt 2 mit der Erzeugung einer neuen TAN. Diese TAN ist der Beleg für eine erfolgreiche Registrierung.

Jede TAN, die der AS ausgibt, folgt der gleichen Syntax. Sie beginnt mit einer Kundennummer (hier z. B. 213) gefolgt von einer kundenspezifischen Transaktionsnummer. Die erste Ziffer der Kundennummer (hier 2) legt fest, wie viele Ziffern folgen. Die kundenspezifische Transaktionsnummer ist 1, da es Freds erste Transaktion ist [Nützel 03a]. Die TAN wird auf den Rechner des Erstanbieters Fred in den Dateinamen eingefügt. In [Hasselbach 02] wird ein signiertes Java-Applet erstellt, welches an den AS den SHA1-Hash über die Datei und weitere Metadaten sendet und die zurückgesendete TAN automatisch in den Dateinamen einfügt. Der folgende EBNF-Ausdruck beschreibt die dabei benutzte Vorschrift für die Umbenennung:

```
<Alter_Name> ::= <root> <dot> <extension>
<Neuer_Name> ::= <root> <delimiter> <TAN> <dot> <extension>
<dot> ::= '.'
<delimiter> ::= '4fo'
```

In Schritt 3 gelangt die Datei mit dem geänderten Namen auf den Rechner von Ginny (oder eines anderen Interessenten). Ohne eine Zusatzinformation von Fred weiß Ginny allerdings nicht, wie sie Weiterverkäufer werden kann. Mittels eines zweiten Applets [Hasselbach 02] wird in Schritt 4 die TAN aus dem Namen extrahiert und an den AS gesendet. Damit Ginny auch die Gewissheit hat, dass die TAN sich auch an der richtigen Datei befindet, ermittelt das Applet wiederum den Hash der Datei und sendet diesen ebenfalls an den AS. Der AS zeigt darauf die bei der Registrierung gespeicherten Metadaten und den Preis an. Führt Ginny die Zahlung aus und registriert sich auf dem AS, erhält sie das Weitervertriebsrecht, welches in Schritt 5 durch eine neue TAN quittiert wird. Die TAN wird ebenfalls durch das Applet in den Dateinamen eingefügt. Ginny gibt in Schritt 6 die Datei an einen nächsten Nutzer (Harry) weiter.

Obwohl der Dateiname leicht geändert werden kann, stellt dies kein sicherheitskritisches Problem dar. Die Verknüpfung von TAN und Dateiname ist beim AS fälschungssicher hinterlegt. Die im Dateinamen eingefügte TAN hat lediglich informativen Charakter. Weder Käufer noch Weiterverkäufer können sich durch Veränderung der TAN einen Vorteil erschleichen.

8.2.4 Schutz gegen unerlaubte Registrierung

Über den in Schritt 1 übermittelten Hash kann der AS feststellen, ob die Datei, die der Konsument vorliegen hat, auch diejenige ist, die vom Anbieter registriert wurde. Ebenso kann in Schritt 1 festgestellt werden, ob die identische Datei bereits durch einen anderen Anbieter registriert wurde. Hash-Verfahren sind allerdings kein wirksamer Schutz gegen den Versuch fremde Musik als die eigene auszugeben. Erst der Einsatz von Audio-Fingerprinting-Technologien wie z. B. Audio-ID [HerCre 04] ist es

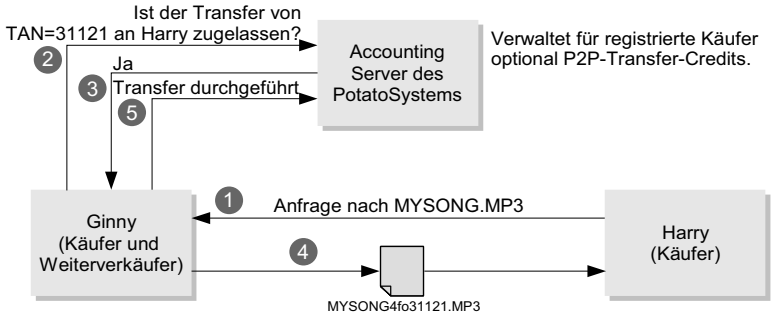
möglich, Klangähnlichkeiten festzustellen. Ein Audio-ID-Fingerprint ist eine Exzerpt von wenigen Kilobytes, welches eine Musikaufnahme repräsentiert. Mittels dieser Fingerprint-Dateien wäre es dem AS möglich, verschiedene Musikaufnahmen, die in sehr unterschiedlicher Qualität vorliegen, dem selben Musikstück zuzuordnen. Es lässt sich für Musik, die auf keinen Fall über das PotatoSystem vertrieben werden darf, auch eine Negativliste (*black list*) aufbauen. Wird bei der Registrierung ein Fingerabdruck aus dieser Liste (bzw. Datenbank) gefunden, so wird die Registrierung abgewiesen.

8.2.5 Zusätzliche Anforderungen im P2P-Umfeld

In der Grundidee des PotatoSystems werden die Nutzdaten den potentiellen Kaufinteressenten von den Weiterverkäufern gezielt (peer-to-peer) zugesendet bzw. zugänglich gemacht. Den Empfängern der Nutzdaten steht es hierbei frei, diese auch ohne Bezahlung zu konsumieren. Zwei Aspekte führten dazu, dass dieser Ansatz in dieser Form nicht kommerziell umgesetzt wurde:

- Musik, die von Mitgliedern der GEMA [GEMA 05] komponiert bzw. getextet wurde, darf nicht in Dateiform kostenlos verteilt werden. Denn auch für jede kostenlos verteilte Kopie muss eine Pauschale an die GEMA abgeführt werden. Dies macht die Grundidee nicht kalkulierbar, da nicht abgeschätzt werden kann, wie viele kostenlose Kopien benötigt werden, um einen Kauf zu veranlassen.
- Als Betreiber des Accounting-Servers könnte man sich zwar auf den Standpunkt stellen, dass die kostenlose Verteilung der Nutzdaten außerhalb des Systems stattfindet. Allerdings würde dann das System darauf aufbauen, dass die Nutzer das Urheberrecht verletzen bzw. sich in eine rechtliche Grauzone begeben.

Abbildung 8.4
Zentral limitierter Peer-to-peer-Transfer



Dirk Michael erstellte in [Michael 03] auf der Basis von JXTA (vgl. Seite 44) einen P2P-Client für das PotatoSystem. Diese Applikation wurde P2P-Messenger genannt, da er auch einen einfachen Chat ermöglicht. In diesem als signiertes Java-Applet realisierten Prototypen, können von registrierten Nutzern nur die Dateien transferiert werden, die auch im Accounting-Server registriert sind.

Um die zuvor beschriebenen Probleme anzugehen, wurden in [Nützel 03a] und [Biedermann 03] Modelle für eine zentral gesteuerte Beschränkung der P2P-Trans-

fermöglichkeiten diskutiert. Harry (ein potentieller Käufer in Abbildung 8.4) kann nur in einem limitierten Umfang von anderen Nutzern (wie bspw. Ginny) zur Verfügung gestellte Dateien kostenlos beziehen. Der Gesamtwert der transferierbaren Dateien richtet sich dabei nach dem Gesamtwert der bereits von Harry getätigten Käufe. Bei einem Transferwert (P2P-Credits), der bspw. beim 10-fachen der getätigten Käufe liegt, kann Harry, der bisher einen Song im Wert von einem Euro gekauft hat, anschließend Dateien im Gesamtwert von zehn Euro kostenfrei zur Probe peer-to-peer beziehen. Vor jedem P2P-Transfer wird deshalb (hier von Ginny) geprüft, ob die zentral auf dem AS verwalteten P2P-Credits ausreichend sind (vgl. Schritt 2 und 3 in Abbildung 8.4). Wurde schließlich der Transfer in Schritt 4 erfolgreich durchgeführt, meldet dies der P2P-Client in Schritt 5 an den AS zurück. Als Folge von Schritt 5 verringert der AS die Transfer-Credits von Harry.

Das in Abbildung 8.4 beschriebene Protokoll bringt für den AS einen hohen zusätzlichen Kommunikations- und Verwaltungsaufwand. Dieser zusätzliche Aufwand kann deutlich reduziert werden, wenn Ginny eine Liste der Nutzer führt, die auf Ihre Dateien zugreifen dürfen (w*hite list*). Parallel dazu vermerkt Ginny in einer Log-Datei die erfolgreichen Zugriffe dieser Nutzer. Ebenso werden auch die Anfragen von Nutzern, die noch nicht auf ihrer Positivliste stehen in dieser Log-Datei festgehalten. Die Log-Datei wird sporadisch an den AS gesendet. Der AS aktualisiert dabei aufgrund der zentral gespeicherten P2P-Credits Ginnys Positivliste. Nutzer, die auf der Positivliste stehen werden gelöscht. Neue Nutzer, deren Anfragen in der Log-Datei vermerkt wurden, werden in die Liste aufgenommen. Auf diese Weise wird effektiv verhindert, dass Trittbrettfahrer (vgl. Seite 119) unlimitiert kostenlose P2P-Transfers durchführen.

8.2.6 Client-Server-Variante

Aufgrund der beschriebenen Schwierigkeiten im P2P-Umfeld wurde in [Nützel 03a] eine Client-Server-Variante der PotatoSystem-Grundidee vorgestellt, die auch die Anforderungen der GEMA berücksichtige. Hierbei werden die Nutzdaten nicht peer-to-peer von Käufer zu Käufer verteilt. Die Erstanbieter und Weiterverkäufer verteilen so genannte Verkaufslinks, die auf den Server des PotatoSystems verweisen und als GET-Parameter eine TAN enthalten. Die Einfügung der TAN in den Dateinamen ist in diesem Fall nicht mehr zwingend notwendig. Die unverschlüsselten Nutzdaten werden dem Käufer erst nach der Bezahlung über einen Client-Server-Download (analog dem Paybest-Proxy, vgl. Seite 90) zugänglich gemacht. Die Umsetzung dieser Client-Server-Variante wird in Kapitel 8.3 beschrieben.

Damit die Musik auch schon vor der Bezahlung gehört und getestet werden kann, wird parallel zum Verkaufslink ein Vorhörlink angeboten. Über den Vorhörlink wird ein maximal 45 Sekunden langer Ausschnitt auf das Endgerät gestreamt. Für diese gestreamten Ausschnitte verlangt die GEMA keine Abgabe. Das Anbieten einer Vorhörmöglichkeit wird an die GEMA pauschal abgegolten.

Vorhörmöglichkeiten nicht über Streams vom Server anzubieten, sondern über spezielle P2P-verteilte Preview-Dateien wird in [AiPuHa 04] vorgeschlagen.

8.2.7 Superdistribution mit DRM

Das Prinzip, Käufer zu Weiterverkäufern zu machen, kann auch in Verbindung mit DRM umgesetzt werden. Aufgrund von den bereits dargelegten Überlegungen (vgl. Seite 8.1.1) verzichtet das PotatoSystem bewusst auf DRM. Werden wie bei dem

System Weedshare [Weedshare 05], welches die Käufer ebenfalls zu Vertriebspartnern macht, DRM-geschützte Windows-Media-Dateien durch die Nutzer verteilt, so spricht man von Superdistribution (vgl. Seite 31). Bei Superdistribution werden die verschlüsselten Nutzdaten primär durch die Konsumenten verteilt. Die zum Abspielen benötigte Lizenz erhält der Konsument nach der Bezahlung vom offiziellen Anbieter.

Im Falle von Weedshare, welches nur mit WMRM arbeitet, steht der Lizenz-Server zusammen mit einer Käuferkennung im unverschlüsselten Header der Windows-Media-Datei. Da der serverseitig signierte Header einer WMA-Datei nicht auf dem Endgerät verändert werden kann, muss der Käufer die Datei erneut vom Server herunter laden, bevor er sie an potentielle neue Käufer weiterschicken kann. Beim OMA DRM 2.0 [OMA2 06] kann das Endgerät am Ende der Datei ein TAN verändern.

8.3 Umsetzung des PotatoSystems

Das PotatoSystem [Potato 05] ging als Client-Server-System im April 2004 mit Zustimmung der GEMA in den kommerziellen Betrieb über. Das PotatoSystem konzentriert sich dabei auf den Verkauf von Dateien im MP3-Format, obwohl es nicht auf dieses Format beschränkt ist. Hier soll nun die Umsetzung des PotatoSystems näher beleuchtet werden. Es werden zuerst die zentralen Prinzipien beschrieben. In Kapitel 8.4 werden erweiterte Funktionen und Dienste, die nicht zum unverzichtbaren Kern des PotatoSystems gehören, beschrieben. Zum Teil sind diese Funktionen beim Abschluss dieser Arbeit im Mai 2005 noch nicht in die Praxis überführt. Die aktuellen Forschungen gelten der Übertragung des PotatoSystems in den mobilen Anwendungskontekt. Dies wird abschließend in Kapitel 8.5 kurz skizziert.

Bei den folgenden Darstellungen werden Konzepte und Schnittstellen, die für Einbettung des Systems in verschiedene Anwendungskontexte wichtig sind beschrieben.

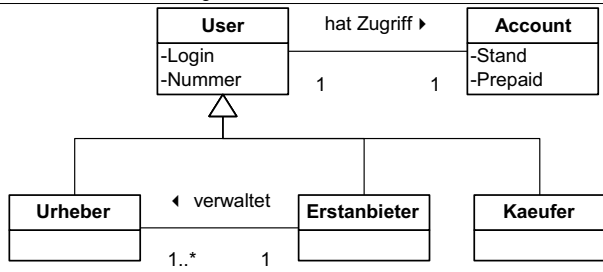
8.3.1 Akteure und ihre Rollen im PotatoSystem

Die Teilnehmer des PotatoSystem nehmen verschiedene Rollen ein. Im Weiteren wird auf diese Rollen Bezug genommen. Bestimmte Aspekte werden allerdings erst im weiteren Fortgang der Arbeit verdeutlicht.

- Das **PotatoSystem** positioniert sich selbst als ein zentraler Verwalter und Dienstleister, der zwischen den Erstanbietern (vgl. Seite 128) mit ihren Urhebern und den Käufern vermittelt. Das PotatoSystem verwaltet für diese Akteure (*User*) Accounts (vgl. Abbildung 8.15). Die User im PotatoSystem werden entweder über ihren selbst gewählten Login-Namen oder ihre zugewiesene Kundennummer (*Nummer*) identifiziert. Alle User haben Zugriff auf ihren Account, in dem erwirtschaftete Umsätze (*Stand*) und vorausbezahlte Beträge (*Prepaid*) getrennt gespeichert werden. Das PotatoSystem verzichtet bewusst darauf, die Rolle eines zentralen Musikportals einzunehmen. Das PotatoSystem tritt auch gegenüber den Web-Seiten der Erstanbietern und Weiterverkäufer in den Hintergrund. Es versteht sich nicht als Download-Portal, das in Konkurrenz zu den Weiterverkäufern agiert, sondern als Dienstleister, wie bspw. die Bezahlsysteme PayPal und Firstgate (vgl. Kapitel 5.3). Der Betreiber des PotatoSystems ist die 4FO AG [4FO 05].

- **Bezahlsysteme** haben im PotatoSystem die Aufgabe, Zahlungen der Konsumenten im Namen der 4FO AG entgegenzunehmen. Die 4FO AG greift hierbei auf die Systeme von Paybest [Paybest 05] (vgl. Kapitel 5.4) zurück.
- Urheberrechtsgesellschaften wie die **GEMA** [GEMA 05] vertreten die Komponisten und Texter von musikalischen Werken. Das PotatoSystem vergütet die GEMA direkt, indem nutzungsabhängige Gebühren an die GEMA abgeführt werden.

Abbildung 8.5
Vereinfachtes statisches Klassendiagramm zu den verschiedene Rollen



- **Erstanbieter** sind diejenigen Personen bzw. Firmen, die die virtuellen Waren im PotatoSystem registrieren. Erstanbieter müssen die Rechte für den Vertrieb der virtuellen Waren im Internet besitzen. Da das PotatoSystem zwar die Verkäufe vermittelt, aber die Nutzdaten nicht selbst vorhält (hostet), müssen die Erstanbieter die Dateien auf ihren eigenen Servern bereitstellen (vgl. Abbildung 8.10). Umsätze der Erstanbieter werden in deren Accounts (*Stand*) verwaltet. Erstanbieter können auch auf die ihnen untergeordneten Urheber-Accounts, die sie selbst angelegt haben, zugreifen. Erstanbieter können selbst Käufe tätigen und somit auch fremde Inhalte weiterverkaufen.
- Künstler, Interpreten bzw. **Urheber** spielen eine eigene Rolle im PotatoSystem. Virtuelle Waren – speziell Musik – werden nicht nur im PotatoSystem nach Interpreten sortiert verwaltet. Erstanbieter erstellen für die Registrierung von Inhalten so genannte Urheber-Accounts, die im Falle von Musik speziellen Interpreten oder Bands zugeordnet sind. Der Urheber im PotatoSystem ist allerdings nicht mit dem Texter oder Komponisten im Sinne der GEMA gleichzusetzen. Dem Erstanbieter ist es beim Anlegen von Urheber-Accounts freigestellt, die Zugangsdaten zu den untergeordneten Urheber-Accounts den Urhebern auch selbst zugänglich zu machen. Sind die Urheber wie bspw. eine Band selbst der Erstanbieter, so verwaltet die Band einen Erstanbieter-Account und einen untergeordneten Urheber-Account. Mit einem Urheber-Account können keine Käufe und Weiterverkäufe getätigt werden.
- **Labels** sind im PotatoSystem Erstanbieter. Labels nehmen in der Regel alle Rechte mehrerer Urheber direkt in Anspruch. Typischerweise verwalten sie auch selbst die Accounts ihrer Urheber.
- Jeder **Käufer**, der sich im PotatoSystem registriert, erhält einen Käufer-Account. Mit einem Käufer-Account wird er im PotatoSystem automatisch zum **Weiterverkäufer**.

- **Professionelle Weiterverkäufer** sind Personen oder Firmen, die im großen Umfang virtuelle Waren, die im PotatoSystem registriert sind, als Weiterverkäufer anbieten. Auch professionelle Weiterverkäufer können erst mitverdienen, wenn sie die virtuelle Ware zuvor gekauft haben (vgl. Kapitel 8.4.1).
- **Portale** sind Erstanbieter mit erweiterten Rechten, die ein eigenes Download-Portal betreiben. Portale können über die extern zugängliche Web-Service-Schnittstelle (vgl. Kapitel 8.4.3) Inhalte direkt von ihrem Server aus im PotatoSystem registrieren.

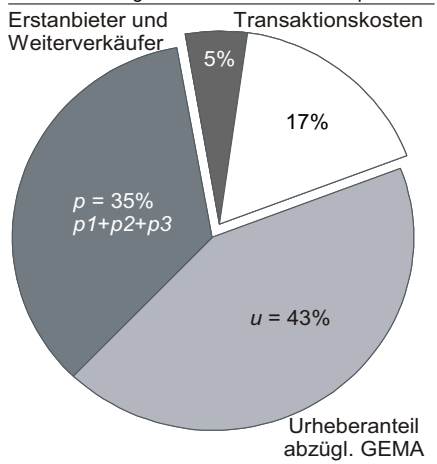
8.3.2 Preis- und Provisionsmodell

In [Biedermann 03] wurden unterschiedliche Preis- und Provisionsmodelle für das PotatoSystem gegenübergestellt. Bei ihrer endgültigen Festlegung wurde besonderer Wert auf einfache Kommunizierbarkeit gelegt. Erstanbieter, Urheber und Weiterverkäufer sollen sich möglichst einfach ihre potentiellen Umsätze ausrechnen können.

Preise, Rabatte und Kostenstruktur

Der Erstanbieter legt für die Dateien, die er registriert, den Verkaufspreis inkl. gesetzlicher Umsatzsteuer fest. Dieser nominelle Preis P_{nom} gilt global für alle Weiterverkäufer. Alternative Überlegungen, den Preis bspw. entlang der Weiterverkäufer-Kette (*Downline*) fallen zu lassen, wurden wegen mangelnder Transparenz verworfen. Auch dem Weiterverkäufer einen Spielraum bei der Preisgestaltung einzuräumen, wurde nicht umgesetzt. Das PotatoSystem möchte bewusst nicht den Wettbewerb über den Preis zusätzlich fördern. Im Web würde sich durch den Einsatz von Suchmaschinen sehr schnell der billigste Weiterverkäufer durchsetzen. Bei einem direkten Face-to-Face-Weiterverkauf über das Konzept der Aktivierungscodes dagegen, kann der Weiterverkäufer den Preis frei festlegen (vgl. Kapitel 8.4.2).

Abbildung 8.6
Feste Aufteilung des rabattierten Verkaufspreises



Da das PotatoSystem das Inkasso für Erstanbieter und Weiterverkäufer selbst übernimmt, kann es auch als zusätzlichen Verkaufsanreiz im systemeigenen Warenkorb **Rabatte** r auf die nominellen Preise P_{nom} geben. Sind virtuelle Waren mit einem nominellen Gesamtpreis P'_{nom} von über 5 Euro (ab dieser Schwelle reduzieren sich die Transaktionskosten bestimmter Bezahlsystem, vgl. Kapitel 5.2.3) im PotatoSystem-Warenkorb, so reduziert sich der Verkaufspreis (P_{rab}, vgl. Formel 8.1) der einzelnen Waren um 5% (r = 0,05); bei über 15 Euro sind es 10% Rabatt (r = 0,10) und

bei über 25 Euro gibt es eine 15%dige (r = 0,20) Ermäßigung. Hierbei ist es irrelevant, ob die Artikel im Warenkorb von unterschiedlichen Erstanbietern stammen.

Nachdem das PotatoSystem den Rabatt ausgerechnet hat, kann der Nutzer sich für ein Bezahlsystem entscheiden. Hier erhebt das PotatoSystem bei einem Teil der angebotenen Bezahlsysteme **Aufschläge** auf den rabattierten Gesamtpreis P'_{rab}. Ziel der Aufschläge ist es, trotz der unterschiedlichen Transaktionskosten der verschiedenen Bezahlsysteme eine einfache Kostenstruktur umzusetzen (vgl. Abbildung 8.6). Zur Berechnung der relativen (*rel*) und konstanten (*fix*) Aufschläge, werden für jedes Bezahlsystem ein- oder mehrere Parametersätze verwaltet.

Formel 8.1

$$P'_{rab} = P'_{nom} \cdot (1 - r(P'_{nom}))$$

$$r(x) = \begin{cases} 0 & 0 \leqslant x < 500 \\ 0{,}05 & 500 \leqslant x < 1500 \\ 0{,}10 & 1500 \leqslant x < 2500 \\ 0{,}15 & 2500 \leqslant x \end{cases}$$

Ein Parametersatz für das Bezahlsystem b enthält die folgenden vier Parameter:

- *min*, die untere Grenze für P'_{nom} ab der der Parametersatz mit *rel* und *fix* gilt,
- *max*, die obere Grenze P'_{nom} bis zu der der Parametersatz mit der *rel* und *fix* gilt,
- *fix*, der konstante Aufschlag auf P'_{nom} und
- *rel*, der prozentuale Aufschlag auf P'_{nom}.

Die Formel 8.2 definiert schließlich, wie der vom Käufer zu zahlende Rechnungsbetrag P'_{bez} sich aus dem rabattierten Gesamtpreis P'_{rab} bei der Verwendung des Bezahlsystems b mit dem Parametersatz (rel_b, fix_b, min_b und max_b) errechnet.

Formel 8.2

$$P'_{bez} = P'_{rab} \cdot (1 + rel(P'_{rab})) + fix(P'_{rab})$$

$$rel(x) = \begin{cases} 0 & 0 \leqslant x < min_b \\ rel_b & min_b \leqslant x \leqslant max_b \\ 0 & max_b < x \end{cases}$$

$$fix(x) = \begin{cases} 0 & 0 \leqslant x < min_b \\ fix_b & min_b \leqslant x \leqslant max_b \\ 0 & max_b < x \end{cases}$$

Bei PayPal bspw. verlangt das PotatoSystem bis 3,10 Euro (P'_{rab}) einen Aufschlag von 35 Cent. Damit lauten für b = PayPal die vier Parameter: min_{PayPal} = 0, max_{PayPal} = 310, rel_{PayPal} = 0 und fix_{PayPal} = 35.

Vom rabattierten Gesamtpreis behält die 4FO AG 5% als Lizenzgebühr für das PotatoSystem zurück. Für die Abwicklung der Bezahlungen werden als Mischkalkulation pauschal 15% veranschlagt. Weitere 2% werden für die MP3-Lizenz abgezogen. Nach dem Abzug dieser Transaktionskosten bleiben 78% (u+p). 43% (u=0,43) werden nach Abzug der GEMA-Gebühren auf die Accounts der Urheber gebucht. 35% (p=0,35) werden nach Abbildung 8.7 zwischen dem Erstanbieter und den Weiterverkäufern aufgeteilt.

Provisionsmodell

Grundprinzip des Provisionsmodells im PotatoSystem ist es, dass es keine Rolle spielt, bei welchem Verkäufer ein spezieller Song gekauft wird. Der Käufer muss immer das gleiche Weiterverkaufsrecht mit den gleichen Verdienstmöglichkeiten erhalten. Verkauft ein Käufer den Song, für den er das Weiterverkaufsrecht erworben hat, so erhält er einen festen Prozentsatz *p1* vom rabattierten Verkaufspreis P_{rab} auf seinen Account gutgeschrieben. Damit ein Weiterverkäufer ein Interesse daran hat, dass seine Käufer auch weiterverkaufen, wird er an deren Umsätzen ebenfalls mit einem festen Prozentsatz *p2* (mit *p2* < *p1*) beteiligt. Um das Provisionsmodell für Weiterverkäufer noch etwas interessanter zu machen, gibt es noch eine dritte Provisionsstufe mit dem Prozentsatz *p3 (mit p3 < p2)*. Auf weitere Stufen wurde im Interesse der Transparenz verzichtet.

Abbildung 8.7
Provisionsmodell des PotatoSystems am Beispiel einer Vertriebslinie mit 4 Generationen

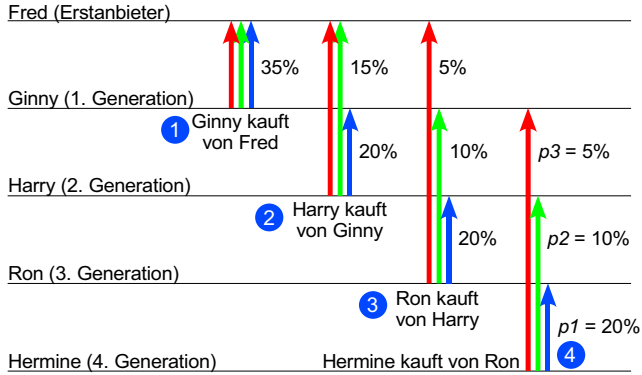


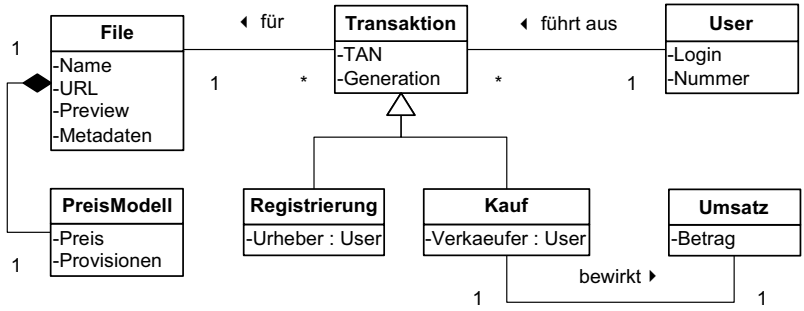
Abbildung 8.7 zeigt das im PotatoSystem gewählte dreistufige Provisionsmodell mit *p1* = 0,2, *p2* = 0,1 und *p3* = 0,05. In Schritt 1 kauft Ginny direkt vom Erstanbieter Fred. Da in diesem Fall kein Weiterverkäufer beteiligt ist, stehen Fred alle drei Provisionsstufen (*p* = *p1*+*p2*+*p3*) zu. In Schritt 2 wird Ginny zur Weiterverkäuferin, indem sie an Harry den Song weiterverkauft. Ginny erhält hierbei die erste Provisionsstufe *p1* gutgeschrieben. Die beiden anderen Stufen (*p2*+*p3*) fallen dem Erstanbieter zu. In Schritt 3 tut es Harry Ginny gleich und verkauft den Song an Ron weiter. Auch Harry erhält wieder die Provision *p1*. Ginny erhält *p2* und Fred *p3*. In Schritt 4 ist zu sehen, wie Fred bei den Provisionen ab der 4. Generation nicht mehr berücksichtigt wird. Im PotatoSystem hat er allerdings immer Zugriff auf die Urheberanteile *u*.

Berechnung der Provisionen

Die im Accounting-Server des PotatoSystems gespeicherten Transaktionen bilden die Basis für die Erzeugung der Transaktionsnummern (TAN) und die Berechnung der Provisionen. Abbildung 8.6 zeigt in vereinfachter Form das Klassendiagramm, das die Beziehungen zwischen den gehandelten Dateien und den durch die User

(Nutzer) getätigten Transaktionen. User **führen** sowohl Kauf- als auch Registierungstransaktionen **für** ein *File* **aus**.

Abbildung 8.8
Vereinfachtes statisches Klassendiagramm zu den Transaktionen



Registrierungstransaktion werden von Erstanbietern ausgeführt. Kauftransaktionen können alle User durchführen. Das registrierte bzw. gekaufte File besitzt einen *Namen*, eine *URL* (Adresse auf dem Server des Erstanbieters), die Adresse einer Vorhördatei (*Preview*) und weitere *Metadaten*. Für jedes File ist ein Preismodell hinterlegt, in welchem der nominelle Verkaufspreis (P_{nom}) und die Provisionsstufen (*p1*,*p2*,*p3*) festgelegt sind. Alle Transaktionen besitzen eine *TAN* und eine *Generation*. Die Generation ist bei der Registrierung Null. Bei der Vergabe der TAN wird nicht zwischen Kauf oder Registrierung unterschieden. Eine TAN setzt sich aus der Kundennummer des ausführenden Users und einer fortlaufenden Nummer zusammen (vgl. Kapitel 8.2.3). Bei der Registrierung wird zusätzlich der Urheber gespeichert, für den das File registriert wurde. Beim Kauf wird darüber hinaus der Verkäufer (bzw. Weiterverkäufer) vermerkt. Erfolgt der Kauf von einem Erstanbieter, so ist die Generation gleich Eins. Erfolgt der Kauf von einem Weiterverkäufer, dann ist die Generation größer gleich Eins.

Abbildung 8.9
Berechnung der Provisionen in Pseudocode

```
PROGRAM ProvisionsBerechnung BEGIN
  t := Finde_Transaktion(TAN)
  g := Generation(t)
  u := User(t)
  f := Finde_File(t)
  Account[u] := Account[u] + Prab * p1
  IF g = 0 THEN // Ohne Weiterverkäufer
    Account[u] := Account[u] + Prab * (p2+p3)
  ELSE BEGIN
    u := Verkaeufer(t)
    Account[u] := Account[u] + Prab * p2
    IF g = 1 THEN // Ein Weiterverkäufer
      Account[u] := Account[u] + Prab * p3
    ELSE BEGIN // 2 o. mehr Weiterverkäufer
      t := Finde_Transaktion(f,u)
      u := Verkaeufer(t)
      Account[u] := Account[u] + Prab * p3
    END
  END
END
```

Für den Kauf wird weiterhin der rabattierte Verkaufspreis P_{rab} vermerkt. Er bildet die Basis für die Provisionsberechnung. Der Algorithmus (siehe Abbildung 8.9) hierzu, der bei jeder Kauftransaktion abläuft, ist so allgemein ausgelegt, dass für jedes File ein getrenntes Provisionsmodell mit unterschiedlichen Prozentsätzen und individueller Stufenanzahl verarbeitet werden kann. Der in Abbildung 8.9 gezeigte Pseudocode geht dabei davon aus, dass bereits die Provisionsstufen (*p1*,*p2*,*p3*) und der rabattierte Preis *Prab* ermittelt wurden.

Bevor die Provisionen auf bis zu drei Accounts verteilt werden können, muss über die TAN die zugehörige

Transaktion *t* ermittelt werden. In der Transaktion *t* findet sich die Generation *g* und der ausführende User *u*. Über die Funktion *Verkaeufer* kann der als Verkäufer an einer Transaktion beteiligt User ermittelt werden. Die in der Transaktion gespeicherte Generation ermöglicht eine einfache Fallunterscheidung. Bei *g*=0 ist der Verkäufer der Erstanbieter, der somit als einzige Partei alle drei Stufen erhält. Bei *g*=1 ist ein Weiterverkäufer beteiligt, somit werden die Provisionen auf zwei Parteien verteilt. Erst bei *g*>1 sind in jedem Fall drei Parteien beteiligt.

■ Wert einer Vertriebslinie (Downline)

In [Emer 04] wurden die potentiellen Verdienstmöglichkeiten im PotatoSystem untersucht. Neben einer detaillierten Beschreibung von Multi-Level-Provisionssystemen und Netzwerk-Ökonomien wurde eine Analysewerkzeug erstellt, mit dem Verkäufer ihre sich innerhalb des PotatoSystems ausbreitenden Vertriebsnetzwerke untersuchen können. Besonderen Wert wurde auf die Untersuchung der Vertriebslinie (*Downline*) einzelner Dateien gelegt. Die Downline umfasst alle Personen, die ein Verkäufer direkt oder indirekt als Vertriebspartner gewonnen hat.

Der konkrete Wert eines bereits bestehenden Weitervertriebsrechts für eine Datei und einen Verkäufer ist durch die Downline beschrieben. In einer komplexeren Analyse ließe sich aus einer bestehenden Downlinie eine Prognose für zukünftige Provisionen berechnen.

8.3.3 Die Gesamtarchitektur

Das PotatoSystem wurde als Client-Server-System umgesetzt. Die Gesamtarchitektur dieses Systems, die intensiv von der Web-Service-Technologie (vgl. Seite 91) Gebrauch macht, lässt sich am besten anhand eines Download-Verkaufsvorgangs beschreiben, da in diesem Fall alle Internet-Server (vgl. Abbildung 8.10) des PotatoSystems beteiligt sind. Allerdings ist nur ein Teil dieser Server in der direkten Einflusssphäre des PotatoSystem-Betreibers.

■ Accounting-Server des PotatoSystems

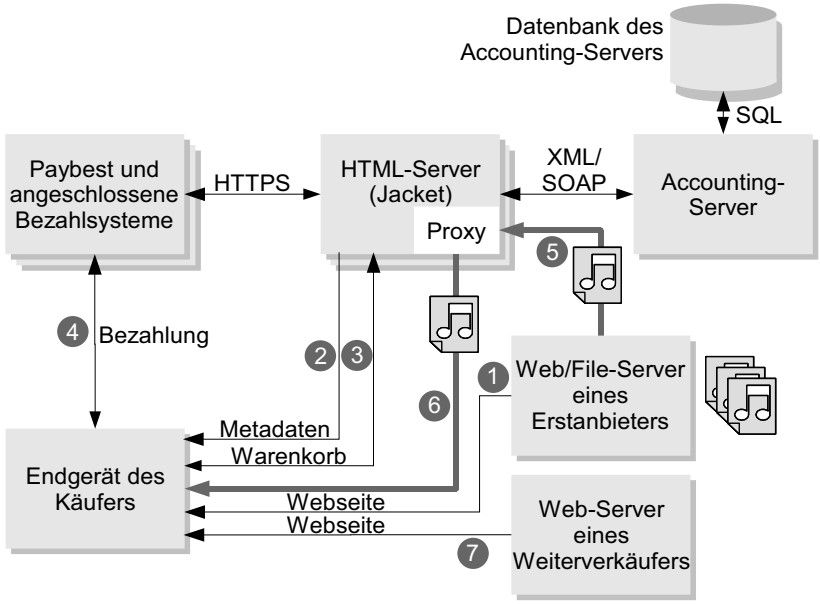
Kernstück des Gesamtsystems ist der von der 4FO AG betriebene Accounting-Server. Alle Kauf- und Registrierungstransaktionen werden in der Datenbank des Accounting-Servers gespeichert. Neben der reinen Datenhaltung der Accounts für Nutzer und Anbieter erfolgt auf dem Accounting-Server unter anderem auch die bereits beschriebene Berechnung der Provisionen und Rabatte für den Warenkorb.

Der schreibende und lesende Zugriff auf die Dienste und Daten des Accounting-Servers wird ausschließlich über eine PotatoSystem-interne Web-Service-Schnittstelle veranlasst. Über diesen internen Web-Service sind die HTML-Server des PotatoSystems angebunden. Die Einführung dieser internen Schnittstelle ermöglichte eine leichtere Partitionierung und Verteilung der zentralen Server-Komponenten des PotatoSystems auf mehrere Rechner.

Für den Zugriff von PotatoSystem-fremden Rechnern bietet das PotatoSystem eine externe Web-Service-Schnittstelle mit öffentlich zugänglicher WSDL-Beschreibung (vgl. Kapitel 8.4.3).

HTML-Server (Jacket-Server)

Abbildung 8.10
Datei-Download in der Gesamtarchitektur



Die HTML-Server des PotatoSystems, welche ebenfalls von der 4FO AG betrieben werden, realisieren für den Käufer und Erstanbieter die visuelle Hülle (daher auch *Jacket*-Server genannt) der Schnittstelle zum Accounting-Server. Nutzer und Anbieter kommunizieren über HTML und HTTPS mittels eines Standard-Browsers (wie z. B. Internet Explorer oder Firefox). Das Jacket bereitet die mittels SOAP vom Accounting-Server anforderten XML-formatierten Daten mittels HTML und CSS optisch auf. Ebenso nimmt das Jacket Eingaben der Nutzer und Anbieter über HTML-Formulare entgegen, prüft diese auf Plausibilität und leitet sie danach per SOAP an den Accounting-Server weiter. Anbieter registrieren hierüber ihre Dateien im System. Bei der Registrierung geben die Anbieter Preise und Metadaten an. Über zusätzliche Masken können sie ebenso ihre Umsätze kontrollieren. Zusätzlich zu den Administrationsdiensten stellt das Jacket eine Warenkorb-Funktion (vgl. Seite 136) bereit.

Darüber hinaus koordiniert das Jacket die Kommunikation mit den angeschlossenen Payment-Systemen. Des Weiteren realisiert es einen sicheren Proxy, der die Auslieferung der gekauften Dateien steuert und kontrolliert. Der Nutzer erhält über das Proxy nur mittelbar Zugang zu den Dateien, die auf den Servern der Erstanbieter gehostet werden. [NütGri 05]

Die im Weiteren noch beschriebenen Mini-HTML-Seiten (vgl. Seite 135), die per HTML-iFrame-Befehl in jede Web-Seite eingebettet werden können, werden ebenfalls vom HTML-Server bereitgestellt und als statische HTML-Seite zwischengespeichert, so dass nur beim ersten Abruf dieser HTML-Seiten der AS für die angezeigten Metadaten angefragt werden muss. Das gleiche gilt für die PotatoSystem-Info-Seiten

[Potato 05]. Da die HTML-Server keine Datensicherung, sondern nur eine zeitlich limitierte Zwischenspeicherung übernehmen, können sie sehr leicht skaliert werden [Nützel 04].

Paybest-Server

An den HTML-Server ist das Multi-Payment-System Paybest (vgl. Kapitel 5.4) über HTTP-POST-Kommunikation angekoppelt. Bei dieser Form der Kopplung wird der Paybest-Proxy (vgl. Seite 90) nicht benutzt. Paybest spielt für das PotatoSystem die Rolle eines Multi-Payment-Brokers, der nicht nur die eigenen entwickelten Bezahllösungen bereitstellt, sondern auch den Zugang zu einer Reihe weitere Drittanbieter-Systeme vermittelt. Bei der Integration ins PotatoSystem wird die Auswahlseite für die Bezahlsysteme vom HTML-Server bereitgestellt. Dies ermöglicht eine Anpassung an das Design des PotatoSystems und die Umsetzung von bezahlsystemspezifischen Preisaufschlägen (vgl. Seite 130).

File-Server des Erstanbieters

Der Erstanbieter von Nutzdaten (bspw. MP3-Dateien), muss diese auf einem Web-Server selbst bereithalten. Die Verzeichnisse, in welchem die Dateien liegen, sind über spezielle *.htaccess* Dateien [htaccess 05] nur dem Proxy des HTML-Servers zugänglich gemacht.

Neben den kostenpflichtigen Nutzdaten müssen die Erstanbieter auch Vorschau- bzw. Vorhördateien (MP3-Format) mit einer maximalen Spieldauer von 45 Sekunden bereitstellen. Der HTML-Server erstellt zu diesen MP3-Vorhördaten automatisch M3U-Dateien, die dafür sorgen, dass die Vorhördatei gestreamt wird. Das M3U-Format ist ein Text-Format, welches von der Firma Winamp zur Codierung von MP3-Playlists eingeführt wurde. Die von dem HTML-Server erzeugte M3U-Datei enthält nur einen Eintrag mit einer URL, die auf die bereitgestellte MP3-Vorhördatei verweist.

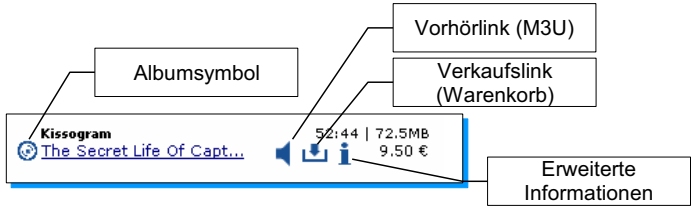
Sowohl die maximale Spieldauer von 45 Sekunden, als auch das Streaming sind Anforderungen der GEMA.

Web-Server des Erstanbieters oder Weiterverkäufers

Sowohl die Web-Server des Erstanbieters, als auch die Web-Server der potentiellen Weiterverkäufer benötigen neben einer standardisierten Web-Server-Software (z. B. Apache), die statische HTML-Seiten ausliefert, keinerlei zusätzliche Server-Software. Die auf den Web-Servern abgelegten HTML-Seiten enthalten entweder die Verkaufslinks (bspw. https://www.potatosystem.com/process/sell?tan=624480932), die die TANs als GET-Parameter enthalten. Verkaufslinks öffnen den Warenkorb (vgl. Seite 136) und fügen die Datei bzw. das Album, welches zu dieser TAN gehören, in den Warenkorb ein. Alternativ können per HTML-iFrame-Befehl **Mini-HTML-Seiten** eingebettet werden.

Diese Mini-HTML-Seiten werden direkt vom Jacket-Server bereitgestellt. Sie enthalten neben dem eigentlichen Verkaufslink weitere Informationen zum Song wie z. B. über Künstler, Titel, Länge, Dateigröße, Preis, Vorschau- und Info-Link. Abbildung 8.11 zeigt eine solche Mini-HTML-Seite für ein Album und den zugehörigen HTML-Code, der notwendig ist, um diese Mini-Web-Seite in die Web-Seite des Erstanbie-

Abbildung 8.11
Eine Mini-HTML-Seite die der Jacket-Server bereitstellt




```
<iframe style='{width:225pt; height:30pt;}'
src='http://data.potatosystem.com/process/iFrame?tan=624480932'
marginwidth='0' marginheight='0' scrolling='no' frameborder='0'>
</iframe>
```

ters oder Weiterverkäufers anlog einer Bitmap-Grafik einzubetten. Weitere Details hierzu (z. B. wie die Farbe der Mini-HTML-Seite geändert werden kann) finden sich in der Erstanbieteranleitung [PotatoInfo 05] des PotatoSystems.

8.3.4 Die Umsetzung der zentralen Dienste des PotatoSystems

Die zentralen Dienste des PotatoSystems unterteilen sich in Dienste für Käufer, für Weiterverkäufer und für Erstanbieter.

Dienste für Käufer

Die Umsetzung der wichtigsten Dienste für Käufer lassen sich entlang eines Kaufvorgangs verdeutlichen. Bei einem Kaufvorgang laufen nacheinander die folgenden Schritte ab (siehe Abbildung 8.10):

- Der Käufer gelangt auf die Web-Seite des Erstanbieters (Schritt 1 in Abbildung 8.10). In die Web-Seite sind Mini-HTML-Seiten vom Jacket-Server oder direkt die Verkaufslinks eingefügt (Schritt 2).
- Nachdem der Käufer über die Mini-HTML-Seite den Song vorhören konnte, klickt er den Verkaufslink an. Es öffnet sich darauf ein neues Fenster mit dem anbieterübergreifenden Warenkorb (Schritt 3). Abbildung 8.12 zeigt den Warenkorb in dem sich bereits ein Album und ein Einzel-Song befinden. Die Warenkorbeinträge werden über ein Browser-Cookie auf dem Endgerät einen Monat lang gespeichert. Der Käufer kann die Einträge einzeln löschen. Im Warenkorb werden die vom Accounting-Server berechneten Rabatte angezeigt. Aus dem Warenkorb gelangt der Käufer über den Link „>>Zur Kasse>>“ in den Anmeldedialog, der im PotatoSystem für einen anonymen Kauf auch übersprungen werden kann. Allerdings kann der Käufer dann auch nicht zum Weiterverkäufer werden bzw. einmal bezahlte Songs erneut kostenlos herunterladen.
- Nach der Anmeldung bzw. Neuregistrierung gelangt der Käufer in Schritt 4 zur Auswahl eines über Paybest eingebundenen Bezahlsystems. Ist der Käufer bereits ein erfolgreicher Weiterverkäufer, so kann er auch seinen PotatoSystem-Account zur Begleichung der Rechnung nutzen.

Abbildung 8.12
Warenkorb des Jacket-Servers mit zwei Einträgen

- Nach erfolgreicher Bezahlung erhält der Käufer die Möglichkeit, die gekauften Dateien einzeln herunter zu laden. Der Download erfolgt über das Proxy des Jacket-Servers (in Schritt 5 und 6). Wird die Datei häufiger zum Download angefordert, so wird die Datei direkt aus dem Proxy ausgeliefert, ohne sie vom Server des Erstanbieters erneut anzufordern (Schritt 6 entfällt).

Dienste für Weiterverkäufer

Wenn der Käufer sich im PotatoSystem registriert hat, ist er im PotatoSystem mit den Mitteln zum Weiterverkauf ausgestattet.

Der Accounting-Server hat dem Käufer für jede gekaufte Datei und jedes gekaufte Album eine neue Transaktionsnummer (TAN) zugeordnet. Möchte der Käufer nun das Album von Abbildung 8.11 weiterverkaufen, dann muss er die entsprechende Mini-HTML-Seite mit seiner persönlichen TAN in seine Web-Seite einfügen. Der Jacket-Server bietet dem Weiterverkäufer einen Dialog an, mit dem er die Mini-HTML-Seite über zusätzlich eingefügte Parameter farblich anpassen kann. In der Erstanbieteranleitung [PotatoInfo 05] sind alle Optionen für die Anpassung beschrieben. Bei klassischer Musik kann bspw. der Komponist anstelle des Interpreten angezeigt werden.

Der Weiterverkauf von der Web-Seite eines Weiterverkäufers beginnt in Abbildung 8.10 mit Schritt 7 und setzt sich danach analog dem Verkauf durch den Erstanbieter mit Schritt 2 fort. Für den Jacket-Server besteht der Unterschied in der TAN, die Teil des iFrame-Codes. An dieser TAN kann der Accounting-Server erkennen, wer der provisionsberechtigte Weiterverkäufer ist. Für Nutzer, die keine eigene Webpräsenz besitzen, generiert der HTML-Server des PotatoSystems automatisch so genannte **Nutzer-Homepages**. Auf dieser Homepage werden unter der URL: http://data.potatosystem.com/process/homepage?user=loginname alle Songs und Alben, für die der Nutzer das Weiterverkaufsrecht besitzt zum Kauf aufgelistet. Die automatisch generierte Nutzer-Homepage benutzt das PotatoSystem beim Nutzer-Matching (vgl. PotatoMatch in Abbildung 8.12).

Dienste für Erstanbieter

Die Erstanbieter haben gegenüber den normalen Käufern einen erweiterten Login-Bereich auf dem HTML-Server, über den sie alle Dienste des PotatoSystems über einen normalen Browser nutzen können. Neben der Echtzeit-Verkaufsstatistik haben sie die Möglichkeit, neue Künstler und neue Dateien im System anzumelden. Ebenso können sie mehrere Dateien eines Künstlers zu einem **Album** verbinden. Für dieses Album können sie unabhängig von den Einzelpreisen einen neuen Preis festlegen. Der Accounting-Server generiert für diese Alben eigene TANs.

8.4 Erweiterte Funktionen und Dienste

Die bisher beschriebenen zentralen Dienste stellen die Basisausstattung des PotatoSystems dar. Für eine optimale Unterstützung von Erstanbietern und Weiterverkäufern beim viralen Vertrieb virtueller Waren, werden erweitere Funktionen und Dienste benötigt.

8.4.1 Automatischer Kauf für professionelle Weiterverkäufer

Professionelle Weiterverkäufer registrieren keine Dateien im PotatoSystem. Sie wollen aber dennoch möglichst viele oder möglichst erfolgversprechende virtuelle Waren aus dem PotatoSystem über ihre Website verkaufen. Um die notwendigen Weiterverkaufsrechte zu erhalten, müssten sie, wie bereits beschrieben, die Inhalte manuell kaufen. Dies kann aus zwei Gründen ungeeignet sein:

- Möchte der Anbieter möglichst viel Content aus dem PotatoSystem anbieten, so müsste er sehr viel Geld in den Kauf der Inhalte investieren, von denen er aber nicht sicher sein kann, ob diese überhaupt jemals verkauft werden.
- Der Anbieter möchte nur ausgewählten Content verkaufen, der sich bereits gut verkauft hat. Er kann sich vom PotatoSystem eine Bestenliste (z. B. die *Top-10-Downloads*) geben lassen. Da diese Liste sich aber dynamisch verändert, müsste er ständig die Neuzugänge in dieser Liste manuell kaufen.

Eine Lösung für dieses Problem, die zum bisherigen System kompatibel ist, ist der automatische Kauf beim ersten Verkauf. Die Option des automatischen Kaufs kann nur speziellen Nutzern angeboten werden, die bereit sind, auf Ihrem Prepaid-Account für die automatischen Käufe in Vorleistung zu gehen.

Der automatisch Kauf wurde im PotatoSystem durch die Erweiterung der TAN umgesetzt. Es wird eine existierende TAN um einen Unterstrich ("_") als Trennzeichen und die Kundennummer des professionellen Weiterverkäufers erweitert. Da der im Verkaufslink und dem iFrame-Link enthalten TAN-Parameter unverändert an den Accounting-Server übertragen wird, muss der Jacket-Server für den automatischen Kauf nicht erweitert werden.

8.4.2 Aktivierungscodes (AC)

Aktivierungscodes (AC) sind zufällige, unter Vermeidung von Dubletten vom Accounting-Server erstellte, 16-stellige (case-insensitive) Buchstaben-Ziffern-Kombinationen. ACs werden bei jeder Kauftransaktion, für die sich kein Käufer registriert (bei je-

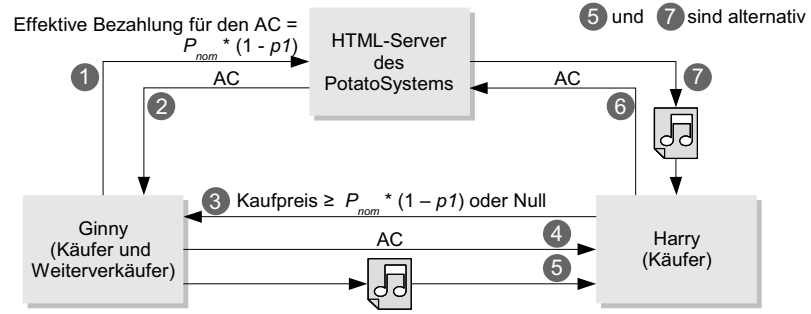
dem anonymen Kauf) automatisch erzeugt und der anonymen Transaktion zugeordnet. Die Kenntnis eines gültigen ACs ermöglicht einem registrierten Nutzer sich nachträglich kostenlos als Käufer dieser anonymen Kauftransaktion zuordnen zu lassen. Nach dieser Zuordnung verliert der AC seine Gültigkeit. Jeder Nutzer (Käufer oder Erstanbieter) im PotatoSystem kann für die Songs für die er bereits ein Weitervertriebsrecht besitzt, Aktivierungscodes erstellen. Er kauft sich quasi selbst die Songs anonym ab und erhält hierfür einen AC. Der anonyme Kauf ist allerdings unpraktikabel, wenn mehrere ACs für den gleichen Song benötigt werden. Das PotatoSystem bietet daher im Login-Bereich des Nutzers einen separaten Menüpunkt an, um in einem Schritt mehrere ACs zu kaufen.

Die ACs kann der Nutzer entweder verschenken oder auf eigene Rechnung verkaufen. Beim Verkauf auf eigne Rechnung ist der Weiterverkäufer nicht an den im PotatoSystem vorgegebenen Preis gebunden. Er kann mehr verlangen oder einen Nachlass von bis zu 20% gewähren. Ein AC kostet effektiv 80% des nominellen Verkaufspreises P_{nom}, da 20% (die erste Provisionsstufe *p1*) an den Nutzer als Provision sofort wieder zurückfließen (vgl. Kapitel 8.3.2).

Anwendungsfälle für Aktivierungscodes

Mit ACs lassen sich eine Reihe von Szenarien (Anwendungsfälle) umsetzen. Abbildung 8.13 zeigt das allgemeine Szenario, bei dem beispielhaft die Weiterverkäuferin Ginny einen AC, den sie in Schritt 1 und 2 beim PotatoSystem erworben hat, an Harry weitergibt. In Schritt 3 erhält sie direkt von Harry, nachdem sie den Song Harry vorgespielt hat, den Kaufpreis. Der Kaufpreis kann zwischen beiden frei vereinbart werden. Natürlich kann der AC auch verschenkt werden. In Schritt 4 übergibt Ginny den AC. Stehen sich beide Personen direkt (face-to-face) gegenüber, kann in Schritt 5 auch der Song peer-to-peer übertragen werden. In Schritt 6 kann Harry den AC online einlösen um damit das Weiterverkaufsrecht zu erhalten. Wenn er den Song in Schritt 5 noch nicht von Ginny erhalten hat, kann er ihn alternativ in Schritt 7 über das PotatoSystem herunterladen.

Abbildung 8.13
Weiterverkauf mit Aktivierungscodes (AC)



Dieses beschriebene allgemeine Szenario kann auf unterschiedliche Anwendungsfälle angepasst werden. Im Folgenden sind einige exemplarisch aufgelistet:

- *Legales Verschenken von Musik*. Ginny übergibt den AC kostenlos mit oder ohne den Song an ihren Freund Harry. Beim Einlösen des ACs erhält Harry auch die Gewissheit, dass er die Musik legal erhalten hat.
- *Verkauf von Musik in einem stationären Ladengeschäft*. Ginny betreibt einen Laden und verkauft Songs auf selbst gebrannten CDs oder per Kopie auf einen USB-Speicher-Stick. Zu den Songs erhält Harry mit dem Kassenzettel einen Ausdruck mit den zugehörigen individuellen ACs.
- *Verkauf von Musik zusammen mit Konzertkarten*. Ginny verkauft Konzertkarten von Fred auf denen als Zugabe ein individueller AC abgedruckt ist.
- *Face-to-face-Verkauf von Musik*. Ginny hat auf ihr mobiles Endgerät einen Song und einen AC geladen. Ginny trifft Harry (face-to-face), der ebenfalls ein (dazu kompatibles) mobiles Endgerät mit sich führt. Ginny spielt Harry den Song vor. Harry gefällt der Song und bezahlt den vereinbarten Preis in bar. Ginny überträgt per Infrarot (IRDA) oder Funk (Bluetooth) den AC auf Harrys Endgerät. Harry geht mit dem Endgerät online, löst den AC ein und lädt den Song auf sein Endgerät. Alternativ hätte er den Song auch direkt von Ginny erhalten können. Frank Zimmermann hat im Rahmen seiner Diplomarbeit [Zimmermann 03b] den Face-to-face-Verkauf prototypisch umgesetzt.
- *Online-Verkauf von Musik aus dem PotatoSystem ohne den Warenkorb des PotatoSystems*. Erstanbieter können auch im Web mit den ACs auf eigene Kasse Musik aus dem PotatoSystem verkaufen. Sie bieten den Käufern einen eigenen Warenkorb mit eigener Bezahlsystem-Integration an. Nach der Bezahlung erhält der Käufer einen Link, der auf das PotatoSystem zeigt und den individuellen AC als Parameter enthält.

ACs für Erstanbieter

Für Erstanbieter ist es ökonomisch riskant, ACs im voraus zu bezahlen, denn sie können nicht sicher sein, alle ACs zu verkaufen. Vertrauenswürdige Erstanbieter erhalten die ACs in Kommission. Erst bei ihrer Einlösung werden sie in Rechnung gestellt. Für einen AC fallen dabei die 22% Transaktionskosten (vgl. Abbildung 8.6) zuzüglich der GEMA-Gebühr an.

Für Werbezwecke kann ein Erstanbieter auch im begrenzten Umfang ACs für GEMA-freie Musik kostenlos erhalten. Bei der Einlösung solcher Promotion-Codes wird dem Nutzer mitgeteilt, dass für diese ACs kein Geld verlangt werden darf.

8.4.3 Externe Web-Service-Schnittstelle

Der Einsatz von Web-Services im PotatoSystem erfolgt nicht nur zur *internen* Trennung von Teilsystemen (siehe Abbildung 8.10). Der im Folgenden beschriebene so genannte *externe* Web-Service ist auf dem HTML-Server implementiert und dient primär der Umsetzung zweier Anwendungsfälle (vgl. auch [NütGri 05]):

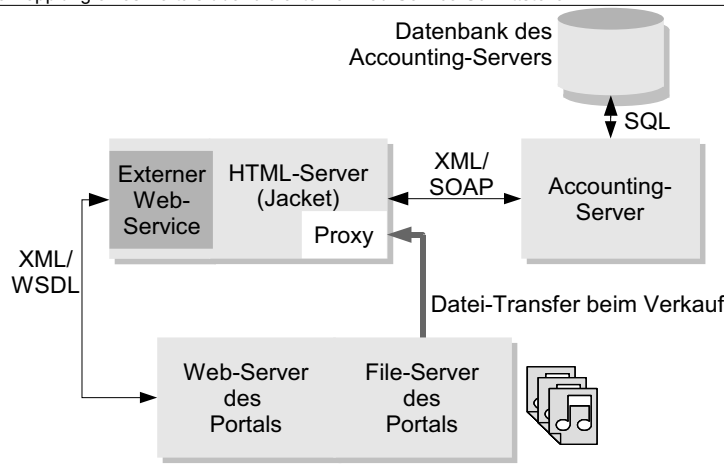
- Ein Erstanbieter, der eine größere Anzahl von Urhebern verwaltet, möchte den Content dieser Künstler bequem in das PotatoSystem einpflegen, ohne dabei permanent online sein zu müssen. Für diesen Anwendungsfall wird vom PotatoSystem eine spezielle PC-Anwendung – der PotatoLister – angeboten, die ähnlich wie beim Turbo-Lister von eBay [EbayLister 05] die Offline-Verwaltung angebotener

Artikel bzw. virtueller Güter ermöglicht. Der PotatoLister wird eine eigene Datenbank nutzen und zugehörige Import- und Export-Schnittstellen (CSV) bereitstellen, so dass z. B. auch Daten mit anderen System ausgetauscht werden können. Der Erstanbieter kann jederzeit seine lokale Datenbank über den externen Web-Service mit dem PotatoSystem abgleichen. Um PC- und Macintosh-Anwender gleichzeitig bedienen zu können wird der PotatoLister plattformunabhängig in Java erstellt.

- Beim zweiten Anwendungsfall für den externen Web-Service stehen größere Erstanbieter im Mittelpunkt. Diese Erstanbieter betreiben Download-Portale, welche das PotatoSystem als ASP (*Application Service Provider*) nutzen. Sie koppeln ihren Web-Server über den externen Web-Service direkt an das PotatoSystem (vgl. Abbildung 8.14) an. Diese Portale haben die Absicht, eine möglichst große Bandbreite an Musikrichtungen oder Regionen anzubieten. Sie bieten Künstlern deshalb nicht nur eine Verkaufsplattform, sondern auch eine unmittelbare Registrierungs- und Upload-Möglichkeit. Die von den Künstlern bspw. in ein Web-Formular eingegebenen Metadaten können dann direkt an das PotatoSystem übertragen werden.

Der Web-Service des PotatoSystems, dessen WSDL-Spezifikation unter https://www.potatosystem.com/services/PotatoWebServicePortalPort?wsdl abrufbar ist, ist in mehrere Gruppen mit jeweils mehreren Aufruf-Methoden aufgeteilt. Um die Komplexität auf der Client-Seite zu reduzieren, verzichtet der Web-Service auf eine Sitzungsverwaltung. Dies wird dadurch möglich, dass jeder Methoden-Aufruf die Login-Daten des jeweiligen Nutzers (Label- oder Portal-Account) enthält.

Abbildung 8.14
Direkte Kopplung eines Portals über die externe Web-Service-Schnittstelle



Label und Portale nutzen zwar den gleichen Web-Service, allerdings mit unterschiedlichen Rechten. Während Label mit dem PotatoLister nur eine Session mit einer sehr limitierten Zugriffsfrequenz erhalten, bekommen Portale die Möglichkeit, parallele Web-Service-Zugriffe mit höherer Frequenz durchzuführen.

Die über die Web-Service-Schnittstellen abgerufenen Informationen sind sehr sensibel, da sie auch die protokollierten Transaktionen, die sich auf ein spezielles Label oder Portal beziehen, enthalten. Dies macht den externen Web-Service zu einer sicherheitskritischen Stelle im PotatoSystem.

Gefahren drohen vor allem durch Lauschangriffe, unautorisierte Veränderungen oder unberechtigte Eingaben in fremdem Namen. Ebenso sind Denial-of-Service-Angriffe (DoS) eine Gefahr. Entsprechend muss der Web-Service abgesichert werden. SSL-Verschlüsselung kann die Vertraulichkeit sicherstellen, und in gewissem Umfang auch die Integrität. Als Zugriffsschutz werden in der gegenwärtigen Fassung Passwörter eingesetzt. Schwache Passwörter könnten durch eine Brute-Force-Attacke herausgefunden werden. Hier würde eine digitale Signatur Abhilfe schaffen [NütGri 05].

Aktuell werden fehlgeschlagene Login-Versuche mitgezählt. Nach dem fünften Fehlversuch wird der Web-Service-Zugang für diesen Account durch den HTML-Server gesperrt. Da Web-Services besonders leicht von Maschinen angesteuert werden können, müssen höhere Sicherheitsanforderungen als bei normalen Websites gelten. Der HTML-Server hat eine weitere Logik implementiert, die DoS-Angriffe nicht bis zum Accounting-Server durchlässt. Werden Web-Service-Zugriffe mit einer Frequenz über einem definierten Wert abgesetzt, werden weiter Zugriffe nicht an den Accounting-Server weitergeleitet.

8.4.4 Empfehlungssysteme und User-Matching

Der Wunsch, durch Personalisierung des Online-Angebots neue und für die Kunden interessante Waren zum Kauf vorzuschlagen, motivierte die Entwicklung und den Einsatz von so genannten Empfehlungssystemen (engl. *recommender systems*). Diese Systeme sind aus dem E-Commerce inzwischen nicht mehr wegzudenken, um Interessen von Kunden erkennen, vergleichen und vorhersagen zu können und darauf basierend, Käufern maßgeschneiderte Anregungen zu Produkten zu bieten. Der Online-Buchladen Amazon, der die GroupLens-Techniken [Resnik u.a. 94] nutzt, ist das bekanntestes Beispiel hierfür. Ein potentieller Kunde, der ein Buch aus dem Online-Katalog ausgewählt hat wird, mit dem folgenden Satz: „*Kunden, die dieses Buch gekauft haben, haben auch die folgenden Bücher gekauft*“ auf weitere Bücher aufmerksam gemacht. Der Online-Musik-Shop Musicload nutzt diesen Ansatz in ähnlicher Weise für virtuelle Waren.

Man kann die Empfehlungssysteme nach [BrHeKa 98] in Speicher- und Modell-basierte Systeme unterteilen. Bei Speicher-basierten Systemen müssen zur Berechnung der Ähnlichkeit von Nutzerprofilen diese im Speicher während der Laufzeit des Algorithmus vorliegen. Modell-basierte Systeme (z.B. Clustering-Systeme, Assoziations-Regeln) hingegen basieren auf probabilistischen Ansätzen und halten nur während der Algorithmuslaufzeit das Ergebnis der Modell-basierten Berechnungen im Speicher. Die beiden wichtigsten Ausrichtungen Speicher-basierter Systeme sind das so genannte *Content-based-Filtering* (CB) und das *Collaborative-Filtering* (CF). Baumann [Baumann 05] ergänzt CF um *Social-Filtering*. CB und CF sollen nun durch ihre Merkmale charakterisiert werden, wobei auch Mischformen existieren. [Kubek 05]

Content-based-Filtering

Diese Systeme basieren auf der Auswertung des Inhalts oder der Metadaten zu den Objekten. Typischerweise (aber nicht nur) arbeiten solche Systeme auf Textebene und verarbeiten explizite Suchanfragen wie zum Beispiel: „*Finde mir Nachrichten zum Thema Ratzinger und Golf*“ oder implizite Suchanfragen wie bspw.: „*Ich lese gerade ein Buch über Java-Programmierung. Ich interessiere mich für weitere Bücher zu diesem Thema!*“. Weiterhin kann durch Beobachtungen des Verhaltens des Nutzers bei wiederholten Anfragen ein Nutzerprofil gewonnen werden, welches dann bei zukünftigen Anfragen zur Verbesserung der Suchergebnisse herangezogen werden kann. Dabei fungiert das Nutzerprofil als Eingabe an das Empfehlungssystem. Das Profil kann aus explizit und implizit gewonnenen Daten bestehen, wobei erstere bspw. aus direkten Produktbewertungen eines Nutzers bestehen und letztere etwa durch das Erfassen von Nutzeraktivitäten beim Besuch einer Produkt-Webseite ermittelt werden können. Zusammengefasst befassen sich CB-Systeme mit dem Vergleich des Inhalts oder Beschreibung des betrachteten Objektes als mit den Meinungen und Wertungen anderer Nutzer darüber. Deshalb wird hierbei auch von Objekt-zu-Objekt-Korrelation gesprochen. Die im folgenden Kapitel über CF-Systeme angesprochenen Distanzmaße wie der Pearson`sche Korrelationskoeffizient (vgl. Formel 8.4) und die Vektorähnlichkeit lassen sich durch Parameteranpassung auch für CB-Systeme nutzen, um Objektähnlichkeiten zu berechnen, wobei hier die Vektoren die Merkmale der einzelnen Objekte enthalten. Ein sehr ausführliches Tutorial mit dem Thema *Adaptive Personalizatio*n findet man bei Nicholas Kushmerick [Kushmerick]

Möchte man sich bei Musik nicht nur auf textuell vorliegende Informationen stützen kommen Verfahren zum tragen, die aus der Musikaufnahme selbst Klangähnlichkeiten ermitteln. Die Dissertation von Baumann [Baumann 05] gibt einen Überblick über den Stand der Forschung in diesem Bereich.

Collaborative-Filtering

Collaborative-Filtering bildet eine weitere Klasse von Empfehlungssystemen [BrHeKa 98]. Hierbei werden Empfehlungen auf Grundlage von Nutzerbewertungen, Käufen oder anderen Kundenaktivitäten ausgesprochen. Die Aufgabe dieser Systeme liegt in der Repräsentation von Kundenprofilen und der Berechnung der Ähnlichkeit von Kundenprofilen. Daher wird in diesem Fall von Nutzer-Nutzer-Korrelation gesprochen. Das einleitend angesprochene GroupLens-System fällt in diese Klasse.

Ein sehr einfaches Kundenprofil mit nur einem Parameter *p* wie z. B. der Kauf (*purchase*) eines Produktes durch den Kunden, kann durch einen Vektor p_i repräsentiert werden. Alternativ könnte ein Profil durch Nutzerwertungen entstehen.

Formel 8.3

$$P = \begin{pmatrix} p_{11} & p_{12} & \cdots & p_{1n} \\ p_{21} & p_{22} & \cdots & p_{2n} \\ \vdots & & & \\ p_{m1} & p_{m2} & \cdots & p_{mn} \end{pmatrix}$$

Hat der Kunde ein Produkt gekauft ist p=1, andernfalls ist p=0. Bei n Produkten hat der Vektor die Länge n. Grundlage der Berechnung der Ähnlichkeit von Profilen bildet die Kunden-Produkt-Matrix P (vgl. Formel 8.3), in der alle Profile der m Kunden zeilenweise zusammengefasst sind.

Die Berechnung eines linearen Ähnlichkeitsmaßes zwischen dem Kundenprofil p_b und dem Profil p_a erfolgt über die Berechnung des Pearson'schen Korrelationskoeffizienten $corr_{ab}$ (vgl. Formel 8.4) [WikiKorr 05]. Der Koeffizient $corr_{ab}$ kann dabei Werte zwischen -1 und 1 annehmen, wobei Werte nahe 1 eine hohe positive Korrelation, Werte nahe -1 jedoch eine starke negative Korrelation ausdrücken. Werte um 0 bedeuten, dass keine Korrelation zwischen zwei Nutzern existiert. Möchte man dem Nutzer a eine Empfehlung abgeben, so muss prinzipiell zuerst der Koeffizient für alle anderen *m*-1 Kundenprofile berechnet werden. Die Profile, bei denen der berechnete Koeffizient über einer gewissen Schwelle liegt werden zur Produktempfehlung weiterverarbeitet.

Formel 8.4

$$corr_{ab} = \frac{\sum_i (p_{ai} - \overline{p_a})(p_{bi} - \overline{p_b})}{\sqrt{\sum_i (p_{ai} - \overline{p_a})^2 \sum_i (p_{bi} - \overline{p_b})^2}}$$

In [BrHeKa 98] wurden noch weitere Verfahren, die diese Basismethode verbessern beschrieben und miteinander verglichen.

PotatoMatch: User-Matching im PotatoSystem

Zentraler Gedanke bzw. Grundidee des PotatoSystems ist es, Käufer zu Weiterverkäufern zu machen (vgl. Kapitel 8.2.1). Denn nur, wenn die Käufer eine realistische Chance sehen, beim Weiterverkauf erfolgreich zu sein, werden sie das Weiterverkaufsrecht als einen zusätzlichen Gebrauchswert (vgl. Kapitel 3.4.2) einschätzen, der sie zusätzlich zum Kauf motiviert.

Da der durchschnittliche Käufer selten eine stark frequentierte Website besitzt, über die er die Musik mit großer Reichweite anbieten kann, ist er auf unterstützende verkaufsfördernde Maßnahmen von Seiten des PotatoSystems angewiesen. Aufbauend auf den automatisch generierten Nutzer-Homepages (vgl. Seite 137), die das Nutzerprofil repräsentieren, bietet das PotatoSystem ein einfaches Collaborative-Filtering-Empfehlungssystem auf Basis der nicht-anonymen Kauf- und Registrierungstransaktionen an. Im Gegensatz zu bisher beschriebenen Systemen empfiehlt es allerdings nicht direkt Produkte, sondern Weiterverkäufer, die diese Waren anbieten können. Das PotatoSystem nutzt somit direkt die aus dem Collaborative-Filtering ermittelten Nutzer-Nutzer-Korrelation.

Der beschriebene Algorithmus ist sehr rechenintensiv. Aktuell wird auf dem PotatoSystem eine stark vereinfachte Variante im Warenkorb angewendet (vgl. Abbildung 8.12), die auch bei jeder Änderung des Warenkorb aufgerufen werden kann. Hierbei bilden die Songs im Warenkorb das Nutzerprofil p_a. Der gleiche Algorithmus wird im PotatoSystem immer dann dazwischen geschaltet, wenn eine Suchanfrage oder die Top-10-Download-Liste konkrete Produkte liefert, die zum Kauf ausgewählt werden können. PotatoMatch sorgt dafür, dass automatisch möglichst immer ein Weiterverkäufer bei der Vermittlung des Verkaufes zwischen geschaltet wird. Der auf dem Accounting-Server ausgeführte PotatoMatch-Algorithmus (ein Variante findet sich in [Zimmermann 03a]) arbeitet wie folgt:

- Es werden die Nutzer mittels geeigneter Datenbankabfragen (SQL-Querys) ermittelt, die alle Songs aus dem Warenkorb, bzw. den einen, der aus den Top-10-Download ausgewählt wurde, ebenfalls anbieten können. (Der Algorithmus wird

allerdings aus Performance-Gründen im Warenkorb bei nur bei bis zu fünf Songs aufgerufen.)

- Da optimal korrelierende Weiterverkäufer ($p_a = p_b$) keine zusätzlichen Produkte anbieten können, werden diese aus der ermittelten Nutzerliste gestrichen.
- Die Nutzerliste wird sortiert, so dass die Nutzer nach oben kommen, die die meisten Songs bieten können.

Ein weites Feld für Experimente und Verbesserung bietet sich bei der Frage, welche Weiterverkäufer im User-Matching durch die Sortierung bevorzugt werden sollen, wenn sehr viel konkurrierende Nutzer auf der Liste erscheinen. Sollen diejenigen gefördert werden, die besonders viel in letzter Zeit gekauft haben? Oder diejenigen, die noch wenig oder gar nichts verkauft haben? Durch die besondere Zielstellung des PotatoSystems ergeben sich zusätzlich Fragestellungen, die nur empirisch beantwortet werden können.

8.5 Der mobile Anwendungskontext

Mobile Endgeräte mit breitbandigem Internet-Zugang über UMTS sind inzwischen (Mai 2005) in ausreichender Auswahl und Qualität verfügbar. Die Endgeräte sind nutzerprogrammierbar (vgl. Seite 38), besitzen teilweise sogar wechselbaren Permanentspeicher und können die Musikformate AAC und MP3 abspielen. Einige unterstützen auch OMA DRM Version 1.0 (vgl. Kapitel 4.4.4). Das Nokia 6630 [Nokia6630 05] oder das Nokia N91 (welches auch WMA unterstützt) sind solche Endgeräte, welche all diese Eigenschaften vereinen und dennoch die Größe eines üblichen Handys haben.

Abbildung 8.15
Mobile Music Messenger auf dem Nokia 6630

8.5.1 Der Mobile Music Messenger

Der Mobile Music Manager bildet die technische Plattform für den mobilen Anwendungskontext des PotatoSystems. Mario Kubek entwickelte bei der 4FO AG eine mobile (MIDP V2.0) Java-Anwendung (MIDlet). Diese prototypische Anwendung mit dem Namen *Mobile Music Messenger* (MMM) basiert auf der mobilen Variante der P2P-Systems JXTA (JXME) (vgl. Seite 44). Abbildung 8.8 zeigt das Nokia 6630, für das die J2ME-Applikation getestet wurde, mit dem Start-Screen.

Ziel des MMM ist die Realisierung eines Musik-Chats, bei dem die Nutzer sich nicht nur über Musik schreiben können, sondern sich auch gegenseitig die Musik vorspielen können, um sich damit zu einem Kauf zu motivieren. Der MMM setzt dieses Szenario folgendermaßen um:

- Im PotatoSystem können registrierte Nutzer (wie z. B. Ginny) mit dem MMM peer-to-peer Text-Nachrichten austauschen. Dazu wurde ein Chat-System implementiert, das auf dem Handy die Verwaltung einer persönlichen Buddy-Liste (Kontaktliste) ermöglicht.
- Neben der Buddy-Liste verwaltet der MMM das persönliche Musik-Profil (PMP) von Ginny auf dem Handy. Das PMP enthält Einträge zu Songs aus dem PotatoSystem. Ein PMP-Eintrag enthält neben dem Titel und Interpreten eines Songs, den Vorhör- und Verkaufslink. Der Verkaufslink enthält die TAN. Ginny kann den Vorhörlink auswählen, um 45 Sekunden des Songs als MP3 über den Medien-Player des Nokia 6630 vorzuhören. Der Verkaufslink öffnet den Warenkorb des PotatoSystems. Hierzu wird der WAP 2.0 Browser genutzt. Allerdings ist die Bezahlung bspw. über PayPal auf dem kleinen Display nicht sinnvoll durchführbar. Für diesen Zweck wurde der Prepaid-Account eingeführt.
- Ginny kann vom HTML-Server die Liste ihrer bereits gekauften Songs in ihr PMP importieren. Sie kann einzelne Einträge lokal löschen.
- Ginny kann im Chat neben Text-Nachrichten auch Einträge aus ihrem PMP versenden, um andere Nutzer wie z. B. Harry auf einen Song aufmerksam zu machen.
- Harry kann den PMP-Eintrag von Ginny in sein PMP importieren. Damit kann das PMP eines Nutzers Einträge von eigenen Songs und von Songs anderer Nutzer enthalten.

8.5.2 Verbindung mit dem Potato-Matching

So wie der mobile *Music Messenger* vom HTML-Server die Liste der gekauften Songs importieren kann, könnte er den zentralen User-Matching-Algorithmus nutzen, um sich Kontakte vermitteln zu lassen. Der hohe Berechnungsaufwand von Collaborative-Filtering-Verfahren (vgl. Seite 143) erfordert allerdings dezentrale Alternativen. In [Nützel 03b] wurden bereits erste Ansätze dezentraler P2P-Szenarien diskutiert. In [Kubek 05] werden diese Arbeiten fortgesetzt, mit dem Hintergrund des mobilen Anwendungskontextes.

8.6 Zusammenfassung und Bewertung

Der Autor möchte dieses Kapitel, welches zum großen Teil den innovativen und schöpferischen Anteil der Arbeit darstellt, nicht ohne eine abschließende Zusammenfassung und Bewertung beenden. Einerseits sollen die Möglichkeiten, die durch das geschaffene technischen Rahmenwerk des PotatoSystems entstehen, aufgezeigt werden, anderseits sollen auch nicht bestehenden Einschränkung vergessen werden.

■ Was wird durch das PotatoSystem möglich?

Das beschriebene PotatoSystem bildet die technische und organisatorische Basis für die Umsetzung eines neuartigen Geschäftsmodells, bei dem Käufer das Weiterverkaufsrecht erhalten. Nicht DRM-Systeme mit Kopierschutz, die zu einer Konfrontati-

on zwischen Anbieter und Nutzer führen, bilden hierbei die Basis, sondern ausschließlich Verfahren und Konzepte, die die Interessen von Anbietern und Nutzern zu einer möglichst großen Übereinstimmung bringen. Die Möglichkeit als Konsument mitzuverdienen und der Verzicht auf Kopierschutztechniken tragen dazu bei, den durch Misstrauen blockierten Musikmarkt wieder zu beleben.

Musik kann im PotatoSystem durch den Konsumenten sehr einfach ohne zusätzliche Software-Installationen im Standard-Browser bezahlt und heruntergeladen werden. Die verschiedenen eingebundenen sich ergänzenden Bezahlsysteme decken dabei die unterschiedlichsten von den Kunden gewünschten Bezahlmethoden ab. Ein Rabattsystem im anbieterübergreifenden Warenkorb motiviert Käufer zusätzlich weitere Songs zu kaufen.

Im PotatoSystem muss der Kunde sich nicht generell registrieren. Aber erst, wenn er sich registriert, erhält er automatisch das Weiterverkaufsrecht und die Möglichkeit Songs mehrmals herunterzuladen. Das User-Matching und die Nutzer-Homepage ermöglichen es, dass auch Käufer ohne eine eigne Home-Page Weiterverkäufer werden können. Weiterverkäufer, die eine Website ihr Eigen nennen, können dort ohne Programmierkenntnisse wie die Erstanbieter einen eignen Musik-Download-Shop betrieben. Die Mehrstufigkeit des Provisionsmodell gestattet es den Weiterverkäufern, nicht nur für den Kauf ihrer Songs Werbung zu machen, sondern parallel dazu auch für den Weiterverkaufsgedanken des PotatoSystems. Denn an ihren Käufern, die ihrerseits zu Weiterverkäufern werden, verdienen sie mit. Die Option mit der gekauften Musik Geld zu verdienen, erhöht für viele Nutzer den subjektiven Wert der virtuellen Ware. Dies ermöglicht es dem Anbieter höhere Preis zu verlangen.

Verschiedene Techniken, wie bspw. die Mini-HTML-Seiten und der Download-Proxy des HTML-Servers, sorgen für eine einfache Einbettung in die Internet-Welt. Neben diesen Techniken, die es kleinen und mittleren Anbieter leicht machen, Musik über das ihre Website zu verkaufen, bietet die externe Web-Service-Schnittstelle eine hohe Flexibilität bei der Umsetzung individueller Portal-Lösungen. Die Aktivierungscodes ermöglichen erweiterte Vertriebsszenarien, die sogar eine Integration des PotatoSystems in den stationären Handel ermöglichen.

Die Erweiterung des PotatoSystems um den mobilen Anwendungskontext verbindet die etablierte mobile Kommunikation, den bereits populären mobilen Musikkonsum mit dem kommenden mobilen Vertrieb.

Der bewusste Verzicht des PotatoSystems sich als zentrales Verkaufsportal zu positionieren, wie bspw. Apples iTunes oder Musicload, soll den Wettbewerb zwischen den Anbietern und den Weiterverkäufern im Interesse aller fördern. Das PotatoSystem tritt lediglich als Dienstleister für Erstanbieter und Weiterverkäufer in Erscheinung.

Offene Fragen

Natürlich kann das PotatoSystem derzeit nicht alle offenen Fragen beantworteten. Zum einen sind es Fragen, die von außen an die Entwickler und Forscher herangetragen werden:

- Was ist mit Labels oder Künstlern die das PotatoSystem nutzen wollen, aber keine eigene Website betreiben?
- Was passiert mit den Weiterverkäufern, wenn die Erstanbieter ihre Songs aus dem Angebot des PotatoSystems nehmen?

- Sind bereits alle wichtigen Marktteilnehmer im PotatoSystem berücksichtigt? Was ist bspw. mit den Dienstleistern, die mehrere Erstanbieter verwalten wollen?
- Ist das PotatoSystem ausreichend gegen Plagiatsversuche geschützt? Wie kann verhindert werden, dass geistiges Eigentum unter falscher Urheberschaft angboten wird?
- Wie können Radiosender das PotatoSystem nutzen?

Dann gibt es auch Fragen, die die Entwickler und Forscher sich selbst stellen und (noch) nicht beantworten können:

- Können die Ängste großer Anbieter, die DRM-Kontrolle wünschen, zerstreut werden? Oder bleibt das System auf kleine und mittlere Anbieter beschränkt?
- Welche Weiterverkäufer sollen durch das User-Matching speziell gefördert werden? Wie effektiv wirkt das User-Matching überhaupt?
- Wird der Weiterverkaufsgedanke nur für ausgewählte Käuferschichten interessant bleiben, oder ist eine breite „Ebayisierung“ (= alle Kaufen und Verkaufen) virtueller Waren durch das PotatoSystem möglich?

Da das PotatoSystem Anfang Mai 2005 erst rund 1500 Songs von ca. 150 relativ unbekannten Künstlern im Angebot hat, kann man noch nicht endgültig sagen, ob dieser alternative Ansatz ein kommerzieller Erfolg wird. Sicher ist, dass er innerhalb der Musik-Branche entsprechende Aufmerksamkeit genießt. Es bleibt abzuwarten, wie das System sich entwickelt, wenn zusätzliche Marketingmaßnahmen durchgeführt wurden und weitere Anbieter gefunden wurden.

9. Kapitel

Zusammenfassung und Ausblick

Die flächendeckende Verfügbarkeit breitbandiger Internet-Zugänge und die breite Akzeptanz von Online-Bezahlsystemen bei den Konsumenten bilden die Basis für die erfolgreiche Umsetzung neuer Geschäftsmodelle für virtuelle Waren, bei denen der Konsument die direkte Erlösquelle darstellt. Die informatorischen Aspekte virtueller Güter und Waren umschreiben einen neuartigen Teilbereich der Informatik. Im Mittelpunkt dieses Teilbereichs stehen Verfahren und Systeme, zur technischen Realisierung von bekannten und neuartigen Geschäftsmodellen für virtuelle Waren.

Stand der Technik und seine Erweiterung

Der Einsatz von Peer-to-Peer-Systemen, um großflächig das Urheberrecht zu umgehen, und die Einführung von DRM-Systemen, um dem wieder Herr zu werden, zeigen zwei technische Systeme, die die wissenschaftliche Beschäftigung mit virtuellen Waren in das Rampenlicht brachten. Ebenso gehören auf virtuelle Waren spezialisierte Bezahlsysteme, deren Wichtigkeit in der Öffentlichkeit oft unterschätzt wird, zum Stand der Technik in diesem Wissenschaftsgebiet.

Die vorliegende Arbeit wird diesem Stand der Technik gerecht und geht darüber hinaus, indem neue Konzepte beigetragen werden. Die Neuerungen betreffen eine veränderte Sicht auf die virtuellen Güter selbst, spezielle Erweiterungen bei den Bezahlsystemen, Arbeiten zur Erweiterung des Shareware-Prinzips, die Mitarbeit am leichtgewichtigen DRM und schließlich die Erfindung und Umsetzung des PotatoSystems.

Kritik am bekannten DRM

Der Autor legt ganz bewusst den Schwerpunkt der Arbeit auf die Beschreibung der Grundidee und der Umsetzung des PotatoSystems. Der Autor vertritt die Meinung, dass virtuellen Waren – auch nicht unter Zuhilfenahme von DRM – die Geschäftsmodelle realer Waren erfolgreich übergestülpt werden können. Virtuelle Waren stellen durch ihre Digitalisierbarkeit eine neue Warengruppe mit eigenen Gesetzmäßigkeiten dar. Dadurch, dass die Nutzdaten, welche die virtuellen Waren vollständig verkörpern, unbegrenzt, verlustlos und dazu noch nahezu kostenfrei kopierbar sind, stellen diese Nutzdaten für viele Konsumenten keine seltenes und knappen Gut mehr dar. Für viele Konsumenten besitzen Nutzdaten, die von ihrem physikalischen Träger losgelöst wurden keinen eigenen Wert mehr. Der Versuch den Wert zu erhöhen, indem durch technische Maßnahmen wie DRM den Nutzdaten die Kopierbarkeit genommen wird, verkehrt sich oft ins Gegenteil, denn viele Konsumenten empfinden gerade die verlustlose Kopierbarkeit als einen wichtigen Zusatznutzen.

Das PotatoSystem

Das PotatoSystem trägt dieser Erkenntnis Rechnung und versucht nicht direkte Erlösmodelle durch Kontroll- und Verhinderungstechniken abzusichern. Es baut dagegen auf ein neuartiges Anreizsystem auf, welches Käufer zu Weiterverkäufern macht. Die Arbeiten am PotatoSystem zeigten, dass die Umsetzung eine Reihe weiterer Fragen nach sich zieht. Besonders die Beantwortung der Frage, ob der Weiterverkauf von Musik Spezialisten vorbehalten bleibt oder ob durch das PotatoSystem eine „Ebayisierung" virtueller Güter gelingt, muss abgewartet werden. Sicherlich wird die Einbettung in den mobilen Anwendungskontext einen wichtigen Beitrag zur Verbreitung der Grundidee liefern können; zukünftige Forschungen werden sich deshalb auf dieses Gebiet konzentrieren.

Ausblick

Der Autor sieht große Entwicklungspotentiale beim mobilen Konsum und Kauf von Musik. Allerdings möchte er selbst keine besonders komplexe Interaktion mit Endgeräten dabei vollführen müssen. Ein UMTS-Handy, welches zusätzlich die Möglichkeit besitzt digitale Radiostationen (z. B. über DVB oder DAB) zu empfangen, soll bspw. einfach nur die Musik spielen, die dem Autor am besten gefällt. Nutzer sollen nicht gezwungen sein, einen speziellen Sender zu wählen. Durch das Drücken einer einzigen Taste bei Nichtgefallen der gehörten Musik (wie im Autoradio praktiziert) soll es bereits möglich sein, dem System mitzuteilen, welchen Musikgeschmack man hat. Das Endgerät kann entweder den Sender wechseln, den Sender auffordern das Programm zu ändern oder sich mit anderen Endgeräten austauschen. In [NütKau 04] wurde diese automatische Betriebsart bereits skizziert. Die Umsetzung eines solchen Systems macht allerdings nur Sinn, wenn geeignete Erlösmodelle für die Betreiber gefunden werden. Es bleibt abzuwarten, in wieweit, das PotatoSystem hier eine Rolle spielen kann.

Literaturverzeichnis

[4FO 05] *Website der 4FriendsOnly.com Internet Technologies AG, www.4fo.de, letzter Abruf: 28.3.2005*

[AicHas 03] *Aichroth, P.; Hasselbach, J.: Incentive Management for Virtual Goods - About Copyright and Creative Production in the Digital Domain. Virtual Goods Workshop, Ilmenau, Mai 2003, http://virtualgoods.tu-ilmenau.de/2003/incentive_management.pdf*

[AiPuHa 04] *Aichroth, P.; Puchta, S.; Hasselbach, J.: Personalized Previews: An Alternative Concept of Virtual Goods Marketing. Virtual Goods Workshop, Ilmenau, Mai 2004, http://virtualgoods.tu-ilmenau.de/2004/personalized_previews.pdf*

[AllPay 05] *Website der allPAY GmbH, www.allpay.info, letzter Abruf: 14.2.2005*

[Anypay 05] *Website des Anypay Systems, www.anypay.com, letzter Abruf: 13.2.2005*

[BaFin 04] *Internet-Portal der Bundesanstalt für Finanzdienstleistungsaufsicht, www.bafin.de, letzter Abruf: 18.11.2004*

[Baumann 05] *Baumann, Stephan: Artificial Listening Systems - Modellierung und Approximation der individuellen Perzeption von Musikähnlichkeit. TU-Kaiserslautern, 2005, www.dfki.uni-kl.de/~baumann/pdfs/Thesis.pdf*

[Behrendt 03] *Behrendt, Dirk: Konzeption und Realisierung einer Nutzerschnittstelle unter Einbeziehung von Web-Services für die Verwaltung von Nutzerkonten. Diplomarbeit TU-Ilmenau 2003-11-05/070/IN97/2231, 2003, www.4fo.de/de/students.htm#behrendt*

[Biedermann 02] *Biedermann, Kathleen: Gnutella und Co: Ein Praxisbericht über aktuelle Peer-to-Peer-Systeme. Hauptseminar TU-Ilmenau , 2002, www.4fo.de/de/students.htm#biedermann*

[Biedermann 03] *Biedermann, Kathleen: Das Geschäftsmodell des Potato-Systems. Projektarbeit TU-Ilmenau , 2003, www.4fo.de/de/students.htm#biedermann2*

[Bieger u.a. 02] *Bieger, T.; Bickhoff, N.; Caspers, R.; Knyphausen-Aufseß, D. zu; Reding, K.: Zukünftige Geschäftsmodelle - Konzept und Anwendung in der Netzökonomie. , Springer-Verlag, Berlin, 2002*

[BrHeKa 98] *Breese, J.; Heckerman, D.; Kadie, C.: Empirical Analysis of Predictive Algorithms for Collaborative Filtering. 14th Conf. on Uncertainty in AI (UAI-98), San Francisco, CA, 1998, http://research.microsoft.com/research/pubs/view.aspx?tr_id=166*

[BrNeKuSiSp 02] *Brandenburg, K.; Neubauer, C.; Kulessa, R.; Siebenhaar, F.; Spinnler, W.: Vorrichtung und Verfahren zum Erzeugen von verschlüsselten Daten, zum Entschlüsseln von verschlüsselten Daten und zum Erzeugen von umsignierten Daten, Offenlegungsschrift , DE 000010220925 A1, Anmeldung: 10.5.2002, Offenlegung: 27.11.2003*

[BucKüg 04] *Buchheit, Marcellus; Kügler, Rüdiger: Secure Music Content Standard - Content Protection with CodeMeter. 2nd Virtual Goods Workshop, Ilmenau, 2004, http://virtualgoods.tu-ilmenau.de/2004/SecureMusicContentProtection_VG2004.pdf*

[Buhse 01] *Buhse, Willms: Systematisierung von Geschäftsmodellen für Online-Musik unter Berücksichtigung von Marktunsicherheiten. WIRTSCHAFTSINFORMATIK, 43 4/2001 , 2001 www.wirtschaftsinformatik.de/wi_artikel.php?sid=793*

[Centano 02] *Centano, Clara: Paybest, an emerging micropayment solution for digital goods and services. ePSO-Newsletter, 12 Februar, 2002 http://epso.jrc.es/newsletter/vol12/*

[ChCoEtHaLa 03] *Chong, C. N.; Corin, R.; Etalle, S.; Hartel, P.; Law, Y. W.: LicenseScript: A Novel Digital Rights Language. Virtual Goods Workshop, Ilmenau, Mai 2003, http://virtualgoods.tu-ilmenau.de/2003/licensescript.pdf*

[Dittmann 00] *Dittmann, Jana: Digitale Wasserzeichen. , Xpert.press. Springer, Berlin, Heidelberg, 2000*

[DMP 05] *Website des Digital Media Project, www.dmpf.org, letzter Abruf: 26.4.2005*

[EbayLister 05] *Website des Turbo-Listers von eBay, http://pages.ebay.de/turbo_lister/, letzter Abruf: 28.4.2005*

[Eberhardt 04] *Eberhardt, Robert: Konzeption und Realisierung einer skalierbaren portierbaren Peer-to-Peer-Infrastruktur für kommerzielle Anwendungsfälle. Diplomarbeit TU-Ilmenau 2004-08-02/062/IN98/2231, 2004, www.4fo.de/de/students.htm#eberhardt*

[Emer 04] *Emer, Jeannine: Die Netzökonomie digitaler Güter am Beispiel des Potato-Systems - Entwicklung eines Informationssystems. Diplomarbeit TU-Ilmenau , 2004, www.4fo.de/de/students.htm#emer*

[EU31 00] *Richtlinie 2000/31/EG über den elektronischen Geschäftsverkehr und ihre Vorarbeiten. Richtlinie, Luxemburg Juni 2000, http://europa.eu.int/comm/internal_market/de/ecommerce/index.htm#dir200031*

[EU46 00] *Richtlinie 2000/46/EG über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten. Richtlinie, Brüssel September 2000, http://europa.eu.int/comm/internal_market/payments/emoney/index_de.htm#200046*

[EUCD 01] *Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates. Richtlinie, Mai 2001, http://europa.eu.int/information_society/topics/multi/digital_rights/documents/index_en.htm*

[FastTrack 04] *Online Dokumentation zum bekannten Teil des FastTrack-Protokolls, http://cvs.berlios.de/cgi-bin/viewcvs.cgi/gift-fasttrack/giFT-FastTrack/PROTOCOL?rev=1.9, letzter Abruf: 6.3.2004*

[FIPS197 01] *NIST: Federal InformationProcessing Standards Publication 197. , 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf*

[Firstgate 04] *Internet-Portal der Firstgate AG, www.firstgate.de, letzter Abruf: 2.8.2004*

[Freenet 05] *Website des Freenet Projektes, http://freenet.sourceforge.net, letzter Abruf: 11.4.2005*

[Frings 03] *Frings, Gabriele: Konzeption und Realisierungeines plattformübergreifenden Web-Services zur Verwaltung von Nutzerkonten für virtuelle Waren. Diplomarbeit TU-Ilmenau 2003-07-14/048/IN98/2231, 2003, www.4fo.de/de/students.htm#frings3*

[Gabler 04] *Alisch, K.; Winter, E.; Arentzen, U.: Gabler Wirtschaftslexikon. 16. Auflage, Gabler Verlag, Wiesbaden, 2004*

[GEMA 05] *Internet-Portal der GEMA, www.gema.de, letzter Abruf: 9.7.2005*

[Gnutella 05] *Website zur Gnutella Protokoll Entwicklung, http://rfc-gnutella.sourceforge.net, letzter Abruf: 11.4.2005*

[GriAic 04] *Grimm, Rüdiger; Aichroth, Patrick: Privacy Protection for Signed Media Files - A Separation-of-Duty Approach to the Lightweight DRM (LWDRM) System. ACM Multimedia and Security Workshop, Magdeburg, September 2004, http://wwwiti.cs.uni-magdeburg.de/iti_amsl/acm/acm04/*

[Grimm 04a] *Grimm, Rüdiger: Digital Rights Management: technisch-organisatorische Lösungsansätze. Seite(n):93-106 in Digital Rights Management, Münchner Kreis Hrsg.: Picot, Arnold, Springer-Verlag, Berlin, Heidelberg, New York, 2004*

[Grimm 04b] *Grimm, Rüdiger: Shannon verstehen - Eine Erläuterung von C. Shannons mathematischer Theorie der Kommunikation, Diskussionsbeiträge , 2004,*

[GriNüt 02a] *Grimm, Rüdiger; Nützel, Jürgen: Geschäftsmodelle für virtuelle Waren. DuD, 05/2002 , 2002 www.4fo.de/de/papers.htm#grinuet02a*

[GriNüt 02b] Grimm, Rüdiger; Nützel, Jürgen: A Friendly Peer-to-Peer File Sharing System with Profit but Without Copy Protection. Seite(n):133-142 in Innovative Internet Computing Systems, 2nd International Workshop LNCS 2346 Hrsg.: Unger, Herwig; Böhme, Thomas; Mikler, Armin, Springer, Kühlungsborn, 2002 www.4fo.de/de/papers.htm#grinuet02b

[GriNüt 02c] Grimm, Rüdiger; Nützel, Jürgen: Security and Business Models for Virtual Goods. ACM Multimedia Security Workshop, Juan le Pins, Frankreich, Dezember 2002, www.4fo.de/de/papers.htm#grinuet02c

[GriNüt 02d] Grimm, Rüdiger; Nützel, Jürgen: Peer-to-Peer Music-Sharing with Profit but Without Copy Protection. Seite(n):17-22 in , 2nd Int. Conference on WEB Delivering of Music Hrsg.: Busch, C.; Arnold, M.; Nesi, P.; Schmucker, M., IEEE Computer Society, Darmstadt, 2002 www.4fo.de/de/papers.htm#grinuet02d

[Hartmann 04] Hartmann, André: Konzeption und prototypische Realisierung einer Client-Komponente für die digitale Musikdistribution mittels personalisierter Inhaltsproben. Diplomarbeit TU-Ilmenau 2004-11-03/095/IN99/2231, 2004, www.4fo.de/de/students.htm#hartmann

[HASP 05] Website des HASP Systems der Firma Aladdin, www.aladdin.com/HASP/, letzter Abruf: 25.4.2005

[Hasselbach 02] Hasselbach, Jens: Konzeption und Realisierung der Client-Komponenten für ein P2P-File-Sharing-System mit Umsatzbeteiligung für die Benutzer. Diplomarbeit TU-Ilmenau 2002-11-04/053/IN96/2231, 2002, www.4fo.de/de/students.htm#hasselbach

[Heinrich 01] Heinrich, Jürgen: Medienökonomie. 2. Auflage, Westdeutscher Verlag, Opladen, 2001

[Heise54607] Heise-Newsticker: Urheberrecht soll "digitale Revolution für alle" ermöglichen, www.heise.de/newsticker/meldung/54607, letzte Änderung: 24.12.2004

[HerCre 04] Herre, Jürgen; Cremer, M.arcus: AudioID: MPEG-7 audio fingerprinting. Seite(n): in MMIR MultiMedia Information Retrieval, AIDA Hrsg.: Raieli, Roberto; Innocenti, Perla, AIDA, Rom, 2004

[htaccess 05] Apache HTTP Server Version 1.3 online Dokumentation: .htaccess files, http://httpd.apache.org/docs/howto/htaccess.html, letzter Abruf: 31.1.2005

[Iannella 01] Iannella, Renato: Digital Rights Management (DRM) Architectures. D-Lib Magazine, Volume 7 Number 6 Juni, 2001 http://www.dlib.org/dlib/june01/iannella/06iannella.html

[IIS 05] Die Watermarking Webseite des Fraunhofer IIS, www.iis.fraunhofer.de/amm/techinf/water/, letzter Abruf: 10.2.2005

[Iosono 05] Website der IOSONO GmbH, www.iosono-sound.com, letzter Abruf: 11.4.2005

[iPod 05] Website der Apple Computer Inc zum Apple iPod, www.apple.com/ipod/, letzter Abruf: 29.4.2005

[IPRSys 05] Website der IPR Systems, www.iprsystems.com, letzter Abruf: 10.2.2005

[ISO2382] ISO/IEC 2382-1: Information technology -- Vocabulary -- Part 1: Fundamental terms. Norm, 1993, www.iso.org

[ISO7498 94] ISO/IEC 7498-1: Open Systems Interconnection (OSI) -- Basic Reference Model: The Basic Model. Norm, 1994, www.iso.org

[JanLan 02] Jantke, K. P.; Lange, S.: Risiken beim Bezahlen im Internet - Bedrohungsanalysen und Bewertungen. NetSiKom, Köln, April 2002, www.dfki.de/~jantke/papers/Jantke-Lange-NetSiKom2002-preprint.pdf

[JAR 04] Sun Microsystems: Java Archive (JAR) Files. , 2004, http://java.sun.com/j2se/1.5.0/docs/guide/jar/

[JXTA 04] Internet-Portal des JXTA-Projektes, www.jxta.org, Letzter Abruf: 2.8.2004

[JXTAProg 05] Sun Microsystems, Inc.: JXTA v2.3.x: Java Programmer's Guide. , 2005, www.jxta.org/docs/JxtaProgGuide_v2.3.pdf

[KetStr 02] Hrsg.: Ketterer, Karl-Heinz; Stroborn, Karsten: Handbuch ePayment. , Deutscher Wirtschaftsdienst, Köln, 2002

[Krauß 02] Krauß, Holger: Konzeption und Realisierung der Server-Komponente für ein P2P-File-Sharing-System, bei dem die User am Umsatz beteiligt sind. Diplomarbeit TU-Ilmenau 2002-09-04/040/IN95/2231, 2002, www.4fo.de/de/students.htm#krauss

[Kubek 05] Kubek, Mario: Verteiltes Nutzer- und Content-Matching in mobilen Kommunikationssystemen im Umfeld des PotatoSystems. Diplomarbeit (in Bearbeitung) TU-Ilmenau 2005-09-29/097/IN98/2231, 2005, www.4fo.de/de/students.htm#kubek

[Kunze 04] Kunze, Michael: Konzeption und Realisierung eines fairen Software-Kopierschutzes basierend auf einer Client-Server-Architektur. Diplomarbeit TU-Ilmenau 2004-08-02/063/IN96/2231, 2004, www.4fo.de/de/students.htm#kunze

[Kushmerick] Nicholas Kushmerick Lehrmatrial zu "Adaptive Personalization", www.cs.ucd.ie/staff/nick/home/COMP-UMS3/, letzter Abruf: 2.5.2005

[KWG 04] Gesetz über das Kreditwesen (Kreditwesengesetz - KWG), www.bafin.de/gesetze/kwg.htm, letzte Änderung: 5.4.2004

[LangLong 84] Procter, Paul: Dictionary of Contemporary English. 5. Druck, Langenscheidt-Longman, Gütersloh, 1984

[LeiStr 03] Leibold, Kay; Stroborn, Karsten: Internet-Zahlungssysteme aus Sicht der Verbraucher - Ergebnisse der Online-Umfrage IZV6, Studie Universität Karlsruhe (TH), 2003, www.iww.uni-karlsruhe.de/izv/pdf/izv6_gliederungexecutive.pdf

[LiBrLe 86 S.379] Lindner, H.; Brauer, H.; Lehmann, C.: Taschenbuch der Elektrotechnik und Elektronik. 2. Auflage, VEB Fachbuchverlag, Leipzig, 1986

[LICBerliner 02] The Library of Congress: Emile Berliner and the Birth of the Recording Industry. , 2002, http://lcweb2.loc.gov/ammem/berlhtml/

[Lorenz 04] Lorenz, Oliver: Konzeption und Realisierung eines anbieterunabhängigen Web-Services zur Autorisierung von Online-Zahlungstransaktionen. Diplomarbeit TU-Ilmenau 2004-03-03/026/IN98/2231, 2004, www.4fo.de/de/students.htm#lorenz

[LWDRM 04] Internet-Portal des LWDRM-Systems, www.lwdrm.com, letzter Abruf: 2.8.2004

[Marx 62] Marx, Karl: K. Marx/F. Engels - Werke. , Dietz Verlag, Berlin/DDR, 1962

[MarxForum 04] Karl Marx-Forum, www.marx-forum.de, Letzter Abruf: 9.7.2004 Buchenberg, Wal

[Mbookers 05] Website der Moneybookers Ltd., www.moneybookers.com, letzter Abruf: 13.2.2005

[Medion 05] Website des Musik-Download-Dienstes Medionmusic, www.medionmusic.com, letzter Abruf: 11.4.2005

[Michael 03] Michael, Dirk: Implementierung eine P2P-Clients als Applet mit Hilfe der JXTA-Technologie zur Einbindung in das Potato-System. Studienjahresarbeit TU-Ilmenau , 2003, www.4fo.de/de/students.htm#michael2

[MicroMoney 05] Website von MicroMoney, www.micromoney.de, letzter Abruf: 13.2.2005

[Mori 89] Mori, Ryoichi: What Lies Ahead. Byte Magazine, Januar, 1989

[MPay 05] Web-Seite zu Vodafones m-pay, www.vodafone.de/business/enabling_services/32747.html, letzter Abruf: 14.2.2005

[MPEG21 04] MPEG-21, ISO/IEC TR 21000-1:2004, http://www.itscj.ipsj.or.jp/sc29/29w42911.htm, letzter Abruf: 20.4.2005

[Müller 04] Müller, Beate: "cross border payment"- in P2P-Systemen. Projektarbeit TU-Ilmenau , 2004, www.4fo.de/de/students.htm#mueller

[MusicTrace 05] Website der MusicTrace GmbH, www.musictrace.de, letzter Abruf: 10.2.2005

[NeBrSi 02] Neubauer, C.; Brandenburg, K.; Siebenhaar, F.: Technical Aspects of Digital Rights Management Systems, Paper 5688. 113th AES-Convention, LA, Oktober 2002,

[NeKuHe 01] Neubauer, C.; Kulessa, R.; Herre, J.: A Compatible Family of Bitstream Watermarking Schemes. 110th AES Convention, Amsterdam, Mai 2001,

[Nokia6630 05] Hersteller-Website zum Nokia 6630, www.nokia6630.com, letzter Abruf: 28.4.2005

[NokiaDRM 04] Nokia: DRM Developer's Guide for Nokia Devices v2.1. , 2004, www.forum.nokia.-com/ndsCookieBuilder?fileParamID=6135

[NüBöStSc 00] Nützel, J.; Böhme, T.; Stein, M.; Schwetschke, S.: Verfahren zur Verfügbarmachung von multimedialen Datenmengen, Patentschrift , DE 0010059230 C2, Anmeldung: 29.11.00, Veröffentlichung: 28.11.02

[NütGri 03] Nützel, J.; Grimm, R.: Potato System and Signed Media Format - an Alternative Approach to Online Music Business. Seite(n):23-26 in , 3rd Int. Conference on WEB Delivering of Music Hrsg.: Ng, Kia; Busch, C.; Nesi, P., IEEE Computer Society, Leeds, 2003 www.4fo.de/de/papers.htm#nuetgri03

[NütGri 05] Nützel, J.; Grimm, R.: Musikvertrieb mit Potato Web Services. DuD, 03/2005 , 2005 www.4fo.de/de/papers.htm#nuetgri05

[NütKau 04] Nützel, J; Kaufmann, M.: Sharing Systems for Future HiFi Systems. Seite(n):128-135 in , 4th Int. Conference on WEB Delivering of Music Hrsg.: Delgado, J.; Nesi, P.; Ng, Kia, IEEE Computer Society, Barcelona, 2004 www.4fo.de/de/papers.htm#nuetkau04

[Nützel 01] Nützel, Jürgen: The Game Feature Platform. 46th International Scientific Colloquium, Ilmenau, September 2001, www.4fo.de/de/papers.htm#nuetzel01

[Nützel 02] Nützel, Jürgen: Virtuelle Waren bezahlbar machen. Seite(n): in Von e-Learning bis e-Payment, Leipziger Informatik Tage Hrsg.: Jantke, K.P.; Wittig, W.S.; Herrmann, J., Akademische Verlagsgesellschaft Aka, Leipzig, 2002 www.4fo.de/de/papers.htm#nuetzel02

[Nützel 03a] Nützel, Jürgen: Wie kann man mit dem Potato-System eine Ware verkaufen, die alle schon haben?. 2. Thüringer Medienseminar, Erfurt, Mai 2003, www.4fo.de/de/papers.htm#nuetzel03a

[Nützel 03b] Nützel, Jürgen: Matching Algorithms in File-sharing Systems to find new Users having new Content. Seite(n):180-188 in Innovative Internet Community Systems, 3rd International Workshop LNCS 2877 Hrsg.: Böhme, Thomas; Heyer, Gerhard; Unger, Herwig, Springer, Leipzig, 2003 www.4fo.de/de/papers.htm#nuetzel03b

[Nützel 04] Nützel, Jürgen: Das PotatoSystem - mehr als Content Management und Bezahlservice für digitale Musik. Seite(n):113-122 in Von e-Learning bis e-Payment, Leipziger Informatik Tage Hrsg.: Fähnrich, K.-P.; Jantke, K. P.; Wittig, W. S., Akademische Verlagsgesellschaft Aka, Leipzig, 2004 www.4fo.de/de/papers.htm#nuetzel04

[Nützel 99] Nützel, Jürgen: Objektorientierter Entwurf verteilter eingebetteter Echtzeitsysteme auf Basis höherer Petri-Netze. , Verlag Isle, Ilmenau, 1999

[ODRL 05] Website der ODRL-Initiative, www.odrl.net, letzter Abruf: 15.4.2005

[OMA 05] Website der Open Mobile Alliance, www.openmobilealliance.org, letzter Abruf: 20.4.2005

[OMA1 04] OMA Digital Rights Management V1.0 Approved Enabler, www.openmobilealliance.org/release_program/drm_v10.html, letzte Änderung: 25.6.2004

[OMA2 06] OMA Digital Rights Management V2.0 Approved Enabler, www.openmobilealliance.org/release_program/drm_v2_0.html, letzte Änderung: 3.3.2006

[OpenOffice 04] Internet-Portal des OpenOffice-Projektes, www.openoffice.org, Letzter Abruf: 2.8.2004

[OSD 04] The Open Source Definition, http://www.opensource.org/docs/definition, letzter Abruf: 26.8.2004

[Pago 05] Website zur Pago Online-Überweisung, www.online-ueberweisung.info, letzter Abruf: 14.2.2005

[Paybest 05] Internet-Portal des Multipayment-Systems Paybest, www.paybest.de, letzter Abruf: 28.3.2005

[PaybestTech 04] 4FO AG: Technische Beschreibung des Micro-Payment-Systems Paybest. Anleitung , 2004, www.paybest.de/tech/ Ilmenau

[PayboxAT 05] Website der paybox austria AG, www.paybox.at, letzter Abruf: 13.2.2005

[Paypal 04] *Deutsche Website von Paypal (Europe) Ltd., www.paypal.com/de/, letzter Abruf: 28.12.2004*

[Paysafe 05] *Website der paysafecard.com Wertkarten AG, www.paysafecard.com, letzter Abruf: 13.2.2005*

[Pietrek 02] *Pietrek, Matt: An In-Depth Look into the Win32 Portable Executable File Format, Part 2. MSDN Magazine, 03 März, 2002 http://msdn.microsoft.com/msdnmag/issues/02/03/PE2/*

[Potato 05] *Das Internet-Portal des PotatoSystems, www.potatosystem.com, letzter Abruf: 28.3.2005*

[PotatoInfo 05] *PotatoSystem Infoseite der 4FO AG: Erstanbieteranleitung, www.potatosystem.-com/info/ger/provider.html, letzter Abruf: 10.4.2005*

[Raepple 98] *Raepple, Martin: Sicherheitskonzepte für das Internet. , dpunkt-Verlag, Heidelberg, 1998*

[Rechenberg 03] *Rechenberg, Peter: Zum Informationsbegriff der Informationstheorie. Informatik-Spektrum, Band 26, Nummer 5 Oktober, 2003 http://www.springerlink.com/openurl.asp?genre=article&issn=0170-6012&volume=26&issue=5&spage=317*

[Resnik u.a. 94] *Resnick, P.; Iacovou, N.; Suchak, M.; Bergstrom, P.; Riedl, J.: GroupLens: An Open Architecture for Collaborative Filtering of Netnews. Conference on Computer Supported Cooperative Work, New York, 1994, www.si.umich.edu/~presnick/papers/cscw94/GroupLens.htm*

[RFC2045 96] *The Internet Society: RFC 2045 Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies. , 1996, www.ietf.org/rfc/rfc2045.txt*

[RFC2046 96] *The Internet Society: RFC 2046 Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types. , 1996, www.ietf.org/rfc/rfc2046.txt*

[RFC2047 96] *The Internet Society: RFC 2047 MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text. , 1996, www.ietf.org/rfc/rfc2047.txt*

[RFC3280 02] *The Internet Society: RFC 3280 Internet X.509 Public Key Infrastructure. , 2002, http://www.ietf.org/rfc/rfc3280.txt*

[Rijmen 04] *Die Rijndael Web-Seite, http://www.esat.kuleuven.ac.be/~rijmen/rijndael/, Letzter Abruf: 5.8.2004 Rijmen, Vincent*

[RivShaAdl 78] *Rivest, R. L.;Shamir, A.; Adelman, L. M.: A Method for Obtaining Digital Signatures and Public-Key-Systems. Comm. ACM, Bd.21 H.2 , 1978*

[RoePer 99] *Röhm, W. R.; Pernul, G.: COPS: A Model and Infrastructure forSecure and Fair Electronic Markets. Thirty-Second Hawaii International Conference on S, Hawaii, Januar 1999, www-ifs.uni-regensburg.de/PDF_Publikationen/roepe99.pdf*

[RoTrMo 02] *Rosenblatt, B.; Trippe, B.; Mooney, S.: Digital Rights Management, Business and Technology. , M&T Books, New York, 2002*

[RSALabs 05] *Website der RSA Laboratories, www.rsasecurity.com/rsalabs/, letzter Abruf: 10.2.2005*

[Rump 04] *Rump, Niels: Managing Meaning - How can standards help?. , Ilmenau, Mai 2004, http://virtualgoods.tu-ilmenau.de/2004/VirtualGoodsRump.pdf*

[ScTaWo 04] *Schmidt, A. U.; Tafreschi, O.; Wolf, R.: Interoperability Challenges for DRM Systems. , Ilmenau, 2004, http://virtualgoods.tu-ilmenau.de/2004/Interoperability_Challenges_for_DRM_Systems.pdf*

[SDMI 04] *Website der Secure Digital Music Initiative (SDMI), http://www.sdmi.org/, letzter Abruf: 7.8.2004*

[Shannon 48] *Shannon, C. E.: A Mathematical Theory of Communication. The Bell System Technical Journal,, Vol. 27 Juli, Oktober, 1948*

[Shareit 05] *Website der ShareIt! Inc., www.shareit.com, letzter Abruf: 19.4.2005*

[SiNeSp 03] *Siebenhaar, F; Neubauer, C.; Spinnler, W.: Technische Aspekte eines neuartigen digitalen Rechtemanagementsystems. 2. Thüringer Medienseminar, Erfurt, Mai 2003,*

[SpGrNüLa 02] *Sporer, Thomas; Grimm, Rüdiger; Nützel, Jürgen; Langbein, Marko: Verfahren zur Kennzeichnung einer virtuellen Ware und Vorrichtung zur Bereitstellung einer Kennzeichnung für eine virtuelle Ware, Offenlegungsschrift , DE 000010217862 A1, Anmeldung: 22.4.2002, Offenlegung: 13.11.2003*

[SpinOff 02] *Web-Portal des PC-Spiels SpinOff, http://spinoff.4fo.de/ger/feature/, letzte Änderung: 6.4.2002*

[Spranger 22] *Spranger, Eduard: Lebensformen. 3. Auflage, Verlag von Max Niemeyer, Halle, 1922*

[Spread 05] *The fascinating story of the lamarr/antheil spread-spectrum patent, http://www.ncafe.com/chris/pat2/, letzter Abruf: 11.4.2005 Beaumont, Chris*

[Stähler 02] *Stähler, Patrick: Geschäftsmodelle in der digitalen Ökonomie: Merkmale, Strategien und Auswirkungen. 2. Auflage, Josef Eul Verlag, Lohmar - Köln, 2002*

[Stelzer 04] *Stelzer, Dirk: Produktion digitaler Güter. Seite(n):233-250 in Entwicklungen im Produktionsmanagement, Hrsg.: Braßler, Axel; Corsten, Hans, Vahlen, München, 2004*

[Tanenbaum 92] *Tanenbaum, Andrew S.: Computer-Netzwerke. 2. Auflage, Wolfram's Fachverlag, Attenkirchen, 1992*

[TDDSG 97] *Gesetz über den Datenschutz bei Telediensten - TDDSG. Gesetz, Juli 1997, http://bundesrecht.juris.de/bundesrecht/tddsg/*

[Timmers 00] *Timmers, Paul: Electronic Commerce: Strategies and Models for Business-to-Business Trading. , John Wiley & Sons, Chichester, 2000*

[TPay 05] *Website des T-Pay-Systems, www.t-pay.de, letzter Abruf: 13.2.2005*

[UML 04] *UML (Unified Modeling Language) Resource Page, www.uml.org, letztes Update: 29.3.2004*

[UrhG 03] *UrhG, Gesetz über Urheberrecht und verwandte Schutzrechte. Gesetz, September 2003, http://bundesrecht.juris.de/bundesrecht/urhg/gesamt.pdf*

[Völz 82] *Völz, Horst: Information I. , Akademie Verlag, Berlin, 1982*

[Völz 83] *Völz, Horst: Information II. , Akademie Verlag, Berlin, 1983*

[Völz 87] *Völz, Horst: Taschenbuch der Elektrotechnik. Seite(n):156-171 in Grundlagen der Informationstechnik, Band 2 Hrsg.: Philippow, Eugen, VEB Verlag Technik, Leipzig, 1987*

[Völz 91] *Völz, Horst: Grundlagen der Information. , Akademie Verlag, Berlin, 1991*

[W3C 02] *W3C: Web Services Architecture (Working Draft). , 2002, www.w3.org/TR/2002/WD-ws-arch-20021114/*

[W3CODRL 02] *W3C: Open Digital Rights Language (ODRL) Version 1.1. , 2002, http://www.w3.org/TR/odrl/*

[WEBDE 05] *Webportal WEB.DE, http://web.de, letzter Abruf: 13.2.2005*

[Weber 98] *Weber, Ricarda: Chablis - Market Analysis of Digital Payment Systems, Forschungsbericht , 1998, www.cg.cs.tu-bs.de/V3D2/pubs.collection/chablis-marktanalyse.pdf*

[Weedshare 05] *Website des Weedshare Systems, www.weedshare.com, letzter Abruf: 26.4.2005*

[Wiener 65] *Wiener, Norbert: Cybernetics or the Control and Communication in the Animal and the Machine. Second Edition, MIT Press, Cambridge, 1965*

[WikiCMS 05] *Wikipedia-Eintrag zu Content-Management-System, http://de.wikipedia.org/wiki/Content_Management_System, letzte Änderung: 6.4.2005*

[WikiDAT 04] Wikipedia-Eintrag zum Begriff DAT (Digital Audio Tape), http://en.wikipedia.org/wiki/DAT, letzter Abruf: 7.8.2004

[WikiDFSG 05] Wikipedia Eintrag zu den Debian Free Software Guidelines, de.wikipedia.org/wiki/Debian_Free_Software_Guidelines, letzte Änderung: 25.2.2005

[WikiECC 04] Wikipedia-Eintrag zum Begriff Elliptic curve cryptography, http://en.wikipedia.org/wiki/Elliptic_curve_cryptography, Letzter Abruf: 5.8.2004

[WikiEntropie 04] Wikipedia-Eintrag zum Begriff Entropie, http://de.wikipedia.org/wiki/Entropie_(Informationstheorie), letzte Änderung: 21.10.2004

[WikiFelten 04] Wikipedia-Eintrag zur Person Edward Felten, http://en.wikipedia.org/wiki/Edward_Felten, letzter Abruf: 7.8.2004

[WikiFrankel 05] Wikipedia-Eintrag zu Justin Frankel, http://en.wikipedia.org/wiki/Justin_Frankel, letzte Änderung: 17.2.2005

[WikiFreeRider 05] Wikipedia-Eintrag zum Free-Rider-Problem, http://en.wikipedia.org/wiki/Free_rider, letzte Änderung: 25.2.2005

[WikiGeld 04] Wikipedia-Eintrag zum Begriff Geld, http://de.wikipedia.org/wiki/Geld, Letzter Abruf: 2.8.2004

[WikiGut 05] Wikipedia-Eintrag zum Begriff Ökonomisches Gut, http://de.wikipedia.org/wiki/Gut_(ökonomisch), letzte Änderung: 5.2.2005

[WikiInfo 04] Wikipedia-Eintrag zum Begriff Information, http://de.wikipedia.org/wiki/Information, letzte Änderung: 13.10.2004

[WikiKorr 05] Wikipedia Eintrag zum Korrelationskoeffizienten, http://de.wikipedia.org/wiki/Korrelationskoeffizient, letzte Änderung: 23.4.2005

[WikiNapster 05] Wikipedia-Eintrag zum Napster P2P-System, http://en.wikipedia.org/wiki/Napster, letzte Änderung: 8.4.2005

[WikiNGSCB 04] Wikipedia-Eintrag zum Begriff NGSCB, http://de.wikipedia.org/wiki/NGSCB, Letzter Abruf: 5.8.2004

[WikiObfus 05] Wikipedia Eintrag zu Code Obfuscation, http://en.wikipedia.org/wiki/Obfuscation, letzte Änderung: 17.4.2005

[WikiPGP 05] Wikipedia-Eintrag zu PGP (pretty good privacy), http://en.wikipedia.org/wiki/Pretty_Good_Privacy, letzte Änderung: 10.2.2005

[WikiPhono 04] Wikipedia-Eintrag zum Thema Phonograph, http://en.wikipedia.org/wiki/Phonograph, letzte Änderung: 31.7.2004

[WikiSignatur 04] Wikipedia-Eintrag zum Thema Digitale Signatur, http://de.wikipedia.org/wiki/Digitale_Signatur, letzte Änderung: 16.8.2004

[WikiSWare 05] Wikipedia-Eintrag zu Shareware, http://en.wikipedia.org/wiki/Shareware, letzte Änderung: 7.5.2005

[WikiTGC 04] Wikipedia-Eintrag zum Begriff Trusted Computing Group, http://de.wikipedia.org/wiki/Trusted_Computing, Letzter Abruf: 5.8.2004

[WikiTPM 04] Wikipedia-Eintrag zum Begriff Trusted Platfom Module, http://de.wikipedia.org/wiki/TPM, Letzter Abruf: 5.8.2004

[WikiVWL 04] Wikipedia-Eintrag zur Volkswirtschaftslehre, http://de.wikipedia.org/wiki/Volkswirtschaftslehre, letzte Änderung: 15.9.2004

[WikiWiener 04] Wikipedia-Eintrag zu Norbert Wiener, http://de.wikipedia.org/wiki/Norbert_Wiener, letzte Änderung: 10.9.2004

[WikiXP 04] Wikipedia-Eintrag zur Produktaktivierung von Windows XP, http://en.wikipedia.org/wiki/Windows_XP_Professional#Product_activation, letzte Änderung: 6.9.2004

[WirKle 00] Wirtz, B. W.; Kleineicken, A.: Geschäftsmodelltypen im Internet. WiSt - Wirtschaftswissenschaftliches Studium, Heft 11 November, 2000

[WMRM 05] *Website von Micrsoft zum Windows Media Rights Manager, www.microsoft.com/windows/windowsmedia/drm/, letzter Abruf: 9.4.2005*

[Wobst 98] *Wobst, Reinhard: Abenteuer Kryptologie. 2. Auflage, Addison-Wesley-Longman, Bonn, 1998*

[Wöhner 05] *Wöhner, Thomas: Analyse und Bewertung von Kopierschutzverfahren für Audio-CDs. Seite(n):175-188 in Sicherheit, GI LNI 62 Hrsg.: Federrath, Hannes, Bonner Köllen Verlag, Regensburg, 2005*

[XRML 05] *Website der Firma ContentGuard zu XrML, www.xrml.org, letzter Abruf: 20.4.2005*

[Zerdick u.a. 01] *Zerdick, A.; Picot, A.; Schrape, K.; Artopé, A.; Goldhammer, K.; Lange, U.: Die Internet-Ökonomie - Strategien für die digitale Wirtschaft. 3. Auflage, Springer-Verlag, Berlin, Heidelberg, 2001*

[Zheng 97] *Zheng, Y.: Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption).. Seite(n):165-179 in Advances in Cryptology, CRYPTO '97 LNCS 1294 Hrsg.: Kaliski Jr, B. S., Springer, Berlin, Heidelberg, 1997*

[Zimmermann 03a] *Zimmermann, Frank: Entwurf und Implementierung eines User-File-Matching-Algorithmus unter Verwendung eines MySQL-Datenbanksystems im Potato-System. Studienjahresarbeit TU-Ilmenau , 2003, www.4fo.de/de/students.htm#zimmermann*

[Zimmermann 03b] *Zimmermann, Frank: Entwurf und Realisierung neuer Infrastrukturen für den Offline-Handel von virtuellen Waren mit mobilen Endgeräten. Diplomarbeit TU-Ilmenau 2003-10-07/063/IN98/2231, 2003, www.4fo.de/de/students.htm#zimmermann2*

[Zimmermann 95] *Zimmermann, Philip R.: The Official PGP User's Guide. , The MIT Press, Cambridge, 1995*

[Zobel 02] *Zobel, Angelika: Kriterien zur Bewertung elektronischer Zahlungssysteme. Diplomarbeit TU-Ilmenau , 2002, www.tu-ilmenau.de/site/mma/Diplomarbeiten.795.0.html*

Erklärung

Ich erkläre hiermit, dass ich die vorliegende Arbeit ohne unzulässige Hilfe Dritter und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe. Das aus anderen Quellen direkt oder indirekt übernommene Material ist als solches unter der Angabe der Quelle gekennzeichnet.

Bei der Durchführung der Forschungsarbeiten, die dieser Arbeit zugrunde liegen, und der Erstellung der Arbeit selbst waren die nachstehend aufgeführten Personen in der jeweils beschriebenen Weise beteiligt:

- Der von mir betreute und angeleitete Diplomand Oliver Lorenz recherchierte zum Thema Online-Bezahlsysteme. Diese Recherche beeinflusste meine Ausführungen zu Bezahlsystemen in Kapitel 5.1 und 5.2.
- Die Studentin Kathleen Biedermann lieferte im Rahmen ihrer von mir betreuten Studienarbeit diverse Anregungen auf dem Gebiet der Erlös- und Geschäftsmodelle. Dies floss in die Kapitel 3.5 und 3.6 ein.

Die Arbeit wurde bisher weder im Inland noch im Ausland in gleicher oder ähnlicher Form einem anderen Prüfungsgremium vorgelegt.

Ilmenau, den 4.5.2005

Statistik:

Datum	*Wörter*	*Buchstaben/10*	*Größe/MB*10000*
07.09.03	386	283	240
27.09.03	742	545,3	230
05.10.03	1328	971,4	410
24.10.03	2140	1550,5	620
24.10.03	2140	1550,5	620
04.01.04	3450	2549,2	2340
04.01.04	3450	2549,2	2340
04.01.04	3450	2549,2	2340
28.03.04	5396	3988,5	16500
02.05.04	6720	5041,8	16100
02.05.04	6720	5041,8	16100
12.07.04	10224	7707	18600
01.08.04	15253	11380	20100
30.08.04	21591	15993,9	22900
20.10.04	23172	17140,3	25900
31.10.04	23579	17438,9	26000
20.11.04	26469	19609,7	26600
30.11.04	27069	20049,4	26600
02.01.05	30607	22594,3	27300
14.01.05	32753	24109,8	28000
01.02.05	33809	24862,5	28200
17.02.05	35934	26439,2	30100
01.03.05	37180	27362,1	30200
23.03.05	38871	28575,3	29500
01.04.05	41336	30353,1	30100
21.04.05	46346	33953,6	31500
02.05.05	50987	37320	34500
10.05.05	54182	39665,6	34700