# Abschlussbericht

DFN-Projekt TK 602-SD 116
gefördert vom Bundesministerium für Bildung und Forschung

# Zahlungsserver Chablis PS (Chablis Payment Server)

Projektleitung: Prof. Dr. Anne Brüggemann-Klein

Martin Stumpf, Thomas Schöpf
Technische Universität München

30. März 2004

# Inhaltsverzeichnis

# 1 Einleitung

Das Projekt „Chablis PS“ wurde gefördert durch den Verein zur Förderung eines Deutschen Forschungsnetzes – DFN-Verein – aus Mitteln des Bundesministeriums für Bildung und Forschung – BMBF – unter der Nummer TK 602-SD116.
Das Projekt lief von 1. Oktober 2000 bis 31. Dezember 2003. Die Projektaufgabe bestand darin, einen Zahlungsserver zu entwickeln, der es Händlern im Internet ermöglicht, ihre Waren, Dokumente und Dienstleistungen anzubieten und von den Kunden auf elektronischem Weg bezahlen zu lassen. Für diese Bezahlung greift der Zahlungsserver auf Zahlungssysteme zurück, die für die Verbindung in das Netz von Banken und Kreditkartengesellschaften u.ä. sorgen. Er bietet aber auch wichtige zusätzliche Funktionen. So stellt der Zahlungsserver den Dienstanbietern und Dienstnutzern die Funktionen von unterschiedlichen elektronischen Zahlungssystemen unter einer einheitlichen Schnittstelle zur Verfügung.
In diesem Abschlussbericht werden die Ergebnisse und Erkenntnisse dargestellt, die während der Projektlaufzeit erreicht wurden.

# 2 Funktionalität des Zahlungsservers

Die Funktionalität des Chablis Zahlungsservers soll hier aus den drei unterschiedlichen Perspektiven von Kunden, Händlern und Administratoren beschrieben werden. Dabei handelt es sich um eine Black-Box-Sicht, die nur die nach außen hin sichtbare Funktionalität beschreibt, aber nicht die interne Implementierung.

## *2.1 Kundensicht*

Der Kunde ist die Person, die bei einem Händler einkauft, der den Chablis Zahlungsserver einsetzt. Im Normalfall wird sich für den Kunden im Zahlungsablauf nichts im Vergleich zum Einkauf bei einem anderen Händler ohne Chablis ändern. Dies ist von Vorteil, da sich der Kunde damit nicht auf eine andere Vorgehensweise umstellen muss. Der Kunde braucht nur den üblichen Web-Browser und muss keine zusätzliche Software installieren. Der Kunde kann eines der vom Zahlungsserver angebotenen Zahlungssysteme (z. B. Kreditkarte, Lastschrift, Paybox) auswählen und über dieses die Transaktion abwickeln. Vor der finalen Zahlungsbestätigung wird dem Kunden von Chablis noch einmal der Inhalt des Warenkorbs angezeigt, wie er vom Händler übermittelt wurde. D. h. hier kann der Kunde eine letzte Überprüfung vornehmen und sich diese Informationen gegebenenfalls auch abspeichern.
Ein Sonderfall im Zahlungsablauf tritt dann auf, falls der Händler eine Authentifizierung des Kunden verlangt. Dann muss der Kunde ein entsprechendes X.509 Zertifikat in seinem Browser installiert haben, das ihn als vertrauenswürdig ausweist. Abgesehen davon, läuft auch hier die Zahlung so wie üblich ab. In beiden Fällen werden alle Transaktionen von Chablis mitprotokolliert, so dass im Streitfall bezüglich des Zahlungsvorgangs zwischen Händler und Kunden die Auftragsdatensätze vom Chablis-Betreiber zur Überprüfung bereitgestellt werden können.

## *2.2 Händlersicht*

Für den Händler sind neben der Schnittstelle zum Kunden noch zwei andere Schnittstellen von Chablis interessant: zum einen die Schnittstelle für die Integration in seinen Shop und zum anderen die Schnittstelle zur Integration in seine Buchhaltung.

Wenn der Händler keinen Zahlungsserver wie Chablis einsetzt, besteht die Shopintegration aus der Anbindung jedes einzelnen gewünschten Zahlungssystems. Diese Integration fällt für jedes Zahlungssystem erneut an. Beim Einsatz von Chablis muss der Händler dagegen nur einmal den Chablis Zahlungsserver anbinden und kann dann auf Grund der virtualisierten Schnittstelle jedes dort integrierte Zahlungssystem nutzen, ohne dass er weiteren Aufwand betreiben muss. Dadurch kann Einiges an Arbeitszeit und Kosten gespart werden. Sobald neue Zahlungssysteme in Chablis integriert werden, stehen diese automatisch auch im Shop zur Verfügung.
Wird eine Zahlung von einem Kunden des Händlers angestoßen, werden die Bestelldaten von Chablis kontrolliert und anschließend die Zahlung angewiesen. Sobald die Transaktion vom ausgewählten Zahlungssystem akzeptiert wurde, wird das Händlersystem von Chablis benachrichtigt, dass die Auslieferung erfolgen kann.
Die Integration in die Buchhaltung betrifft zum einen die nachträglichen Buchungsmöglichkeiten und zum anderen den Geldfluss. Nachträgliche Buchungsmöglichkeiten bestehen in Form von Teilbuchungen, Gutschriften und Stornos.
Der Geldfluss läuft bei jedem Zahlungssystem proprietär in Form von eigenen Rechnungsformaten und Gebührenverrechnungsmodellen ab. Chablis übernimmt auch hier eine Virtualisierung. So werden die Buchungen gesammelt und in regelmäßigen Abständen an die Händler überwiesen. Dies geschieht zahlungssystemübergreifend, so dass für verschiedene Zahlungssysteme keine eigenen Buchhaltungsanpassungen mehr nötig sind.
Diese Virtualisierung läßt sich auch einsetzen bei Abrechnungen von Umsätzen für Einrichtungen der öffentlichen Hand. Hier müssen in der Regel Zahlungen in der selben Höhe eingehen, wie sie dem Käufer in Rechnung gestellt wurden. Da die Zahlungssysteme jedoch im Normalfall eine Provision einbehalten, kann diese Anforderung durch einen Chablis-Betreiber gewährleistet werden, der die Gutschriften in voller Rechnungshöhe vornimmt und die einbehaltenen Provisionen der Einrichtung getrennt in Rechnung stellt.

## *2.3 Administratorsicht*

Die dritte und letzte Sicht ist die des Administrators. Hierbei kann man wiederum zwischen dem Administrator des Händlers und des Betreibers des Chablis Zahlungsservers unterscheiden. Der Administrator des Händlers hat eine eingeschränkte Funktionalität und sieht nur die Daten, die zum eigenen Shop gehören und kann natürlich auch keine Systemeinstellungen verändern. Alle Einstellungen sind über eine Web-Schnittstelle zugreifbar. So können Protokolle, Statistiken, Transaktionen, gespeicherte Zahlungsdaten und die aktuelle Auslastung des Servers abgefragt werden.
Für den Betreiber besteht zusätzlich die Möglichkeit, die allgemeine Konfiguration des Servers sowie angepasste Konfigurationen von Händlern und Zahlungssystemen im laufenden Betrieb neu zu laden. Daneben können neue Händler und neue Zahlungssysteme ohne Neustart des Servers eingerichtet werden.
Zur Datensicherung und -archivierung können die Datenbankinhalte in XML-Dateien exportiert werden.

## *2.4 Bedienungsanleitung*

Eine detailliertere Beschreibung der Funktionalität, die den Kunden, den Händlern und den Administratoren zur Verfügung steht, ist im Handbuch zum Chablis Zah-

lungserver zu finden. Das Handbuch steht im Internet unter http://chablis.in.tum.de/papers/handbuch.pdf zum Download zur Verfügung.
Das Handbuch beschreibt sowohl die Installationsanforderungen und -durchführung des Zahlungsservers als auch die Integration in bestehende Shopsysteme und die Bedienung der Verwaltungsschnittstellen.
Es werden die Einstellungen erläutert, die zur Konfiguration des Zahlungsbetriebs und des Loggings dienen. Das Handbuch stellt alle Möglichkeiten zur Administration in der Web-Schnittstelle dar und beschreibt die Integration in einen Shop, die anhand eines Beispiels erklärt wird.
Daneben wird dort die Schnittstelle für die Integration neuer Zahlungssysteme in den Zahlungsserver dokumentiert. Die bereits angebundenen Zahlungssystemmodule (zum Zeitpunkt der Handbucherstellung waren das Paybox und Telecash X-Pay) sind ebenfalls dort beschrieben.

## *2.5 Bestell- und Warenkorbverwaltungskomponente*

In der Händlerverwaltungsschnittstelle wird eine Übersicht über alle bislang getätigten Transaktionen angeboten. Jede Transaktion besitzt eine Transaktionsnummer (eindeutig für den Händler und den Kunden), eine ProcessId (eindeutig innerhalb von Chablis), eine Händlerkennung, die Kundennummer, das ausgewählte Zahlungssystem und Informationen über die Zeitpunkte der Bestellung (beim Händler) sowie den Eingang der Transaktion bei Chablis.
Für jede Bestellung eines Kunden bei einem Händler wird eine solche Transaktion erzeugt. Der Administrator des Händlers kann sich nur die Transaktionen seiner Mall ansehen, während der Chablis-Administrator Zugriff auf die Transaktionen aller Malls besitzt.
Die Transaktionen können nach verschiedenen Kritierien gefiltert werden (z. B. nur bestimmte Kunden, nur ein bestimmter Zeitraum, nur ein bestimmtes Zahlungssystem oder nur Transaktionen mit einem bestimmten Status).
Für jede Transaktion ist außerdem der Inhalt des Warenkorbs gespeichert, den der Kunde bestellt hat. Auf diese Weise kann der Administrator im Nachhinein noch auf diese Daten zugreifen.

## *2.6 Administrations- und Statistikschnittstelle (Betreiber/Händler)*

In der Administrations- und Statistikschnittstelle sind verschiedene Verwaltungsmöglichkeiten für den Händler und den Chablis-Administrator verfügbar. Diese Schnittstelle arbeitet mit clientauthentifiziertem HTTPS, d. h. für den Zugriff muss im Browser ein entsprechendes Zertifikat vorhanden sein.
Bevor Chablis verwendet werden kann, muss die Datenbank angelegt werden. Dies kann im Datenbank Manager bei Bedarf manuell erledigt werden. Normalerweise erkennt Chablis jedoch automatisch, wenn Datenbanktabellen erzeugt oder aktualisiert werden müssen, und führt die entsprechenden Operationen durch. Neben der Erzeugung der Datenbanken können die Datenbanken selektiv gelöscht werden oder es können manuelle Updates durchgeführt werden. Außerdem können ausgewählte Module in eine XML Datei exportiert und Daten aus einer XML Datei wieder zurück importiert werden. Über die Funktion „Log und Transaktionen aufräumen“ können alle Datenbankeinträge für das Log und für Transaktionen gelöscht werden, die vor einem bestimmten Datum liegen.
Über den Punkt „Modul Installation“ kann der Chablis-Administrator speziell vorbereitete Software-Module nachinstallieren. Insbesondere Module für neue Zahlungs-

systeme bieten sich hier an, allerdings könnte auch Chablis selbst auf diesem Weg aktualisiert werden. Zunächst wird das neue Modul in Form einer JAR-Datei (Java ARchive) hochgeladen. Anschließend können (je nach Modul) Konfigurationen vorgenommen werden. Zum Schluss werden die neuen Dateien in die WAR-Datei (Webapplication ARchive) von Chablis übertragen. Die Ursprungsdatei wird dabei vorher gesichert. Ein Neustart von Chablis muss vom Administrator manuell durchgeführt werden.
Im Log werden die Protokollmeldungen von Chablis angezeigt. Es gibt verschiedene Schweregrade und die Einträge können nach verschiedenen Kriterien gefiltert werden.
In der Statistikschnittstelle werden Daten über bereits abgelaufene Zahlungen angezeigt. Dabei werden die Daten sowohl zusammengefasst für alle Malls als auch getrennt für jede Mall einzeln dargestellt. Darüberhinaus werden noch die einzelnen Zahlungssysteme getrennt aufgeschlüsselt.
In der aktuellen Auslastung wird die Anzahl der aktuell ablaufenden Zahlungen angezeigt. Der Chablis-Administrator sieht die Auflistung sowohl für den gesamten Zahlungsserver als auch für die einzelnen angeschlossenen Malls. Die Mall- Administratoren haben nur Zugriff auf die Auflistung für ihren Shop. Die Auflistung ist unterteilt in die verschiedenen Zahlungssysteme und die unterschiedlichen Zahlungsarten. Neben den aktiven Zahlungen werden auch sogenannte wartende Zahlungen gezählt. Dabei handelt es sich um Zahlungen, die noch nicht aktiv sind, da ein eingestelltes Parallelitätslimit für aktive Zahlungen im Zahlungsserver erreicht ist.
In der Zahlungssystemliste werden alle angeschlossenen Zahlungssysteme aufgelistet. Der Chablis- Administrator hat die Möglichkeit, die gesamte Zahlungsschnittstelle zu deaktivieren (z.B. um einen Systemneustart vorzubereiten) oder nach Änderungen in der Konfiguration die Zahlungssysteme neu zu laden. Dieses Deaktivieren/Neustarten ist auch selektiv für einzelne Zahlungssysteme möglich. Außerdem wird bei einem Klick auf die Zahlungssystem-Kennung die Konfiguration des Zahlungssystems angezeigt.
In der Händlerliste werden alle angeschlossenen Händler (Malls) aufgelistet. Die verfügbaren Funktionen sind gegenüber der Zahlungssystemliste etwas eingeschränkt. So stehen nur die Möglichkeiten zur Verfügung, eine Mall zu deaktivieren/aktivieren und die Einstellungen neu zu laden. Ein Klick auf die MallId zeigt die aktuellen Einstellungen dieser Mall an.
Im Abschnitt „Chablis-Einstellungen“ kann der Chablis-Administrator die Einstellungen für den Chablis Zahlungsserver einsehen. Die Einstellungen sind in zwei Bereiche unterteilt. Der erste Bereich deckt den eigentlichen Zahlungsserver ab, während der zweite die Einstellungen für das Logging festlegt.
Chablis liest an mehreren Stellen den Inhalt von Dateien oder URLs ein und gibt ihn wieder aus. Zur Verbesserung der Performance können dabei Inhalte, die statischen Charakter besitzen (z.B. Stylesheet Dateien) beim ersten Zugriff in einen internen Cache abgelegt werden und müssen so beim nächsten Mal nicht erneut eingelesen werden. Diese Übersicht listet alle aktuellen Einträge des Cache auf. Neben der Quelle und der Größe wird auch angezeigt, wie oft der Inhalt bereits aus dem Cache verwendet wurde. Der Chablis-Administrator hat die Möglichkeit, den gesamten Cache zu leeren, oder nur einzelne Einträge aus dem Cache zu entfernen.
Wenn es vom Händler gewünscht und vom Zahlungssystem unterstützt wird, kann Chablis die Zahldaten des Kunden speichern. Dies kann verwendet werden, um beim nächsten Besuch des Kunden die Formularfelder mit den Zahldaten vorzuinitialisieren. Dazu wird der zuletzt eingegebene Wert verwendet. In dieser Übersicht

werden die Zahlungsdaten für jede Mall, für jedes Zahlungssystem und jeden Kunden angezeigt, zusammen mit der Information, wann der letzte Zugriff auf diese Daten erfolgte.
Zu den in der Statistikschnittstelle angezeigten Informationen gehören etwa die Anzahl der erfolgreich durchgelaufenen Transaktionen, die noch offenen Transaktionen, die nicht erfolgreichen Transaktionen und Zahlungen sowie Informationen über die zeitliche Verteilung der Transaktionen inkl. einer graphischen Darstellung der Transaktionsvolumina. Daneben werden die aufgetretenen Fehlerursachen ausgewertet und angezeigt.

## *2.7 Guthabenkonten (Vorkassezahlungssystem)*

Neben den angebundenen Zahlungssystemen von anderen Anbietern wurde ein weiteres Zahlungssystem speziell für Chablis entwickelt. Dieses Vorkassesystem ist ein im Chablis-Zahlungsserver integriertes Zahlungssystem. Bei ihm kann ein vorher erstelltes Vorkassekonto mit Hilfe der anderen im Chablisserver integrierten Zahlungssysteme aufgeladen werden. Anschließend steht dem Kunden ein entsprechender Geldbetrag zur Verfügung, den er nun über das Vorkassezahlungssystem im Chablisserver ausgeben kann. Für kreditwürdige Kunden kann auch ein Sammelbuchungsmodus freigeschaltet werden, der den Kunden erst bei Erreichen seines Kreditlimits zur Zahlung seiner Transaktionen auffordert. Der Kunde muss dann nicht mehr in Vorleistung treten. Beide Varianten haben den Zweck, durch Transaktionssammlung Micropayments mit Zahlungssystemen zu ermöglichen, die dafür selbst eigentlich zu teuer sind.
Neben der Zahlfunktionalität hat der Kunde auch Zugang zu einem Servicebereich. Nach einer entsprechenden Authentifizierung über Login und Passwort kann er sich in Form eines „Einzelverbindungsnachweises“ alle von ihm getätigten Transaktionen auflisten lassen, seine Zugangsdaten aktualisieren oder auch sein Konto aufladen.
Der Administrator kann sich anhand des Verwaltungssystems einen Überblick über die Kunden und ihre Konten verschaffen und eventuell notwendige Aktionen (Kundensperrung, Kreditlimitanpassung, Sammelbuchungsmodus) durchführen.

## *2.8 Abrechnungsautomatisierung*

In Chablis fallen für jeden Zahlungsvorgang interne Buchungsdaten an, die in der Bestellverwaltungskomponente einsehbar sind. Allerdings existieren diese Buchungen zunächst nur innerhalb des Rechners und werden zeitverzögert auf dem Bankkonto vorgenommen. Wie dies genau geschieht, d. h. mit welcher Zeitverzögerung und mit welcher Granularität, liegt am einzelnen Zahlungssystem. Grundsätzlich können folgende Situationen auftreten:

1. Eine Buchung in Chablis entspricht genau einer Buchung auf dem Konto.
2. Eine Buchung in Chablis führt zu mehreren Buchungen auf dem Konto.
3. Mehrere Buchungen in Chablis werden zu einer einzigen Buchung auf dem Konto zusammengefasst.

Chablis bietet eine Schnittstelle, um die Buchungsdaten des Bankkontos über das Datenträgeraustauschformat (DTAUS) zu importieren. Dabei werden alle drei genannten Fälle berücksichtigt. Nur die zahlungssystemabhängige Zuordnung konnte noch nicht implementiert werden, da die erforderlichen DTAUS-Daten leider nicht zur Verfügung standen.

## *2.9 Unterstützung unterschiedlicher Währungen*

Chablis arbeitet intern währungsunabhängig und unterstützt somit alle Währungen, die auch die angeschlossenen Zahlungssysteme verarbeiten können. Es kann für jedes Zahlungssystem und für jeden Händler ausgewählt werden, welche der unterstützten Währungen er seinen Kunden anbieten möchte.

## *2.10 Treuhänderfunktion*

Die Treuhänderfunktion von Chablis ergibt sich für den Fall, dass Chablis von einem unabhängigen Betreiber betrieben wird. Wenn der Kunde einen Warenkorb zusammengestellt hat und diesen bezahlen will, wird zunächst der Inhalt dieses Warenkorbs an Chablis übermittelt. Chablis zeigt dem Kunden den Warenkorb noch einmal an, bevor dieser die Bezahlung ausführt. Dadurch hat Chablis den Nachweis, daß der Kunde den Warenkorb noch einmal gesehen und bestätigt hat.
Vergleichbares gilt für den Händler. Dieser schickt Chablis vor der Bezahlung durch den Kunden den Warenkorb auf einem gesicherten Weg erneut zu und Chablis vergleicht diesen Warenkorb mit den Daten, die vom Kunden kamen.
Dadurch kann Chablis nachweisen, dass sowohl Kunde als auch Händler den gleichen Warenkorb gesehen haben. Im Falle von Streitigkeiten zwischen Händler und Kunde (z. B. wegen einer Falschlieferung) können diese Daten verwendet werden, um den Streit zu klären.

## *2.11 Erweiterung des Zahlungsservers*

Zum Zeitpunkt des Projektantrags war bereits eine prototypische Zahlungsserver-Software vorhanden, die in einem Vorgängerprojekt (gefördert von der DFG im Rahmen des V3D2 Programms) entwickelt wurde.
Diese Software sollte nach einer Konsolidierung in diesem Entwicklungsschritt um einige Funktionen erweitert werden, die noch nicht vorhanden waren.
In der Konsolidierungsphase gleich nach Beginn des Projekts wurde jedoch klar, dass diese Software nicht sinnvoll weiter zu verwenden war, da die internen Abläufe und Programmstrukturen sehr eng mit den angebundenen Zahlungssystemen verknüpft waren. Diese Zahlungssysteme (CyberCash, eCash, MilliCent, MiniPay) waren bereits bei Projektbeginn in einem Zustand, der größere Anpassungen erforderlich machte: CyberCash und MiniPay waren in einer neuen Version auf dem Markt erschienen, die nicht mehr kompatibel zur alten Version war. CyberCash war nicht lauffähig und wurde während der Phase der Fehlersuche zu Gunsten eines neuen, inkompatiblen Verfahrens vom Betreiber eingestellt. Compaq/DEC fand für MilliCent keine Partner für die USA und Europa und entschloss sich daher, dieses Zahlungssystem nur noch in Japan weiter zu unterstützen, wo bereits ein Partner vorhanden war.
Neue Zahlungssysteme hätten nur mit sehr hohem Anpassungsaufwand integriert werden können. Ingesamt wäre die Umstellung, Anpassung und Erweiterung der bestehenden Software höchstens mit einem solch erheblichen Arbeitsaufwand möglich gewesen, dass es sinnvoller war, eine Neuentwicklung zu beginnen. Bei dieser Neuentwicklung wurden dann zum einen die Schnittstellen zu den Zahlungssystemen derart gestaltet, dass zukünftige Zahlungssysteme integriert werden können, ohne am internen Ablauf des Chablis-Servers erneut Veränderungen vornehmen zu müssen. Zum anderen wurde die Schnittstelle zu den Shop-Systemen der Händler deutlich vereinfacht. Bislang erfolgte die Kommunikation zwischen Händlershop und Chablis Zahlungsserver über einen eigenen TCP Kanal. Beim Neuentwurf wurden, wie von anderen, kommerziellen Zahlungsservern (z.B. Telecash/Brokat X-Pay, Atos Posei-

don) auch, einfache CGI-Aufrufe benutzt, so dass der Zahlungsserver von den Shopbetreibern deutlich einfacher zu integrieren ist.
Neben der oben beschriebenen Umstellung und Neuentwicklung wurden auch die weiteren im Projektantrag angestrebten neuen Funktionalitäten integriert.

### *2.11.1 Rückvergütung und Zahlungsstornierung*

Die Unterstützung von Rückvergütungen und Zahlungsstornierungen wurde für alle Zahlungssysteme integriert, die diese Funktionalität unterstützen. Manche Zahlungssysteme wie etwa Kreditkarte unterstützen die Zahlungsstornierung nur in einem bestimmten Zeitraum (in diesem Fall bis zum Ende des Geschäftstages), danach kann jedoch eine Rückvergütung durchgeführt werden.
Beide Funktionalitäten (Rückvergütung und Zahlungsstornierung) sind in die Warenkorb- und Bestellverwaltungskomponente integriert. Der Administrator des Händlers und der Chablis-Administrator haben hier die Möglichkeit, die verfügbaren Operationen durchzuführen. Im Ergebnis wird dann zur vorhandenen Transaktion eine weitere Zahlung angelegt, über die der Administrator den Erfolg der Rückvergütung bzw. Stornierung einsehen kann.

### *2.11.2 Transaktionssicherung*

Bei den eingesetzten Zahlungssystemen handelt es sich um fertige Software, die von einem Drittanbieter zur Verfügung gestellt wird. Dementsprechend stellt diese Software eine Black-Box dar und läßt sich durch Chablis nicht verändern. Auch das Verhalten der Zahlungssysteme (z. B. wann tatsächlich gebucht wird und welche Widerrufsrechte dem Kunden eingeräumt werden) sind nicht veränderbar. Um eine technische Sicherung einer Transaktion in dem Sinne zu erreichen, dass die Lieferung untrennbar mit der Bezahlung verknüpft wird, wäre dies jedoch erforderlich. Das, was Chablis allerdings tun kann, ist, den Ablauf der Transaktion soweit zu protokollieren und festzuhalten, dass bei Streitigkeiten festgestellt werden kann, an welcher Stelle die Transaktion unterbrochen wurde. Wenn nun der Chablis Zahlungsserver von einer vertrauenswürdigen, unabhängigen Einrichtung betrieben wird und die Gelder über das Betreiberkonto fließen, kommt dies einer Treuhänderfunktion gleich.

### *2.11.3 Integration neuer Zahlungssysteme*

Wie bereits erwähnt wurde, funktionierte durch die Weiterentwicklung bei den Zahlungssystemen die ursprüngliche Anbindung an Chablis nicht mehr. Daher wurden alle Zahlungssysteme im Laufe des Projekts neu und erstmalig angebunden. Zunächst waren dies die Bezahlarten Kreditkarte (per SSL und SET), Lastschrift und Geldkarte. Die Anbindung an das Bankennetz wurde von der Firma Telecash zur Verfügung gestellt, die im Laufe des Projekts ihren Dienst jedoch auf eine neue Software umstellte, so dass auf der Seite von Chablis diese neue Schnittstelle integriert wurde. Damit waren wieder die Bezahlarten Kreditkarte (SSL) und Lastschrift (SSL) möglich. Außerdem wurde zwischen dieser Umstellung das Zahlungssystem Paybox angebunden.
Die Integration weiterer Zahlungssysteme war nicht möglich, da deren Anbieter technische Informationen und die erforderliche Software nur nach Abschluß eines kostenpflichtigen Vertrages zur Verfügung stellen wollten. Diese Verträge hätten nur von der TIB Hannover (Technische Informationsbibliothek) abgeschlossen werden können. Dort gab es jedoch die Vorgabe, dass das Zahlungssystem nicht mehr als 3% Transaktionsgebühr verlangen darf, was für kein weiteres Zahlungssystem zutraf.

# 3 Verwendete Technologien

Zur Entwicklung des Chablis Zahlungsservers wurde auf Standardsoftware aus dem Open-Source-Bereich zurückgegriffen: als Server wird die Kombination von Apache und Tomcat eingesetzt. Dementsprechend wurden für die Implementierung Java Servlets und Java Server Pages verwendet. Der Datenbankzugriff läuft über die JDBC-Schnittstelle von Java. Dabei wurde eine interne Abstraktionsschicht eingezogen, so dass die darunter liegende Datenbank ausgetauscht werden kann. Momentan kann wahlweise Oracle oder das freie PostgreSQL eingesetzt werden. Entsprechend dem SSL-Standard basiert die Sicherheitsarchitektur auf einer X.509 Public Key Infrastructure, die dazu kompatibel ist. Der Server ist daher komplett mit freier Software einsatzfähig, so dass keine Lizenzkosten für den Betrieb anfallen.
Es fallen lediglich Gebühren dafür an, dass die Zahlungssysteme die Zahlungsanforderungen in das Backend des jeweiligen Anbieters übertragen können. Dies lässt sich jedoch nicht vermeiden.

# 4 Betriebsplanung

## *4.1 Elektra*

Im Projektantrag war ursprünglich ein Testbetrieb des Chablis-Servers zusammen mit dem Elektra-System der Bibliothek der TU München geplant. Elektra sollte um einen Warenkorb erweitert werden, der das Bestellen und anschließende Bezahlen von Dokumenten über Chablis ermöglicht. Diese Testintegration konnte jedoch nicht vorgenommen werden, weil die Elektra-Software zwischenzeitlich an die Firma Sisis verkauft wurde. Diese Firma stellte jedoch keine Dokumentation zur Verfügung und war auch nicht bereit, Unterstützung zur Integration zu leisten. Sisis machte ihre Unterstützung von einer Zusage des DFN-Vereins abhängig, den Zahlungsserver nach Fertigstellung zu betreiben, die jedoch Mitte 2001 versagt wurde. Deshalb wurde im Chablis-Projekt ein eigenes Testsystem entwickelt, das die gleichen Testmöglichkeiten anbietet und zusätzlich als Beispiel für eine Warenkorbintegration auf anderen Händlersystemen verwendet werden kann. Wegen der oben beschriebenen Zusammenhänge konnte es zu keinem Testbetrieb mit Elektra kommen.

## *4.2 Subito/TIB*

Als eigentlicher Pilotbetreiber wurde im Antrag die subito-Arbeitsgemeinschaft genannt. Stellvertretend für diesen Verbund von über 25 Bibliotheken wurde die TIB Hannover, die eine führende Rolle unter den subito-Bibliotheken einnimmt, damit beauftragt, die Anpassung am vom subito-Verbund verwendeten DOD-System[1] für die gesamte Gemeinschaft vorzunehmen und in ein lauffähiges System zu überführen. Während des dortigen Chablis-Betriebs wurden von der subito-Arbeitsgemeinschaft allerdings Planungsänderungen vorgenommen, die von interaktiven Zahlungen im Web Abstand nahmen und stattdessen nachträgliche Sammelrechnungen im Batch-Betrieb ohne Kundeninteraktion einführten. Ein Webzahlungsserver konnte daher bei subito nicht mehr eingesetzt werden. Stattdessen wurde der Betrieb an der TIB im TIBORDER-System weiterhin angeboten. Die Einstellung des Betriebs an der TIB Hannover erfolgte am 30. September 2003 wegen mangelnder Nutzung (siehe Abschnitt

1 „Document Order receive and Delivery“. Das System verwaltet die Bestellung und Auslieferung von Dokumenten.

Betriebserfahrung). Die mangelnde Nutzung rührte im wesentlichen von zwei Punkten her. Erstens werden über TIBORDER zu einem hohen Anteil Bestellungen von Großkunden abgewickelt, die eigene Abrechnungsverfahren mit der TIB ausgehandelt haben. Zweitens bestand weiterhin die Möglichkeit, erst nach Rechnungsstellung per Überweisung zu bezahlen. Diese Zahlungsart ist nach wie vor im Internet die beliebteste Variante bei den Kunden. Entgegen der Erwartungen hielten die Kunden weiterhin an dieser Zahlungsart fest und nahmen die neuen Zahlungssysteme nur sehr zögerlich an. Ebenfalls sind die Kunden der TIB nur deutlich seltener als zunächst erwartet berechtigt, elektronische Zahlungsmittel einzusetzen.

# 5 Betriebsproblematik

## *5.1 Betrieb als Finanzdienstleister*

Im Laufe des Projekts wurde immer wieder nach zusätzlichen Anbietern gesucht, die Gelder über Chablis einziehen könnten (BSB, TUMorrow, Proprint, Nipon, Bremer Institut für Seeverkehrswirtschaft und Logistik, TUMTech). Dabei stellte sich den potentiellen Anbietern immer wieder die Frage, wer den Betrieb des Zahlungsservers gewährleistet. Öffentliche Einrichtungen wie die TU München oder die TIB Hannover können einen solchen Dienst nicht leisten, weil Finanzdienstleistungen nicht in ihren Aufgabenbereich hineinfallen. Bezüglich der grundsätzlichen Betriebsfähigkeit konnten bisher keine rechtlichen Bedenken festgestellt werden (siehe dazu Abschnitt 13.8, Rechtsgutachten).

Deshalb wurde bei verschiedenen Firmen und Vereinigungen angefragt: TUMTech, TUMorrow, DFN, DINI, Sisis. Leider konnten wir aber keinen Betreiber finden, der das finanzielle Risiko eingehen wollte bzw. eine zeitliche Planungsperspektive zugelassen hätte. Die Geschäftsführung der TUMorrow GmbH wäre zwar zum Betrieb bereit gewesen und hatte auch bereits ein Geschäftsmodell aufgestellt. Der Betrieb scheiterte aber am Aufsichtsrat, weil dieser grundsätzlich keinen vertraglichen Bindungen zustimmt, die über ein Jahr hinausgehen. Dies liegt daran, dass die Geschäftsführung der TUMorrow GmbH turnusmäßig einmal im Jahr wechselt.

## *5.2 Eigenverantwortlicher Betrieb*

Ein Kandidat für den eigenverantwortlichen Betrieb von Chablis ist das Rechenzentrum der Uni Kaiserslautern. Eigenverantwortlich heißt hier, dass der Betreiber nur Gelder für sich selbst und nicht für Dritte einzieht. Dies ist natürlich auch öffentlichen Einrichtungen erlaubt. Das Rechenzentrum der Uni Kaiserlautern hat Chablis bereits in sein IP-basiertes Accounting integriert und mit Testzahlungen erfolgreich getestet. Folgen sollte außerdem noch das Projekt Nipon, das ein nutzerbasiertes Accounting und die zugehörige Abrechnung zuläßt. Nach aktueller Planung wird das Rechenzentrum Kaiserslautern in Zusammenarbeit mit der Uni Trier einen solchen eigenverantwortlichen Betrieb durchführen.

Trotz des technisch erfolgreichen Betriebs an der TIB Hannover konnten ansonsten keine weiteren Händler oder neuen Dienste akquiriert werden, da alle Interessenten als erste Anforderung eine sichere Betriebsperspektive erwarteten. So wollte der Print-On-Demand-Dienst ProPrint Chablis als Zahlverfahren einbinden. Auch hier wurde die Integration von Chablis bereits in Angriff genommen, erreichte aber keinen lauffähigen Status mehr und wurde auf Grund der fehlenden längerfristigen Betriebsperspektive nicht mehr weiter verfolgt. Dies liegt auch am Projektstand von Pro-

Print, das erst in Kürze einen uni-internen Testbetrieb „in Produktion“ aufnehmen wird und auch noch nicht abschätzen kann, wieviele Nutzer den Dienst wirklich in Anspruch nehmen werden. Daher wurde zunächst auf eine vorhandene Abrechungsschnittstelle in der SUB[2] Göttingen zurückgegriffen, die zwar nicht die Möglichkeiten von Chablis besitzt, für den Testbetrieb jedoch vorerst ausreichend ist.

### *5.3 Dienstnutzer*

Die Bayerische Staatsbibliothek meldete zu zwei verschiedenen Gelegenheiten Interesse an. Ursprünglich hätte in Zusammenarbeit mit Sisis ein Verfahren für die Abrechnung der Mahngebühren eingeführt werden sollen. Dies scheiterte an Sisis, das sich wegen des Fehlens eines gesicherten Betreibers weigerte, die erforderlichen Änderungen an ihrer Software vorzunehmen.
Als weiteres Projekt der BSB sollten die Sondersammelgebiete im Rahmen eines DFG-Projekts um eine kostenpflichtige Recherche erweitert werden. Da diese Planungen erst im Oktober 2003 in Angriff genommen wurden, scheiterte der Betrieb auch hier an der fehlenden längerfristigen Betriebsgarantie. Gleiches gilt für das Bremer Institut für Seeverkehrswirtschaft und Logistik, das ein ähnliches Projekt in Planung hat.
Ein Projekt für die Abrechnung von größeren Transaktionssummen hätte sich aus den Verhandlungen für einen Betrieb durch die TUMorrow GmbH ergeben können. Auch wenn der Betrieb dort wegen der eigenen nur kurzen Planungssicherheit vom Aufsichtsrat abgelehnt wurde, wurde dort der Wille bekundet, die Abrechnung von Tagungsanmeldungen über einen zukünftigen Chablis-Betreiber abzuwickeln.

## 6 Betriebsbericht

### *6.1 Zahlungssystementwicklung*

Bei Projektbeginn sah die Welt der Zahlungssysteme völlig anders aus, als zu Projektende. Während anfangs Zahlungssysteme mit eigenen Clientprogrammen den Markt dominierten, sind heute hauptsächlich Zahlungssysteme ohne eigene Clientprogramme auf dem Markt. Die Annahme des Projektantrags, dass eine große Fluktuation auf dem Markt der elektronischen Zahlungssysteme herrscht, wurde damit bestätigt. Einen wirklichen Marktführer gibt es nach wie vor nicht. Allerdings sind die ersten Zahlungssysteme inzwischen so weit, dass man davon ausgehen kann, dass die Marktposition weitgehend gesichert ist.
Überträgt man die Erfahrungen der Welt der herkömmlichen Zahlungssysteme auf die Welt der Internetzahlungssysteme, liegt die Vermutung nahe, dass langfristig nur wenige Zahlungssysteme den Markt unter sich aufteilen werden. In der realen Welt kann man den Markt im wesentlichen auf fünf Systeme aufteilen: Lastschrift, Kreditkarte, Überweisung nach Rechnung, Vorkasse und Nachnahme. Mit einer solchen Konzentration ist wahrscheinlich auch im Onlinemarkt zu rechnen. Vor allem deshalb, weil diese konventionellen Zahlungsverfahren in modifizierter Form auch im Internet verwendet werden.
Die ursprünglich angebundenen bzw. geplanten Zahlungssysteme waren zunächst CyberCash/CyberCoin, eCash, Millicent, Minipay, Paybox, Lastschrift SSL, Geldkarte, Kreditkarte SSL und SET. Lastschrift, Geldkarte und Kreditkarte wurde über den X-

2 Staats und Universitätsbibliothek

Pay-Server des damaligen Marktführers Brokat angebunden. Im Laufe des Projekts wurden alle oben genannten Internetverfahren eingestellt. Kreditkarte SSL und Lastschrift SSL ist daher inzwischen über eine andere Software namens Click&Pay Easy von Telecash angebunden, die keine Unterstützung von Geldkarte oder SET mehr vorsieht. Paybox wurde von der Firma Moxmo übernommen und versucht sich wieder auf dem Markt zu etablieren. Ob die damalige Anbindung noch funktioniert, konnte nicht verifiziert werden.
Neue Zahlungssysteme sind inzwischen trotzdem auf den Markt gekommen. Firstgate Click&Buy, Telekom T-Pay und paysafekey sind zur Zeit wohl die wichtigsten Anbieter. Bei den Micropayments basieren fast alle Verfahren auf der Sammlung von Zahlungen, die dann zusammen gebucht werden. T-Pay und paysafekey sind außerdem „Zahlungssystemklassen", d.h. sie bieten unter einer Schnittstelle verschiedene Varianten an. Neben diesen drei Systemen gibt es noch viele sogenannte Dialerverfahren, die über Telefonverbindungen abrechnen.
Anbindungen dieser Zahlungssysteme an Chablis wurden aus zwei Gründen nicht vorgenommen. Erstens wären die Gebühren (zur Zeit bis 35%, anfangs teilweise noch höher) zu hoch gewesen. Zweitens besteht bei den Zahlungssystemen kein Zugang zu den Schnittstellendokumentationen solange nicht ein Vertrag in Aussicht gestellt werden kann. Dies dürfte vor allem darin begründet sein, dass die Unternehmen seit dem Börsenkrach am Neuen Markt gezwungen sind Geld zu sparen und es sich nicht leisten können, Support und Testmöglichkeiten für „Kunden" anzubieten, die keine Gewinne bringen.

## *6.2 Benutzungsstatistik*

Die Benutzungsstatistik der TIB Hannover kann leider nicht als repräsentativ angesehen werden, da dafür die Benutzung zu gering ist. Trotzdem soll sie hier kurz dargestellt werden. In den folgenden drei Tabellen sind nur die wirksamen Zahlungen für tatsächlich erfolgte Lieferungen berücksichtigt worden (daneben gab es einige wenige Stornierungen sowie Testbestellungen). Die Tabellen stellen nacheinander dar, wie sich die Bestellungen auf die Monate (Tabelle 1), die Länder (Tabelle 2) und die Kundengruppen (Tabelle 3) verteilten.

| *Jahr* | *Monat* | *Anzahl Bestellungen* |
|---|---|---|
| 2002 | Juni | 1 |
| | Juli | 4 |
| | August | 2 |
| | September | 6 |
| | Oktober | 7 |
| | November | 2 |
| | Dezember | 4 |
| 2003 | Januar | 21 |
| | Februar | 4 |
| | März | 8 |
| 2003 | April | 13 |
| | Mai | 0 |
| | Juni | 2 |
| | Juli | 18 |
| | August | 13 |
| | September | 2 |
| Summe | | 107 |

*Tabelle 1: Benutzungsstatistik nach Monaten*

| *Land* | *Anzahl Bestellungen* |
|---|---|
| Deutschland | 41 |
| Neuseeland | 16 |
| Ägypten | 9 |
| Österreich | 8 |
| USA | 6 |
| Island | 6 |
| Russland | 5 |
| Schweden | 5 |
| Niederlande | 3 |
| Tschechien | 2 |
| Schweiz | 2 |
| Australien | 1 |
| China | 1 |
| Ukraine | 1 |

| *Land* | *Anzahl Bestellungen* |
|---|---|
| Slowenien | 1 |
| Summe | 107 |

*Tabelle 2: Benutzungsstatistik nach Ländern*

| *Preisgruppe* | *Anzahl Bestellungen* |
|---|---|
| ch (Hochschulen) | 63 |
| cp (Privatpersonen) | 8 |
| ci (Industrie) | 36 |
| Summe | 107 |

*Tabelle 3: Benutzungsstatistik nach Kundengruppen*

## *6.3 Lasttest*

Um die Belastbarkeit des Chablis Zahlungsservers auszutesten, wurden eine Reihe von Hilfsprogrammen erstellt. Mit deren Hilfe ist es möglich, einen Zahlungsablauf komplett zu durchlaufen, ohne dass ein realer Benutzer interagieren muss. Dadurch ist es möglich, in kurzer Zeit sehr viele Transaktionen abzuarbeiten.
Für den Lasttest wurde die folgende Hardware verwendet: der Chablis Server lief auf einem AMD Athlon 750 MHz PC mit 384 MB Hauptspeicher unter Debian GNU/Linux 3.0. Der Datenbankserver war eine Sun Blade 100 mit 500 MHz UltraSPARC-IIe Prozessor und 1.2 GB Hauptspeicher mit Oracle 8i unter Solaris 8.
Die Ergebnisse des Lasttests waren sehr erfreulich. In Bezug auf Stabilität des Servers sind überhaupt keine Probleme aufgetreten. Getestet wurden verschiedene Parallelitätsstufen. Die Werte müssen hier teilweise erklärt werden. Angegeben ist immer, in welchem Zeitraum wieviele Transaktionen abgearbeitet wurden bei wievielen parallelen Zahlanfragen. Die Timeouts geben an, wie oft Chablis nicht innerhalb von einer Minute die Bezahlanfrage bedienen konnte. Das Limit von einer Minute gibt die Zeit von Beginn der Zahlung bis zur Auslieferung an und wurde zum Test willkürlich so festgelegt. Im Wirkbetrieb ist dieser Wert deutlich höher zu setzen, so dass dann auch sehr viel weniger lastbedingte Timeouts zu erwarten sind. Die Durchschnittsdauer gibt die Verarbeitungszeit der Zahlung innerhalb von Chablis an. Das beinhaltet das Abspeichern aller Daten, aber nicht die Zeit, die das angeschlossene Händlersystem zur Verarbeitung benötigt. Der Durchsatz gibt an, wieviele Zahlungen pro Minute bedient wurden.

| *Beschreibung* | *<= 5 parallele Anfragen* | *<= 10 parallele Anfragen* | *<= 30 parallele Anfragen* |
|---|---|---|---|
| **Anzahl der Transaktionen** | 3946 | 11800 | 8347 |
| **Zeitraum** | 02:30 Stunden | 3:30 Stunden | 2:30 Stunden |
| **Timeouts (Dauer > 1 min.)** | 0 | 1 | 8 |
| **Durchschnittsdauer** | 1,55 Sekunden | 2,33 Sekunden | 6,57 Sekunden |
| **Durchsatz** | 26 pro Minute | 56 pro Minute | 56 pro Minute |

*Tabelle 4: Ergebnisse des Lasttests*

Insgesamt wurden inzwischen deutlich über 100.000 Testzahlungen durchgeführt. Da der Chablis-Rechner zeitweise nebenher anderweitig genutzt wurde und wegen den laufenden Entwicklungsarbeiten auch mehrfach geändert wurde, sind nur die obigen Transaktionen ausgewertet worden.
Die Parallelität wurde bei den Tests nicht weiter erhöht, weil die angeschlossenen Zahlungssysteme selbst nur noch niedrigere Parallelität akzeptieren. Chablis enthält daher einen Mechanismus, mit dem die Anfragen an die Zahlungssysteme serialisiert werden können. Der Parallelitätsgrad lässt sich spezifisch einstellen.
Wenn man die Zahlen von weiter oben aus der Tabelle 4 heranzieht und die 240.000 Transaktionen auf 200 Arbeitstage im Jahr und 6 Stunden pro Tag verteilt, so wären in diesen 6 Stunden ca. 1200 Transaktionen abzuwickeln. Unser Lasttest hat auf bereits älterer Hardware in 2.5 Stunden bis über 8000 Transaktionen abgewickelt. Hier sind also keine Engpässe zu erwarten.

## *6.4 Installation des konsolidierten, erweiterten Zahlungsservers an der TIB*

An der TIB Hannover sollte im Laufe des Projekts die erste Version des Chablis-Zahlungsservers durch die konsolidierte und erweiterte Version ersetzt werden. Von einer vollständigen Umstellung wurde jedoch trotz Fertigstellung des erweiterten Zahlungsservers Abstand genommen. Zum einen war der Bedarf sehr gering, da auch die Nutzung des Server in Hannover Ende September 2004 beendet wurde. Zum anderen wurden regelmäßig Änderungen vom konsolidierten Zahlungsserver auf diese Version übertragen.

## *6.5 Fortsetzung des Betriebs über das Vertragsende hinaus*

Im ursprünglichen Projektantrag war geplant, den Betrieb des Zahlungsservers noch ein Jahr über das Vertragsende hinaus mit Eigenmitteln und gesonderten Fördermitteln zu leisten. Die geplanten Projektergebnisse (Erstellung einer Bedienungsanleitung und Konsolidierung des Zahlungsservers) wurden bereits fertig gestellt.
Trotzdem läuft das Projekt an der TU-München aus Eigenmitteln noch weiter. Bisher wird der Betrieb des Testservers für Studienarbeiten weiter gewährleistet. Desweiteren wird angestrebt bei der Uni Kaiserslautern die Einführung des Chablisbetriebs zu unterstützen, damit wieder ein Chablisserver im Wirkbetrieb arbeitet. Gelingt der dortige Betrieb, wird ein Betriebsbericht erstellt, wie im Projektantrag vorgesehen.

Im Rahmen der Dissertation von Herrn Stumpf werden außerdem noch weitere Untersuchungen über Zahlungssysteme durchgeführt, um Zahlungssysteme in Zukunft besser und ganzheitlich analysieren, klassifizieren und beurteilen zu können.

## 7 Geschäftsmodelle

Im Laufe des Projekts wurde versucht, verschiedene Geschäftsmodelle umzusetzen. Das ursprünglich im Projektantrag geplante Modell für den Betrieb an der Technischen Informationsbibliothek Hannover bzw. bei subito konnte nicht die Erwartungen erfüllen. Die Möglichkeit der Onlinezahlung wurde nicht wie erwartet von den Kunden akzeptiert, was möglicherweise auch damit zusammenhing, dass die Lieferung der Dokumente auf Grund des erforderlichen Scanvorgangs der bestellten Artikel nur zeitversetzt erfolgen konnte.

In Zusammenarbeit mit der TUMorrow GmbH wurden daher weitere Geschäftsmodelle entwickelt. Diese sind in der unten erwähnten Wettbewerbsanalyse unter http://chablis.in.tum.de/papers/SWOT-Chablis.pdf abrufbar. Das Geschäftsmodell von TUMorrow geht von einem anderen Händlermodell aus. Nicht nur die Bibliotheken sind Händler, sondern auch die Hochschulen treten als Händler auf. Als Waren werden genuin digitale Dokumente gesehen, unter der Annahme, dass dieser Markt wachsen wird, was zur Zeit der Fall ist. Pro Transaktion sollte ein fester Gebührensatz von 0,50 € erhoben werden. Der Betrieb sollte von einem speziellen Betreiber geleistet werden. Als Zahlen liegen 1,9 Millionen Studenten in Deutschland zugrunde, die pro Jahr 33.000 Bezahlvorgänge über Chablis abwickeln. Das entspricht einem Anteil von 0,75% der heute von Studenten nachgefragten Literatur. Bei diesem Szenario mit jährlichen Kosten von 87.000 € und einer Anfangsinvestition von 55.000 € hätte eine Amortisation auf absehbare Zeit nicht stattgefunden. Allerdings wurde ein weiteres Szenario vorgeschlagen, das von TUMorrow als realistischer eingeschätzt wurde und das berücksichtigte, dass nicht nur Studenten sondern auch Mitarbeiter und Externe einen gewissen Literaturbedarf haben. Dieses Szenario wäre umgerechnet auf die Studenten auf einen Marktanteil von etwa 3% gekommen und hätte sich bei gleichen Kosten nach acht Jahren amortisiert (siehe hierzu http://chablis.in.tum.de/papers/SWOT-Chablis.pdf ).

Auch für den Betrieb durch den DFN-Verein wurden Überlegungen angestellt. Dieses Betriebsmodell basiert auf der Annahme, dass durch den Skaleneffekt Ersparnisse auftreten, weil ab gewissen Umsatzgrenzen die Gebühren der Zahlungssystembetreiber sinken. Diese Ersparnisse sind erreichbar, wenn ein Betreiber für mehrere Händler abrechnet. Die Kosten wurden dabei auf einen jährlichen Aufwand von 65.000 € pro Jahr geschätzt. Darin enthalten ist eine Personalstelle, so dass anfallende Arbeiten wie Anpassungen an neue Softwareversionen, Systemwartung und Betreuung erledigt werden können. Die jährlichen Kosten sind aus zwei Gründen geringer, als beim Modell von TUMorrow: Zum einen fallen keine Kosten für Miete an, da der Server an einer Universität aufgestellt werden kann. Von TUMorrow wurden Mietkosten in Höhe von 6.600 € pro Jahr veranschlagt. Zum anderen wird die grundsätzliche Administration des Rechners und des Netzwerks von einer Rechnerbetriebsgruppe erledigt, die bereits vorhanden ist. Bei TUMorrow fällt diese Stelle mit 16.800 € ins Gewicht.

Da bei einem Skaleneffekt von 0,10 € pro Transaktion 650.000 Transaktionen pro Jahr notwendig gewesen wären, um einen kostenneutralen Betrieb zu gewährleisten, wurde ein Mischmodell vorgeschlagen. Dieses besteht sowohl aus einer geringen

Transaktionsgebühr von 0,20 € als auch aus dem oben erwähnten Skaleneffekt. Der Break-even ist dann bei 217.000 Transaktionen im Jahr erreicht. Als Haupteinnahmequelle sieht dieses Modell allerdings nicht nur die Abrechnung genuin digitaler Dokumente, sondern auch der Netzdienstleistungen für den privaten Gebrauch der Studenten vor.
Ein Betrieb dieses Modells konnte nicht umgesetzt werden, da die vorhandenen Mittel für den Betrieb nur ein Jahr gereicht hätten. Mit dem Erreichen des Break-even konnte aber realistischerweise erst in mehreren Jahren gerechnet werden, da andere Anbieter zum Einsatz des Chablis-Servers erst dann bereit sind, wenn der Betrieb bei einem Pilotbetreiber erfolgreich mit größeren Transaktionszahlen erfolgt und wenn eine sichere Betriebsaussicht besteht.

# 8 Wettbewerbsanalyse

Im Laufe des Projekts wurde in Zusammenarbeit mit der TUMorrow GmbH eine Wettbewerbsanalyse durchgeführt, bei der Chablis mit anderen Systemen verglichen wurde. Dabei wurden zwei Grundtypen von Systemen untersucht. Einmal die Systeme aus dem privatwirtschaftlichen Bereich und einmal die Systeme aus dem universitären Umfeld. Inklusive Chablis wurden neun Systeme verglichen: BASILIKA, CO-POS, GZS Paymaster, paysafekey, Powercash 21, QENTA, Verisign Payflow und Rate One.
Resultat der Untersuchung war, dass Chablis bereits im aktuellen Leistungsumfang für universitäre Einsatzzwecke geeignet ist. Die kommerziellen Systeme haben Vorteile im Bereich des Support, da hier andere Möglichkeiten vorhanden sind, als bei einem Universitätsprojekt. Als wichtigste nicht-kommerzielle Konkurrenz wurde das Projekt BASILIKA identifiziert, bei dem allerdings eine Chipkarteninfrastruktur aufgebaut werden soll, mit der dann auch Zahlungen möglich sein könnten. BASILIKA wird schon vereinzelt zur Bezahlung der Rückmeldegebühr von Studenten eingesetzt. Die Analyse kann unter http://chablis.in.tum.de/papers/SWOT-Chablis.pdf eingesehen werden.

# 9 Sicherheitsanforderungen an Chablis

## *9.1 Zertifizierung von Serverkomponenten in Chablis*

Bei der Antragstellung des Projekts war noch nicht klar, ob für den Chablis Server eine Zertifizierung mit dem Prädikat „Evaluationsstufe E4, hoch“ nach den europäischen ITSEC-Kriterien notwendig ist. Die TIB war daher dazu beauftragt, eine solche Notwendigkeit zu prüfen. Diese Prüfung bei der TIB Hannover hatte ergeben, dass eine solche Zertifizierung für den Einsatz an der TIB nicht erforderlich ist. Eine Zertifizierung wurde daher nicht vorgenommen.

## *9.2 Anonyme Zahlung*

Bei der Antragsstellung wurde davon ausgegangen, dass die Ermöglichung anonymer Bezahlung einen größeren Benutzerkreis schaffen würde. Durch anonyme Zahlungen ist es für die Kunden möglich, ohne langwierige Registrierungsprozeduren Spontankäufe zu erledigen und seine Einkäufe nicht offenzulegen. Dieser Vorteil wurde deutlich überschätzt. Zunächst muss beachtet werden, dass die Benutzerregistrierung po-

tentielle Kunden immer dann abschreckt, wenn hierfür der Aufwand im Verhältnis zum Wert des bestellten Gutes überproportional ist. Das ist vor allem bei Kleinstzahlungen der Fall. Die Bestellung über TIBORDER fällt aber nicht mehr in diesen Bereich, da allein die Kostendifferenz zwischen billigster und teuerster Benutzergruppe fast zehn Euro beträgt: die Verwertungsgesellschaft Wort hätte aber verlangt, dass bei anonymen Zahlungen automatisch diese teuerste Benutzergruppe gewählt wird. Damit hätte ein Kunde, der die neue Technik genutzt hätte, deutlich mehr zahlen müssen als ein registrierter Kunde auf herkömmlichem Weg. Damit war an eine Erweiterung des Benutzerkreises über eine anonyme Kundengruppe nicht zu denken.
Das zweite Problem, das sich beim Pilotbetrieb zeigte, war, dass die meisten Kunden aus dem Firmenbereich oder öffentlichen Institutionen kamen. Auch deshalb bestand kein Interesse an Anonymität. Vielmehr waren dort im allgemeinen Sammelrechnungsverfahren gewünscht, die natürlich nur mit Angabe der Adresse funktionieren.
Aus diesem Grund wurde die Möglichkeit von Chablis, Zahlungen anonym abzuwickeln, nicht verwendet und ist im Bibliotheksbereich solange nicht einsetzbar, wie auf Grund der Vorgaben von Verwertungsgesellschaften Kundendaten erfasst werden müssen.

## *9.3 Public Key Infrastructure*

Die in Chablis eingesetzten Techniken zur Absicherung der Kommunikation basieren auf weit verbreiteten Standards. Dementsprechend wurde für die Kommunikation das SSL/TLS-Protokoll zur Sicherstellung der Vertraulichkeit und Authentifizierung verwendet. Damit kann jeder Anwender einen normalen Browser verwenden, ohne Zusatzsoftware installieren zu müssen. Ein Händler, der per Browser auf Chablis zugreifen will, benötigt ein Zertifikat nach dem X.509 Standard. Dadurch war die Verwendung der DFN-PCA zunächst ausgeschlossen. Die DFN-PCA basierte ursprünglich nur für die Serverzertifikate auf X.509. Für die Benutzerzertifikate wurde dagegen PGP verwendet. Dies ist zwar im Bereich von E-Mail nach wie vor üblich, aber inkompatibel zur SSL-Kommunikation. X.509 Clientzertifikate waren bei der DFN-PCA zunächst nur für Pilotzwecke erhältlich. Die Übernahme der X.509 Clientzertifikate in den Regeldienst ist aber für die Nahe Zukunft geplant. Außerdem gibt es viele Firmen wie Telesec, Verisign oder Web.de, die bereits große Nutzerbasen auf Public-Key-Infrastrukturen nach dem X.509 Standard haben.

## *9.4 Signaturgesetz*

Nachdem jetzt auf die verwendeten Technologien eingegangen wurde, muss im Rahmen der Sicherheit auch auf die daraus resultierende Rechtssicherheit eingegangen werden.
Nach dem Signaturgesetz sind die digitale Signaturen in die drei Klassen eingeteilt:

- Einfache elektronische Signatur: Sie ist definiert als Daten, die anderen Daten beigefügt sind oder mit ihnen logisch verknüpft sind und zur Authentifizierung dienen. Eine genauere Spezifizierung findet nicht statt.
- Fortgeschrittene elektronische Signatur: Der wesentliche Unterschied zur einfachen Signatur ist, dass der Schlüsselinhaber identifizierbar sein muss und dass die Signaturmittel vom Inhaber unter Kontrolle gehalten werden können.
- Qualifizierte elektronische Signatur: Zusätzlich zur fortgeschrittenen Signatur muss die Signatur mit Hilfe einer sicheren Signaturerstellungseinheit erzeugt werden und auf einem gültigen qualifizierten Zertifikat beruhen.

Nach dem Signaturgesetz ist die Beweiskraft der einfachen und der fortgeschrittenen Signatur nicht geregelt. Abhängig vom Richter können sie aber evtuell zur Beweiserleichterung dienen. Nur die qualifizierten Signaturen sind rechtsgültig wie eine Unterschrift. Die Signatureinheiten müssen aber so konstruiert sein, dass die Signatur nur durch persönliche Bestätigung einer natürlichen Person ausgeführt werden kann. Eine Automatisierung auf Händlerseite ist damit nicht mehr möglich. Abgesehen davon gibt es auch noch keine allgemein anerkannten und weit verbreiteten Verfahren, die entsprechende Signaturen in den Bezahlvorgang einbinden. Jede Eigenentwicklung würde eine große Einstiegshürde für Chablis bedeuten, weil die Anwender sich teure Hardware beschaffen müssten. Sowohl die fehlende Automatisierbarkeit als auch das Hardwareproblem führten wiederum zu dem Schluss, dass Standardtechniken die sinnvollere Alternative sind. So wurde zu Lasten der hundertprozentigen Rechtssicherheit, wie oben bereits angesprochen, das SSL/TLS-Protokoll verwendet.

### *9.5 Stufenmodell*

Das HTTP bzw. HTTPS Protokoll läßt im Prinzip drei Sicherheitsstufen zu. Einmal normales, also unverschlüsseltes HTTP. Diese unsicherste Variante wird von Chablis nicht unterstützt. Die zweite Sicherheitsstufe ist normales HTTPS, bei dem sich der Server gegenüber dem Kunden authentifiziert. Das ist das Standardverhalten von Chablis. Damit können auch anonyme Kunden sicher bezahlen.
In der dritten und höchsten Sicherheitsstufe wird eine wechselseitige Authentifizierung verlangt. Sowohl Server als auch Kunde müssen sich mit Zertifikaten ausweisen. Chablis protokolliert in dieser Stufe mit, von welchem Kunden die Zahlung autorisiert wurde. Der Händler kann dieses Verfahren fordern, wenn es z. B. um höhere Transaktionssummen geht. Allerdings gilt auch hier, dass das SSL-Protokoll keine rechtsverbindlichen Transaktionen zuläßt. Eine Absicherung gegenüber Missbräuchen ist es aber allemal.
Für die Clientauthentifizierung haben die Händler zwei Möglichkeiten. Entweder legt der Händler selbst fest, welche Kundenzertifikate er akzeptieren möchte, oder aber der Chablis-Betreiber legt hier eine allgemeine Policy fest. Für die Wahl der Zertifizierungsstellen besteht keine Einschränkung. Das heißt, es können von den Händlern bzw. vom Chablisbetreiber eigene Zertifikate ausgestellt werden, oder es können beliebige Zertifizierungsstellen als vertrauenswürdig akzeptiert werden.

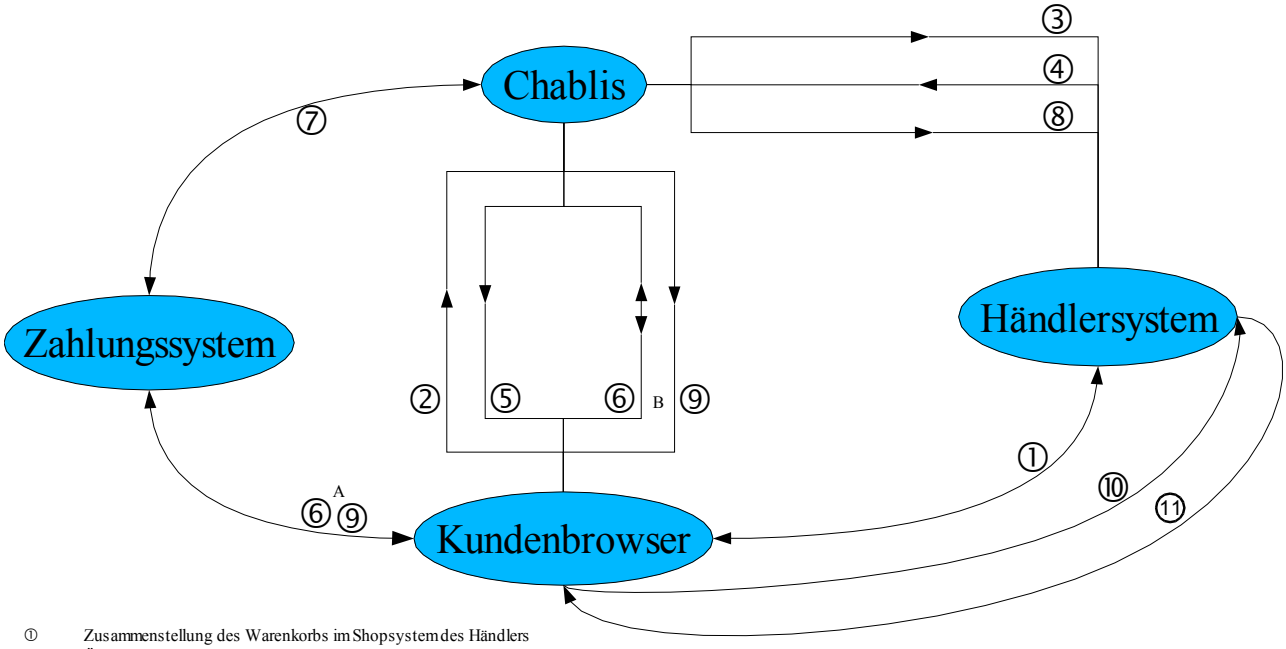
## 10 Bedrohungsanalyse des Chablis Zahlungsservers

In Zusammenarbeit mit Frau Prof. Dr. Claudia Eckert wurden bereits früh im Projekt Bedrohungsbäume erstellt, damals noch für ein spezielles TIB-Szenario. Dieses Szenario wurde jedoch durch einen allgemeineren Ansatz ersetzt, so dass die Bedrohungsbäume keine weitere Verwendung fanden. Stattdessen wurde die Kommunikation von Chablis genauer untersucht.
Wie im Projektantrag vorgegeben, liegt die Einbruchssicherheit des Servers und damit auch der Datendiebstahl von der Festplatte im Zuständigkeitsbereich des Rechenzentrums, das den Server betreibt. Trotzdem wurde bei der Entwicklung darauf geachtet, dass der Server keine vertraulichen Informationen speichert, wenn dies nicht explizit eingeschaltet wird. Auch für die Verhinderung von Denial of Service (DoS) Angriffen sind keine Strategien in Chablis vorgesehen. DoS-Attacken werden von

Chablis nur in soweit beachtet, als dass im Rahmen der Recovery-Fähigkeit keine inkonsistenten Zustände entstehen können.

## *10.1 Kommunikationswege*

Wir beachten hier die Kommunikation zwischen Händler und Chablis auf der einen Seite und zwischen Kunde und Chablis auf der anderen Seite. Desweiteren besteht noch eine Kommunikation zwischen Chablis und dem Zahlungssystembetreiber. Bei dieser Kommunikation sind wir aber auf das Protokoll des Betreibers angewiesen, das wir nicht ändern können. Deshalb wird dieser Kommunikationsweg nicht weiter beachtet. Gleiches gilt für die Kommunikationsschritte, an denen Chablis nicht beteiligt ist. Im Zahlungsablauf sind die rechtwinkligen Pfeile relevant. Auf die kurvigen Pfeile hat Chablis keinen Einfluss.




① Zusammenstellung des Warenkorbs im Shopsystem des Händlers
② Über ein HTML-Formular wird der Kunde an Chablis weitergeleitet und stößt den Zahlvorgang an
③ Chablis erfragt die Bestelldaten beim Händler
④ Der Händler liefert/bestätigt die Bestelldaten
⑤ Chablis präsentiert die fertige Bestellung dem Kunden in einem HTML-Formular, das diesen zum Zahlungssystem weiterleitet.
⑥ Je nach Zahlungssystem kommuniziert der Kunde jetzt entweder direkt mit dem Zahlungssystem oder mit Chablis
⑦ Im Hintergrund läuft das entsprechende Protokoll des Zahlungssystems ab.
⑧ Chablis meldet das Resultat der Zahlung an den Händler
⑨ Entweder Chablis oder das Zahlungssystem liefert eine Seite, die den Kunden auf die Auslieferungsseite des Händlers umleitet.
⑩ Der Kundenbrowser fordert die Auslieferungsseite des Händlers an.
⑪ Der Händler liefert an den Kunden aus

*Abildung 1: Zahlungsablauf bei ChablisPS*

Bedrohungsanalysen sind sehr komplex und müssen daher genau auf die zu untersuchenden Bereiche fokussieren. Dazu wird ein Ausschnitt des Gesamtsystems unter der Annahme untersucht, dass der Rest ordnungsgemäß funktioniert. Wie bereits im Projektantrag beschrieben, wurde in Chablis davon ausgegangen, dass die Rechner einbruchssicher vom Rechenzentrum betrieben werden. Außerdem muss die Kommunikation nach den Zahlungssystemprotokollen als gegeben hingenommen werden und kann nicht verändert werden. Diese Bereiche gelten also im weiteren als „sicher“ und wurden bei der Bedrohungsanalyse nicht weiter untersucht. Auch auf die Kommunikation zwischen Händlersystem und Kundenbrowser besteht kein Einfluss. Insgesamt werden also die Schritte 1, 6A, 7, 9A, 10 und 11 nicht weiter beachtet.

## *10.2 Bedrohungsmatrix*

In der unten stehenden Bedrohungsmatrix sind die Kommunikationsschritte einzeln aufgeführt. Die gelb und blau markierten Felder sind abgesichert. Die grauen Bereiche befinden sich außerhalb des Einflussbereichs von Chablis. Die weißen Bereiche sind an sich kein Sicherheitsproblem sondern ein Transaktionsproblem. Dazu wurde im Abschnitt über die Transaktionssicherheit Stellung genommen. Die beiden rechten Spalten geben an, ob für Händler oder Kunde ein Verlust entstanden ist. Kritisch sind die Fälle, die rot markiert sind. Hier droht für den Kunden eben durch dieses Transaktionsproblem der Verlust des Geldes, da er keine Ware erhält.

| | | Angriffsmöglichkeiten | | | | | Auswirkungen bei Transaktionsabbruch | |
|---|---|---|---|---|---|---|---|---|
| Kommunikationsschritt | Übertragene Daten | Abhören | Verbindungsabbruch | Wiedereinspielen | Verändern | Eigene Nachricht | Geld | Ware |
| 1 | Unbekannt | *Kommunikation ohne Beteiligung von Chablis, keine Einflussmöglichkeit* | | | | | Keine Zahlung | Keine Lieferung |
| 2 | Händleridentifikation, händlerspezifische Kundennummer, Transaktionsnummer, optional zusätzlich Warenkorbinformationen | Erstellung nicht personenbezogener Nutzungsprofile | Transaktion wird abgebrochen, DoS | Nochmalige Auslieferung, Käufertransaktion wird abgebrochen, Angreifer übernimmt die Transaktion und muss zahlen, DoS | Transaktion wird abgebrochen, DoS | Wird nicht vom System angenommen, DoS | Keine Zahlung | Keine Lieferung |
| 3 | Händleridentifikation, händlerspezifische Kundennummer, Transaktionsnummer | Kundennummern/Transaktionsnummern können abgehört werden | Transaktion wird abgebrochen, DoS | *Muss vom Händlersystem erkannt werden* | Transaktion wird abgebrochen, DoS | *Muss vom Händlersystem erkannt werden* | Keine Zahlung | Keine Lieferung |
| 4 | Händleridentifikation, händlerspezifische Kundennummer, Transaktionsnummer, Warenkorbinformationen | Nicht personenbezogene Nutzungsprofile, Warenkorb mit Auslieferadresse abhörbar | Transaktion wird abgebrochen, DoS | Wird nicht angenommen, da die Transaktion nicht mehr im Wartezustand ist | Transaktion wird abgebrochen, DoS | Könnte eine gerade wartende Transaktion abbrechen | Keine Zahlung | Keine Lieferung |
| 5 | Händleridentifikation, händlerspezifische Kundennummer, Transaktionsnummer, Warenkorbinformationen | Nicht personenbezogene Nutzungsprofile | Transaktion wird abgebrochen, DoS | *Wird vom Kundenbrowser verhindert* | Trojanisches Pferd an den Kunden schicken, angezeigten Warenkorb/Summe verändern (nicht relevant für Zahlung) | *Wird vom Kundenbrowser verhindert* | Keine Zahlung | Keine Lieferung |
| 6A | Unbekannt | *Kommunikation ohne Beteiligung von Chablis, keine Einflussmöglichkeit* | | | | | Zahlungssystemabhängig | |
| 6B | Zahldaten des Kunden | Zahldaten ausspionieren und einer Kundennummer zuordnen | Transaktion wird abgebrochen, DoS | Wird nicht angenommen, da die Transaktion nicht mehr im Wartezustand ist | Fremdes Konto belasten oder Transaktion scheitern lassen | Könnte eine gerade wartende Transaktion abbrechen | Keine Zahlung | Keine Lieferung |
| 7 | Abhängig vom Zahlungssystem, mindestens der Buchungsresultat und Bezugsnummer | *Chablis muss sich an das Zahlungssystemprotokoll halten und hat keine Einflussmöglichkeiten* | | | | | Zahlungssystemabhängig | |
| 8 | Händleridentifikation, händlerspezifische Kundennummer, Transaktionsnummer, Buchungsresultat, Bezugsnummer für Buchhaltung | Bezugsnummer für Stornos/Teilbuchungen abhören, Summen und Kundennummern abhören | Zahlung wurde bereits durchgeführt, Liefertransaktion wird abgebrochen, DoS | *Muss vom Händlersystem erkannt werden* | Auslieferung verhindern oder erschleichen/Transaktionsabbruch | *Muss vom Händlersystem erkannt werden* | Zahlung | Keine Lieferung |
| 9A | Unbekannt | *Kommunikation ohne Beteiligung von Chablis, keine Einflussmöglichkeit* | | | | | Zahlungssystemabhängig | |
| 9B | Adresse der Resultats-/ Auslieferungsseite | Auslieferadresse abhören | Zahlung wurde bereits durchgeführt, Liefertransaktion wird abgebrochen, DoS | *Wird vom Kundenbrowser verhindert* | Falschlieferung | *Wird vom Kundenbrowser verhindert* | Zahlung | Keine Lieferung |
| 10 | Unbekannt, normalerweise HTTP-Request der Auslieferung | *Kommunikation ohne Beteiligung von Chablis, keine Einflussmöglichkeit* | | | | | Zahlung | Keine Lieferung |
| 11 | Unbekannt, normalerweise Auslieferung/Quittung | *Kommunikation ohne Beteiligung von Chablis, keine Einflussmöglichkeit* | | | | | Zahlung | Keine Lieferung |
| Kommunikation zwischen Chablis und dem Kundenbrowser ist mittels SSL und temporären Sessions abgesichert. Im Normalfall authentifiziert nur der Chablis-Server gegenüber dem Kunden. Der Händler kann aber zusätzlich noch eine Clientauthentifizierung des Kunden erzwingen, falls bestimmte Zertifizierungshierarchien anerkannt werden sollen. | | | | | | | | |
| Die Kommunikation ist per SSL gesichert, bei dem sich das Händlersystem gegenüber Chablis ausweisen muss. Zusätzlich wird dem Händler empfohlen, die Möglichkeit zur gegenseitigen Authentifizierung von Chablis zu nutzen. Außerdem sollten zur weiteren Sicherheitserhöhung IP-Filter eingesetzt werden, die nur die Kommunikation zwischen Chablis und dem Händler zulassen. | | | | | | | | |

*Tabelle 5: Bedrohungsmatrix*

Aus der mehrseitigen Sicherheit sind im allgemeinen noch andere Schutzziele bekannt, als die, die oben in den Spalten angegeben sind:

- Vertraulichkeit: Geheimhaltung der Daten bei der Übertragung. Wird in der Tabelle unter „Abhören“ behandelt.
- Verdecktheit: Versteckte Übertragung von vertraulichen Daten, damit nur die Kommunikationspartner die Existenz vertraulicher Kommunikation erkennen können. Bei Chablis werden alle Daten verschlüsselt übertragen. Kennt der Angreifer den Kommunikationsablauf von Chablis, dann weiß er auch, wann vertrauliche Daten übermittelt wurden. Die Daten selbst kennt er aber nicht.
- Anonymität: Die Nutzer können Chablis benutzen, ohne ihre Identität zu offenbaren. Chablis erfährt nur die IP-Adresse. Über den Gerichtsweg oder eine Kooperation mit dem Händler (sofern dieser keine Anonymität unterstützt) wäre eine Aufdeckung der Kundenidentität denkbar.
- Unbeobachtbarkeit: Nutzer können Chablis nicht benutzen, ohne dass andere dies (durch Abhören des Netzverkehrs) beobachten können. Eine Unbeobachtbarkeit ist damit in keinem Fall gegeben.
- Integrität: Wie obige Tabelle zeigt, ist die Integrität der Kommunikation per SSL gesichert.
- Zurechenbarkeit: Sendern und Empfängern kann das Senden bzw. der Empfang der Informationen bei SSL nicht bewiesen werden.
- Verfügbarkeit/Erreichbarkeit: Die Verfügbarkeit/Erreichbarkeit kann durch DoS, Netzwerk- und Systemfehler beeinträchtigt werden. Auf diese Punkte wird im Rahmen des Abschnitts „Verfügbarkeit“ eingegangen.
- Rechtsverbindlichkeit: Auf die fehlende Rechtsverbindlichkeit wurde bereits eingegangen. Rechtlich können die Protokolle von Chablis allerdings als Anscheinsbeweis gewertet werden, wenn das Gericht dies zuläßt.
- Authentizität: Die Nachrichtenauthentizität ist unter Zurechenbarkeit und Rechtsverbindlichkeit bereits abgehandelt. Hier wird auf die Authentizität des Servers und des Clients eingegangen. Mindestens der Server wird vom Client über ein X.509-Zertifikat authentifiziert. Vom Client kann dies wahlweise verlangt werden.

## *10.3 Kommunikationssicherheit*

Für die Risikoanalyse ist relevant, ob das Verhältnis zwischen Angriffsaufwand und dem Gewinn bei einem erfolgreichen Aufwand lohnend ist. Man muss dabei unterscheiden zwischen externen Angreifern und böswilligen Händlern bzw. Kunden. Angriffe auf SSL gelten als schwierig und nur mit hohem Aufwand umsetzbar[3]. Dieser Aufwand müsste für jede einzelne Verbindung erneut geleistet werden. Mit Angriffen auf die SSL-Kommunikation kann der externe Angreifer aber maximal die Zahlung oder die Auslieferung verändern bzw. abbrechen. Er kann sich dadurch keinen eigenen Vorteil verschaffen. Die Auslieferung selbst betrifft eigentlich nicht Chablis sondern den Händler. Dessen Auslieferung (z. B. eines Dokuments) könnte bei einem erfolgreichen Angriff abgehört und kopiert werden. Dort besteht die einzige Bereicherungsmöglichkeit für den Angreifer.

3 Eckert, Claudia; IT-Sicherheit – Konzepte, Verfahren, Protokolle; Oldenbourg Verlag, 2000

## *10.4 Datensicherheit*

Interessant ist damit aus Sicht des externen Angreifers also der Schädigungsversuch und nicht die eigene Bereicherung. Die Schädigung kann durch Datendiebstahl oder durch DoS-Angriffe erfolgen. Datendiebstahl ist bei einem Einbruch ins System möglich, der vom Betreiber zu verhindern ist. Gelingt der Einbruch, stellt sich natürlich trotzdem die Frage, was Chablis abspeichert und was für den Angreifer interessant sein kann. In der Grundkonfiguration kann der Angreifer nur Umsatzprofile der einzelnen Händler erstellen, gegebenenfalls nach Kundennummern sortiert. Manche Zahlungssysteme bieten aber die Möglichkeit die Zahldaten für „One-Click-Zahlungen“ abzuspeichern. Ist diese Option eingeschaltet, wäre auch der Diebstahl von Zahldaten möglich. Gegen böswillige Veränderungen müssen Backup-Strategien ein Rücksetzen ermöglichen. Ein angreifender Kunde kann durch den Angriff nicht mehr erreichen, als ein normaler Angreifer. Um Transaktionen zu löschen, müsste er auch bei den Zahlungssystembetreibern einbrechen. Bereicherungsmöglichkeiten bestünden nur für den Händler, der seinen Umsatz mit Luftbuchungen erhöhen könnte.

## *10.5 Sicherheit der Chablisschnittstellen*

DoS ist für Chablis aus der Perspektive interessant, dass das System über eine Chablis-Schnittstelle lahm gelegt werden könnte. Da die verwendete Technik Pufferüberläufe verhindert, besteht über diesen Weg keine Möglichkeit zum Angriff. Abgesehen davon, läuft der Chablisserver in einem getrennten Benutzeraccount ohne Root-Rechte, so dass sich potentielle Angreifer hier ohne Root-Exploit des Betriebssystems keine weiteren Rechte verschaffen können.

Allerdings kann der Server über eine zu große Anzahl von Aufträgen oder fehlerhaften Aufträgen angegriffen werden. Aufträge durchlaufen zunächst Plausibilitätstests, so dass fehlerhafte Aufträge abgelehnt werden. Inkonsistente Zustände können dadurch nicht entstehen. Im Zweifelsfall wird die zugehörige Transaktion abgebrochen.

Einer Überlastung durch zu viele Aufträge beugt Chablis vor, indem die maximale Anzahl von Aufträgen begrenzt werden kann. Die Beschränkung kann auf drei verschiedenen Systemebenen vorgenommen werden. Entweder systemglobal oder händler- bzw. zahlungssystemspezifisch. Wird eines der Limits überschritten, wird in diesem Bereich kein neuer Auftrag zugelassen.

## *10.6 Sicherheit der Weboberfläche*

Der Zugriff auf die Geschäftsdaten der Händler erfolgt über einen Browser. Dementsprechend erfolgt auch hier der Zugriff per HTTPS. Die Zugreifer müssen sich per Clientauthentifizierung ausweisen. Es gibt zwei verschiedene Benutzerklassen, eine für die Administratoren und eine für die Händler. Während die Administratoren alle Funktionen verwenden können und insbesondere auch auf die Daten aller angeschlossenen Händler zugreifen können, besteht für die Händler nur der Zugriff auf die eigenen Daten. Um später nachvollziehen zu können, wer über die Geschäftsdatenschnittstelle welche Aktionen veranlasst hat, wird der Name (Eintrag in jedem Zertifikat) mitprotokolliert. Jeder Händler kann so mehrere berechtigte Angestellte haben und trotzdem nachvollziehen, von wem eine Aktion ausgelöst wurde.

# 11 Sicherheit bei Zahlungssystemen

Die Sicherheit von Zahlungssystemen wird hier von der Schnittstelle des Kunden und des Händlers untersucht. Das heißt eine Abschätzung, ob die Sicherungsmaßnahmen des Zahlungssystembetreibers für seine eigenen Systeme ausreichend sind, wird hier nicht gegeben. Außerdem gilt als vorausgesetzt, dass der Zahlungssystembetreiber vertrauenswürdig ist.

## *11.1 Kunde*

Wie dem Bedrohungsbaum des Kunden zu entnehmen ist, können die Bedrohungen in vier Kategorien eingeteilt werden. Der Zahlungsablauf betrifft die Kommunikation, die bei Benutzung des Zahlungssystems auftritt. Bei Systemsicherheit wird untersucht, ob eventuell nötige Installationen das Kundensystem beeinträchtigen können. Ist die Bedienungsschnittstelle sehr komplex, z. B. wenn eine gewisse Bankingfunktionalität eingeschlossen ist, kann es zu Bedienungsfehlern kommen. Die beiden übrigen Bedrohungen betreffen nicht den Zahlvorgang als solches, sondern eher die Abwicklung nach der Lieferung. Das größte Problem dürften in der Realität unseriöse Händler sein. Auch im Fall von Produktfehlern, kann eine Unterstützung von Seiten des Zahlungssystems einen Vorteil im Sinne des Käufers bedeuten.

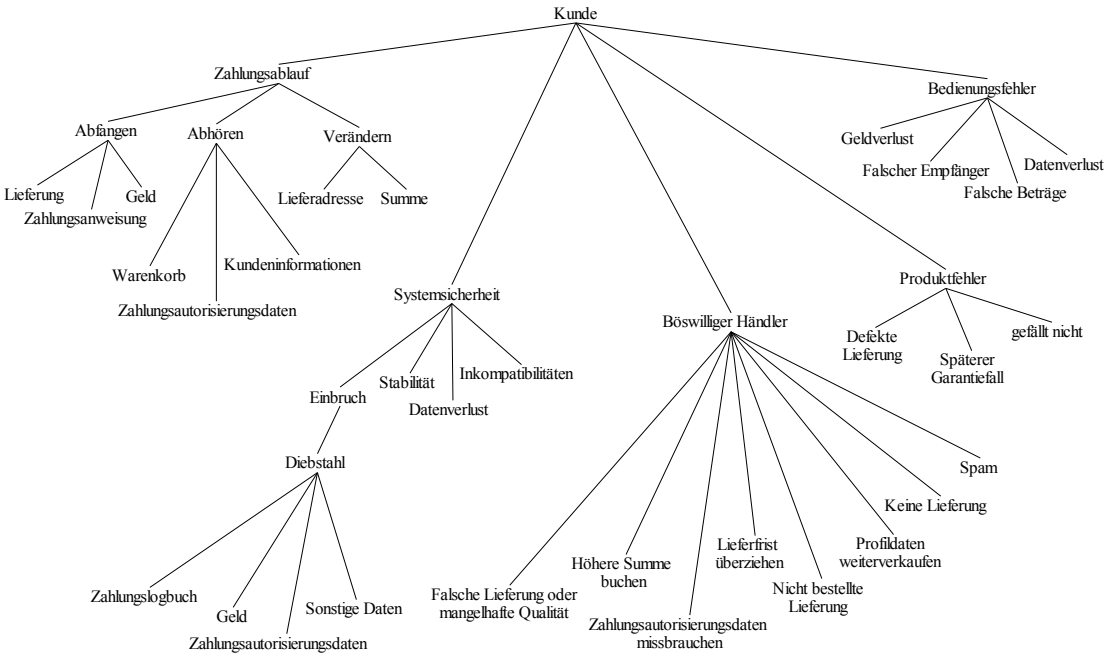



*Abbildung 2: Bedrohungen für den Kunden*

Aus dem Bedrohungsbaum ist erkenntlich, dass nur etwa die Hälfte der Einträge mit der eigentlichen technischen IT-Sicherheit zu tun hat. Alle weiteren Bedrohungen müssen eher mit Hilfe von Kulanz oder Rechtsmitteln abgewickelt werden. Beim Gang des Rechtsweges muss der Kunde mit einem Kostenrisiko von über 250 Euro rechnen, selbst wenn es sich nur um eine Kleinstzahlung handelt. Deshalb werden selbst im niedrigen dreistelligen Eurobereich die meisten Kunden keine Rechtsmittel einlegen, wenn keine Rechtschutzversicherung besteht. Daher ist es durchaus interessant, welche Mittel die Zahlungssysteme zur Verfügung stellen, damit der Kunde wieder an sein Geld kommt, ohne dass er Rechtsmittel einlegen muss. In diesem Zu-

sammenhang muss auch geklärt werden, welche Rechte der Kunde gegenüber dem Händler hat.

### *11.1.1 Erklärungsirrtum/Übertragungsfehler*

Bei einem Erklärungsirrtum oder einem Übertragungsfehler im Bereich des Kunden kann dieser die Bestellung widerrufen. Er muss dem Händler allerdings die regelmäßigen Kosten für dessen Arbeitsaufwand erstatten.

### *11.1.2 Widerrufsrecht/Rückgaberecht*

Laut dem Fernabsatzgesetz hat der Kunde ein 14 tägiges Umtauschrecht ohne Angabe von Gründen. Diese Frist fängt bei Erhalt der Ware an zu laufen. Bei Bestellungen bis 40 Euro kann der Händler dem Kunden die Versandkosten für die Rücksendung auferlegen. Ein Rückgaberecht/Widerrufsrecht besteht nicht bei entsiegelten Datenträgern, Waren die keine Rücksendung zulassen (z.B. Verfallsdatum), bei Spezialanfertigungen und bei Dienstleistungen, die auf ausdrücklichen Wunsch des Kunden vor Ende der Widerrufsfrist ausgeführt wurden.
Ein Spezialfall, der speziell für das Chablis-Umfeld interessant ist, ist der Anstoß der Auslieferung durch Mausklick des Kunden auf einen Link zum Download. Auch hier gilt kein Widerrufsrecht.

### *11.1.3 Gewährleistung*

Die gesetzliche Gewährleistungsfrist beträgt zwei Jahre. Im ersten halben Jahr wird bei einem Defekt grundsätzlich davon ausgegangen, dass ein Produktionsfehler vorlag. Der Händler ist zum Austausch oder zur Nachbesserung verpflichtet. Danach ist die Beweislast umgekehrt. Der Kunde muss nachweisen, dass es sich wirklich um einen Gewährleistungsfall handelt. Die Gewährleistung tritt auch bei falschen Werbeaussagen, falscher Bedienungsanleitung oder bei Bagatellschäden ein, die den Produktwert nur unwesentlich mindern. Im Gewährleistungsfall hat immer der Händler die Kosten zu tragen.

### *11.1.4 Rechtsverbindlichkeit*

Wie bereits erwähnt, werden bei Onlinebestellungen zur Zeit noch keine Signaturen nach dem Signaturgesetz verwendet. Beim Kauf entstehen also keine Privaturkunden, die rechtlich bindend wären. Die einzige Möglichkeit des Beweises ist meist der Ausdruck von gespeicherten Daten. Diese sind keine Privaturkunden und unterliegen der freien richterlichen Beweiswürdigung nach § 286 ZPO[4]. Als Augenscheinobjekte haben solche Daten nur einen geringen Beweiswert. Aufgrund dieser Beweisproblematik kann man sich bei Vertragsabschlüssen über das Internet nie sicher sein, dass im Fall des Falles der Abschluss bewiesen werden kann. Vor allem lässt sich auch durch vertragliche Vereinbarungen (z. B. AGB) keine Beweiskraft festlegen. Eine solche Festlegung ist für ein Gericht nicht bindend, da dieses immer an die ZPO gebunden ist.
Der Rechtsweg ist daher vor allem für den Kunden ein Wagnis, da er normalerweise im Gegensatz zum Händler kaum über Protokolle verfügt. Hier kann ein Protokoll mit Bestellungsinhalt, das vom Zahlungssystemdienstleister geführt wird, eventuell zur Beweiserleichterung gegenüber dem Händler beitragen. Im Missbrauchsfall ist allerdings eher das Gegenteil der Fall.

4 Zivilprozeßordnung

### *11.1.5 Wertung*

Mit dem Wissen über die rechtlichen Grundlagen können nach dem obigen Bedrohungsbaum verschiedene Zahlungssysteme analysiert werden. Dabei ist zu beachten, dass auch herkömmliche Zahlverfahren in die Bewertung eingingen, da diese die Hauptkonkurrenten für die innovativen Verfahren sind.

Grundlage der Analyse ist der ehrliche Kunde. Das heißt der Kunde streitet keine Bestellungen ab, wenn dies nicht erlaubt ist, auch wenn das die einfachste Lösung seiner Probleme wäre.

Desweiteren wird davon ausgegangen, dass der Kunde sich an die Sicherheitsvorschriften der Zahlungssysteme hält und folglich nicht grob fahrlässig den Mißbrauch des Zahlungssystems ermöglicht. Tritt der Mißbrauchsfall trotzdem ein, stellt sich die Frage, welcher Schaden auf ihn zukommt. Dabei ist zu beachten, dass sichere Systeme zur Beweislastumkehr gegen den Kunden führen können und der Kunde beweisen muss, dass er nicht grob fahrlässig gehandelt hat. Dies gilt trotz der Tatsache, dass bisher keine Zahlungssysteme existieren, deren Sicherheit bewiesen ist.

Von Angreifern wird angenommen, dass sie sich selbst bereichern oder den Ruf des Händlers oder des Zahlungssystembetreibers schädigen wollen. Auch ein Schädigungsversuch gegenüber dem Benutzer ist denkbar. Allerdings geht die Analyse davon aus, dass eine Absicherung auf SSL-Niveau für die Kommunikation ausreicht. Bisher sind auch keine erfolgreichen Mißbräuche bekannt, die auf Angriffen der SSL-Kommunikation basieren. Wichtiger ist also die Frage, ob ein Zahlungssystem bei einem der Beteiligten neue Angriffsmöglichkeiten eröffnet.

Die Zahlungssystemsicherheit wird auch dann als kritisch beurteilt, wenn der Kunde vertrauliche Daten auf seinem System abspeichern muss, da den meisten Nutzern das Wissen zur korrekten Absicherung fehlt. Selbst mit sicheren Algorithmen verschlüsselte Daten werden häufig von Benutzern nur durch unsichere Passwörter geschützt. Wenn ein Angreifer in der Lage ist, ein Passwort zu erraten, weil dieses schlecht gewählt ist, dann erlangt er auch Zugriff auf die Daten.

Bedienungsfehler können ein weiteres Sicherheitsrisiko darstellen. Dies betrifft im Normalfall allerdings eher die Verwaltung der Daten als den Zahlungsvorgang an sich. Trotzdem gibt es Zahlungssysteme wie z. B. die Überweisung nach Rechnung, die nicht verhindern, dass ein falscher Empfänger das Geld erhält.

Das größte Sicherheitsproblem sieht die Analyse beim böswilligen Händler. Dies ist gerade für „Schnäppchenjäger“ das größte Risiko, da sie sich oft auf unbekannte Händler einlassen müssen.

Aber selbst bei vertrauenswürdigen Händlern können Produktfehler auftreten. Diese Fälle sind gesetzlich geregelt. Trotzdem kann eine Unterstützung bei der Abwicklung durch das Zahlungssystem sich positiv auswirken, da dies möglicherweise die Position des Kunden stärkt.

Die oben beschriebenen Bedrohungen fließen in drei Risiken für den Kunden zusammen.

- Rechnersicherheit: Falls neue Software installiert werden muss, können Inkompatibilitäten auftreten oder neue Angriffsmöglichkeiten entstehen.
- Geldverlust: Kann der Kunde bei einen Transaktionsabbruch oder durch Mißbrauch (Datenklau) Geld verlieren?
- Warenproblem: Unterstützt das Zahlungssystem den Kunden bei Reklamationsfällen?
- Rechtslage: Es wird beurteilt, ob der Kunde vertraglich und durch Einsatz entsprechender Authentifizierungsmaßnahmen in Beweisnöte kommen kann. Der Be-

wertung liegt dabei zu Grunde, dass die Gerichte bei EC-Karten-Urteilen meist dann zu Gunsten der Bank geurteilt haben, wenn das Verfahren auf dem aktuellen Stand der Technik war. Diese Annahme wird auf die Zahlungssysteme übertragen, die sich auf besondere Sicherungsmaßnahmen berufen.

Die Beurteilung, wie wichtig dem Nutzer die einzelnen Bereiche sind, bleibt diesem selbst überlassen und wird auch stark davon abhängen, inwieweit er seinen Händlern vertraut.

| ***Zahlungssystem*** | ***Rechner-sicher-heit*** | ***Geldverlust*** | ***Warenproblem*** | ***Rechts-lage*** |
|---|---|---|---|---|
| Kreditkartenverfahren | | | | |
| Kreditkarte (KK) SSL | + | + (abstreiten, kein rechtlich bindender Auf-trag) | o (kostenpflichtige Schlichtung) | + |
| KK SET | - | - | + (kostenpflichtige Schlichtung, Trans-aktionsinhalt beleg-bar) | - |
| KK Verified By... | + | - | o (kostenpflichtige Schlichtung) | - |
| KK T-Pay | + | - | o (kostenpflichtige Schlichtung) | - |
| KK paysafekey | + | - | o (kostenpflichtige Schlichtung) | - |
| KK Amazon Payments | + | o (3xGarantie) | o (kostenpflichtige Schlichtung oder 3xGarantie, Händ-ler bleibt pseudony-misiert) | - |
| Micropayments | | | | |
| Firstgate Click&Buy | + | - | o (Angebotssper-rung/Vermittlung) | - |
| paysafecard | + | - | - | - |
| T-Pay MicroMoney | + | - | - | - |
| T-Pay Telefonrechnung | + | - | o | - |
| T-Pay PayByCall | + | o (Transaktions-abbruch?) | o | - |
| Geldkarte | - | o (Transaktions-abbruch?) | - | - |

| *Zahlungssystem* | *Rechner-sicher-heit* | *Geldverlust* | *Warenproblem* | *Rechts-lage* |
|---|---|---|---|---|
| Lastschrift/Rechnungsverfahren | | | | |
| Lastschrift | + | + (Widerruf) | + (Widerruf) | + |
| Paybox | + | o (Transaktions-abbruch?) | - | - |
| iclear | + | + (Storno) | + (Storno) | - |
| paysafekey Lastschrift | + | - | - | - |
| T-Pay Lastschrift | + | + (Widerruf) | + (Widerruf) | - |
| Amazon Payments Lastschrift | + | o (3xGarantie) | o (3xGarantie, Händler bleibt pseudonymisiert) | - |
| Herkömmliche Verfahren | | | | |
| Vorüberweisung | + | - | - | keine on-line Auto-risierung |
| Rechnung nach Liefe-rung | + | + | + | |
| Nachnahme | + | + | o | |

*Tabelle 6: Bewertung der Zahlungssysteme aus Kundensicht*

## *11.2 Händler*

Der Bedrohungsbaum des Händlers ist sehr ähnlich zu dem des Kunden. Produktfeh-ler, die unabhängig vom Zahlungssystem immer das Risiko des Händlers sind, werden hier nicht beachtet. Der böswillige Händler wird im Baum durch den böswilligen Kunden ersetzt. Bei der Systemsicherheit ist zu beachten, dass der Händler im Gegen-satz zum Kunden bei fast jedem Zahlungssystem eine Verbindung zum Zahlungssys-tembetreiber benötigt und das Händlersystem daher mehr potentielle Angriffs-möglichkeiten bietet als das Kundensystem, auf dem meist keine zusätzlichen Kom-munikationsschnittstellen notwendig sind. Beim Schutz des Zahlungsablaufs hat der Händler zusätzlich zum Kundenschutz das Ziel, seine Transaktionsdaten vor der Kon-kurrenz zu schützen, da dies für ihn überlebenswichtig sein kann. Andererseits hat er natürlich den Wunsch, die Kundendaten für seine Zwecke zu nutzen. In dieser Analy-se ist das kein Gegensatz zu dem Kundenschutzziel der „Spamsicherheit“, da wir hier davon ausgehen, dass der Händler gutartig ist und die Daten nicht mißbräuchlich verwendet.

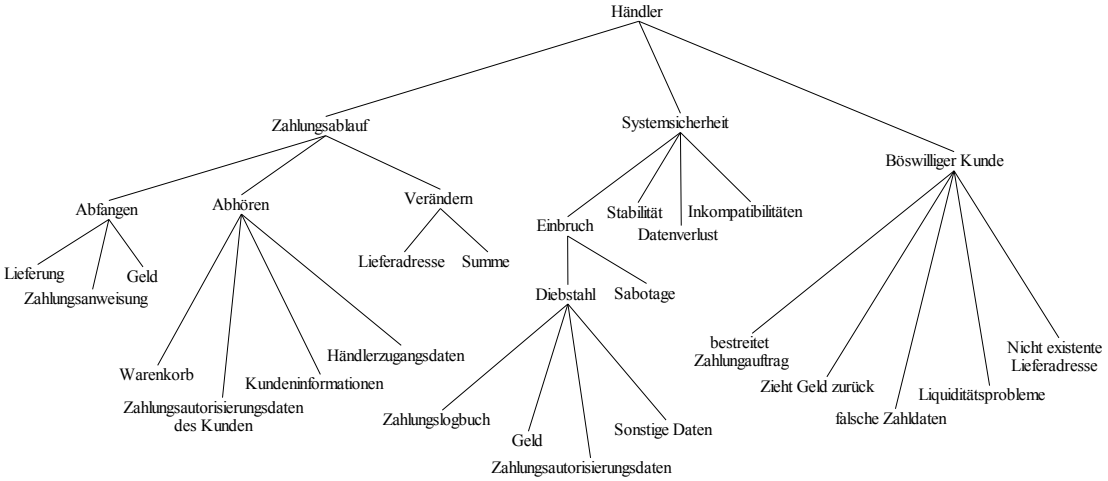



*Abbildung 3: Bedrohungen für den Händler*

Die Hauptbedrohung für den Händler ist der böswillige Kunde. Für den Händler stellt sich hier die Frage, ob ein Zahlungsverlust trotz Lieferung auftreten kann. Beim Zahlungsablauf existiert diese Bedrohung in der Form nicht, weil Internetzahlungssysteme die Zahlung mindestens autorisieren, bevor sie den Händler zur Auslieferung auffordern. Desweiteren ist die Systemsicherheit für den Händler von besonderer Bedeutung, da bei einem Einbruch Betriebsgeheimnisse offengelegt werden können und außerdem die Vertrauenswürdigkeit des Händlers stark geschädigt werden kann. Zu diesem Vertrauensverlust kann es auch kommen, wenn der Zahlungsablauf unsicher ist und Daten verändert oder abgehört werden können.
Wie beim Kunden wird bei den Zahlungssystemen eine Untersuchung der Rechnersicherheit und der Rechtslage vorgenommen. Die Rechtslage gibt an, ob der Händler im Zweifelsfall eine „sichere“ Authentifizierung nachweisen kann. In der folgenden Tabelle ist die Händlersicht dargestellt. Die Spalten „Geldverlust“ und „Warenproblem“ aus der Tabelle aus Kundensicht sind hier durch „Ablaufsicherheit“ und „Zahlungsausfall“ ersetzt.

| ***Zahlungssystem*** | ***Rechner-sicherheit*** | ***Ablauf-sicher-heit*** | ***Zahlungs-ausfall*** | ***Rechtslage*** |
|---|---|---|---|---|
| Kreditkartenverfahren | | | | |
| Kreditkarte (KK) SSL | o | + | + | - |
| KK SET | o | + | + | + |
| KK Verified By... | o | + | + | + |
| KK T-Pay | + | + | + | + |
| KK paysafekey | + | + | + | + |
| KK Amazon Payments | + | - | + | + (der Kunde erhält die Händleradresse nur bei Anzeige oder bei Einsatz der 3xGarantie) |

| ***Zahlungssystem*** | ***Rechner-sicherheit*** | ***Ablauf-sicher-heit*** | ***Zahlungs-ausfall*** | ***Rechtslage*** |
|---|---|---|---|---|
| Micropayments | | | | |
| Firstgate Click&Buy | + | + | o (Angebots-sperrung/-Vermitt-lung) | + |
| paysafecard | + | + | + | + |
| T-Pay MicroMoney | + | + | + | + |
| T-Pay Telefonrechnung | + | + | o | + |
| T-Pay PayByCall | + | + | o | + |
| Geldkarte | - („Geld“ wird auf dem Rechner gespeichert) | + | + | + |
| Lastschrift/Rechnungsverfahren | | | | |
| Lastschrift | o | + | - (Wider-ruf) | - |
| Paybox/Moxmo | o | + | + | + |
| iclear | + | - | + (Zah-lungsgaran-tie) | + |
| paysafekey Lastschrift | + | + | + | + |
| T-Pay Lastschrift | + | + | - (Wider-ruf) | + |
| Amazon Payments Lastschrift | + | - | + | + (der Kunde erhält die Händ-leradresse nur bei Anzeige oder bei Einsatz der 3xGarantie) |
| Herkömmliche Verfahren | | | | |
| Vorüberweisung | + | + | + | keine online Autorisierung |
| Rechnung nach Liefe-rung | + | - | - | |
| Nachnahme | + | + | + | |

*Tabelle 7: Bewertung der Zahlungssysteme aus Händlersicht*

## *11.3 Synthese der Kunden- und Händlerempfehlungen*

Schließt man die herkömmlichen Verfahren ein, sollte der Händler immer Vorkasse anbieten und der Kunde Rechnung nach Lieferung fordern. Als Kompromiss kann hier die Bezahlung per Nachnahme gesehen werden, die wenigstens die Nichtlieferung für den Kunden ausschließt. Ansonsten werden in diesem Kapitel nur die medienbruchfreien Zahlungssysteme untersucht.

### *11.3.1 Kreditkartenverfahren*

Abgesehen von Kreditkarte SSL sind alle Verfahren abgesichert, um zu verhindern, dass die Kreditkartennummer unautorisiert verwendet werden kann. Bei diesen Verfahren kann das Geld nicht einfach zurückgezogen werden, sondern es muss der im allgemeinen kostenpflichtige Schlichtungsdienst in Anspruch genommen werden. Damit muss der Kunde für diese Verfahren im Fehlerfall mit Kosten rechnen. Der Händler hat in Deutschland inzwischen bei allen Kreditkartenverfahren eine Zahlungsgarantie, wenn er sich an die Vorgaben der Zahlungsinstitute hält. Langfristig ist allerdings damit zu rechnen, dass die Händler das reine SSL-Verfahren nicht mehr anbieten dürfen. Trotzdem sollte ein Händler dieses Verfahren momentan noch anbieten, da es bei den Kreditkartenzahlungen das vorteilhafteste für den Kunden ist und es außerdem das einzige Kreditkartenverfahren ist, bei dem keine gesonderte Registrierung des Kunden bei einem Zahlungssystembetreiber notwendig ist, um Internetzahlungen durchführen zu können.
Längerfristig wird dieses Verfahren durch Verified By Visa/Mastercard Secure Code ersetzt werden. Dieses Verfahren wird langfristig nötig sein, wenn Kunden aus dem Ausland angesprochen werden sollen. Ist das nicht der Fall, können auch T-Pay oder paysafekey verwendet werden. Die bessere Marktposition dürfte hier T-Pay haben. Für diese Verfahren spricht im Gegensatz zu den reinen Kreditkartenverfahren, dass unter einer Schnittstelle verschiedene Verfahren bedient werden können. Amazonpayments ist ein Sonderfall, der nur in einem Amazonshop verwendet werden kann.

### *11.3.2 Lastschrift/Rechnungsverfahren*

Das normale Lastschriftverfahren schützt den Kunden durch eine sechswöchige Rückzugsmöglichkeit. Für den Händler ist kein Schutz vorgesehen. Kennzeichen der autorisierenden Lastschriftverfahren ist eine vertragliche Absicherung der Händler, indem den Kunden der Rückzug bei Bestätigung mittels PIN untersagt wird. Den besten Kompromiss liefert hier das Lastschriftverfahren von T-Pay. Der Kunde ist zwar nach wie vor berechtigt das Geld zurückzuziehen, der Händler hat aber im Streitfall gute Karten vor Gericht, weil T-Pay die Zahlung mittels Passwortverfahren autorisiert hat. Für das reine Lastschriftverfahren ist das Risiko für den Händler eigentlich zu hoch, um es empfehlen zu können.
Sonderfälle sind Paybox/Moxmo und iclear. Mit Paybox/Moxmo kann sich der Händler möglicherweise einen Kundenkreis im Mobile-Commerce erschließen. Der Kunde muss beim Einsatz des Verfahrens allerdings damit rechnen, dass er im Schadensfall auf die Kooperation des Händlers angewiesen ist. Durch die netzexterne Authentifizierung kann das Verfahren aber als sicher angesehen werden. Das iclear-Verfahren hat den Nachteil, dass es von verschiedenen Händlern unsicher ohne SSL angebunden wird und so eventuell zum Vertrauensverlust führen könnte. Rechtlich gesehen ist das Verfahren allerdings sicher, da der Händler eine Zahlungsgarantie erhält und der Kunde eine zugesicherte Stornomöglichkeit während der Widerrufsfrist des Fernabsatzgesetzes hat, auch wenn der Händler nicht kooperiert.

### *11.3.3 Micropayments*

Bei Micropayments ist der Käufer grundsätzlich im Nachteil. Er muss bei allen Verfahren bezahlen, bevor er die Ware zu sehen bekommt. Im Fehlerfall ist der Schaden so klein, dass sich ein größerer Aufwand für eine Reklamation nicht lohnt. Für den Kunden ist daher am ehesten interessant, ob er neben dem Händler noch einen weiteren Ansprechpartner hat, der möglicherweise vermittelt. Auf dieses Problem gehen nur Firstgate, Telekomrechnung und PayByCall in ihren allgemeinen Geschäftsbedingungen ein. Diese Verfahren sind daher möglicherweise etwas sicherer für den Kunden. Geht man aber davon aus, dass die Kundenbindung bei Konfliktfällen zunimmt, die zur Zufriedenheit der Kunden gelöst wurden, darf dieser Passus nicht überbewertet werden. Von der Verbreitung her ist Firstgate der Marktführer. Das gilt aber nach wie vor nur für eine ziemlich kleine Basis. Der Registrierungsaufwand bei T-Pay ist für Neukunden deutlich geringer. Allerdings können nur Telekomkunden mit T-Pay bezahlen. Der Vorteil, der hier am schwersten wiegt, dürfte sein, dass bei T-Pay ein ganzes Spektrum von Zahlungssystemen unter einer einheitlichen Schnittstelle angeboten wird. Für die paysafe-Verfahren gilt dies zwar auch, aber bei diesen ist die Verbreitung in Deutschland bisher nur sehr gering.
Die Geldkarte muss getrennt von den anderen Verfahren behandelt werden. Dieses Verfahren hat Gebühren, die um den Faktor 100 niedriger sind als bei den anderen Verfahren. Der Nachteil ist allerdings die notwendige Hardware sowohl für Händler als auch für die Kunden. Dies ist vor allem für die Kunden eine fast unüberwindbare Hürde. Ein weiterer Nachteil ist, dass die eingenommenen Gelder auf einem Rechner des Händlers gespeichert werden müssen. Ein Verlust dieser Gelder kann daher nicht mit 100%iger Sicherheit ausgeschlossen werden. Die Geldkarte dürfte außerdem das Verfahren sein, bei dem der Kunde im Reklamationsfall die schlechtesten Aussichten hat, da die Geldkarte im Prinzip wie Bargeld verwendet wird.

### *11.3.4 Einsatzempfehlung*

Ein Händler muss heutzutage auf Grund der Zahlungssystemvielfalt mehrere Zahlungssysteme anbieten, um konkurrenzfähig zu sein. Empfohlen wird deshalb die Kombination von normaler Kreditkartenzahlung mittels SSL-Formular in Kombination mit den Varianten des T-Pay Verfahrens. Als Minimallösung können die T-Pay Verfahren alleine angeboten werden. Optional könnte dieses Portfolio wegen der vergleichsweise weiten Verbreitung um das Firstgateverfahren ergänzt werden. Sollen physische Güter angeboten werden, ist das Rechnungsverfahren iclear interessant.
Abgeraten wird im besonderen von Lastschrift per SSL-Formular, da das Risiko für den Händler zu hoch ist. Gegen die anderen Systeme spricht in erster Linie die geringe Verbreitung. Die Sicherheitsunterschiede sind eher marginal.

# 12 Zuverlässigkeit

## *12.1 Verfügbarkeit*

Bei der Entwicklung wurden einige Maßnahmen ergriffen, um die Verfügbarkeit des Zahlungsservers zu erhöhen. Diese Maßnahmen werden im Folgenden kurz vorgestellt.

### *12.1.1 Replikation und Lastverteilung*

Eine wichtige Möglichkeit, um die Verfügbarkeit zu verbessern, ist die Installation mehrerer Server. Chablis benötigt für die Erbringung der technischen Leistung eine Datenbank im Hintergrund, in der alle anfallenden Daten abgespeichert werden. Beim Einsatz eines entsprechendes Datenbanksystems wie beispielsweise von Oracle kann die Datenhaltung repliziert erfolgen.
Daneben ist es auch möglich, mehrere Chablis Server zu installieren, die von den Händlern gemeinsam benutzt werden können. Neben einer Verbesserung der Verfügbarkeit ermöglicht dieser Ansatz auch eine Lastverteilung.

### *12.1.2 Teilabschaltung fehlerhafter Zahlungssysteme*

Es ist immer möglich, dass in einem Zahlungssystemmodul Fehler auftreten, sei es durch fehlerhafte Programmierung oder durch Fehler außerhalb des Einflussbereichs von Chablis wie etwa Netzwerk- und Serverausfällen auf Seiten des Zahlungssystem-Anbieters. Solche Fehler in einem Zahlungssystem dürfen nicht dafür sorgen, daß andere Zahlungssysteme oder gar der Chablis-Server selbst dadurch in Mitleidenschaft gezogen werden. Aus diesem Grund werden Zahlungssysteme beim Auftreten eines entsprechend schwerwiegenden Fehlers automatisch deaktiviert und bis zur Beseitigung des Problems dem Kunden nicht mehr angeboten. Der Administrator kann Konfigurationsänderungen vornehmen und das Zahlungssystem neu laden.

## *12.2 Recoveryfähigkeit*

Im Verlauf einer Transaktion kann es zu verschiedenen Fehlersituationen kommen. Computersysteme können abstürzen, ebenso können Netzwerke ausfallen. Diese Fehler dürfen jedoch nicht dazu führen, dass Transaktionen in einen undefinierten Zustand geraten und möglicherweise der Kunde bezahlt hat, aber keine Ware mehr geliefert bekommt. Bei der Entwicklung von Chablis wurde deshalb Wert darauf gelegt, dass nach solchen Ausfällen ein Recovery durchgeführt wird. Ebenso muss der Chablis-Server selbst nach einem Systemabsturz wieder in einem definierten Zustand sein.
Die exakten Recovery-Fähigkeiten hängen jedoch stark von dem bei der Transaktion verwendeten Zahlungssystem ab. Das liegt daran, dass das Zahlungssystem selbst über weiter reichende Informationen über den aktuellen Bearbeitungsstand der Zahlungsanforderung verfügt, da diese Daten proprietär sind und bei jedem Zahlungssystem unterschiedlich aussehen.
Das Recovery wird daher von Chablis so realisiert, dass in allen Situationen, in denen ein Recovery benötigt wird, beim Start von Chablis das Zahlungssystem über eine festgelegte Schnittstelle den aktuellen Stand der Bearbeitung mitteilt. Diese Informationen verwendet Chablis wiederum, um die Transaktion abzuschließen und den Händler über die erfolgreiche Zahlung zu informieren. Falls die Transaktion vor der Zahlung abgebrochen ist, wird sie als fehlerhaft gekennzeichnet. Bei Zahlungssystemen, die kein automatisches Abschließen ermöglichen, ist eine Interaktion mit dem Administrator erforderlich (z. B. weil das Zahlungssystem den Status des Zahlungsversuches nicht kennt). In solchen Fällen erhält der Administrator eine Liste der entsprechenden Transaktionen und kann diese manuell abschließen. Chablis ist jedoch unabhängig davon wieder verwendbar.
Die Recoveryfähigkeiten wurden unfreiwillig dadurch getestet, dass im Server über einige Zeit ein Hauptspeicherbaustein defekt war.

# 13 Administratives Umfeld

Während des Projekts stellte sich heraus, dass die Rahmenbedingungen für den Einsatz von digitalen Zahlungssystemen an öffentlichen Einrichtungen, im speziellen den Hochschulen, nicht optimal sind. Das gilt sowohl für den Fall, dass eine öffentliche Einrichtung als Händler auftreten will, als auch für den Fall, dass ein Angestellter der Hochschule bei einem Händler einkaufen will, der nur digitale Zahlungssysteme anbietet.
Der öffentliche Dienst ist stark an haushaltsrechtliche Regelungen gebunden und kann daher nicht frei agieren, wenn er digitale Zahlungssysteme einsetzen möchte. Im Folgenden wird die Situation in wissenschaftlichen Einrichtungen vorgestellt. Im allgemeinen sind die Rahmenbedingungen aber auch auf andere öffentliche Einrichtungen übertragbar.

## *13.1 Hochschulrahmengesetz*

Im Hochschulrahmengesetz sind die Aufgaben der Hochschulen geregelt. Darin heißt es: „Das Hochschulwesen dient der Pflege und Entwicklung der Wissenschaften und der Künste durch Forschung, Lehre und Studium. Die Hochschulen bereiten auf eine berufliche Tätigkeit vor, welche die Anwendung wissenschaftlicher Erkenntnisse und wissenschaftlicher Methoden oder die Fähigkeiten zu künstlerischer Gestaltung erfordert.“ (Art. 2 Abs. 1) Andere Aufgaben dürfen einer Hochschule nur übertragen werden, wenn sie mit den oben genannten Aufgaben zusammenhängen (vgl. Abs. 8).
Daraus ergibt sich, dass die Hochschule in genehmigten Forschungsprojekten alle dafür nötigen Voraussetzungen schaffen darf, auch wenn diese selbst ohne das Forschungsprojekt nicht der Forschung dienen. Ist das Forschungsziel erreicht, heißt das aber gleichzeitig, dass eine solche Tätigkeit nach dem Projektabschluss wieder einzustellen ist.
Die Einnahme von Geldern für Dritte wäre genau eine solche Tätigkeit, die während des Projekts möglich wäre, aber mit Abschluss wieder eingestellt werden müsste. Eine dauerhafte Betriebslösung für Dritte ist daher an Hochschulen nicht möglich.

## *13.2 Kontoführung der bayerischen Hochschulen*

Gerade bei Tätigkeiten im Bereich des Kreditwesens gibt es weitere, schwierige Rahmenbedingungen. Die Geldflüsse an öffentliche Einrichtungen sind sehr starr geregelt. Dies betrifft sowohl die Art der Kontoführung als auch die Verwendung von Einnahmen. Änderungen in diesem Ablauf hätten an der TU München einen so großen Personalaufwand bedeutet, dass von einer Inbetriebnahme des Chablis-Servers, die ja nur für die Projektlaufzeit möglich gewesen wäre, abgesehen werden musste.

- Die Gelder fließen über ein Konto der Staatsoberkasse. Das Anlegen weiterer Konten ist nur in Ausnahmefällen möglich und hier nur zeitlich begrenzt.
- Alle Einzahlungen müssen vorher in exakter Höhe bekannt sein. Dies kann nicht bei allen Zahlungssystemen garantiert werden. Unbekannte Einnahmen landen auf einem Verwahrkonto.
- Bei Gebührenabzügen durch die Zahlungssysteme müssten die Einnahmevereinbarungen angepasst werden.

## *13.3 Verwaltungskostengesetz*

Das Verwaltungskostengesetz (VwKostG) regelt die Kosten (Gebühren und Auslagen) öffentlich-rechtlicher Verwaltungstätigkeit der Behörden des Bundes, der

Länder, der Gemeinden und der diesen unterstehenden juristischen Personen des öffentlichen Rechts (vgl. VwKostG § 1). Es enthält die Grundsätze der Gebührenbemessung, Gebührenpflicht und Gebührenfreiheit sowie die Regelung über Gläubiger, Schuldner, Fälligkeit und Verjährung.
Für uns ist § 3 (vgl. auch § 9 Gebührenbemessung) über die Gebührengrundsätze relevant: „Die Gebührensätze sind so zu bemessen, dass zwischen der den Verwaltungsaufwand berücksichtigenden Höhe der Gebühr einerseits und der Bedeutung, dem wirtschaftlichen Wert oder dem sonstigen Nutzen der Amtshandlung andererseits ein angemessenes Verhältnis besteht. Ist gesetzlich vorgesehen, dass Gebühren nur zur Deckung des Verwaltungsaufwandes erhoben werden, sind die Gebührensätze so zu bemessen, dass das geschätzte Gebührenaufkommen den auf die Amtshandlungen entfallenden durchschnittlichen Personal- und Sachaufwand für den betreffenden Verwaltungszweig nicht übersteigt."
An das VwKostG haben sich auch die anderen Gebührenordnungen zu halten. Daraus ergibt sich offensichtlich ein Problem. Die digitalen Zahlungssysteme decken ihre Kosten großenteils über transaktionsbezogene Gebühren. Diese Gebühren sind zum Teil nicht unerheblich und sind unabhängig vom Personal- oder Sachaufwand der Verwaltungstätigkeit. Es ist nicht klar geregelt, ob gebührenbehaftete Zahlungssysteme zur Begleichung rein kostendeckender Verwaltungsgebühren zulässig sind. Hier müssten möglicherweise die Kosten solcher Zahlungssysteme aufgeschlagen werden.

### *13.4 Bayerisches Kostengesetz*

Das Kostengesetz (KG) ist die Umsetzung des VwKostG in bayerisches Recht. Die Gebühren zu den Verwaltungstätigkeiten sind im zugehörigen Kostenverzeichnis (KVz) festgelegt. In diesem sind auch die Gebühren des Hochschulwesens festgelegt. Zur Fälligkeit von Verwaltungskosten ist in Art. 15 KG festgelegt, dass die Kosten mit der Bekanntgabe fällig werden.
Im Hochschulbereich heißt das, dass die Gebühren mit der Immatrikulation/Rückmeldung bzw. der Anmeldung zu einer Bildungsveranstaltung fällig werden. Die meisten Zahlungssysteme nehmen aber nur eine Autorisierung vor und die eigentliche Zahlung erfolgt erst später, so dass die Gebühren defacto nicht bei Fälligkeit beglichen werden.

### *13.5 Einnahmen*

Weiterhin muss beachtet werden, dass eigene Einnahmen den Hochschulen nur zum Teil zur Verfügung stehen. Laut Angabe der TU-Rechtsabteilung dürfen nur 95% der Einnahmen im selben Jahr wieder ausgegeben werden. Außerdem fallen für Einnahmen Steuern an, was beim normalen Gebührenaufkommen nicht der Fall ist.
Statt Steuern abzuführen ist für das normale Gebührenaufkommen in der Hochschulgebührenverordnung (HSchGebV) § 5 (Zuständigkeit, Gebührenaufkommen) festgelegt, dass hier sogar nur 80 v. H. der Hochschule zusteht.

### *13.6 Drittmittel*

Im Fall eines Zahlungsserverdienstes sind aber vor allem die Verwaltungsvorschriften zur Annahme und Verwendung von Mitteln Dritter an Hochschulen (DriMiR) interessant. Bei Gewinnen durch einen solchen Zahlungsserver würde es sich formal um Drittmittel handeln. „Drittmittel sind Zuwendungen, Spenden, Sponsoring und sonstige Leistungen aus einseitig verpflichtenden oder gegenseitigen Verträgen sowie alle

sonstigen geldwerten Vorteile, die die Hochschule zur Erfüllung ihrer Aufgaben erhält.“ (DriMiR 1.2.1)
„Die Verwaltung der Drittmittel soll durch die Hochschule erfolgen. Die Einnahmen und Ausgaben sind im Haushaltsplan nachzuweisen. Die Drittmittel und die aus drittmittelfinanzierten Vorhaben fließenden Erträge sind rechtzeitig und vollständig zu erheben und entsprechend den Regeln ordnungsgemäßer Buchführung, insbesondere nach den Grundsätzen der Bilanzwahrheit und Bilanzklarheit, zu verwalten.“ (DriMiR 3.1) Ausnahmsweise kann für Forschungsvorhaben eine Sonderkontenverwaltung bei der Hochschulleitung beantragt werden (vgl. DriMiR 3.2).
Durch die Form der Verrechnungspflicht der Einnahmen im Haushaltsplan wird die Innovation gehemmt, da das Geld erstens nicht vollständig wiederverwendet werden darf und außerdem möglicherweise mit Einnahmeeinbußen in Form von Streichung öffentlicher Gelder gerechnet werden muss, da die Einnahmen im Haushaltsplan bereits berücksichtigt sind. Im Bayerischen Hochschulgesetz (BayHSchG) Art. 7 Abs. 3 ist dies genauer geregelt: „Die Einnahmen der Hochschulen mit Ausnahme der Einnahmen nach Art. 95 Abs. 2 fließen in den staatlichen Haushalt. Von diesen Einnahmen stehen den Hochschulen Betriebseinnahmen nach Maßgabe des Haushalts zur Verfügung.“ Projekte sind damit in gewisser Weise zu einem Nullsummenspiel verpflichtet, was der Intention des Betriebs eines Zahlungsservers zuwider läuft.

## *13.7 Rechtliche Erfahrungen der Technischen Informationsbibliothek Hannover*

Die Technischen Informationsbibliothek Hannover (TIB) war als Projektpartner des Chablisprojekts damit beauftragt, den Wirkbetrieb des Chablis-Servers zu gewährleisten. Hier soll kurz auf das dazu angestrebte Verfahren und die damit verbundenen Probleme eingegangen werden.
Um einen umfassenden Betrieb und Test zu ermöglichen, sollten zunächst Bedingungen geschaffen werden, die einen Test ohne Beeinträchtigung der bisherigen Buchführung ermöglichen sollten.
Dabei zeigte sich schnell, dass Fragen bezüglich der Kontoführung bis an die zuständigen Ministerien (Wissenschaft und Kultur bzw. Finanzen) geleitet werden mussten. Die Anfragen nach einer Testkreditkarte und dem Zugang zu elektronischen Abrechnungsdaten der Zahlungssysteme wurde abgelehnt. Händlerverträge für die Zahlungssysteme Kreditkarte, elektronische Lastschrift und Paybox wurden auch sehr lange geprüft. Sie wurden schließlich unter den folgenden Gesichtspunkten genehmigt:

- Die Anbindung neuer Zahlungssysteme musste kostenneutral sein, d. h. aus Projektmitteln oder bereits vorhandenen Eigenmitteln gedeckt werden.
- Der zweite wesentliche Faktor war die Zahlungssicherheit. Durch ein neues Zahlungssystem darf das Risiko des Zahlungsausfalls nicht steigen. In unserem Fall war bisher nur ein nachträgliches Rechnungsverfahren eingesetzt. Da die neuerdings eingesetzten Zahlungssysteme vor der Lieferung die Zahlung autorisierten, wurde vom zuständigen Justiziariat festgestellt, dass dies das Insolvenzrisiko hinsichtlich der Konsumenten minimiert. Dies bedingt, dass die Wahrscheinlichkeit des Zahlungsausfalls abnimmt. Folglich wurden die Verträge genehmigt.
- AGB der Zahlungssysteme: Während des Vertragsabschlusses änderte sich das deutsche Recht hinsichtlich der auf jetzt zwei Jahre verlängerten Verbrauchergarantie. Der Paybox-Vertrag berücksichtigte dies noch nicht und verwies auf eine sechsmonatige Gewährleistungsfrist. Auch wenn bei Verträgen mit der öffentlichen Hand solche Bedingungen ausgehandelt werden können, wie das auch unter

Vollkaufleuten der Fall ist, verursachte diese Abweichung vom BGB eine zeitliche Verzögerung beim Vertragsabschluß von mehreren Monaten.

Daraus ergeben sich drei kritische Punkte für den Zahlungssystemeinsatz in der öffentlichen Hand:

- Eine kostenneutrale Anbindung ist im Normalfall nicht möglich, es sei denn es stehen speziell für diesen Zweck Projektmittel zur Verfügung. Dabei wird außer acht gelassen, dass durch den Einsatz digitaler Zahlungssysteme die Buchhaltungskosten sinken können.
- Die Zahlungssicherheit erhöht sich normalerweise nur im Fall von Rechnungszahlung. Dies ist ein Spezialfall, der an der TIB gegeben ist. Normalerweise werden Gebühren aber bar beglichen. Hier ist die Zahlungsautorisierung, die von den meisten Systemen durchgeführt wird, weniger sicher, weil meist ein nachträglicher Widerruf des Kunden möglich ist. Allerdings stellt sich auch hier die Frage, ob dieser Nachteil durch die Ersparnis des Bargeldhandlings wieder aufgehoben wird.
- Der dritte Punkt trifft mehr die Zahlungssystemhersteller. Sie sollten die Öffentliche Hand nicht vor unnötige Herausforderungen stellen und sich auch bei den Händlerverträgen möglichst an das BGB halten.

## *13.8 Rechtsgutachten*

Auf Grund der vielen Betriebsprobleme wurde ein Rechtsgutachten von der Forschungsstelle Recht des DFN-Verein erstellt, ob der problembehaftete Bereich der Zahlungssystemvertragsabschlüsse und des Serverbetriebs nicht aus dem Öffentlichen Bereich ausgelagert und von einem externen Betreiber geleistet werden könnte.

Rechtlich gesehen ist es danach möglich, durch den Chablis-Betreiber Dienstleister und Händler, insbesondere Bibliotheken davon zu entlasten, verschiedene Verträge mit unterschiedlichen Zahlungssystemanbietern abzuschließen. Chablis unterhält jeweils zu den verschiedenen Zahlungssystemanbietern Vetragsverhältnisse (i.d.R. Geschäftsbesorgungsverträge, bzw. Bestandteile von Geschäftsbesorgungsverträgen). Durch eine bedingte Globalzession (unter der Bedingung der Zahlung via Internet) ist Chablis als neuer Gläubiger dazu berechtigt, die Forderungen gegen den jeweiligen Kunden bei dessen Bank geltend zu machen. Durch eine regelmäßige Saldierung (etwa monatlich) überweist Chablis die angefallenen Entgelte an die jeweilige Bibliothek. Das Gutachten ist einsehbar unter http://chablis.in.tum.de/papers/DFN-Gutachten.pdf.

Wie im Gutachten empfohlen, wurde sicherheitshalber zusätzlich zum Gutachten eine Anfrage an die Bundesanstalt für Finanzdienstleistungsaufsicht gestellt, die klären sollte, ob der Betrieb gemäß § 32 KWG erlaubnispflichtig ist. Eine Antwort war auf Grund der Arbeitsbelastung dieses Instituts im Laufe der Projektlaufzeit leider nicht erhältlich.

## *13.9 Hochschule als Kunde*

Im Internet steigt inzwischen die Anzahl kostenpflichtiger Inhalte. Bei größeren Beträgen sind meist Kreditkartenzahlungen möglich. Niedrigpreisige Artikel sind dagegen nur über Micropayments abrufbar. Je größer das Angebot wird, desto häufiger wird auch der Bedarf der öffentlichen Einrichtungen sein, auf solche Dokumente zuzugreifen. Schon heute bieten viele kommerzielle Forschungsinstitute ihre Studien nur gegen Gebühren an. Deren Ergebnisse können aber durchaus auch für öffentliche Forschungseinrichtungen interessant sein. Es stellt sich also die Frage, wie sich öffentliche Einrichtungen Zugriffsmöglichkeiten auf solche Informationen offen halten

können. Gerade bei Angeboten aus dem Ausland ist es meist nicht möglich, eine Sonderbehandlung wie eine getrennte Rechnungsstellung für die öffentliche Hand zu erhalten. Schon aus Kostengründen kommt ein solches Verfahren bei kleinen Beträgen generell nicht in Frage. Kann die öffentliche Hand also neuartige Zahlungsverfahren nutzen?
Digitale Zahlungssysteme sind momentan für die öffentliche Hand noch nicht verfügbar. Als Ausnahme kann hier höchstens die Kreditkarte gesehen werden, die inzwischen zum Teil auch in öffentlichen Einrichtungen zur Verfügung steht. Eine Lösung des Problems für digitale Zahlungssysteme kann hier natürlich nicht gegeben werden. Dies ist Sache des Gesetzgebers. Aber immerhin soll darauf aufmerksam gemacht werden, dass es sinnvoll ist, schon jetzt klare Grundlagen zu schaffen, um einen Einsatz dieser neuen Zahlungsverfahren zu ermöglichen. Dies sollte in einer Form geschehen, die unabhängig von einem speziellen Zahlungssystem ist, weil die Fluktuation im Bereich der Internetzahlungssysteme noch zu groß ist. Ein Einsatz erst mit großer Verspätung wie bei der Kreditkarte ist in einer Zeit, in der die Entwicklung im Bereich des Internet und der Telekomunikation sehr viel schneller vorangeht, auf keinen Fall akzeptabel. Die Forschungseinrichtungen sind sonst von einem Teil der Entwicklungen abgeschnitten.
Sinnvoll bei einer Neuregelung wäre es außerdem, darauf zu achten, dass die Verfügungsberechtigten selbst Zugriff auf die Verfahren haben und nicht alles über eine Zentrale laufen muss. Hier können die Zahlungssystemanbieter ihren Teil beitragen, indem sie ein Abrechnungsverfahren implementieren, das vergleichbar mit Corporate-Kreditkarten verwendet wird. Dort haben verfügungsberechtigte Angestellte eine Firmenkreditkarte auf ihren Namen. Sie können so im Rahmen ihres Budgets neben Rechnung ein weiteres Zahlungsverfahren nutzen, ohne von umständlichen Verwaltungsverfahren behindert zu werden. Diese Änderung wäre auch für Kreditkartenverfahren denkbar, da bei Kreditkartenbestellungen bisher immer mehrere Angestellte tätig werden müssen.

# 14 Fazit

Im Betriebsverlauf hat sich gezeigt, dass die elektronischen Zahungssysteme inzwischen betriebstauglich für den realen Einsatz geworden sind. Allerdings sind sie weiterhin noch nicht so wirtschaftlich stabil, dass sich ein fester Standard herauskristallisiert hätte. Es treten immer noch neue Zahlungssysteme auf den Markt, ebenso verschwinden immer wieder Zahlungssysteme, wenn auch nicht mehr ganz so häufig wie noch vor einigen Jahren.
Daneben zeichnet sich ein eindeutiger Trend ab, hin zu virtualisierenden Schnittstellen unter denen unterschiedliche Zahlungsverfahren (oder Abrechnungsverfahren) integriert werden (z. B. T-Pay der Deutschen Telekom). Das zeigt, dass der Ansatz von Chablis, einen Wrapper um die Zahlungssysteme zu legen, absolut richtig war und inzwischen auch von kommerziellen Produkten vollzogen wird.
Der sinnvolle Einsatzbereich elektronischer Zahlungssysteme liegt eindeutig im Bereich der digitalen Waren. Hier kommen die Vorteile wie etwa das Einkaufen ohne Medienbruch voll zur Geltung. Trotzdem bevorzugen Kunden das traditionelle Rechnungsverfahren sehr stark, da dieses das Risiko alleine auf den Händler schiebt.
Im Projektzeitraum hat sich auch gezeigt, dass die Märkte in denen öffentliche Einrichtungen als Händler oder Kunden tätig sind, Unterschiede und Besonderheiten im Vergleich zur sonstigen Wirtschaft aufweisen. So kommen Angestellte nicht als di-

rekte Kunden in Frage, da sie in der Regel über keinen Zugang zu elektronischen Zahlungssystemen verfügen.
Als Händler können öffentliche Einrichtungen nur in begrenztem Maße tätig werden, d. h. so lange es zu ihrem Aufgabenbereich zählt. Sie können generell nicht Gelder für Dritte einnehmen und deshalb auch nicht als Betreiber eines Zahlungsservers für Andere auftreten.
Zu guter letzt besteht bei Geschäftsbeziehungen zwischen zwei öffentlichen Einrichtungen ein Vertrauensverhältnis, so dass hier Sammelabrechnungen zum Einsatz kommen, in denen die angesammelten Beträge regelmässig in Rechnung gestellt werden. Der Einsatz von digitalen Zahlungssystemen kommt in entsprechenden Vertragsbeziehungen daher nicht in Frage.
Ein etwa einjähriger Betrieb hätte von den Restmitteln des Projektes finanziert werden können. Damit konnte aber keine langfristige Planungssicherheit gewährleistet werden. Diese Rahmenbedingung hatte zur Folge, dass sich keine Kunden finden ließen, die den Server benutzen wollten, da keine weitere Betriebsgarantie gegeben werden konnte und damit die Nachhaltigkeit nicht gesichert war.
In der Konsequenz empfehlen wir dem DFN-Verein für den Fall, dass er seinen Mitgliedern eine elektronische Bezahlmöglichkeit anbieten möchte, den Einsatz von T-Pay. T-Pay bietet wie Chablis eine virtualisierte Schnittstelle für die Händler. Die Palette der angebotenen Systeme ist ziemlich breit, aber nur von Seiten der Telekom erweiterbar. Wenn hier eine Art Rahmenvertrag zwischen DFN-Verein und der Telekom für alle Mitglieder des Vereins geschlossen werden kann, fällt die Suche nach einem Betreiber weg und die Software wird von T-Pay selbst betreut.

## 15 Veröffentlichungen/Vorträge

- Juni 2001, Düsseldorf: 15. DFN-Jahrestagung über Kommunikationsnetze
  Chablis: Eine Abrechnungs- und Zahlungs-Infrastruktur für digitale Bibliotheken
  http://chablis.in.tum.de/papers/dfntag.pdf

- März 2002, Kassel: DFN Tagung der Verantwortlichen der Rechenzentren der deutschen Universitäten
  Elektronische Zahlung für RZ-bezogene Netzdienste anhand des DFN Projekts Chablis PS

- Juni 2003, Siemensforum München: Workshop Sicherheit in Wissenschaft und Wirtschaft
  IT-Sicherheit und Rechtssicherheit bei Zahlungssystemen im Internet

- September 2003, Leipziger Informatiktage LIT'03: Von e-Learning bis e-Payment 2003
  Chablis – Ein Zahlungsserver für öffentliche Einrichtungen. Projekterfahrungen aus rechtlicher und technologischer Sicht
  Workshop – Security Engineering in e-Payment Systems
  http://chablis.in.tum.de/papers/litpaper.pdf

## 16 Anlage/Verweise

- Chablis Zahlungsserver – Handbuch vom 30.3.2004
  http://chablis.in.tum.de/papers/handbuch.pdf

- Studie – Stärken-Schwächen-Analyse des Chablis Zahlungsservers vom 29.4.2003
  http://chablis.in.tum.de/papers/SWOT-Chablis.pdf

- Rechtsgutachten der Forschungsstelle Recht zu Rechtsfragen des Chablis Projektes vom 14.2.2003
  http://chablis.in.tum.de/papers/DFN-Gutachten.pdf

- Projektablauf/Projektberichte: http://chablis.in.tum.de/project.html