research

an der Universität
Regensburg

Sichere Zahlungsverfahren für E-Government

Der hier vorliegende Text ist ein Modul aus dem

E-Government-Handbuch

http://www.e-government-handbuch.de

Redaktion: Projektgruppe E-Government im **Bundesamt für Sicherheit in der Informationstechnik (BSI)**

Kontakt: egov@bsi.bund.de

Inhaltsübersicht

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AGB	Allgemeine Geschäftsbedingungen
AO	Abgabenordnung
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BAM	Bundesanstalt für Materialforschung und -prüfung
BdB	Bundesverband deutscher Banken
BDSG	Bundesdatenschutzgesetz
BfF	Bundesamt für Finanzen
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BHO	Bundeshaushaltsordnung
BIC	Bank Identifier Code
BLZ	Bankleitzahl
BMF	Bundesministerium der Finanzen
BMI	Bundesministerium des Innern
BPA	Bundespresseamt
BpG	Buchungspostengebühr
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerwG	Bundesverwaltungsgericht
CSC	Card Security Code
CVC	Card Verification Code
CVC2	Card Verification Code2
CVV	Card Verification Value
CVV2	Card Verification Value2
DIMDI	Deutsches Institut für Medizinische Dokumentation und Information
ec	electronic cash
edd	electronic direct debit
Elster	Elektronische Steuererklärung
ELV	Elektronisches Lastschriftverfahren
EMV	Europay/Mastercard/Visa
eps	e-payment standard
ERP	Enterprise-Resource-Planning
FSA	Financial Services Authority
HBCI	Home Banking Computer Interface
HKR	Haushalts-, Kassen- und Rechnungswesen des Bundes

IBAN	International Bank Account Number
ibi	Institut für Bankinnovation
ID	Identification, dt.: Identifikation
IT	Informationstechnologie
KLR	Kosten- und Leistungsrechnung
KPN	Kartenprüfnummer
MAC	Message Authentication Code
MDStV	Mediendienstestaatsvertrag
MPI	Merchant Server Plug-in
pdf	Portable Document Format (Dateinamen-Erweiterung)
PIN	Persönliche Identifikationsnummer
POS	Point of Sale
POZ	Point of Sale ohne Zahlungsgarantie
SAGA	Standards und Architekturen für E-Government-Anwendungen
SEPA	Single European Payment Area
SET	Secure Electronic Transaction
SIM	Subscriber Identification Module
SLA	Service Level Agreement
SMS	Short Message Service
SSL	Secure Sockets Layer
StDÜV	Steuerdaten-Übermittlungsverordnung
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TAN	Transaktionsnummer
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
USt.	Umsatzsteuer
UStG	Umsatzsteuergesetz
WAP	Wireless Application Protocol
WWW	Word Wide Web
xls	Excel Sheet (Dateinamen-Erweiterung)
ZKA	Zentraler Kreditausschuss
ZÜV	Zahlungsüberwachungsverfahren
ZVP	Zahlungsverkehrsplattform

Informationen zum Modul

Status	Beitrag von ibi research an der Universität Regensburg GmbH Schloss Thurn und Taxis Emmeramsplatz 5 93047 Regensburg Telefon +49 (0)9 41 9 43 – 19 01 Telefax +49 (0)9 41 9 43 – 18 88 http://www.ibi.de/ info@ibi.de
Autoren	Markus Breitschaft, Thomas Krabichler, Dr. Ernst Stahl, Georg Wittmann (alle ibi research)
Ansprechpartner/Kontakt	Dr. Timo Hauschild (BSI), egov@bsi.bund.de

Änderungsverzeichnis

Datum	Name	Änderung
10.05.2005	ibi research	Aktualisierung und Ergänzung
18.02.2005	Herbolsheimer	Geringfügige Korrekturen
28.06.2004	Hauschild	Geringfügige Korrekturen
23.04.2004	Hauschild	erste Version

0 Management Summary

Viele Dienstleistungen, die den Kunden der öffentlichen Verwaltung angeboten werden, sind gebührenpflichtig. Werden diese Leistungen im Rahmen von E-Government im Internet zur Verfügung gestellt, so muss auch über die Zahlungsabwicklung und damit über die Bereitstellung geeigneter Zahlungsverfahren nachgedacht werden. Im Rahmen der Zahlungsabwicklung kommt der Sicherheit dabei eine besondere Bedeutung zu, da bei mangelnder Sicherheit sehr schnell das Vertrauen in die Verfahren und damit auch die Akzeptanz von E-Government verloren gehen kann.

Um über die Geldarten Bargeld, Buchgeld und E-Geld verfügen zu können, stehen grundsätzlich drei (originäre) Zahlungsverfahren zur Verfügung: Geldbörsenzahlung, Überweisung und Lastschrift. Aus diesen originären Zahlungsverfahren lassen sich weitere Verfahren ableiten, die insbesondere den neuen technischen Entwicklungen Folge leisten.

Zur Bestimmung geeigneter Zahlungsverfahren für Dienstleistungen der öffentlichen Verwaltung werden repräsentative Zahlungsverfahren in dem vorliegenden Modul ausführlich beschrieben und bewertet. Die wesentlichen Merkmale von Zahlungsverfahren wurden in Tabellen und Diagrammen zusammengefasst und geben somit in kurzer Form einen Überblick über wesentliche Ergebnisse.

Bei der Auswahl geeigneter Zahlungsverfahren für E-Government-Dienstleistungen hat die Integration in die Systemlandschaft der Behörde einen besonderen Stellenwert, da mit Zahlungen an die öffentliche Verwaltung weitere innerbehördliche Prozesse verbunden sind, wie etwa die Initiierung der Leistungserstellung bzw. der Auslieferung oder die Verbuchung von Zahlungen, die in den IT-Systemen der Behörde abgebildet werden müssen. Eine Schnittstelle zu diesen Systemen und die Interoperabilität müssen gegeben sein.

Bei der Auswahl von Zahlungsverfahren sind die gestellten Anforderungen (fachspezifische Anforderungen, Betragsbereich und Kostenstruktur, Sicherheitsanforderungen, Integrierbarkeit in den E-Governement-Prozess) zu berücksichtigen.. Die Tabellen und Diagramme in diesem Modul geben dabei eine Hilfestellung. Grundsätzlich wäre hier aus Sicht der Behörde ein Zahlungsverfahren wünschenswert, das bei den Kunden weit verbreitet ist und gleichzeitig eine hohe Zahlungsgarantie sowie eine optimale Integration in die Prozesse der Behörde bietet. Jedoch erfüllt keines der heute verfügbaren Verfahren alle drei Anforderungen gleichzeitig.

Bei der (klassischen) Kreditkartenzahlung beispielsweise liegt dies im Wesentlichen an der fehlenden Unterschrift, also der rechtsverbindlichen Willenserklärung. Die Erfüllung aller drei Anforderungen wäre jedoch möglich, wenn die handschriftliche Unterschrift auf einem Zahlungsbeleg im Internet durch eine qualifizierte elektronische Signatur ersetzt würde. Durch Bankkarten, die bald über eine (qualifizierte) Signaturfunktionalität verfügen sollen, wird es somit zukünftig möglich sein, im Internet sichere und garantierte Zahlungen abzuwickeln. Für die Behörden hat ein solches signaturbasiertes Zahlungsverfahren neben der sofortigen Zahlungsgarantie den Vorteil, dass die (qualifizierte) elektronische Signatur für die Gestaltung durchgängiger E-Government-Dienstleistungen häufig ohnehin benötigt wird.

Ob es in Zukunft ein Zahlungsverfahren geben wird, das die notwendigen Sicherheitsanforderungen aus Behörden- und Kundensicht optimal erfüllt, hängt im Wesentlichen davon ab, ob die (qualifizierte) elektronische Signatur eine ausreichende Verbreitung erlangen wird. Der Weg, den die Bundesregierung mit der Gründung des Signaturbündnisses eingeschlagen hat, weist diesbezüglich in die richtige Richtung.

1 Einführung

Immer mehr Dienstleistungen der öffentlichen Verwaltung können von Bürgern und Unternehmen im Internet genutzt werden. So sollen im Rahmen der E-Government-Initiative BundOnline 2005[1] bis zum Jahr 2005 rund 440 internetfähige Dienstleistungen der Bundesverwaltung für private und gewerbliche Nutzer online verfügbar gemacht werden. Informationen zu den bereits umgesetzten Dienstleistungen sind im Fortschrittsanzeiger[2] der Initiative BundOnline 2005 zu finden

Zahlungen an Behörden

Viele dieser Leistungen sind gebührenpflichtig. Um die Effizienzsteigerungen, die allgemein durch E-Government erwartet werden, auch realisieren zu können, sind geeignete Verfahren zur Erhebung bzw. Weiterverarbeitung der anfallenden Gebühren erforderlich. Im Gegensatz dazu sind für Zahlungen von der öffentlichen Verwaltung an die Bürger und Unternehmen bereits etablierte Verfahren, wie Scheck oder Überweisung, im Einsatz. Diese werden deshalb nicht weiter betrachtet.

Sicherheit im Zahlungsverkehr: Grundvoraussetzung für erfolgreiches E-Government

Eine herausragende Bedeutung kommt bei Zahlungen an die öffentliche Verwaltung dem Sicherheitsaspekt zu, da die Sicherheit als zentrales Akzeptanzproblem von Zahlungsverfahren gilt. Sowohl Bürger als auch Unternehmen befürchten bei der Nutzung von Zahlungsverfahren im Internet, dass Zahlungen manipuliert und umgeleitet oder von Dritten Leistungen auf Kosten des Kunden bezogen werden könnten. Neben den Geldbeständen der Nutzer sind zudem auch deren persönlichen Daten zu schützen.[3] Aus Sicht der Behörde muss das Zahlungsverfahren in erster Linie einen ausreichenden Schutz vor Zahlungsausfällen bieten. Die unterschiedlichen Sicherheitsanforderungen stellen einen entscheidenden Faktor dar, um die breite Akzeptanz von Zahlungsverfahren im Internet zu fördern und somit auch die Nutzenvorteile des E-Government tatsächlich realisieren zu können.

Weitere Anforderungen an geeignete Zahlungsverfahren

Neben den erwähnten Sicherheitsvoraussetzungen sind bei der Auswahl eines geeigneten Zahlungsverfahrens jedoch weitere Anforderungen zu berücksichtigen. Für viele Anwendungen ist es notwendig, ein Verfahren zu wählen, das weit verbreitet und evtl. auch aus dem Ausland nutzbar ist. Daneben soll das Bezahlverfahren möglichst einfach und schnell in die bestehenden Prozesse der öffentlichen Verwaltung integriert werden können. Ebenso muss darauf geachtet werden, die Kosten des laufenden Betriebs möglichst gering zu halten. Da diese Kriterien vielfach gegenläufig wirken, ist zwischen der Bedeutung der einzelnen Kriterien für den jeweiligen Anwendungsfall abzuwägen.

Markt für Zahlungsverfahren ist unübersichtlich

Erschwert wird die Wahl des Zahlungsverfahrens durch die große Anzahl möglicher Verfahren, deren grundsätzliche Unterschiede auf den ersten Blick nur schwer ersichtlich sind. Hinzu kommt die hohe Dynamik des Marktes für Zah-

---

1 Weitere Informationen unter http://www.BundOnline2005.de/.

2 Weitere Informationen unter: http://www.bund.de/nn_532/Content/BundOnline-2005/Fortschrittsanzeiger/Fortschrittsanzeiger-knoten.html.

3 Zum Datenmissbrauch bei Zahlungen im E-Government vergleiche das Modul „Datenschutzgerechtes E-Government“, insbesondere die Ausführung im Abschnitt 4.7.6.

lungssysteme, auf dem ständig neue Zahlungsverfahren angeboten werden, andere nach kurzer Marktpräsenz wieder verschwinden. Die Wahl eines geeigneten Zahlungsverfahrens stellt somit keine leicht zu lösende Aufgabe dar und muss situationsabhängig getroffen werden.

Kein universelles Zahlungsverfahren für E-Government

Dem mehrdimensionalen Entscheidungsproblem, welches Zahlungsverfahren sich für welche Situation (im Folgenden Szenario genannt) am besten eignet, soll im Rahmen dieses Moduls begegnet werden. Als Ergebnis kann dabei kein universelles Zahlungsverfahren für E-Government präsentiert werden. Vielmehr soll Entscheidern in der öffentlichen Verwaltung aufgezeigt werden, welche Kriterien bei der Wahl eines Zahlungsverfahrens zu berücksichtigen sind und wie anhand dieser Kriterien die für ein konkretes Szenario am besten geeigneten Zahlungsverfahren ermittelt werden können.

Vorgehen innerhalb dieses Moduls

Dazu wird im Abschnitt 2 ein Überblick über derzeit am Markt existierende Zahlungsverfahren gegeben. Abschnitt 3 lenkt den Blick auf das zu lösende Entscheidungsproblem und stellt verschiedene Kategorisierungsmöglichkeiten für Online-Transaktionen vor, die für die Auswahl eines Zahlungsverfahrens von Bedeutung sind. Anschließend werden sechs Beispielszenarien beschrieben, die unterschiedliche Kombinationen der genannten Kategorisierungsmöglichkeiten darstellen. Abschnitt 4 beschäftigt sich mit der Integration des Zahlungsverfahrens in die Systemumgebung einer Behörde.

In Abschnitt 5 wird, aufbauend auf den vorangegangenen Abschnitten, ein Kriterienkatalog vorgestellt, der die Grundlage für die Auswahl eines geeigneten Zahlungsverfahrens bildet. Dafür werden zunächst ausgewählte Zahlungsverfahren aus Abschnitt 2 näher erläutert und anschließend mit Hilfe des Kriterienkatalogs bewertet (Abschnitt 6). In Abschnitt 7 wird daraufhin ein Verfahren vorgestellt, mit Hilfe dessen unter Berücksichtigung der Beziehungen zwischen den Anforderungen die für ein Szenario am besten geeigneten Zahlungsverfahren bestimmt werden können. Dieses Verfahren wird anhand der in Abschnitt 3 beschriebenen Beispielszenarien exemplarisch durchgeführt. Das Modul schließt mit einer Zusammenfassung der wesentlichen Ergebnisse und einem Ausblick auf mögliche zukünftige Entwicklungen in Abschnitt 8.

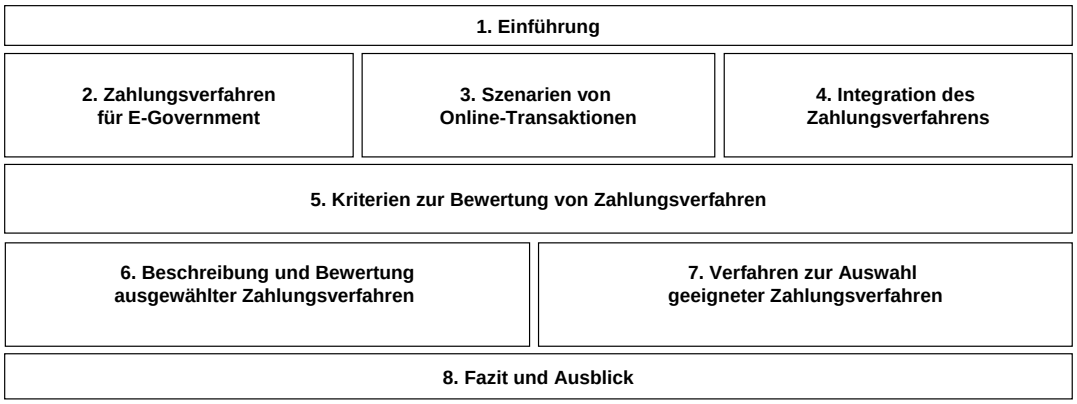


Abbildung 1: Aufbau des Moduls „Sichere Zahlungsverfahren für E-Government“

2 Zahlungsverfahren für E-Government

Bedeutung von Zahlungsverfahren

Die Zahl der verfügbaren Zahlungsverfahren hat sich mit der zunehmenden Bedeutung des Internets für Handelstransaktionen[4] in den vergangenen Jahren vervielfacht. Die meisten der neuen Zahlungsverfahren bauen dabei auf den etablierten Zahlungsverfahren auf oder stellen für den Einsatz über elektronische Medien modifizierte Ausprägungen der etablierten Verfahren dar. Dieser Tatsache soll durch nachfolgende Kategorisierung der Verfahren Rechnung getragen werden.

Internet als Synonym elektronischer Kommunikation

Im Gegensatz zum weiteren Vorgehen in diesem Modul betrachtet dieser Abschnitt sowohl existierende und zukünftig mögliche Verfahren, die in der Behörde vor Ort einsetzbar sind[5], als auch solche, die sich für die Verwendung über elektronische Kanäle eignen. In den darauf folgenden Abschnitten werden dagegen nur noch Zahlungsverfahren für Online-Transaktionen betrachtet, die über ein stationäres oder mobiles Endgerät des Kunden abgewickelt werden. Dabei wird nicht zwischen verschiedenen Endgeräten (wie Mobiltelefon, PDA) unterschieden, sondern stellvertretend für alle Formen elektronischer Kommunikation der Begriff Internet verwendet.

Probleme bestehender Kategorisierungen von Zahlungsverfahren

Aufgrund der hohen Anzahl verfügbarer Zahlungsverfahren stellt sich die Frage, wie diese für einen Überblick sinnvoll klassifiziert werden können. Häufig werden z. B. „pay before“, „pay now“, „pay later“, kontogebundene und kontoungebundene Verfahren oder Online- und Offline-Verfahren verwendet. Beispielsweise stellen die Begriffe „pay before“, „pay now“ und „pay later“ auf den Zahlungszeitpunkt ab: „pay before“ bedeutet Zahlung vor dem Lieferzeitpunkt, „pay now“ Zahlung zum Lieferzeitpunkt und „pay later“ Zahlung nach dem Lieferzeitpunkt. Eine eindeutige Zuordnung ist nach dieser Systematisierung jedoch nicht für jedes Zahlungsverfahren möglich. Zudem ist für den Zahlungsempfänger in erster Linie die Zahlungsgarantie und erst in zweiter Linie der Zahlungszeitpunkt von Bedeutung.

So kann eine über ein Mobiltelefon initiierte Zahlung mit einer sofortigen Zahlungsgarantie für den Händler verbunden sein, womit sie als „pay now“ einzustufen wäre. Wird sie dem Kunden über die abgerechneten Telefoneinheiten in Rechnung gestellt, so kann dies einerseits über die monatliche Telefonrechnung geschehen, was gleichzeitig für eine Einstufung als „pay later“, also nach der Transaktion, sprechen würde. Es könnte sich andererseits jedoch auch um eine Prepaid-Karte handeln, das Verfahren wäre dann der Kategorie „pay before“ zuzuordnen. Ähnlich stellt sich das Problem bei der GeldKarte, die sowohl als kontogebundene als auch als kontoungebundene Variante angeboten wird und am Point of Sale sowie im Internet einsetzbar ist.

---

4 Der Hauptverband des Deutschen Einzelhandels erwartet für 2005 Online-Umsätze in Höhe von 14,5 Milliarden Euro [HDE 2005].

5 Im Zahlungsverkehr hat sich für den physischen Ort, an dem der Zahlungsvorgang durchgeführt wird, der Begriff „Point of Sale“ (POS) eingebürgert und beschreibt somit den Abwicklungspunkt der Kaufs- bzw. Verkaufstransaktion.

Kategorisierung von Zahlungsverfahren nach Wahrnehmung aus Nutzersicht

Für den folgenden Überblick wurde eine Kategorisierung gewählt, die aus Nutzersicht weitgehend ähnliche Verfahren zusammenfasst, unabhängig davon, ob es sich um Zahlungsverfahren am Point of Sale oder im Internet handelt. Für einen schnellen Überblick über die verschiedenen Verfahren ist diese Kategorisierung sehr gut geeignet. Ausgehend von den originären Verfahren in Abschnitt 2.1 stellen sich die Eigenschaften abgeleiteter Verfahren in Abschnitt 2.2 deutlich weniger komplex dar. Die Einordnung der Kategorien in die beiden Klassen zeigt Abbildung 2.

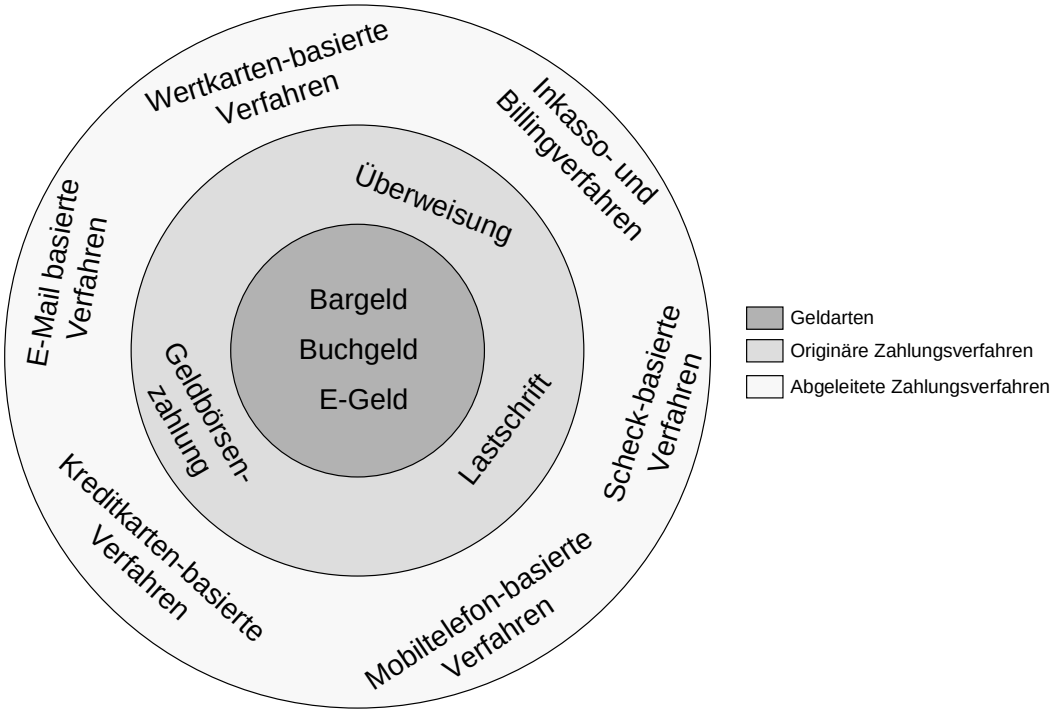


Abbildung 2: Kategorisierung von Bezahlverfahren

Formen von Geld

Im Zentrum von Abbildung 2 befinden sich das Bargeld, d. h. Banknoten und Münzen, das Buchgeld, d. h. Beträge auf Konten bei Kreditinstituten, die für Zahlungszwecke zur Verfügung stehen, und das E-Geld. E-Geld bezeichnet einen monetären Wert in Form einer Forderung gegen die ausgebende Stelle, der auf einem Datenträger gespeichert ist und von anderen Unternehmen als der ausgebenden Stelle als Zahlungsmittel akzeptiert wird. Gemäß der EU-Richtlinie 2000/46/EG darf E-Geld von Kreditinstituten und speziellen E-Geld-Instituten ausgegeben werden.

Verfügungsmöglichkeiten über Geld

Um über diese drei Formen des Geldes verfügen zu können, gibt es wiederum drei originäre Zahlungsverfahren, die sich in der Abbildung um das Zentrum des Kreises anordnen: Geldbörsenzahlung, Überweisung und Lastschrift. Diese drei Verfahren und ihre für den Einsatz im Internet modifizierten Ausprägungen werden in Abschnitt 2.1 behandelt. Die Zahlungsverfahren im äußersten Ring, die Gegenstand von Abschnitt 2.2 sind, greifen bei der Zahlungsabwicklung letzten Endes auf eines der originären Zahlungsverfahren zurück.

2.1 Originäre Zahlungsverfahren

Gemäß der im vorhergehenden Abschnitt vorgestellten Systematisierung stellen Überweisung, Lastschrift und Geldbörsenzahlung drei grundlegende Möglichkeiten dar, um über Bargeld, Buchgeld und E-Geld zu verfügen. Im Rahmen einer Überweisung oder Lastschrift werden die Werteinheiten (der Geldbetrag) in Form von Buchgeld, im Rahmen einer Geldbörsenzahlung in Form von Bargeld oder E-Geld übertragen. Die originären Zahlungsverfahren werden im Folgenden – beginnend mit der Geldbörsenzahlung – näher erläutert.

2.1.1 Geldbörsenzahlung

Geldbörsen

Als „Geldbörsen“ werden Speicherorte für Geldeinheiten bezeichnet, unabhängig davon, ob es sich dabei um physische Geldeinheiten (Banknoten und Münzen, also Bargeld) oder elektronische Geldeinheiten handelt. In Bezug auf physische Geldeinheiten ist dieser Speicherort das Portemonnaie oder die Kasse. Das dazugehörige Zahlungsverfahren ist die Barzahlung, z. B. an der Kasse einer Behörde. Hier erfolgt die Bezahlung eines Gutes oder einer Dienstleistung durch Überreichen der physischen Geldeinheiten in Form von Münzen oder Banknoten.

Elektronische Geldbörsen

Bei elektronischen Geldbörsen handelt es sich um Chipkarten, auf die Geldbeträge (E-Geld) geladen und bei einem Händler zur Bezahlung von Gütern und Dienstleistungen wieder abgebucht werden. Hier zeigt sich die Analogie zum Portemonnaie, das mit Banknoten und Münzen gefüllt und sukzessive beim Bezahlen wieder geleert wird. Das in Deutschland derzeit am weitesten verbreitete Geldbörsensystem ist die GeldKarte, die zurzeit primär am Point of Sale der teilnehmenden Händler (Akzeptanzstellen) einsetzbar ist. Mit einem Kartenlesegerät kann sie jedoch auch im Internet verwendet werden. Im europäischen Wirtschaftsraum haben sich darüber hinaus weitere Geldbörsensysteme wie z. B. Danmønt (Dänemark), Quick (Österreich), Visa-Cash (Spanien) und Proton (Belgien) etabliert.

Scheitern der Umsetzung elektronischer Münzen ohne sicheres Speichermedium

Es wurde in der Vergangenheit auch versucht, das Prinzip der Geldbörse unabhängig von der Chipkarte umzusetzen. Beispiele für solche Verfahren sind eCash und DigiCash[6]. Diese scheiterten jedoch aufgrund fehlender Marktakzeptanz, als deren Ursachen häufig die hohe Komplexität der Systeme sowie hohe Einrichtungs- und Betriebskosten auf Bank- und Händlerseite genannt werden.

2.1.2 Überweisung

Überweisung

Eine Überweisung ist die Übertragung eines Geldbetrages (Buchgeld) vom Konto des Zahlungspflichtigen auf das Konto des Zahlungsempfängers, die durch einen Auftrag des Zahlungspflichtigen ausgelöst wird. Dieser Auftrag kann sich entweder auf die einmalige Durchführung einer Überweisung (Einzelüberweisung) oder

---

6 Bei eCash handelt es sich um von der Deutschen Bank in Zusammenarbeit mit der Firma DigiCash herausgegebene elektronische Münzeinheiten, die zur Bezahlung bei (Internet-) Händlern eingesetzt werden konnten.

auf die regelmäßig wiederkehrende Durchführung von Überweisungen mit dem gleichen Betrag und an denselben Empfänger (Dauerauftrag) beziehen.

Möglichkeiten der Auftragserteilung

Die Auftragserteilung kann durch Abgabe eines beleghaften Überweisungsvordrucks (z. B. in der Filiale), in elektronischer Form (z. B. über Internet, durch Benutzung eines Selbstbedienungs-Terminals der Bank oder durch Austausch von Disketten) oder durch telefonische Anweisung (Telefon-Banking) erfolgen. Insbesondere der Zugangskanal Internet findet seit geraumer Zeit zunehmende Akzeptanz und Verbreitung.[7] Zur Absicherung dieser Online-Transaktionen werden durch die Kreditwirtschaft derzeit das HBCI[8]-Verfahren und das PIN/TAN[9]-Verfahren angeboten.

Online-Überweisung im Rahmen von Internet-Einkäufen

Die Möglichkeit der Auftragserteilung im Internet wird zunehmend auch für Zahlungen im Internet genutzt. Wenn der Kunde nach Abschluss der Bestellung in einem Online-Shop[10] das entsprechende Zahlverfahren wählt, wird der Kunde auf die Internet-Banking-Umgebung seiner kontoführenden Bank umgeleitet. Der Kunde loggt sich dort mit Hilfe seines Benutzernamens (z. B. Konto- oder Kundennummer) und seiner PIN in den geschützten Bereich ein. Dort wird ihm ein bereits mit den Zahlungsdaten vorausgefüllter Überweisungsauftrag bereitgestellt, der noch mit einer TAN zu bestätigen ist. Das Kreditinstitut leitet daraufhin die Auftragsbestätigung sowohl an den Händler als auch an den Kunden weiter. Voraussetzung für dieses Verfahren ist, dass der Kunde über ein online geführtes Konto verfügt, der Händler eine entsprechende Vereinbarung mit der Bank des Kunden getroffen hat und die technische Schnittstelle zum Internet-Banking der Bank des Kunden implementiert. Ein solches Verfahren bietet in Deutschland derzeit beispielsweise die Postbank an.

Übernahme von Mittlerrollen bei Online-Überweisungen

Damit der Händler nicht mit allen in Frage kommenden Banken Einzelvereinbarungen schließen beziehungsweise in seinen IT-Systemen nicht alle technischen Internet-Banking-Schnittstellen zu den Banken seiner Kunden integrieren muss, haben sich spezielle Dienstleister herausgebildet, die für Händler diese Aufgabe übernehmen. Problematisch kann jedoch sein, dass Kunden – je nach technischer Realisierung der zentralen Schnittstelle – gegebenenfalls gegen die mit ihrer Hausbank getroffene Vereinbarung für das Online-Banking mit PIN und TAN verstoßen. So heißt es beispielsweise in den entsprechenden Vereinbarungen der Sparkassen: „Der Nutzer hat dafür Sorge zu tragen, dass keine andere Person Kenntnis von der PIN und den TAN erlangt.“

---

7 Nach Angaben des Bundesverbands deutscher Banken wurden Ende 2002 in Deutschland fast 30 Millionen Konten online geführt [BdB 2003].

8 Bei HBCI (Home Banking Computer Interface) handelt es sich um eine Spezifikation, welche die Schnittstelle zwischen Kundenprodukt und Kreditinstitutssystem beschreibt. Siehe auch http://www.hbci.de/.

9 Eine PIN (persönliche Identifikationsnummer) ist notwendig, um Zugang zu einem geschützten System/Funktionalität zu erlangen. Eine TAN (Transaktionsnummer) dient zur Bestätigung eines Vorgangs, z.B. eines Überweisungsauftrags.

10 Der Begriff Online-Shop wird im Folgenden synonym zu den Begriffen E-Shop, Web-Shop, Internet-Shop, Online-Mall etc. verwendet. Nähere Ausführungen finden sich im Modul „Leitfaden für die Einrichtung einer Internetvertriebsplattform (E-Shop)“.

Landesweiter Standard für Online-Überweisungen in Österreich

In Österreich wurde unter dem Namen „e-payment standard“ (eps)[11] ein Standard für Online-Bezahlvorgänge verabschiedet, der von allen großen österreichischen Banken unterstützt wird. Der eps ist eine normierte technische Schnittstelle zwischen Händler und Bank. Das Verfahren ähnelt der oben vorgestellten Online-Überweisung, die Banken geben jedoch bereits bei Entgegennahme des Auftrags eine Zahlungsgarantie gegenüber den Händlern bzw. Behörden ab.

2.1.3 Lastschrift

Formen der Auftragserteilung

Eine Lastschrift ist der Einzug eines Geldbetrages vom Konto des Zahlungspflichtigen, der durch den Zahlungsempfänger ausgelöst wird. Voraussetzung ist jedoch, dass entweder dem Zahlungsempfänger oder der Bank des Zahlungspflichtigen eine schriftliche Einwilligung des Zahlungspflichtigen vorliegt. Im täglichen Geschäftsverkehr wird diese Einwilligung üblicherweise gegenüber dem Zahlungsempfänger abgegeben, diese Form der Lastschrift wird dann als Einzugsermächtigungs-Lastschrift bezeichnet. Im Gegensatz zur zweiten Möglichkeit, der Abbuchungsauftrags-Lastschrift, kann diese ohne Angabe von Gründen zurückgegeben werden.

electronic cash

Für den Einsatz der Lastschrift am Point of Sale wurden von der deutschen Kreditwirtschaft drei Verfahren entwickelt, die durch die Magnetstreifen und ggf. Chips der ausgegebenen Bankkundenkarten unterstützt werden. Beim „electronic cash“-Verfahren wird die Zahlung durch Eingabe der kartenindividuellen Geheimzahl (PIN) legitimiert. Die benötigten Daten werden vom Kartenterminal aus dem Magnetstreifen ausgelesen. Das Kartenterminal baut eine Verbindung zu bankseitigen Systemen auf, bei denen die PIN, vorliegende Sperren und die Kontodeckung des Zahlungspflichtigen überprüft werden. Sobald das Terminal eine positive Rückmeldung erhält, ist die Zahlung durch das Kreditinstitut des Zahlungspflichtigen garantiert.

electronic cash chip

Um nicht bei jedem Zahlungsvorgang eine gebührenpflichtige Verbindung und Autorisierung durchführen zu müssen, wird beim „electronic cash chip“-Verfahren ein vorautorisiertes Limit (z. B. 500 Euro) im Chip gespeichert. Im Rahmen des Zahlungsvorgangs wird geprüft, ob das Limit auf dem Chip zur Zahlung ausreicht. Die Zahlung wird ebenfalls wie beim ursprünglichen electronic-cash-Verfahren durch Eingabe der Karten-PIN legitimiert, wobei die PIN offline durch den Kartenchip geprüft wird. Im positiven Fall – das Limit reicht aus und die PIN ist korrekt – wird die Transaktion ohne zusätzlichen Verbindungsaufbau zur Bank autorisiert und das Limit um den Zahlungsbetrag reduziert. Sollte das Limit durch die Zahlung überschritten werden, so erfolgt die Prüfung wie beim electronic-cash-Verfahren und das Limit wird wieder heraufgesetzt. Je nach Ausgestaltung des Systems wird z.B. zufalls- oder zeitabhängig eine über die Betragsautorisierung hinausgehende Online-Verbindung aufgebaut. Eine autorisierte Zahlung ist jedoch in jedem Falle garantiert.

---

[11] eps wurde von der bankenübergreifenden Studiengesellschaft für Zusammenarbeit im Zahlungsverkehr (STUZZA) gemeinsam mit den österreichischen Banken erarbeitet. Weitere Informationen unter http://www.stuzza.at/.

POZ

Beim POZ-Verfahren[12] (Point of Sale ohne Zahlungsgarantie) werden die zur Erzeugung einer Lastschrift notwendigen Daten vom Kartenterminal aus dem Magnetstreifen der Bankkundenkarte des Zahlungspflichtigen ausgelesen und auf einer Einzugsermächtigung ausgedruckt, welche der Zahlungspflichtige unterschreibt. Ab einem bestimmten Rechnungsbetrag (üblicherweise 30,68 Euro) muss das Handels- oder Dienstleistungsunternehmen eine Kartensperr-Datei der Kreditwirtschaft abfragen. Eine Zahlungsgarantie wird bei diesem Verfahren nicht abgegeben, der Zahlungspflichtige kann die Lastschrift ohne Angabe von Gründen zurückgeben. Das POZ-Verfahren wurde zum 01.01.2007 durch die Kreditwirtschaft aufgekündigt [ZKA 2004] und wird ab diesem Zeitpunkt nicht mehr unterstützt.

Wildes POS-Verfahren; ELV

Neben diesen von der Kreditwirtschaft herausgegebenen Verfahren hat sich in der Praxis eine vierte Variante der elektronischen Lastschrift herausgebildet, die meist nur als elektronisches Lastschriftverfahren (ELV oder auch „Wildes POS-Verfahren“) bezeichnet wird. Beim ELV werden die Daten zur Lastschriftgenerierung ebenfalls aus dem Magnetstreifen der Bankkundenkarte ausgelesen und elektronisch weiterverarbeitet. Im Gegensatz zu POZ besteht jedoch keine Verpflichtung, eine Liste der gesperrten Karten bei der Bank abzufragen, wodurch die Auskunftsgebühren nicht mehr anfallen. Häufig werden jedoch von großen Handelsketten oder Zahlungsverkehrs-Dienstleistern eigene Sperrlisten aufgebaut. Das elektronische Lastschriftverfahren fußt nicht auf von der Kreditwirtschaft getragenen Vereinbarungen. Während bei POZ die Bank beispielsweise verpflichtet ist, im Falle eines nachträglichen Zahlungswiderspruchs und einer Rückgabe der Belastung durch den Karteninhaber, an den Händler Name und Anschrift des Karteninhabers herauszugeben, ist das Kreditinstitut zur Weitergabe von Name und Anschrift nicht in jedem Falle verpflichtet [Werner 2003, S. 758 ff.].

Rechtskonformität von Lastschriften über das Internet

Auch im Internet stellt die Lastschrift eines der am weitesten verbreiteten Zahlungsverfahren dar. In den meisten Fällen wird dabei nur die Kontonummer und Bankleitzahl des Zahlungspflichtigen an den Händler übertragen, häufig sogar unverschlüsselt. Diese gängige Praxis verstößt damit gegen das Lastschriftabkommen und die Vereinbarungen der Händler mit deren Hausbank, nach der eine schriftliche Einzugsermächtigung des Kunden vorliegen muss.[13] Um die Lastschrift rechtskonform im Internet einsetzen zu können, müsste der Kunde eine Einzugsermächtigung ausdrucken, unterschreiben und auf dem Postweg zum Zahlungsempfänger senden oder ein entsprechendes elektronisches Dokument mit einer qualifizierten elektronischen Unterschrift versehen.

electronic direct debit

Das „electronic direct debit“-Verfahren (edd), das von verschiedenen Banken angeboten wurde, bot eine solche elektronische Einzugsermächtigung, die vom Kunden mit einer elektronischen Signatur versehen wurde. Ein zusätzlicher Vorteil dieses Systems war, dass der Händler die Kontoverbindung und die Bank die

---

12 Rechtsgrundlage hierfür bildet die Vereinbarung zum POZ-System, die zwischen den Spitzenverbänden der Kreditwirtschaft abgeschlossen worden ist. Zu den Vertragswerken für das POZ-System gehören neben der Vereinbarung zum POZ-System die Bedingungen für Ec-Karten, der Konzentratorvertrag, die Händlerbedingungen und die Vereinbarung über die Teilnahme am POZ-System, die zwischen Unternehmer und Netzbetreiber abzuschließen ist. [Werner 2003, S. 773]

13 Vgl. Abschnitt 6.1.1 des Moduls „Rechtliche Rahmenbedingungen für E-Government“.

bezahlten Leistungen nicht sehen konnte. Das Verfahren wurde mittlerweile jedoch wieder eingestellt.

2.2 Abgeleitete Zahlungsverfahren

Abgeleitete Zahlungsverfahren greifen zur Wertübertragung auf originäre Verfahren zurück. Nachfolgend werden die verschiedenen Kategorien abgeleiteter Verfahren mit einigen beispielhaften Ausprägungen näher vorgestellt. Eine Auswahl weiterer abgeleiteter Zahlungsverfahren ist in Anhang A.12 aufgelistet.

2.2.1 Scheck-basierte Verfahren

Scheck

Scheck-basierte Verfahren verbriefen eine Anweisung an das Kreditinstitut des Zahlungspflichtigen, die im Scheck genannte Geldsumme zu Lasten von dessen Konto zu zahlen. Die Zahlungsanweisung wird sofort bei Übergabe des Dokuments fällig. Der Scheck ist eine Urkunde und an die Papierform mit vorgegebenen Inhalten gebunden. Aus Sicherheitsgründen haben die Kreditinstitute Vordrucke entwickelt, zu deren ausschließlicher Annahme sie sich verpflichtet haben.

Barscheck und Verrechnungsscheck

Barschecks werden bei Vorlage bar an den Einreicher ausbezahlt. Die Zahlung erfolgt auch an Nichtkontoinhaber. Bei Verlust der Urkunde besteht das Risiko, dass die Zahlung an Unberechtigte vorgenommen wird. Trägt die Scheckurkunde den Vermerk „Nur zur Verrechnung“, so darf das Kreditinstitut den Betrag dagegen nur im Wege der Gutschrift einlösen.

eurocheque

Sowohl im Inland als auch im Ausland kam dem garantierten eurocheque lange Zeit eine hohe Bedeutung zu. Die am eurocheque-System teilnehmenden Banken verpflichteten sich, formgerecht ausgestellte Euroschecks bis zu einem bestimmten Geldbetrag einzulösen. Die Garantie wurde in Verbindung mit einer Euroscheckkarte (Ec-Karte) gegeben, deren Kartennummer der Aussteller auf der Rückseite des Schecks vermerkte. Der Empfänger des eurocheques musste die Übereinstimmung der Unterschrift auf dem eurocheque mit der Unterschrift auf der zugehörigen Karte prüfen. Am 1. Januar 2002 wurde die Einlösungsgarantie für eurocheques aufgehoben. Die Funktion des eurocheques wird seitdem vom weltweiten Netz an Geldautomaten und der internationalen Variante des electronic-cash-Verfahrens, Maestro, übernommen.

Mit NetCheque gab es bereits einen Versuch, das vom Verrechnungsscheck bekannte Prinzip auf das Internet zu übertragen. Es kam jedoch zu keiner nennenswerten Marktverbreitung. Das System wurde bereits 1995 wieder eingestellt.

2.2.2 Kreditkarten-basierte Verfahren

Kreditkarten-basierte Verfahren

Kreditkarten dienen der Bargeldbeschaffung am Bankschalter oder am Geldautomaten sowie der bargeldlosen Bezahlung von Waren und Dienstleistungen bei Vertragsunternehmen der kartenherausgebenden Organisationen. Sie ermöglichen darüber hinaus häufig eine (kurzfristige) Inanspruchnahme von Krediten. Die Kreditkarte wurde ursprünglich für den Einsatz am Point of Sale konzipiert. Die zur Zahlungsabwicklung erforderlichen Daten werden heute üblicherweise aus

dem Magnetstreifen ausgelesen, sind jedoch auch auf der Karte abgedruckt. Ähnlich wie beim electronic-cash-Verfahren muss für die Erlangung einer Zahlungsgarantie eine Verbindung zur Autorisierungsstelle der Kreditkartengesellschaft hergestellt und die Einhaltung des Verfügungsrahmens der Karte sowie das Vorliegen von Sperren überprüft werden.

Probleme beim Einsatz im Internet

Mit der wachsenden Anzahl von Online-Transaktionen werden Kreditkarten zunehmend auch im Internet eingesetzt. Dies ist möglich, da zur Abwicklung einer Transaktion ein Kreditkartenterminal nicht zwingend erforderlich ist. Es reicht auch die Übermittlung der zur Transaktion erforderlichen Daten aus. Diese wurden jedoch häufig ungeschützt über Internet-Verbindungen übertragen. Dritte konnten somit diese Daten relativ leicht abfangen und die Kreditkartennummern, z. B. für betrügerischen Einkauf, missbrauchen[14]. Es wurden jedoch bereits verschiedene Versuche unternommen, die Sicherheit des Systems vor allem beim Einsatz im Internet zu steigern.

SSL und SET zur Lösung der Probleme

Eine Lösung zur Absicherung der Datenübertragung über das Internet war der Einsatz von kryptographischen Techniken. Insbesondere „Secure Socket Layer“ (SSL) findet mittlerweile starke Verbreitung. Dies löst zwar das Problem, dass Daten ungeschützt über das Internet übertragen werden, jedoch kann der Kunde noch nicht eindeutig als Kreditkarteninhaber authentifiziert werden. Dem sollte „Secure Electronic Transaction“ (SET) entgegentreten. Aufgrund zu hoher Komplexität und enormen Installations- und Betriebsaufwands fand das System jedoch keine nennenswerte Akzeptanz und wurde zum größten Teil wieder eingestellt.

Einführung von Kartenprüfnummern

Als weiteres Sicherheitsmerkmal wurden so genannte Kartenprüfnummern (KPN) eingeführt – von Visa auch Card Verification Code (CVC) und Card Verification Code2 (CVC2), von MasterCard auch Card Verification Value (CVV) und Card Verification Value2 (CVV2) genannt. CVC2 und CVV2 sind für Bestellungen im Internet, per Telefon oder Postkarte gedacht und auf der Rückseite der Kreditkarte sichtbar aufgebracht.[15] Die Kartenprüfnummern für die Bezahlung vor Ort (CVC bzw. CVV) sind im Magnetstreifen hinterlegt. Anhand der Kartenprüfnummer lässt sich durch die Kartenherausgeber feststellen, ob die Karte tatsächlich existent ist oder ob die Kreditkartennummer beispielsweise von einem Computerprogramm zu Betrugszwecken errechnet wurde.

Verified by Visa und MasterCard SecureCode

Als weitere Initiative wird von den beiden weltweit größten Kreditkartengesellschaften – Visa und MasterCard – unter zwei unterschiedlichen Markennamen ein Verfahren eingeführt, das auf dem so genannten 3-D-Secure-Protokoll basiert. Diese werden in folgenden Varianten[16] angeboten:

Variante 1

Die erste Variante beruht auf einer PIN-basierten Authentifizierung. Der Karteninhaber meldet sich dazu einmalig bei seiner kartenherausgebenden Bank für die-

---

14 Aus missbräuchlichen Verfügungen im Internet, die allein auf Kenntnis der Kreditkartendaten beruhen, entsteht nach den geltenden Regelungen kein Haftungsrisiko für den Karteninhaber.

15 CVC2 und CVV2 sind dazu weder Bestandteil der Informationen auf dem Magnetstreifen, noch wird sie auf dem Zahlungsbeleg abgedruckt.

16 Derzeit wird Variante 2 nur von MasterCard angeboten (Stand: Mai 2005). Es ist jedoch zu erwarten, sobald Kreditkarten mit Chip eine stärkere Verbreitung finden, dass weitere Kreditkartenorganisationen diese Variante ebenfalls anbieten werden.

se Verfahrensvariante an. Anschließend erhält der Karteninhaber eine PIN zugeteilt, die er für Transaktionen über Internet einsetzen kann. Sofern ein Internet-Händler diese Variante unterstützt, muss der Kunde beim Bezahlvorgang (in einem Browser-Fenster) seine PIN angeben, welche online verifiziert wird. Im positiven Fall ist der Bezahlvorgang abgeschlossen und die Zahlung garantiert.

Variante 2

Die zweite Variante beruht auf einer Kreditkarte mit Chip (und zugehöriger PIN) und einem EMV[17]-fähigen Kartenleser. Der Käufer wird im Rahmen des Zahlungsvorgangs aufgefordert, seine EMV-Chipkarte in den Kartenleser einzuführen. Anschließend wird eine im Browser-Fenster angezeigte Zahl und der Betrag über die Tastatur des Lesegeräts eingegeben. Nach Eingabe der kartenindividuellen PIN wird im Display des Kartenlesers ein vom Kartenchip erzeugter Code angezeigt, den man in ein Browser-Feld übertragen und abschicken muss. Auch in diesem Falle ist die Zahlung garantiert.

2.2.3 Wertkarten-basierte Verfahren

Wertkarten-basierte Verfahren

Wertkarten-basierte Verfahren unterscheiden sich von elektronischen Geldbörsen dadurch, dass dieselbe Karte nicht wieder aufgeladen werden kann. Bei den Werteinheiten handelt es sich nicht um E-Geld. Zudem ist das Guthaben nicht notwendigerweise auf einem Chip gespeichert. Für den Erwerb der Wertkarte ist grundsätzlich jedes andere Zahlungsverfahren einsetzbar, häufig genutzte Verfahren sind z. B. Barzahlung oder Lastschrift. Beim Bezahlen muss der Kunde z. B. einen auf der Wertkarte aufgedruckten Code und ein zusätzliches Kennwort im Browser eingeben. Anschließend wird das Guthaben von Hintergrundsystemen geprüft und bei ausreichender Deckung um den Kaufpreis reduziert. Das System eignet sich sowohl für einen Einsatz am POS als auch für einen Einsatz im Internet. Es bietet darüber hinaus die Möglichkeit einer vollständig anonymen Zahlung.

Beispiele

Bekannte Beispiele für Wertkarten-basierte Verfahren sind die paysafecard und T-Pay MicroMoney. paysafecard bietet beispielsweise für Jugendliche die <18 paysafecard an, die für die Bezahlung von altersbeschränkten Inhalten im Internet gesperrt ist. Sowohl die paysafecard als auch die T-Pay MicroMoney-Karte können zusätzlich zum Bezahlen von Telefongesprächen eingesetzt werden.

2.2.4 E-Mail-basierte Verfahren

E-Mail-basierte Verfahren

E-Mail-basierte Verfahren nutzen E-Mail-Nachrichten zur Übertragung von Buchungsinformationen. Vom Anbieter des Verfahrens werden mit einer E-Mail-Adresse verknüpfte Referenzkonten geführt. Buchungen auf den Referenzkonten lösen jedoch keine direkten Geldbewegungen auf Bankkonten aus, nur bei Bedarf erfolgt die Umwandlung der Werteinheiten in Geld oder umgekehrt. Üblicherweise darf das Referenzkonto jedoch keinen negativen Saldo aufweisen, d. h. vor der ersten Nutzung muss das Referenzkonto geladen werden.

---

17 Europay/Mastercard/Visa (EMV); weitere Erläuterungen zu EMV in Abschnitt 2.3 bzw. unter http://www.emvco.com/.

Voraussetzungen für E-Mail-basierte Verfahren

Voraussetzung für das Senden oder Empfangen der Werteinheiten ist die Registrierung des Zahlungssenders und Zahlungsempfängers beim Dienstanbieter. Dieser setzt die Existenz eines E-Mail-Kontos, mit der das Referenzkonto verknüpft werden kann, voraus. Als Instrument zur Authentifizierung wird die E-Mail-Adresse in Verbindung mit einem geheimen Kennwort verwendet. Die Akzeptanzstellen (Sender und Empfänger) gehen mit dem Anbieter ein Vertragsverhältnis ein.

Beispiele

Zu den E-Mail-basierten Verfahren zählen z. B. Anypay, PayPal und moneybookers. Die auf den Referenzkonten verbuchten Beträge werden mittels originärer Verfahren (siehe Abschnitt 2.1) auf Bankkonten der Dienstleistungsanbieter übertragen. Diese verbriefen die Beträge anschließend in Form von Werteinheiten, die bei Akzeptanzstellen eingelöst werden können.

Die einzelnen Unternehmen unterscheiden sich jedoch in Breite und Funktionalität ihres Angebotes, in der Gestaltung der Zahlungsprozesse und in den Anforderungen an die Registrierung. Anypay beispielsweise überprüft im Rahmen der Kundenregistrierung die angegebenen Bank-, Kreditkarten- oder Mobiltelefondaten, indem es eine Testgutschrift auf das angegebene Konto veranlasst, bzw. eine Kurznachricht (SMS) an die angegebene Mobiltelefonnummer sendet. Mittels des in der Testgutschrift mitgeteilten Aktivierungscodes wird der Kunde authentifiziert und das Konto freigeschaltet. PayPal, ein US-amerikanischer Dienstleister, ist vorwiegend auf amerikanischem Gebiet verbreitet. Für US-Amerikaner genügt die Registrierung eines Bankkontos, für andere Interessenten ist die Angabe von Kreditkartendaten und eine Teilnahme am „Expanded User Program“ erforderlich, durch das man eine Nummer zur Freischaltung des PayPal-Kontos erhält. Moneybookers ist ein auf englischem Recht beruhendes Unternehmen, das durch die Finanz- und Kapitalmarktaufsicht des Vereinigten Königreichs[18] als Herausgeber von E-Geld lizenziert ist. Moneybookers ist somit berechtigt, auch auf dem deutschen Markt elektronisches Geld herauszugeben.[19] Die Verfahren eignen sich insbesondere für den Einsatz im Internet.

2.2.5 Mobiltelefon-basierte Verfahren

Mobiltelefon-basierte Verfahren

Mobiltelefon-basierte Verfahren nutzen das Mobiltelefon zur Übertragung von Buchungsinformationen. Das Mobiltelefon dient dabei gleichzeitig zur Authentifizierung. Vom Betreiber des Verfahrens wird ein Referenzkonto geführt, das in der Regel mit der Mobiltelefon-Nummer des Kunden verknüpft ist.

Beispiele

Derzeitige Anbieter von Mobiltelefon-basierten Verfahren sind unter anderem Vodafone m-pay, Handypay, allPay und Street Cash, die sich insbesondere in der Form des Zahlungsvorgangs unterscheiden. Unterschiedliche Varianten, wie etwa SMS, Spracheingabe oder Übermittlung von Zahlencodes durch das Tonwahlver-

---

18 Financial Services Authority (FSA), siehe auch http://www.fsa.gov.uk/ .

19 Grundlage hierfür ist die Konformität zur EU-Richtlinie 200/46/EG, die durch die FSA bestätigt wurde. Erst bei Vorliegen einer solchen Lizenz (oder einer Banklizenz) kann bei den Werteinheiten grundsätzlich von elektronischem Geld (E-Geld) gesprochen werden (siehe auch Abschnitt 2.1).

fahren, sind dabei im Einsatz. Beispielsweise wird bei Auswahl des Zahlungsverfahrens Vodafone m-pay, Handypay oder allPay in einem Web-Shop eine Kurznachricht mit einem Bezahlcode an die angegebene Mobilfunknummer versendet. Der Code ist nur für eine bestimmte Zeit gültig und muss zum Abschließen des Bezahlvorgangs im Browser-Fenster angegeben werden. Anschließend wird der Betrag vom Mobilfunkkonto abgebucht bzw. dort reserviert. Eine Registrierung der Kunden ist nicht notwendig, da die Anbieter dieser Verfahren mit Mobiltelefongesellschaften zusammenarbeiten. Bei StreetCash hingegen muss sich der Kunde zunächst registrieren. Die Abrechnung erfolgt in der Regel über das Giro- oder Kreditkartenkonto des Kunden.

2.2.6 Inkasso- und Billingverfahren

Inkasso- und Billingverfahren

Bei Inkasso- und Billingverfahren werden die Abrechnungsbeträge von einem Inkasso-Unternehmen eingezogen. Eine solche Inkassostelle kann z. B. ein Telekommunikationsunternehmen, aber auch ein spezialisierter Dienstleister sein. Neben dem Einzug der Forderung übernimmt die Inkassostelle bei einigen Verfahren auch die Zusammenfassung einzelner Rechnungs-/Zahlungsbeträge bis zu einem bestimmten Termin oder bis zur Erreichung eines Mindestbetrags (Billing). Bei der Begleichung der Beträge gegenüber der Inkassostelle erfolgt ein Rückgriff auf originäre Zahlungsverfahren (siehe Abschnitt 2.1).

Nachnahme

Bei der Nachnahme handelt es sich um ein Zahlungsverfahren, bei dem der Zustelldienst als Inkassostelle auftritt. Die Sendung wird im Gegenzug zur Begleichung der Schuld an den Empfänger ausgehändigt. Eine Begleichung ist mit unterschiedlichen Zahlungsverfahren möglich.

Dialer-/0190-Verfahren

Bei Dialer-Verfahren (z. B. net900 oder MoreCon) wird der Kunde auf eine speziell tarifierte Telefonverbindung (z. B. 0190x/0900x) umgeleitet, wodurch er das Entgelt für die Inanspruchnahme des Dienstes leistet. Hierfür ist entweder die Installation einer speziellen Software notwendig, die bei der Regulierungsbehörde für Telekommunikation und Post registriert sein muss, oder der Kunde ruft eine angegebene Telefonnummer an. Die Beträge werden mit der Telefonrechnung eingezogen. Dabei tritt die Telefongesellschaft als Inkassostelle auf und leitet die Beträge an die Anbieter weiter. Diese wiederum verteilen die Beträge an die angebundenen Händler.

Beispiele

Durch Firstgate click&buy werden Nutzungsgebühren für Inhalte von Webseiten erhoben. Der Endkunde registriert sich hierzu einmalig bei Firstgate click&buy und wählt eine Zahlungsmethode für den Zahlungsausgleich. Die Installation einer zusätzlichen Software ist nicht erforderlich. Webseiten-Anbieter müssen ihre Inhalte so anpassen, dass ein Zugriff auf die Webseite erst nach erfolgter Erfassung der Abrechnungsdaten durch Firstgate möglich ist. Ein weiteres verbreitetes Verfahren, T-Pay, ist ein Produkt der Deutschen Telekom. Neben dem genannten T Pay MicroMoney kann der Kunde zwischen weiteren Varianten wählen: einer Zahlung im Dialer-Verfahren, per Lastschrift oder Kreditkarte oder einer Abrechnung zu Lasten der Telefonrechnung.

2.3 Entwicklungstendenzen

Auch wenn schon eine Vielzahl von Zahlungsverfahren existiert, so werden weiterhin neue Systeme entwickelt und auf den Markt gebracht. Für eine Beurteilung der Erfolgsaussichten solcher Zahlungsverfahren ist insbesondere der Netzeffekt von Bedeutung. Dieser besagt, dass ein Zahlungsverfahren für die Beteiligten umso nützlicher ist, je mehr Personen daran teilnehmen. In diesem Abschnitt sollen Entwicklungstendenzen vorgestellt werden, denen nach diesem Kriterium eine hohe Relevanz für den zukünftigen Markt der Zahlungsverfahren zugesprochen werden kann: die Gründung von Simpay, die Einführung und Verbreitung des EMV-Standards, die Vereinheitlichung des europäischen Zahlungsverkehrsraums, die Entwicklung eines Zahlungsverfahrens in Kombination mit der elektronischen Signatur und der Einsatz biometrischer Verfahren zur Authentifizierung.

Simpay

- Vier international bedeutsame Mobilfunkunternehmen (Orange, Telefónica Móviles, T-Mobile und Vodafone) haben sich im Frühjahr 2003 zur Gründung eines neuen Mobiltelefon-basierten Zahlungsverfahrens zusammengeschlossen. Unter der gemeinsamen Marke Simpay soll ein weltweites mobiles Zahlungsverfahren auf Basis eines offenen Standards etabliert werden. Weitere Unternehmen wie debitel, KPN Mobile group, O_2, TMN und Hutchison 3 G haben ihr Interesse an einer Teilnahme bekundet. Simpay soll als Debit- (Kauf- und Zahlzeitpunkt fallen zusammen) und Credit-Variante (Zahlzeitpunkt liegt nach dem Kaufzeitpunkt) angeboten werden, von jedem Mobiltelefon nutzbar und einfach zu bedienen sein.

  Simpay integriert derzeit Mitglieder in über 20 europäischen Ländern und besitzt das Potenzial, mehr als 300 Millionen Mobiltelefonnutzer zu erreichen. Eine erste Markteinführung ist für Mitte 2005 in Spanien geplant. In Deutschland wird das Verfahren voraussichtlich ab dem Jahr 2006 verfügbar sein.[20]

EMV-Spezifikation

- In Abschnitt 2.2 wurden bereits die Bestrebungen der Kreditkartengesellschaften zur Verhinderung von Betrugsfällen im Internet vorgestellt. Auch bei Zahlungen am Point of Sale nehmen die Betrugsfälle jedoch zu, da Magnetstreifenkarten sehr leicht zu fälschen sind. Bei Chipkarten ist dies weitaus schwieriger. Aus diesem Grund haben sich Europay, MasterCard und Visa zusammengeschlossen, um einen branchenweit interoperablen Standard für Chipkarten zu schaffen, die EMV-Spezifikation[21]. Diese regelt auf technischer Ebene die Interoperabilität zwischen Chipkarte und Lesegerät. Darauf aufbauende Spezifikationen von Visa und MasterCard haben diese (teilweise widersprechend) verfeinert.

  Seit dem 01.01.2005 besteht in Europa eine Haftungsumkehr (Liability Shift): Zukünftig muss derjenige Akteur, der keine EMV-Technologie einsetzt für betrügerische Aktionen haften, die den Betrug durch die Nutzung der EMV-Technologie hätte verhindern können. Ist beispielsweise entweder das Terminal oder die Karte bei einer Transaktion EMV-fähig, trägt diejenige Transak-

---

20 Ausführliche Informationen werden unter http://www.simpay.de/ bereitgestellt.

21 Näheres dazu in [Rankl/Effing 2002], http://www.kartensicherheit.de/ oder http://www.emvco.com/.

tionspartei die Haftung für Schäden aus Kartenfälschungen, die nicht EMV-fähig war. [Zahlungssicherheit 2005]

Vereinheitlichung des europäischen Zahlungsraums: SEPA – Single European Payment Area

- Für grenzüberschreitende Zahlungen sind insbesondere die Entwicklungen von Bedeutung, die durch die Richtlinie 97/5/EG vom 27. Januar 1997 ausgelöst wurden. In dieser hat die Europäische Union angeordnet, den europäischen Zahlungsverkehrsraum zu vereinheitlichen (Single European Payment Area). Dies bedeutet unter anderem, dass Überweisungen innerhalb der EU für die Verbraucher deutlich einfacher und kostengünstiger werden sollen. In Deutschland wurden diese Anforderungen bereits im Überweisungsgesetz verankert.
  Zur Realisierung eines einheitlichen europäischen Zahlungsverkehrsraums schlossen sich im Jahre 2002 die europäischen Bankenverbände zum so genannten European Payments Council (EPC)[22] zusammen. Ziel ist es, gemeinsam die Entwicklung einer SEPA zu unterstützen und zu fördern.

Einsatz der Signaturkarte als Instrument für Zahlungsverfahren

- Um der Verbreitung der elektronischen Signatur einen Schub zu verleihen, haben die Bundesregierung und Organisationen aus der Wirtschaft das Bündnis für elektronische Signaturen[23] ins Leben gerufen. Das Signaturbündnis hat sich zum Ziel gesetzt, die Anwendung, Verbreitung und Einführung chipkartenbasierter elektronischer Signaturen und verwandter Anwendungen zu fördern. Elektronische Signaturen gemäß Signaturgesetz sind der handschriftlichen Unterschrift gesetzlich gleichgestellt und bieten die Möglichkeit, Handelsgeschäfte auch über elektronische Kanäle rechtsverbindlich abzuschließen. Damit lassen sich auch neue Zahlungsverfahren schaffen. Auf der CeBIT wurde bereits in 2004 ein auf Signaturkarten und bestehenden Systemen basierendes Zahlungsverfahren demonstriert.

Biometrische Authentifizierungsmechanismen

- Die zunehmende Entwicklung biometrischer Authentifizierungsmechanismen macht diese auch für Zahlungsverfahren interessant. Bei den derzeit eingesetzten Zahlungsverfahren erfolgt die Authentifizierung meist über den Besitz einer Karte bzw. eines Mobiltelefons (Besitzmerkmal), die Eingabe eines Passworts (Wissensmerkmal) oder eine Kombination der beiden Möglichkeiten. Grundsätzlich könnte die Authentifizierung auch durch einen Fingerabdruck, einen Iris-Scan oder andere biometrische Verfahren erfolgen. So wird bereits ein System[24] angeboten, das den Fingerabdruck zur Einleitung des Zahlungsvorgangs nutzt. Das Mitführen einer Karte oder eines anderen Mediums ist für das Bezahlen am Point of Sale in diesem Fall nicht mehr erforderlich. Auch Visa und MasterCard untersuchen in einem Feldversuch die Tauglichkeit biometrischer Verfahren für den Einsatz im Rahmen von Zahlungsvorgängen [Schieb 2004]. Bei der Speicherung biometrischer Daten ist jedoch ganz besonders darauf zu achten, dass die datenschutzrechtlichen Bestimmungen eingehalten werden.[25]

---

22 http://www.europeanpaymentscouncil.org/

23 http://www.signaturbuendnis.de/

24 Vgl. dazu http://www.it-werke.de/.

25 Weitere Informationen zum Datenschutz finden sich im Modul „Datenschutzgerechtes E-Government“.

Kontaktlose Zahlungen

- Kreditkartenunternehmen arbeiten derzeit an der Einführung Chipkarten-basierter kontaktloser Zahlungsverfahren für den Point of Sale auf Basis von EMV. Beispiele für solche Verfahren sind PayPass von MasterCard, die Visa Contactless Card von Visa Europe oder ExpressPay von American Express. Durch Vorbeiführen der Chipkarte an einem Kartenterminal wird der Zahlungsvorgang bequem und sicher offline abgewickelt. Überschreitet der Transaktionsbetrag oder die Summe mehrerer bereits stattgefundener Transaktionsbeträge ein vorgegebenes Limit, so muss die Transaktion kontaktbehaftet unter Eingabe der PIN online autorisiert werden. Dabei wird das Limit für kontaktlose Zahlungsabwicklungen wieder heraufgesetzt und es können erneut bis zum Erreichen des Limits kontaktlose Transaktionen durchgeführt werden. Händlern wird bei diesen Verfahren voraussichtlich eine Zahlungsgarantie gewährt.

3 Szenarien von Online-Transaktionen

Vielzahl unterschiedlicher Verfahren

Im vorhergehenden Abschnitt wurde deutlich, mit welcher Vielzahl existierender und zukünftig möglicher Zahlungsverfahren sich Anbieter kostenpflichtiger E-Government-Dienstleistungen derzeit auseinander setzen müssen. Jedes dieser Verfahren weist spezifische, situationsabhängige Voraussetzungen sowie Stärken und Schwächen auf, die es zu berücksichtigen gilt. Ein universelles Zahlungsverfahren, das für alle Anwendungsfälle gleichermaßen gut geeignet wäre, gibt es nicht.

Optimales Verfahren von Kriterien abhängig

Noch auf absehbare Zeit wird es deshalb im Internet das gleiche Nebeneinander verschiedener Zahlungsverfahren geben wie in der realen Welt: Auch dort kommen beim Kauf einer Zeitung, beim Tanken und beim Begleichen der Telefonrechnung üblicherweise verschiedene Zahlungsverfahren zum Einsatz. Offensichtlich unterscheiden sich diese Transaktionen anhand bestimmter Kriterien, die jeweils für oder gegen die Verwendung einzelner Zahlungsverfahren sprechen.

Vorstrukturierung des Problems

Im Mittelpunkt des folgenden Abschnitts stehen Kriterien, nach denen sich Online-Transaktionen im E-Government sinnvoll klassifizieren lassen. Je nach Ausprägung der vorgestellten Kriterien ergeben sich unterschiedliche Anforderungen, die bei der Auswahl eines Zahlungsverfahrens zu berücksichtigen sind. Für eine abschließende Empfehlung des optimalen Zahlungsverfahrens reicht die Ermittlung dieser Anforderungen jedoch nicht aus, da sich in vielen Fällen kein Zahlungsverfahren finden wird, das alle Anforderungen ausreichend erfüllt. Zudem ist nicht jedes Kriterium für jede Online-Transaktion gleichermaßen bedeutend. In Abschnitt 7.1 dieses Moduls wird deshalb detailliert auf den Prozess der Anforderungsanalyse eingegangen, der auch eine subjektive Bewertung der Bedeutung einzelner Anforderungen umfassen muss.

Beispielszenarien in Abschnitt 3.2

Durch Kombination der Kriterien existiert eine hohe Anzahl möglicher Szenarien von Online-Transaktionen. Eine abschließende Beschreibung aller möglichen Szenarien ist somit kaum möglich. Stattdessen werden in Abschnitt 3.2 sechs Beispielszenarien vorgestellt, anhand derer in Abschnitt 7.2 dieses Moduls die Vorgehensweise zur Auswahl eines Zahlungsverfahrens beispielhaft vorgeführt wird.

3.1 Kriterien zur Unterscheidung von Online-Transaktionen

Im Folgenden werden sechs Kriterien zur Unterscheidung von Online-Transaktionen näher erläutert, die sich auf die Anforderungen an ein Zahlungsverfahren für E-Government auswirken: Die Höhe des zu zahlenden Betrags, die Häufigkeit der Nutzung, der Nutzerkreis, der Zahlungszeitpunkt, die im Zusammenhang mit der Online-Transaktion erhobenen Nutzerdaten sowie die Zugehörigkeit der Leistung zum hoheitlichen oder nicht hoheitlichen Bereich. Aufgrund dieser Kriterien lässt sich eine Grobstrukturierung der Online-Transaktionen durchführen, die bereits Hinweise auf mögliche Anforderungen an Zahlungsverfahren liefert.

3.1.1 Höhe des Betrags

Die Wahl eines geeigneten Zahlungsverfahrens wird erheblich davon beeinflusst, welche Größenordnung die Beträge üblicherweise aufweisen, die im Zusammenhang mit der Online-Transaktion zu zahlen sind. Die mögliche Bandbreite reicht von wenigen Cents, z. B. für den Abruf von Informationen aus einem Archiv, bis zu mehreren Tausend Euro, z. B. wenn Unternehmen im Außenwirtschaftsverkehr Sicherheiten hinterlegen müssen.

Piko-, Mikro- und Makropayments

Nach der Höhe des zu zahlenden Betrags werden häufig drei Klassen unterschieden: Piko-, Mikro- und Makropayments. Wenn es auch keine einheitliche Definition dieser Begriffe gibt, sollen im Rahmen dieses Moduls Beträge bis zu fünf Cent als Pikopayment, Beträge zwischen fünf Cent und fünf Euro als Mikropayment und Beträge ab 5 Euro als Makropayment bezeichnet werden.

Auswirkungen auf Bedeutung der Kosten und der Zahlungsgarantie

Bei der Wahl eines Zahlungsverfahrens ist insbesondere darauf zu achten, in welchem Verhältnis die Kosten des Verfahrens zur Höhe des zu zahlenden Betrags stehen. Besondere Bedeutung kommt dabei der Kostenstruktur des Verfahrens zu (vgl. Abbildung 3). Auch die Bedeutung der Zahlungsgarantie wird vermutlich mit steigender Betragshöhe zunehmen.

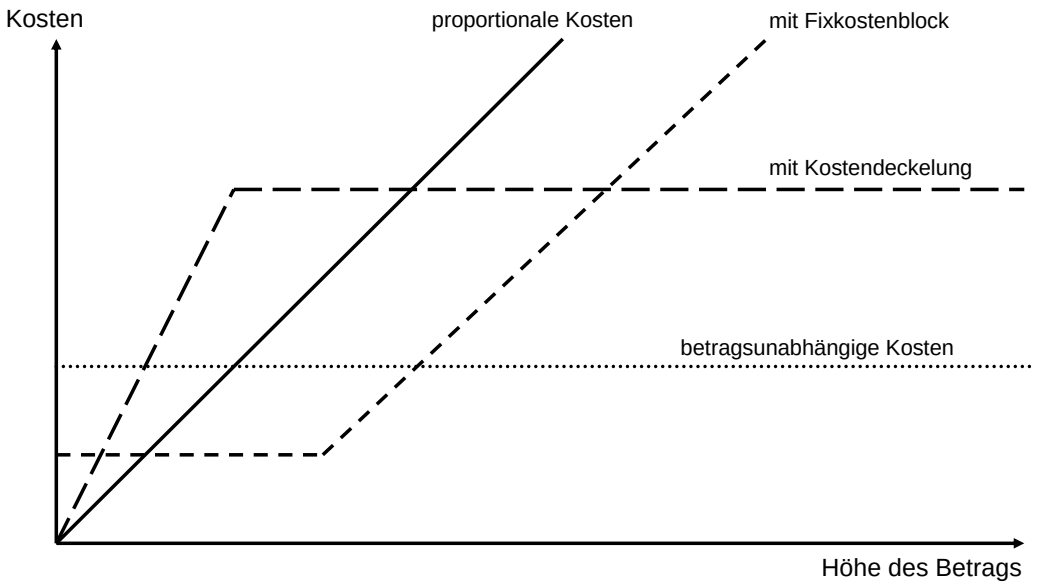


Abbildung 3: Kostenverlauf in Abhängigkeit von der Höhe des Betrags

Eindeutige Zuordnung nicht immer möglich

Trotz der hohen Bedeutung dieses Kriteriums lassen sich allein auf dieser Grundlage noch keine Aussagen über geeignete Zahlverfahren treffen. Ursache dafür ist, dass Piko- und Mikropayments entweder einzeln abgerechnet oder zusammengefasst werden können. Ein Beispiel dafür ist die Telefonrechnung: Obwohl die Kosten der einzelnen Verbindung im Mikropayment-Bereich liegen, ist die monatliche Abrechnung den Makropayments zuzuordnen. Neben der Höhe des zu zahlenden Betrags spielt also auch die Häufigkeit der Nutzung eine wichtige Rolle.

3.1.2 Häufigkeit der Nutzung

Auswirkungen auf Bedeutung der Verbreitung und der Zahlungsgarantie

Die Häufigkeit der Nutzung der Online-Transaktion wirkt sich nicht nur in der Möglichkeit zur Zusammenfassung von Zahlungen aus, auch andere Anforderungen an Zahlungsverfahren werden dadurch beeinflusst. So nimmt der Kunde bei häufig genutzten Leistungen, z. B. dem Abruf eines Handelsregisterauszugs durch ein Unternehmen, vermutlich einen höheren einmaligen Registrierungsaufwand in Kauf als bei selten genutzten Leistungen, z. B. der Online-Beantragung einer Abstammungsurkunde. Die Bedeutung der Verbreitung des Zahlungsverfahrens nimmt damit mit steigender Häufigkeit der Nutzung ab. Auch die Bedeutung der Zahlungsgarantie nimmt ab, wenn die Online-Transaktion häufig von denselben Kunden durchgeführt wird. Viele Internet-Händler erlauben deshalb Wiederholungskäufern die Nutzung von Zahlungsverfahren, die dem Händler ein geringeres Maß an Zahlungssicherheit bieten. Bei Behörden bietet insbesondere die Möglichkeit, säumige Zahler von der Inanspruchnahme der Dienstleistung auszuschließen, ein wirksames Instrument, durch das sich eine fehlende Zahlungsgarantie ausgleichen lässt.

Weitere Unterscheidung: abgeschlossene oder periodisch wiederkehrende Zahlungen

Häufig genutzte Online-Transaktionen können weiter danach unterschieden werden, ob einzelne, abgeschlossene Vorgänge oder periodisch wiederkehrende Zahlungen betrachtet werden. So stellt es beim Fahrkartenkauf einen Unterschied dar, ob es sich um Einzelfahrscheine oder eine Dauerkarte handelt. In letzterem Fall sollte die Zahlung möglichst automatisiert erfolgen, ohne dass der Kunde sie jedes Mal erneut anstoßen muss.

Nicht eindeutig bei Massennutzern

Über die Häufigkeit der Nutzung einer Online-Transaktion lassen sich jedoch keine eindeutigen Aussagen treffen, wenn es bei dieser Transaktion Massennutzer gibt. So ist die Häufigkeit der Nutzung eines Online-Bauantrags für eine Privatperson sehr gering, für einen Architekten aber relativ hoch. Eine eindeutige Zuordnung eines Zahlungsverfahrens lässt sich in diesen Fällen nicht treffen, stattdessen ist eine Fallunterscheidung notwendig.

3.1.3 Nutzerkreis

Inländische und ausländische Nutzer

Neben der Unterscheidung zwischen Massennutzern und Gelegenheitsnutzern ist zudem zwischen inländischen und ausländischen Nutzern zu differenzieren. Während einige Online-Transaktionen, z. B. der Mehrfachantrag für Landwirte, nur durch inländische Nutzer in Anspruch genommen werden, ist für andere auch die Nutzungsmöglichkeit durch Ausländer erwünscht bzw. notwendig[26].

Bei Online-Transaktionen, die auch aus dem Ausland genutzt werden, ist darauf zu achten, dass die entsprechenden Zahlungsverfahren auch im Ausland verfügbar sind. Dies ist bei der Lastschrift z. B. nicht der Fall, da ein Lastschrifteinzug von ausländischen Konten nicht möglich ist. Wie stark ein Verfahren im Ausland verbreitet ist, lässt sich jedoch nicht pauschal bestimmen, da die Verbreitung in den einzelnen Ländern sehr unterschiedlich sein kann.

---

[26] Zu beachten ist insbesondere das Diskriminierungsverbot gegenüber EU-Ausländern.

3.1.4 Zahlungszeitpunkt

Wichtig aus Sicht der Behörde: Zeitpunkt der Zahlungsgarantie

Hinsichtlich des Zahlungszeitpunkts ist zu unterscheiden, ob die Zahlung vor oder nach Lieferung erfolgen muss. Genau genommen ist dabei aus Sicht der Behörde nicht der Zeitpunkt zu betrachten, zu dem eine Zahlung ausgelöst wird, sondern zu dem der Anbieter der Dienstleistung eine Zahlungsgarantie erhält.

Zahlung vor Lieferung nicht immer möglich

Grundsätzlich liegt es im Interesse der Behörde, die Zahlung vor der Lieferung zu erhalten.[27] Es gibt jedoch Fälle, in denen eine „Lieferung" vor der Rechnungsstellung bereits erfolgt ist, beispielsweise bei einem Verwarnungsgeld. In diesen Fällen spielt die Gewährleistung einer Zahlungsgarantie durch ein Zahlungsverfahren kaum eine Rolle, da nicht zu vermuten ist, dass eine Zahlung zunächst initiiert, dann aber nicht eingelöst wird.

Schnelle Zahlungsgarantie vor allem bei digitalen Gütern

Die Frage nach dem Eintritt der Zahlungsgarantie ist besonders kritisch, wenn es sich um digitale Güter oder Dienstleistungen handelt. Während beim Versand physischer Produkte einige Tage Verzögerung in Kauf genommen werden können, bis der Zahlungsbetrag beim Versender eingegangen ist, möchte der Kunde digitale Güter und Dienstleistungen in der Regel sofort nutzen. Das Zahlungsverfahren muss deshalb in sehr kurzer Zeit eine Zahlungsgarantie für den Händler bieten können.

3.1.5 Vorliegende Nutzerdaten

Anonyme oder identifizierte Nutzer

Bei den vorliegenden Nutzerdaten ist vor allem zu beachten, ob der Name des Kunden für den Anbieter der Online-Transaktion bekannt sein muss. Dies ist z. B. der Fall, wenn der Kunde seine Adresse angeben muss, damit ihm ein Bescheid oder ein bestelltes Produkt zugesandt werden kann.

Prinzip der Datensparsamkeit und Datenvermeidung

In allen anderen Fällen soll die Nutzung der Dienste und ihre Bezahlung auch anonym oder unter Pseudonym möglich sein.[28] Im Teledienstedatenschutzgesetz und dem Mediendienstestaatsvertrag sind konkrete Ausprägungen des grundsätzlichen Prinzips der Datensparsamkeit und Datenvermeidung enthalten. Aus diesem Prinzip ergibt sich die Anforderung an ein Zahlungsverfahren, die Erhebung möglichst weniger Daten notwendig zu machen, die nicht ohnehin im Zusammenhang mit der Nutzung der Online-Transaktion erhoben werden müssen.

3.1.6 Art der Verwaltungsleistung

Hoheitlicher oder nicht hoheitlicher Bereich

Online-Transaktionen können zudem danach unterschieden werden, ob die Leistung dem hoheitlichen oder dem nicht hoheitlichen Bereich zuzuordnen ist. Im hoheitlichen Bereich ist die Durchsetzung von Gebührenforderungen wesentlich

---

27 Auf Grund der besonderen Vertrauensstellung der Behörden, wird aus Sicht des Kunden eine Zahlung vor Leistung jedoch im Allgemeinen als unproblematisch eingestuft werden.

28 Diese Anforderung ergibt sich aus § 4 Abs. 6 des Teledienstedatenschutzgesetzes (TDDSG) und § 18 Abs. 6 des Mediendienstestaatsvertrags (MDStV). Vgl. auch die Module „Rechtliche Rahmenbedingungen für E-Government" und „Datenschutzgerechtes E-Government".

vereinfacht, was sich insbesondere auf die Bedeutung der Zahlungsgarantie auswirkt. Sollte die für Leistungen im Rahmen hoheitlicher Aufgaben zu zahlende Gebühr nicht geleistet werden, muss die entsprechende Behörde nicht erst ein Mahnverfahren gegen den Schuldner einleiten, um einen vollstreckbaren Titel zu erhalten, sondern kann unmittelbar eine Vollstreckung einleiten. Die Bedeutung des Schutzes gegen einen Zahlungsausfall des Schuldners ist bei der Auswahl eines Zahlungsverfahrens daher verhältnismäßig gering. Dies gilt allerdings nicht, wenn die Leistung durch ausländische Nutzer in Anspruch genommen wird.

3.2 Beispielszenarien

Im Folgenden werden sechs Beispielszenarien vorgestellt, für die die zuständige Behörde ein geeignetes Zahlungsverfahren bereitstellen muss: Elektronischer Mahnantrag, Elektronische Umsatzsteuer-Voranmeldung, PKW-Kauf bei der Zollauktion im Internet, Elektronische Handelsregisterauskunft, Elektronisches Begleichen eines Verwarnungsgelds für Falschparken und Online-Zugriff auf kostenpflichtige Statistik-Daten. Diese Szenarien werden in Abschnitt 7.2 dieses Moduls dazu verwendet, die Vorgehensweise zur Auswahl eines geeigneten Zahlungsverfahrens beispielhaft vorzuführen. Typische Anforderungen an ein Zahlungsverfahren lassen sich jedoch bereits aus den folgenden Beschreibungen der Beispielszenarien ableiten.

3.2.1 Elektronischer Mahnantrag

Das Mahnverfahren ist ein hoch automatisiertes Massenverfahren[29] zur beschleunigten Durchsetzung von Geldforderungen. Damit ein Antragsteller (Gläubiger) eine Zwangsvollstreckung erwirken kann, benötigt dieser einen gültigen Vollstreckungstitel. Das Mahnverfahren schafft die Voraussetzung, diesen ohne eine Gerichtsverhandlung zu erlangen. Dazu muss der Gläubiger oder ein von ihm Bevollmächtigter beim zuständigen Gericht einen Antrag auf Erlass eines Mahnbescheides stellen, in dem der geltend gemachte Anspruch erläutert wird.

Automatisierung des Mahnprozesses

Um ein möglichst automatisiertes Verfahren zu gewährleisten, ist der Antrag nur auf einem speziell zugelassenen Papierformular oder über eine zugelassene Datenübermittelung beim Mahngericht einzureichen. Letztere wird mehrheitlich von Großkunden genutzt, die dabei eine entsprechende Branchensoftware zur Erstellung der Antragsdateien verwenden. Diese Datensätze können entweder über einen Datenträgeraustausch oder häufig schon mittels spezieller Software-Lösungen (unter anderem Tar/web in Bayern)[30] über das Internet an das Mahngericht über-

29 Beispiel Mahnverfahren in Bayern: Pro Jahr werden etwa 1,5 Millionen gerichtliche Mahnverfahren bei dem zentralen bayerischen Mahngericht (Amtsgericht Coburg) bearbeitet. Ein Großteil der Verfahren, über 60 Prozent, werden bereits elektronisch (Internet bzw. Datenträger) eingereicht. Allerdings gehen trotzdem täglich noch mehr als 2.000 Mahnanträge papiergebunden ein. Diese werden anschließend mit hohem Aufwand in die elektronische Form umgewandelt. [StMJ 2002]

30 Siehe dazu http://www.justiz-coburg.de/tarweb.htm.

tragen werden. Wegen ihrer speziellen Anforderungen und Funktionalitäten sollen Massennutzer in diesem Szenario nicht näher betrachtet und der Fokus auf so genannte „Gelegenheitsmahner“ gelegt werden.

Elektronischer Mahnantrag für mittlere und geringe Antragsaufkommen

Für gelegentliche Nutzer mit einem mittleren oder geringen Antragsaufkommen, die keine entsprechende Software im Einsatz haben, war bis vor kurzem keine elektronische Unterstützung bei der Erstellung möglich; der Antrag musste papierhaft gestellt werden.

Einen erleichternden Einstieg in das gerichtliche Mahnverfahren für eine Vielzahl der Bundesländer bietet der Online-Mahnantrag, ein interaktives und länderspezifisches Antragsformular im Internet auf Erlass eines Mahnbescheids.

Vor allem juristisch unerfahrene Nutzer werden dadurch bei der formal korrekten Erstellung eines Mahnbescheid-Antrags elektronisch geführt: eine integrierte Plausibilitätsprüfung (ca. 2.000 Kriterien) unterstützt das Ausfüllen der interaktiven Antragsformulare und bietet begleitende Hilfe. Somit können fehlerhaft gestellte Anträge – und die damit verbundenen aufwändigen Beanstandungen seitens der Mahngerichte – weitmöglichst im Vorfeld vermieden werden. Allerdings müssen die Anträge teilweise noch auf die entsprechenden Papierformulare ausgedruckt, unterschrieben und verschickt werden.

Online-Einreichung mittels elektronischer Signatur

In mehreren Bundesländern[31] ist das Mahnverfahren auch für Gelegenheitsmahner bereits vollständig elektronisch umgesetzt. So ist dort bereits die Online-Einreichung und die direkte Übermittlung der Daten zu den Großrechnern der Gerichte und somit eine vollständige Medienbruchfreiheit bei der Antragsstellung möglich. Nötig ist dazu allerdings der Einsatz einer qualifizierten elektronischen Unterschrift. Durch E-Government-Anwendungen ergeben sich somit Nutzenpotenziale, wie z. B. die Reduktion von Druck- und Portokosten, die Verringerung von Postlaufzeiten sowie die Vermeidung von Fehlerquellen und dadurch bedingter Zeitverzögerungen bei papierbehafteten Anträgen.

Gerichtskosten

Traditionell erhält der Antragsteller bzw. sein Prozessbevollmächtigter in der Regel erst bei Erlass des Mahnbescheids eine Kostenmitteilung (Rechnung) über das Mahnverfahren, die vor Zustellung des Vollstreckungsbescheids vom Antragsteller zu begleichen ist. Während bei Massennutzern die Teilnahme am elektronischen Mahnverfahren unter der Bedingung einer erteilten Bankeinzugsermächtigung für den Einzug der Gerichtskosten gestellt werden kann, ist dies für den gelegentlichen Antragsteller wenig praktikabel und hinderlich für eine durchgängige Prozessumsetzung.

Grundsätzlich entsteht für das Mahnverfahren eine Gebühr, die sich nach dem Streitwert der Geldforderung berechnet. Die Gerichtskosten [AGM 2004, S. 83] belaufen sich bei einem Streitwert bis 600 Euro bereits auf 18,00 Euro, somit handelt es sich generell um Zahlungen im Makrobereich.

Einführung einer Vorschusspflicht

Im Gegensatz zum Offline-Formularverfahren, in dem das zuständige Mahngericht als Empfänger keine Zahlungsgarantie hat und der Zahlungszeitpunkt erst nach der Leistung erfolgt, bietet es sich für den elektronischen Mahnantrag per Internet an, eine Bezahlfunktion unmittelbar vor dem Abschicken bzw. Signieren

[31] Siehe dazu z. B. http://www.optimahn.de/aktuelles.html.

des komplett erfassten Antragformulars zu integrieren (Vorschusspflicht). Dadurch kann der vormals papierbehaftete Prozessschritt „Rechnungsstellung“ vollständig elektronisch umgesetzt werden. Wichtig ist dabei insbesondere eine Zahlungsgarantie, da ohne Zahlungseingang kein Vollstreckungsbescheid erteilt werden kann. Der weitere Verlauf des Mahnverfahrens ist solange unterbrochen. Für das Zahlverfahren liegen aufgrund der Antragsstellung bereits eindeutige Nutzerdaten vor; ein anonymes Zahlungsverfahren ist daher nicht notwendig.

3.2.2 Elektronische Umsatzsteuer-Voranmeldung

Elster als Verfahren der elektronischen Steuerdatenübermittlung

Im Rahmen des Projektes Elster (Elektronische Steuererklärung) ist die elektronische Einreichung von Steuerdaten möglich. Von den Steuerverwaltungen der Länder und des Bundes wurde eine Software, ElsterFormular, entwickelt, die die Erfassung der Steuerdaten am PC des Steuerpflichtigen unterstützt und anschließend über Internet oder eine direkte Einwahl an das Steuerverwaltungsrechenzentrum überträgt. Bisher musste der Steuerpflichtige (juristische und natürliche Personen) die Daten in der Regel papiergebunden an die zuständige Finanzverwaltung versenden. Im Rahmen einer Vereinbarung zwischen dem Steuerpflichtigen und seinem Finanzamt kann der Steuerdatenaustausch auch elektronisch erfolgen.[32]

Umsatzsteuer-Voranmeldung und Umsatzsteuererklärung

Insbesondere für die Umsatzsteuererklärung bzw. Umsatzsteuer-Voranmeldung ist der elektronische Datenaustausch auf Grund der hohen Aufwandsreduzierung von Interesse. Sowohl die Finanzämter als auch die Steuerpflichtigen können von den Effizienzsteigerungen profitieren. Der Steuerpflichtige ist verpflichtet, die Erklärung oder Voranmeldung fristgerecht beim Finanzamt einzureichen. Er hat darüber hinaus die Pflicht, eine evtl. bestehende Vorauszahlung ebenfalls fristgerecht zu leisten.[33] Eine nicht fristgerechte Voranmeldung und Zahlung seitens des Steuerpflichtigen kann Strafzahlungen zur Folge haben.

Betragshöhe der Zahlungen

Die Betragshöhe der zu leistenden Zahlung ist sehr stark von der Intensität der unternehmerischen Tätigkeit des Steuerpflichtigen abhängig und kann durchaus bei Kleinstbeträgen im Mikropayment beginnen. Die Obergrenze wird von den Umsätzen des Unternehmers bestimmt. Je nach Geschäftstätigkeit unterliegen die Beträge starken oder weniger starken Schwankungen. Beispielsweise können bei Aufnahme einer freiberuflichen Nebentätigkeit die Umsätze zu Beginn sehr gering sein. Bei steigenden Umsätzen können sich die Steuerbeträge sehr rasch im Bereich von mehreren Hundert bis Tausend Euro befinden.

Potenzielle Häufigkeit der Zahlungen

Da in Deutschland der Großteil der Unternehmer umsatzsteuerpflichtig ist, kommt nahezu jede juristische Person und eine Vielzahl natürlicher Personen, etwa aufgrund einer freiberuflichen Tätigkeit oder als Gewerbetreibende, dafür in Betracht.

Zeitpunkt der Zahlungsverpflichtung

Da es sich bei Steuerzahlungen um Leistungen ohne direkte Gegenleistungen handelt, ist die Frage nach dem Bezug zwischen Lieferzeitpunkt und Zahlungs-

---

32 Vgl. Steuerdaten-Übermittlungsverordnung (StDÜV) und Abgabenordnung (AO).

33 Vgl. hierzu § 18 UStG.

ausgleich hinfällig. Der Gesetzgeber hat diesbezüglich die bereits angesprochenen Fristen für die Zahlung definiert.

Schutzbedürfnis von Nutzerdaten

Steuerzahlungen und damit verbundene personenbezogene Daten unterliegen neben den Datenschutzgesetzen auch dem Steuergeheimnis als Amtsgeheimnis. Ein Amtsträger der Finanzbehörde oder eine gleichgestellte Person verletzt das Steuergeheimnis, wenn sie ihr dienstlich oder sonst in amtlicher Stellung bekannt gewordene Verhältnisse eines anderen unbefugt offenbart, verwertet oder entsprechende Daten in einem automatischen Abrufverfahren abruft[34]. Für ein Zahlungsverfahren ergeben sich hieraus besondere Anforderungen an die Vertraulichkeit. Das Bekanntwerden von Zahlungsinformationen ist auf Grund der Sensibilität der Daten (z. B. des Betrages in Verbindung mit einem Kontoinhaber und einem Verwendungszweckhinweis) besonders bedenklich, da hier unter anderem auch wettbewerbliche Aspekte relevant sein können.

3.2.3 PKW-Kauf bei Zollauktion im Internet

Versteigerungsplattform des Zolls

Die Versteigerungsplattform des Zolls bildet ein Teilprojekt der Initiative Bund-Online 2005 und wird vom Bundesamt für Finanzen betrieben. Unter http://www.zoll-auktion.de/ können seit März 2002 gepfändete, beschlagnahmte und ausgesonderte Artikel, wie z. B. Computer, Notebooks, Mobiltelefone, Audio-, Video- und Fernsehgeräte, Fotoapparate, Digitalkameras und Kraftfahrzeuge ersteigert werden. Die 46.545 Bieter, Unternehmen und Privatpersonen, die sich mittlerweile registriert haben, konnten beispielsweise im ersten Quartal 2005 über 900 Artikel ersteigern. Darunter befanden sich auch mehr als 100 Kraftfahrzeuge.

Leistungsumfang

Die Plattform wird derzeit von über 200 Dienststellen auf Bundes-, Landes- und Kommunalebene genutzt. Gegenstand der Dienstleistung ist die Durchführung der Versteigerung im engeren Sinne. Dazu gehört das Einstellen der Artikelbeschreibungen mit Fotos und Mindestgeboten ins Internet, die Durchführung der Auktion und die Bereitstellung der erforderlichen IT-Infrastruktur. Rechtsfragen, Vertragsabwicklungen, Lagerung und ggf. Versand der Gegenstände verbleiben bei den jeweils zuständigen Behörden.

Registrierung

Um einen PKW über die Plattform des Zolls zu ersteigern, muss sich der Nutzer zuerst registrieren. Dafür ist ein frei wählbarer Zugangsname, eine E-Mail-Adresse sowie Vorname, Nachname, Straße, Hausnummer, Postleitzahl und Wohnort anzugeben. Per E-Mail wird dem Nutzer ein persönliches, von ihm änderbares Passwort zugesandt.

Zuschlag

Sobald der Kunde registriert ist, kann er an der öffentlichen Versteigerung durch die Abgabe von Geboten für den PKW teilnehmen. Ist das Gebot des Bieters bei Ablauf der Gebotszeit das höchste, so wird ihm der Zuschlag erteilt. Der Zuschlag wird dem Nutzer durch eine E-Mail mitgeteilt, gleichzeitig werden der anbietenden Dienststelle die Adressdaten des Nutzers übermittelt.

Abholung

Der PKW muss innerhalb von vier Wochen nach der Versteigerung bei der anbietenden Dienststelle abgeholt werden. Vorzulegen sind dabei der Personalausweis

[34] Vgl. § 30 AO.

Anforderungen an ein Zahlungsverfahren

und der Ausdruck der E-Mail über den Zuschlag. Nach Absprache mit der anbietenden Dienststelle ist grundsätzlich auch ein Versand innerhalb Deutschlands möglich, sofern der Gebotsbetrag zzgl. Versandkosten im Voraus entrichtet wird. Wird der PKW nicht abgeholt, wird er erneut versteigert. Der frühere Meistbietende darf bei dieser Auktion nicht mitbieten und haftet, falls bei der erneuten Versteigerung ein geringerer Erlös erzielt wird. Holt ein Nutzer wiederholt ersteigerte Artikel nicht ab, wird er von der Zoll-Auktion ausgeschlossen.

Aus dem in der Regel beträchtlichen Wert eines PKW ergibt sich die Anforderung an ein Zahlungsverfahren, der Behörde spätestens zum Zeitpunkt der Übergabe eine Zahlungsgarantie zu bieten. Aufgrund der besonderen Vertrauensstellung der öffentlichen Verwaltung werden die Kunden wohl auch bereit sein, schon vor Lieferung zu zahlen. Eine anonyme Nutzung dieses Dienstes wäre zwar bei persönlicher Abholung des PKW grundsätzlich denkbar, jedoch müsste der Meistbietende bzw. ein Bevollmächtigter die entsprechende Berechtigung zum Zeitpunkt der Entgegennahme nachweisen können.

3.2.4 Elektronische Handelsregisterauskunft

Im Rahmen des Ausbaus des elektronischen Rechtsverkehrs wurde im Auftrag der Länder Bayern, Nordrhein-Westfalen, Sachsen und Sachsen-Anhalt das Verfahren RegisSTAR zur elektronischen Handelsregistereinsicht entwickelt.[35] Weitere Bundesländer haben sich mittlerweile dem Verbund angeschlossen.[36] RegisSTAR ermöglicht die Online-Einsicht in sämtliche bereits elektronisch geführte Handelsregister A und B sowie Genossenschafts-, Vereins- und Partnerregister.[37]

Grundsätzlich steht die Internet-Handelsregistereinsicht jedem offen, ob Privatperson oder Firma. Für die Nutzung ist keine spezielle Zugangs-Software erforderlich. Voraussetzung zur Einsicht ist jedoch eine vorherige Anmeldung[38] zum elektronischen Abrufverfahren, nach der dem Nutzer eine Kennung und ein Passwort zugewiesen werden.

Bei der Recherche muss die Registerart angegeben werden, optional kann nach verschiedenen Kriterien wie Registernummer, Gerichtsbezirk, Niederlassung/Sitz,

---

35 Die elektronische Handelsregister-Auskunft „RegisSTAR“ wird in diesem Beispiel an Hand der bayerischen Registerauskunft erläutert.

36 Näheres dazu unter http://www.justizregister.de/.

37 Über 215.000 aktuell in das Handelsregister eingetragenen Firmen und Gesellschaften können online eingesehen werden. Die Partnerschaftsregister (nur ca. 300 Partnerschaften in ganz Bayern) werden schrittweise im Laufe des Jahres 2004 online zur Verfügung stehen. Daneben kann zusätzliche auf die gelöschten Registerblätter (vor Einführung von RegisSTAR bereits gelöschte Firmen) zugegriffen werden. [Justizregister Bayern 2005]

38 Die Anmeldung zur Nutzung von RegisSTAR erfolgt durch das Ausfüllen eines pdf-Anmeldeformulars, das im Anschluss ausgedruckt, unterschrieben und auf dem Postweg oder per Fax an das Oberlandesgericht München gesendet werden muss. Anzugeben sind Vorname, Name, Straße und Hausnummer bzw. Postfach, PLZ, Ort und Land. Bei Firmen oder Organisationen ist zusätzlich der Vor- und Nachname des Ansprechpartners zu nennen. Weiterhin werden E-Mail-Adresse und Telefonnummer verlangt, falls abweichend ist die Rechnungsanschrift gesondert einzutragen.

Rechtsform und der Anschrift gesucht werden. Die alleinige Suche nach Unternehmen und die sich daraus ergebende Trefferliste ist kostenfrei. Weitergehende gebührenpflichtige Informationsseiten, wie chronologischer, aktueller[39] oder historischer[40] Ausdruck, allgemeine Firmeninformationen, Vertretungsbefugten- und Prokuristenmaske, können über entsprechende Hyperlinks erreicht werden. Nach dem Anklicken eines Hyperlinks einer gebührenpflichtigen Informationsseite erfolgt der Hinweis auf die Kostenpflicht, um gegebenenfalls den Vorgang noch abbrechen zu können. Im Falle des ungewollten Abbruchs der Handelsregistereinsicht (z. B. nach Zeitüberschreitung von fünf Minuten ohne weitere Eingabe durch den Benutzer), kann jedoch der gleiche Datensatz innerhalb einer Stunde ab dem Zeitpunkt der ersten Anforderung unter Verwendung derselben Kennung kostenfrei erneut angefordert werden.

Bei der Anmeldung kann der Nutzer je nach Nutzungsintensität zwischen zwei Modellen auswählen [Justizregister Bayern 2004]:

- regelmäßige Nutzung, häufig durch Notare, Rechtsanwälte und Kreditinstitute, zu 4 Euro je elektronischem Abruf, anrechenbare Jahresmindestgebühr (per Vorkasse) von 150 Euro sowie
- gelegentliche Nutzung zu 8 Euro je elektronischem Abruf, ohne Jahresmindestgebühr.

Zur Auswahl geeigneter Zahlungsverfahren wird der Fall der Massennutzer (vgl. Abschnitt 3.1.2) nicht weiter betrachtet.

Derzeit wird durch die Fachanwendung ausschließlich die Bezahlung nach Leistungserbringung über die Erstellung einer Rechnung (Versand per E-Mail) unterstützt und erfordert somit zwingend – gesetzlich allerdings nicht notwendig – die Anmeldung/Identifizierung des Nutzers. Es bietet sich jedoch gerade für gelegentliche Nutzer die Einbindung einer E-Payment-Lösung an, die Einzeleinsichten auch ohne vorherige Anmeldung zum Abrufverfahren ermöglicht.

3.2.5 Elektronisches Begleichen eines Verwarnungsgelds für Falschparken

Prozessablauf und erhobene Daten

Die Anordnung von Verwarnungsgeldern betrifft ausschließlich die kommunale sowie staatliche Ebene. Bei der Ordnungswidrigkeit „Falschparken“ wird die Identität des Fahrzeughalters anfänglich nicht ermittelt, sondern stellvertretend nur das amtliche Kennzeichen des falsch parkenden Fahrzeuges verwendet. Dem Fahrzeughalter wird aufgrund einer Übertretung rechtlicher Normen, hier wegen unrechtmäßiger Nutzung eines Parkplatzes, eine Verwarnung mit Zahlungsaufforderung erteilt. Ziel ist die Erzwingung normkonformen Verhaltens. Auf dem entsprechenden Beleg, der am Fahrzeug angebracht wird („Strafzettel“), wird neben dem Kennzeichen des Fahrzeugs, dem zu entrichtenden Betrag und verschiedenen

39 Eine Neuerung zum bisherigen Registerinhalt stellt der aktuelle Auszug dar, der alle relevanten Daten des aktuellen Registerinhaltes übersichtlich darstellt und Löschungen herausfiltert.

40 Der historische Auszug weist alle Eintragungen bis zur Umstellung auf RegisSTAR auf und enthält die alten Papierregister in eingescannter Form.

weiteren Daten, wie der Uhrzeit und der Beschreibung des Vergehens, auch ein Kassenzeichen (Verwarnungsnummer) vermerkt. Verwarnungen mit Zahlungsaufforderungen werden in Deutschland täglich mehrere tausend Mal ausgesprochen.

Verbuchung und Zahlung

Die Kommune oder eine staatliche Einrichtung verbucht die Forderung gegen das Kennzeichen des Fahrzeughalters. Innerhalb einer vorgegebenen Frist (in der Regel eine Woche) ist der Betrag auf das Konto der Behörde zu überweisen. Dazu wird der Verwarnung mit Zahlungsaufforderung bisher ein vorausgefüllter Überweisungsträger beigelegt. Heute wird in der Regel der beigelegte Überweisungsträger zur Begleichung des Betrages genutzt. Zukünftig könnte jedoch auch eine Bezahlung über eine Webschnittstelle (z. B. über PC oder Mobiltelefon) denkbar sein.

Geht die Zahlung fristgerecht ein, wird die Verwarnung damit anerkannt und kein Bußgeldverfahren eingeleitet. Die Forderung wird ausgebucht. Die Person des Zahlenden spielt dabei keine Rolle, so muss z. B. der Verursacher der Ordnungswidrigkeit nicht identisch mit dem Fahrzeughalter sein. Wird die Zahlungsaufforderung nicht fristgerecht beglichen, leitet die zuständige Behörde ein Bußgeldverfahren ein. Dazu ermittelt sie anhand des Kennzeichens die Anschrift des Fahrzeughalters. Bis zu diesem Zeitpunkt war der Behörde nur das (als Pseudonym interpretierbare) Autokennzeichen bekannt. Dem Halter wird dann ein Erinnerungsschreiben zugestellt.

Anforderungen an ein Zahlungsverfahren

Der Zahlungsgarantie kommt beim Verwarnungsgeld für Falschparken keine Bedeutung zu, da eine „Lieferung“, d. h. eine unrechtmäßige Nutzung eines Parkplatzes, bereits erfolgt ist. Da bis zur Einleitung eines Bußgeldverfahrens nur das Pseudonym des Nutzers bekannt ist, sollte mindestens ein Zahlungsverfahren angeboten werden, mit dem die Zahlung anonym erfolgen kann.

3.2.6 Online-Zugriff auf kostenpflichtige Statistik-Daten

Statistik-Shop des Statistischen Bundesamts

Viele Behörden und Gebietskörperschaften verfügen über statistische Daten, die für Bürger und insbesondere für Unternehmen von Interesse sind. Soweit rechtlich möglich, können diese Daten kostenpflichtig im Internet angeboten werden. Der Vertrieb kostenpflichtiger Statistik-Daten ist beispielsweise im Statistik-Shop[41] des Statistischen Bundesamts (Destatis) schon realisiert. Dort werden Publikationen sowie nationale und internationale Statistiken des Amts im Internet angeboten. Die gewünschten Datensammlungen können in gedruckter Form per Post oder in elektronischer Form über das Internet bezogen werden. Im Weiteren soll ausschließlich der Bezug in elektronischer Form betrachtet werden.

Vorliegende Nutzerdaten

Zur Nutzung des Shops zum Erwerb von kostenpflichtigen Veröffentlichungen oder zur Anwendung des Nutzerservices (z.B. Newsletter) ist eine einmalige Registrierung erforderlich. Kostenfreie Downloads stehen ohne Registrierung zur Verfügung. Anmelden können sich sowohl Privatpersonen als auch Firmen aus dem In- und Ausland. Dabei ist die Angabe von Name, Vorname, Straße, Hausnummer, Postleitzahl, Ort, Staat und E-Mail-Adresse verpflichtend, während Te-

41 Nähere Ausführungen finden sich im Modul „Leitfaden für die Einrichtung einer Internetvertriebsplattform (E-Shop)“. Den Statistik-Shop erreicht man unter http://www-ec.destatis.de/.

lefon und Telefax optional angegeben werden können. Ein selbst gewählter Nutzername sowie ein sechsstelliges Passwort ermöglichen den Zugang zum Online-Shop.

Bestell- und Zahlungsabwicklung

Im Statistik-Shop kann der Kunde die gewünschten Datensammlungen in seinen Warenkorb legen und nach Abschluss der Bestellung gesammelt herunterladen. Mit dem Abschluss der Bestellung wird gleichzeitig das Zahlungsverfahren ausgewählt: Möglich sind derzeit die Zahlung per Kreditkarte (MasterCard, VISA oder American Express) oder per Rechnung. Im Inland wird zusätzlich noch die Zahlung per Bankeinzug angeboten[42].

Sowohl Mikro- als auch Makropayments, unregelmäßige Nutzung

Die zu zahlenden Beträge liegen sowohl im Mikro- als auch im Makropayment-Bereich. Die Nutzungshäufigkeit wird bei den meisten Kunden unregelmäßig sein. Es ist durchaus vorstellbar, dass es Massennutzer gibt, mit denen individuelle Nutzungsmodalitäten vereinbart werden.

Anforderungen an ein Zahlungsverfahren

Für einen Online-Zugriff auf kostenpflichtige Statistik-Daten lassen sich drei zentrale Anforderungen an ein ideales Zahlungsverfahren definieren. Erstens sollte es sich um ein Verfahren handeln, das für den Kreis potenzieller Nutzer leicht zugänglich ist. Dieser umfasst sowohl ausländische Unternehmen, die einige der in Deutschland gängigen Zahlungsverfahren nur mit hohem Aufwand nutzen können[43], als auch Privatpersonen im Inland, die z. B. nicht unbedingt eine Kreditkarte besitzen. Zweitens sollte die Zahlungsgarantie zum Schutz vor möglichem Missbrauch vor Lieferung eintreten. Schließlich wäre beim Bezug von Daten in elektronischer Form auch eine anonyme Nutzung des Dienstes möglich, die Registrierung ist nur für die Zustellung der Rechnung erforderlich. Das Zahlungsverfahren müsste deshalb auch eine anonyme Bezahlung des Dienstes ermöglichen.

3.3 Zusammenfassung

Beispielszenarien als Vorlage für weitere Szenarien

Die obigen Beispielszenarien stellen lediglich einen Ausschnitt aus der Vielzahl möglicher Online-Transaktionen dar. Sie sind jedoch so gestaltet, dass man sich bei der Analyse weiterer Szenarien an den Beispielszenarien orientieren kann. So kann der Online-Zugriff auf kostenpflichtige Statistik-Daten mit dem Bezug jeglicher elektronischer Dokumente über das Internet verglichen werden. Dennoch können sich zwei Szenarien, die hinsichtlich der in Tabelle 1 zusammengefassten Kriterien die gleichen Ausprägungen aufweisen, noch in Details unterscheiden, die für oder gegen ein bestimmtes Zahlungsverfahren sprechen. In Abschnitt 7 erfolgt deshalb eine detaillierte Analyse der Anforderungen an ein Zahlungsverfahren.

---

42 Siehe dazu insbesondere https://www-ec.destatis.de/html/liefer.htm#B

43 Für das Lastschriftverfahren ist z.B. der Besitz eines Girokontos in Deutschland erforderlich.

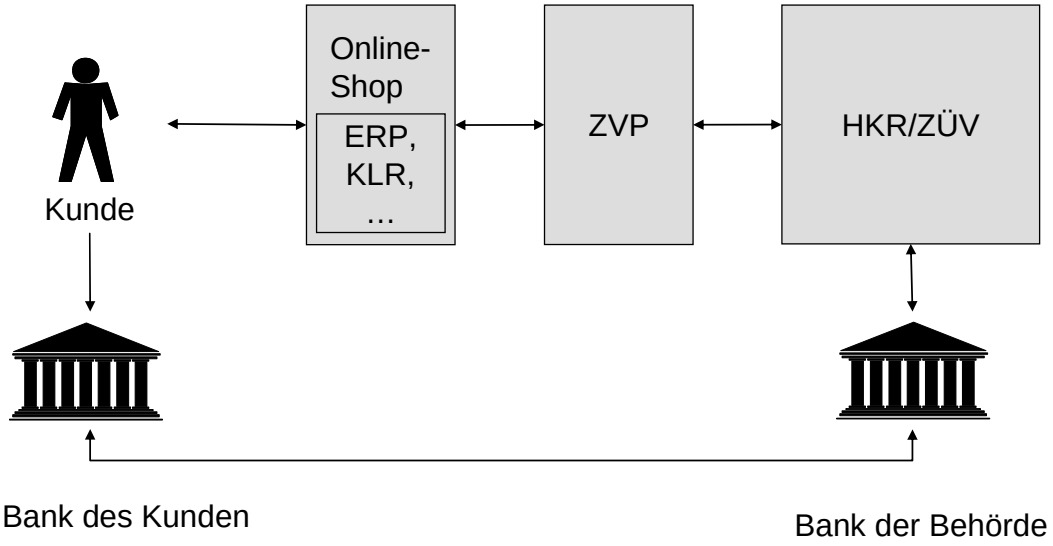
		Unterscheidungskriterien von Online-Transaktionen					
		Höhe des Betrags	Häufigkeit der Nutzung	Nutzerkreis	Zahlungszeitpunkt	Vorliegende Nutzerdaten	Art der Verwaltungsleistung
Beispielszenarien	Elektronischer Mahnantrag (Gelegenheitsnutzer)	Makropayment	unregelmäßig	Nur Inland	Vor Lieferung	Identifizierung nötig	hoheitlich
	Elektronische Umsatzsteuervoran-meldung	Makropayment	regelmäßig	Nur Inland	Nicht zuordenbar[44]	Identifizierung nötig	hoheitlich
	PKW-Kauf bei Zollauktion im Internet	Makropayment	unregelmäßig	Inland und Ausland	vor Lieferung	Identifizierung nötig	nicht hoheitlich
	Elektronische Handelsregister-Auskunft (Gelegenheitsnutzer)	Makropayment	unregelmäßig	Inland und Ausland	vor Lieferung	Keine Identifizierung nötig	hoheitlich
	Elektronisches Begleichen eines Verwarnungsgelds für Falschparken	Mikro- oder Makropayment	unregelmäßig	Inland und Ausland	nach Lieferung	Keine Identifizierung nötig	nicht hoheitlich
	Online-Zugriff auf kostenpflichtige Statistikdaten	Mikro- oder Makropayment	unregelmäßig	Inland und Ausland	vor Lieferung	Keine Identifizierung nötig	nicht hoheitlich

Tabelle 1: Ausprägungen der Beispielszenarien

44 Der Zahlungszeitpunkt kann im Szenario „Elektronische Umsatzsteuervoranmeldung“ nicht eindeutig bestimmt werden, da er auf die Leistung abzielt und es bei der Steuerzahlung keine direkte, auf einen Zeitpunkt bezogene Gegenleistung gibt.

4 Integration des Zahlungsverfahrens

Bei der Frage, wie im Rahmen von E-Government-Dienstleistungen anfallende Gebühren effizient und sicher vereinnahmt werden können, ist neben der Auswahl eines geeigneten Zahlungsverfahrens auch die Integration des Zahlungsverfahrens in die Systemlandschaft der Behörde zu betrachten. Mit Zahlungen an die öffentliche Verwaltung sind weitere innerbehördliche Prozesse verbunden, wie etwa die Initiierung der Leistungserstellung bzw. der Auslieferung oder die Verbuchung der Zahlungen, die in den IT-Systemen der Behörde abgebildet werden müssen. Bevor sich der Rest dieses Moduls wieder der Auswahl eines geeigneten Zahlungsverfahrens widmet, sollen daher im folgenden Abschnitt kurz die an der Zahlungsabwicklung beteiligten Systeme vorgestellt werden.



ERP: Enterprise-Resource-Planning
KLR: Kosten- und Leistungsrechnung
ZVP: Zahlungsverkehrsplattform
HKR: Haushalts-, Kassen- und Rechnungswesen
ZÜV: Zahlungsüberwachungsverfahren

Abbildung 4: Beteiligte Systeme an der Zahlungsabwicklung auf Bundesebene

Die an der Zahlungsabwicklung beteiligten Systeme lassen sich nach ihrer Funktionalität grob in drei Bestandteile gliedern: Einen Online-Shop und damit verbundene, nachgelagerte Systeme auf Behördenseite, ein Zahlungsverkehrssystem und ein Hintergrundsystem für das Haushalts-, Kassen- und Rechnungswesen (HKR). Die Aufgaben dieser Systeme werden im Folgenden am Beispiel eines Zahlungsvorgangs auf Bundesebene vorgestellt (Abbildung 4). Zu beachten ist jedoch, dass die IT-Landschaft der öffentlichen Verwaltung weder über die verschiedenen Ebenen (Bund, Länder, Kommunen) hinweg noch innerhalb der Ebenen homogen ist. Oftmals befinden sich sowohl Eigenentwicklungen als auch Standard-Software-Lösungen im Einsatz. Die in der einzelnen Behörde konkret eingesetzten Systeme können sich in Ihrer Funktionalität daher durchaus stark unterscheiden.

4.1 Online-Shop und nachgelagerte Systeme

Aufgaben eines Online-Shops

Unter einem Online-Shop[45] versteht man eine Internetvertriebsplattform einer Behörde. Der Online-Shop bildet damit die Schnittstelle zwischen Kunde und Behörde, über die verschiedene Funktionen und Services zur Verfügung gestellt werden. Dazu zählen z. B. Kataloge über die Produkte und Dienstleistungen der Behörde und ein elektronischer Warenkorb. Über einen Online-Shop können physische oder digitale Produkte, wie etwa Gesetzestexte oder statistische Daten, aber auch Dienstleistungen, wie die Beantragung eines Anwohnerparkausweises, online angeboten werden.

Realisierungsmöglichkeiten

Für die Realisierung eines Online-Shop gibt es grundsätzlich drei Möglichkeiten: Eigenbetrieb, teilweise Auslagerung an Dritte oder vollständige Auslagerung. Die Art der Realisierung wirkt sich auf die technische Implementierung des Zahlungsverfahrens aus, da bei den letzten beiden Varianten auch die Anforderungen Dritter einbezogen werden müssen. Zudem kann danach unterschieden werden, ob der Shop speziell für eine Behörde entwickelt wurde (Individual-Software) oder ob die Umsetzung mittels Standard-Software-Komponenten erfolgt[46]. Da Standard-Software-Lösungen häufig bereits mehrere Zahlungsverfahren unterstützen, ist die Implementierung eines Zahlungsverfahrens bei Standard-Software in der Regel mit weniger Aufwand verbunden.

Vorgangsbearbeitungs- und ERP-Systeme

Neben dem Online-Shop, der hauptsächlich zur Bestellabwicklung dient, werden auf Behördenseite häufig auch Vorgangsbearbeitungssysteme oder Enterprise-Resource-Planning (ERP)-Systeme zur Leistungserstellung eingesetzt. Während Vorgangsbearbeitungssysteme in erster Linie eine weitgehend medienbruchfreie IT-gestützte Bearbeitung eines Vorgangs, z. B. einer Antragsbearbeitung, ermöglichen[47], integrieren ERP-Systeme die Vorgangsbearbeitung mit weiteren Hintergrundsystemen, z. B. für die Warenwirtschaft, die Personalplanung oder die Kosten- und Leistungsrechnung.

4.2 Zahlungsverkehrsplattform

Vorteile einer Zahlungsverkehrsplattform

Insbesondere wenn mehrere Zahlungsverfahren an einen Online-Shop angebunden werden sollen, lässt sich der Implementierungsaufwand durch Verwendung einer Zahlungsverkehrsplattform im Vergleich zu Eigenlösungen deutlich reduzieren. Aufwendige Verfahrensprüfungen wie Adress- oder Bonitätsprüfungen können durch die Zahlungsverkehrsplattform automatisiert abgewickelt werden. Weitere Vorteile ergeben sich durch die einfache Anbindung weiterer Online-Shops und neuer Zahlungsverfahren.

---

45 Zum Thema Online-Shop vergleiche das Modul „Leitfaden für die Einrichtung einer Internetvertriebsplattform (E-Shop)“.

46 Der Statistikshop des Statistischen Bundesamtes basiert z.B. auf der Standardsoftwarelösung „Intershop 4.2“.

47 Zu den Funktionalitäts- und Kompatibilitätsanforderungen an Vorgangsbearbeitungssysteme vgl. [KBSt 2001].

Bei vielen Unternehmen, die Leistungen über das Internet vertreiben, werden derartige Standardlösungen zur Zahlungsabwicklung bereits seit längerem verwendet. Auch für E-Government werden in einigen Staaten bereits Zahlungsverkehrsplattformen eingesetzt. So findet beispielsweise in Singapur, dessen Bürger eine hohe Affinität zu neuen Formen der Bezahlung besitzen, bereits seit Ende 2002 die zentrale Plattform des Bankenkonsortiums „Network for Electronic Transfers Singapore[48]“ Anwendung. Die Bürger Singapurs können diese Plattform z. B. zur Zahlung von Hundesteuern, Bußgeld-Bescheiden für Verkehrssünden, Arbeitserlaubnissen, Anwohnerparkausweisen und Fernsehgebühren bis hin zu Einkommens- und Vermögenssteuern nutzen.

Die Zahlungsverkehrsplattform des Bundes

Auch in Deutschland wurde im Rahmen der E-Government-Initiative BundOnline 2005 mit der Basiskomponente Zahlungsverkehrsplattform[49] (ZVP) ein zentrales Zahlungssystem für Zahlungen an Bundesbehörden entwickelt. Beim Deutschen Institut für Medizinische Dokumentation und Information (DIMDI), bei der Bundesanstalt für Materialforschung und -prüfung (BAM), beim Bundesverwaltungsgericht (BVerwG) und beim Bundespresseamt (BPA) ist die ZVP bereits im Einsatz[50]. Mittels Funktionsbausteinen (so genannte Web Services) werden Dienstleistungen zur Zahlungsabwicklung zur Verfügung gestellt, die die verschiedenen Online-Shops der Bundesbehörden und das zentrale HKR-System beim Bundesamt für Finanzen (BfF) verbinden. So leitet die ZVP beispielsweise Einnahmeanordnungen an das Zahlungsüberwachungsverfahren (ZÜV) weiter und stellt damit die Verbuchung im HKR-System des Bundes sicher. Die erforderlichen Daten für die Sollstellung werden von den jeweiligen Online-Shops entweder zyklisch oder sofort online an die ZVP übertragen. Einmal täglich überstellt die ZVP dann die Daten aller zu erwartenden Zahlungen dem ZÜV-System. Umgekehrt werden der ZVP die Zahlungseingänge vom ZÜV-System gemeldet. Zusätzliche Funktionen der ZVP sind zum Beispiel das Berichtswesen, die Pflege der Kundenstammdaten, die Verwaltung von Sperrlisten sowie die Prüfung von Kontonummern nach den Prüfziffernverfahren der verschiedenen Banken.

Bedeutung der Kassenzeichen

Jeder Zahlungsvorgang erhält in der ZVP ein eindeutiges Kassenzeichen, das zusammen mit den Zahlungsdaten in einer Datenbank gespeichert wird. Zahlungseingänge oder Einzugsanforderungen können über das Kassenzeichen eindeutig zugeordnet werden. Der Online-Shop ermittelt durch eine tägliche Anfrage beim Web Services Interface der ZVP die Kassenzeichen, zu denen seit der letzten Anfrage Zahlungen eingegangen sind. Kassenzeichen werden für sechs Jahre aufbewahrt und sind recherchierbar.

Zahlungsverfahren

Durch die ZVP des Bundes werden derzeit die Zahlungsverfahren Lastschrift, Überweisung und Kreditkarte (VISA, MasterCard, AmericanExpress) unterstützt. Für die Zahlung per Lastschrift werden zwei Varianten angeboten: Die Lastschrift mit Einzugsermächtigung und die elektronische Lastschrift. Bei der Lastschrift

---

48 Näheres dazu unter http://www.ecitizen.gov.sg/.

49 Weitere Informationen zur ZVP finden sich im Wissensmanagement der Initiative BundOnline 2005 unter http://www.wms.bundonline.bund.de/.

50 Im Wissensmanagement der Initiative BundOnline 2005 wird der Einsatz der ZVP beim DIMDI sowie beim BVerwG unter „Praxisbeispiel für die Basiskomponente Zahlungsverkehrsplattform (ZVP)“ detailliert beschrieben.

mit Einzugsermächtigung muss der Kunde eine Einzugsermächtigung ausdrucken, seine Kontoverbindungsdaten eintragen und das Formular unterschrieben an den Betreiber des Online-Shops schicken. Nach Eingang der Einzugsermächtigung erhält der Kunde eine PIN, mit der er die Behörde über das Internet zum Einzug von Lastschriften ermächtigen kann. Die zweite Variante ist die elektronische Lastschrift ohne schriftliche Einzugsermächtigung. Dabei wird geprüft, ob die vom Kunden angegebenen Kontoverbindungs- und Adressdaten tatsächlich existieren, ob ein Sperrlisteneintrag besteht und ob von diesem Kunden bereits Rücklastschriften vorliegen. Auch bei der Zahlung per Überweisung wird neben der Variante „Zahlung vor Lieferung“ eine Variante „Zahlung nach Lieferung“ angeboten, die mit verschiedenen Sicherheitsabfragen verbunden ist. Bei Zahlungen per Kreditkarte werden vom Kunden die Kreditkartendaten einschließlich der Kartenprüfnummer abgefragt und anschließend bei einem externen Provider online autorisiert. Die Aufnahme weiterer Zahlungsverfahren soll zukünftig bedarfsorientiert erfolgen. So wird derzeit (Mai 2005) die Integration der Online-Überweisung (vgl. Abschnitte 2.1.2 und 6.1.2) geprüft. Während das Bundesamt für Finanzen zentral Wartung und Betrieb der Zahlungsverkehrsplattform steuert, tragen die Behörden die anfallenden Transaktionskosten, die durch Adressverifizierung, Kontonummernprüfung, Kreditkartenautorisierung, oder durch Kreditkartenrückbuchungen entstehen.

Optionen der Online-Shop-Betreiber

Die Online-Shop-Betreiber haben die Möglichkeit, den Kunden manuell unterschiedliche Bonitäten zuzuweisen. Im Falle einer guten Kundenbonität überspringt die ZVP bei der Bonitätsprüfung dann automatisch bestimmte Schritte, wie z. B. die Überprüfung der Kontoverbindungs- und Adressdaten. Säumige und unzuverlässige Kunden können auf eine Sperrliste gesetzt werden, sodass für sie eine Zahlung nach Lieferung ausgeschlossen wird.

Das Retourenmanagement erfolgt in der Regel beim Betreiber des Online-Shops. Storno-Buchungen werden direkt an das ZÜV-System übermittelt. Da alle Buchungsvorgänge täglich aus dem ZÜV-System an die ZVP überstellt werden, kann eine automatische Korrektur in der ZVP erfolgen. Auch bei der Rückabwicklung von Kreditkartenzahlungen kann die ZVP der Einfachheit halber umgangen werden, indem die Behörde den Betrag über das normale Kassengeschäft des Bundes auf das Konto des Kunden überweist.

4.3 HKR/ZÜV

Als HKR wird das IT-System für das Haushalts-, Kassen- und Rechnungswesen des Bundes bezeichnet. Das HKR unterstützt die Haushaltsführung sowie die Haushaltskontrolle, den so genannten Haushaltsvollzug. Nach Abschluss der Haushaltsplanungsphase werden die im Haushaltsgesetz festgelegten Ausgaben, Einnahmen und Verpflichtungsermächtigungen[51] in das HKR übertragen und den am Haushalt beteiligten Stellen zur Verfügung gestellt.

---

51 Unter einer Verpflichtungsermächtigung wird eine Erlaubnis verstanden, in einem Haushaltsjahr bis zu einer bestimmten Höhe Zahlungsverpflichtungen für kommende Haushaltsjahre einzugehen.

Aufgaben des HKR

Ebenso wie im Finanzbuchhaltungs-System eines Unternehmens sollen im HKR-System die Veränderungen der Kassenbestände, der Forderungen und Verpflichtungen sowie der Vermögensgegenstände des Bundes erfasst werden. Statt dem System der Doppik wird zur Darstellung jedoch das kameralistische Sachbuchkonto verwendet, das die folgenden fünf Betragsfelder enthält: die von der übergeordneten Behörde zugewiesenen Haushaltsmittel, die weiter verteilten Haushaltsmittel, die durch Zahlungsverpflichtungen (Verträge) gebundenen Mittel, die zur Annahme bzw. Zahlung angeordneten Beträge und die ein- bzw. ausgezahlten Beträge. Die zentrale Verarbeitung der von den einzelnen Behörden über verschiedene Zugangswege angeordneten Maßnahmen wie Zuweisungen, Zahlungen, Buchungen usw. findet beim Bundesamt für Finanzen statt. [BMF 2002]

Aufgaben des ZÜV

Das Zahlungsüberwachungsverfahren (ZÜV) ist ein Teilsystem des HKR-Systems, das ausschließlich die Einnahmenseite berücksichtigt. Im ZÜV-System erfolgt die Soll-Stellung fälliger Zahlungen, die Überwachung des Zahlungseingangs (§ 34 BHO) und z. B. bei der Lastschrift auch die Weiterleitung des Zahlungsauftrags an die Banken. Das ZÜV kann daher mit der Debitorenbuchhaltung eines Unternehmens verglichen werden. Erst nach dem Eingang der Zahlung wird eine Buchung auf dem zugehörigen Sachbuchkonto des HKR ausgelöst. Um eingehende Zahlungen den entsprechenden Forderungen direkt zuordnen zu können, wird jede Forderung durch ein eindeutiges Kassenzeichen identifiziert. Dieses Kassenzeichen muss deshalb z. B. auch auf dem Überweisungs- bzw. Lastschriftformular enthalten sein.

F-15Z-Verfahren

Die Übergabe von Daten an das ZÜV erfolgt mithilfe einer standardisierten Schnittstelle, dem F-15Z-Verfahren. Die zur Zahlungsabwicklung erforderlichen Daten werden dabei in den F-15Z-Datensatz eingetragen. Vorgesehene Felder dieses Datensatzes sind z. B. Nummer und Haushaltsstelle der betreffenden Behörde sowie Rechnungsadresse und Kontoverbindung des Kunden. Hinzu kommen transaktionsspezifische Daten wie der Kaufbetrag, die Währungsbezeichnung, das Fälligkeitsdatum oder das Kassenzeichen[52].

[52] Vgl. [BfF 2002, S. 60 ff.].

5 Kriterien zur Bewertung von Zahlungsverfahren

Ziel des Abschnitts

In diesem Abschnitt werden die Merkmale von Zahlungsverfahren aus Abschnitt 2 sowie die Kriterien zur Unterscheidung von Online-Transaktionen aus Abschnitt 3.1 wieder aufgegriffen. Ziel des folgenden Kriterienkatalogs ist es, aus der Vielzahl denkbarer Kriterien zur Beurteilung von Zahlungsverfahren bzw. Szenarien diejenigen zu benennen, die eine möglichst eindeutige Zuordnung von Zahlungsverfahren zu bestimmten Szenarien ermöglichen.

Kriterien-kategorien

Die Kriterien wurden im Kriterienkatalog zu vier Kriterienkategorien zusammengefasst: „Fachspezifische Anforderungen“, „Betragsbereich und Kostenstruktur“, „Sicherheitsanforderungen“ und „Anforderungen an die Integrierbarkeit in den E-Government-Prozess“ (Abbildung 5). Diese vier Kriterienkategorien bilden die Grundlage des in Abschnitt 7.1 näher beschriebenen Vorgehensmodells zur Auswahl eines Zahlungsverfahrens.

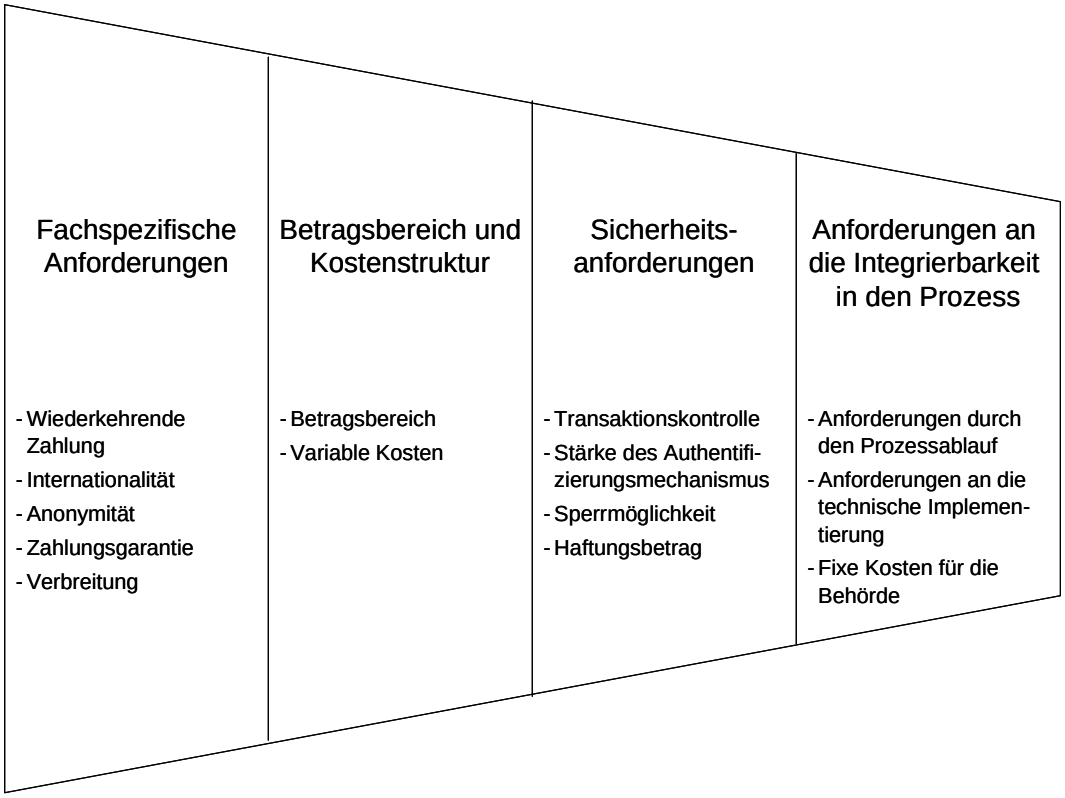


Abbildung 5: Übersicht über die Kriterienkategorien

5.1 Fachspezifische Anforderungen

In dieser Kriterienkategorie wird bewertet, für welche Anwendungsfälle ein Zahlungsverfahren unabhängig von den Kosten und den Sicherheitsanforderungen grundsätzlich geeignet ist. Betrachtet werden dabei im Einzelnen die Kriterien „Wiederkehrende Zahlung“, „Internationalität“, „Anonymität“, „Zahlungsgarantie“ und „Verbreitung“.

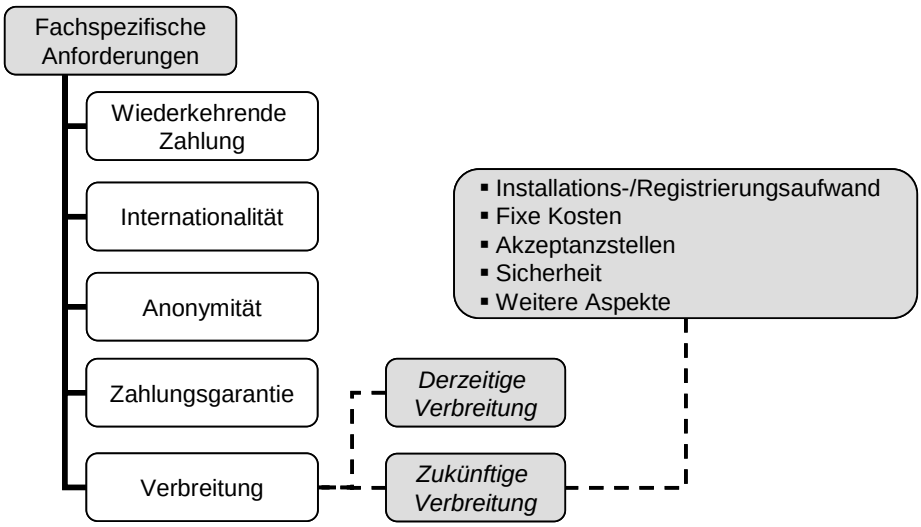


Abbildung 6: Kriterienkategorie "Fachspezifische Anforderungen"

5.1.1 Eignung für wiederkehrende Zahlungen

Wiederkehrende Zahlungen

Wie in Abschnitt 3.1.2 beschrieben, sollten periodisch wiederkehrende Zahlungen (z. B. Müllgebühren, Dauerfahrkarten) nicht jedes Mal erneut vom Kunden angestoßen werden müssen. Diese Möglichkeit bietet z. B. die Lastschrift, bei der die einzelnen Abbuchungen ohne aktives Zutun des Kunden erfolgen können. Ein weiteres Unterscheidungsmerkmal wäre, ob periodisch wiederkehrende Zahlungen in gleicher oder in wechselnder Höhe möglich sind, dies wird in diesem Kriterienkatalog jedoch aus Vereinfachungsgründen nicht berücksichtigt.

Kriterium: Wiederkehrende Zahlungen	
Ja	Periodisch wiederkehrende Zahlungen können automatisch ohne aktives Zutun des Kunden ausgeführt werden.
Nein	Periodisch wiederkehrende Zahlungen können nicht automatisch ohne aktives Zutun des Kunden ausgeführt werden.

Tabelle 2: Ausprägungen des Kriteriums „Wiederkehrende Zahlungen“

5.1.2 Internationalität

Internationalität

Mit dem Kriterium „Internationalität“ (vgl. Abschnitt 3.1.3) wird überprüft, mit welchem Aufwand das Zahlungsverfahren aus dem Ausland genutzt werden kann. Hinter diesem Kriterium steht die Annahme, dass bei einzelnen Szenarien eine

Nutzung auch aus dem Ausland ermöglicht werden soll. Beispielsweise könnte ein ausländisches Unternehmen, das in Deutschland investieren möchte, im Online-Shop des Statistischen Bundesamts Daten über die wirtschaftliche Entwicklung einer bestimmten Region erwerben wollen.

Bei der Bewertung dieses Kriteriums wird beispielsweise berücksichtigt, ob für die Nutzung des Verfahrens der Besitz eines Kontos in Deutschland notwendig ist, wie etwa bei der Lastschrift. Dies würde bedeuten, dass der Kunde zur Nutzung des Verfahrens aus dem Ausland anreisen müsste, um persönlich ein Konto zu eröffnen. In diesem Fall wäre die Internationalität des Verfahrens nicht gegeben. Das Kriterium wäre erfüllt, falls der Kunde über verschiedene Kommunikationsmedien, wie etwa Telefon, Telefax oder Internet, die Möglichkeit hat, sich für ein Zahlungsverfahren anzumelden, oder falls das Zahlungsverfahren auch im Ausland verbreitet ist.

Kriterium: Internationalität	
Ja	Der Kunde kann sich ohne größeren Aufwand im Ausland für das Zahlungsverfahren registrieren bzw. das Verfahren ist im Ausland verbreitet.
Nein	Der Kunde muss nach Deutschland reisen, um das Zahlungsverfahren nutzen zu können (z. B. zur Eröffnung eines Kontos).

Tabelle 3: Ausprägungen des Kriteriums „Internationalität“

5.1.3 Anonymität

Anonymität

Unter Anonymität wird die Anonymität gegenüber der Behörde verstanden, d. h. die Behörde kann aufgrund der durch das Zahlungsverfahren übermittelten Daten nicht feststellen, wer die Zahlung vorgenommen hat. Dieses Kriterium ist notwendig, um den in Abschnitt 3.1.5 erläuterten Forderungen nach Datensparsamkeit und Datenvermeidung nachzukommen. In Bezug auf das Szenario ist kein anonymes Zahlungsverfahren erforderlich, wenn der Name des Kunden für die Inanspruchnahme der Leistung erforderlich ist, z. B. bei Antragsverfahren oder wenn ein bestelltes Produkt auf dem Postweg zugesandt wird. In Bezug auf das Zahlungsverfahren ist das Kriterium der Anonymität auch dann erfüllt, wenn die Behörde ein Pseudonym des Nutzers, z. B. eine E-Mail-Adresse oder eine Telefonnummer, erfährt.

Kriterium: Anonymität	
Ja	Der Name des Nutzers wird nicht an die Behörde übermittelt.
Nein	Der Name des Nutzers wird an die Behörde übermittelt.

Tabelle 4: Ausprägungen des Kriteriums „Anonymität“

5.1.4 Zahlungsgarantie

Zahlungsgarantie

Die Kategorie Zahlungsgarantie beschäftigt sich mit der Fragestellung, ab welchem Zeitpunkt der Händler sicher sein kann, dass die Zahlung nicht aus vom Kunden zu vertretenden Gründen ausfällt. Nicht betrachtet werden Zahlungsausfälle, die z. B. dadurch entstehen, dass der Anbieter des Zahlungsverfahrens in-

solvent wird. Um auch dieses Risiko auszuschließen, müsste von der Behörde auch die Anbieterbonität in den Entscheidungsprozess einbezogen werden. Im Rahmen dieses Moduls kann eine objektive Beurteilung der Anbieterbonität jedoch nicht erfolgen.

Neben der Frage nach dem Zeitpunkt der Zahlungsgarantie ist für die Beurteilung des Zahlungsverfahrens von Bedeutung, welche Schadensszenarien zu einem Zahlungsausfall führen können. Sowohl der Zeitpunkt der Zahlungsgarantie als auch die möglichen Schadensszenarien werden im Folgenden bewertet. Wie in Abschnitt 3.1 beschrieben, hängt die Bedeutung des Kriteriums Zahlungsgarantie von der Höhe des Betrags, der Häufigkeit der Nutzung, den vorliegenden Nutzerdaten, der Art der Verwaltungsleistung und der Produktart (digital/physisch) ab.

Auch wenn sich die Bewertung nur auf elektronische Zahlungsverfahren bezieht, soll darauf hingewiesen werden, dass auch die klassische Bargeldzahlung keine vollständige Zahlungsgarantie bietet. So kann der Fall eintreten, dass die Behörde unbemerkt Falschgeld annimmt und dieses erst bei der Einreichung bei der Hausbank erkannt wird. Das Falschgeld wird dann ohne Ersatz eingezogen.

Kriterium: Zahlungsgarantie	
Hoch	Das Zahlungsverfahren bietet eine sofortige Zahlungsgarantie
Mittel	Die Zahlung könnte aus vom Kunden zu vertretenden Gründen nicht eingelöst werden (mangelnde Kontodeckung o.Ä.)
Gering	Die Zahlung könnte nicht eingelöst werden, weil der Kunde abstreitet, die Zahlung ausgelöst zu haben.

Tabelle 5: Ausprägungen des Kriteriums „Zahlungsgarantie“

5.1.5 Verbreitung

Das Kriterium „Verbreitung“ beschreibt die Anzahl der Kunden in Deutschland, die auf absehbare Zeit in der Lage sein werden, das Verfahren ohne größeren Aufwand zu nutzen. Bei der Zahlung mit der klassischen Kreditkarte wird die derzeitige Verbreitung beispielsweise anhand derjenigen Kunden gemessen, die bereits in Besitz einer Kreditkarte sind. Neben der Feststellung der derzeitigen Verbreitung sollen in die Bewertung des Kriteriums auch Entwicklungstendenzen bezüglich der zukünftigen Verbreitung des Zahlungsverfahrens einfließen.

Zukünftige Entwicklung

Die zukünftige Verbreitung eines Zahlungsverfahrens wird von verschiedenen Faktoren beeinflusst. Wichtig sind der Installations- und Registrierungsaufwand, die Kosten für den Kunden, die Anzahl der Akzeptanzstellen sowie die Sicherheit des Zahlungsverfahrens. Darüber hinaus können jedoch auch weitere Aspekte von Bedeutung sein.

Installations-/ Registrierungaufwand

Der Installations- und Registrierungsaufwand beschreibt den Aufwand, der für eine erstmalige Nutzung des Zahlungsverfahrens erforderlich ist. Dazu zählt zum einen die Anmeldung beim Anbieter des Zahlungsverfahrens, die in manchen Fällen online erfolgt, in anderen Fällen ein persönliches Erscheinen erfordert. Zum anderen wird hierunter der Aufwand für evtl. notwendige Hard- und Software-Installationen gefasst.

Kosten

Daneben spielen auch die transaktionsunabhängigen Kosten für den Kunden eine entscheidende Rolle. Darunter werden die Kosten gefasst, die dem Kunden ent-

stehen, ohne dass dieser Zahlungen tätigt. Dazu zählen sowohl einmalige Anschaffungskosten, z. B. für ein Kartenlesegerät, als auch periodisch wiederkehrende Kosten wie z. B. die Jahresgebühr für eine Kreditkarte. Die transaktionsabhängigen Kosten werden in Abschnitt 5.2 gesondert betrachtet.

Akzeptanzstellen

Ein weiterer Faktor, der die zukünftige Verbreitung eines Zahlungsverfahrens beeinflusst, ist die Anzahl der Akzeptanzstellen. Ist die Zahl der Akzeptanzstellen hoch, so sind die Kunden eher bereit, den Registrierungsaufwand in Kauf zu nehmen.

Sicherheit

Der Faktor Sicherheit beeinflusst ebenfalls die zukünftige Akzeptanz eines Zahlungsverfahrens. Wird ein Zahlungsverfahren von den Kunden als sicher wahrgenommen, so sind diese zur Nutzung des Verfahrens eher bereit.

Weitere Aspekte

Neben den bisher genanten Einflussfaktoren können sich auch weitere Aspekte auf die zukünftige Verbreitung eines Zahlungsverfahrens auswirken. Beispielsweise wird die Umstellung der öffentlichen Zigarettenautomaten auf die ausschließliche Nutzung mit der GeldKarte die Verbreitung dieses Zahlungsverfahrens vermutlich positiv beeinflussen.

Unter Berücksichtigung aller genannten Faktoren muss anschließend eine Einschätzung der Verbreitung vorgenommen werden. Die Bewertung erfolgt in den Stufen hoch, mittel und gering.

Nicht für jedes Szenario ist eine hohe Verbreitung erforderlich. So dürfte ein gering verbreitetes Zahlungsverfahren ausreichen, wenn ein Szenario nur von einer begrenzten Nutzergruppe (z. B. Rechtsanwälte), von dieser jedoch regelmäßig genutzt wird (vgl. Abschnitt 3.1.2). Die Verbreitung des Zahlungsverfahrens sollte hingegen „hoch“ sein, wenn das Szenario nur sehr selten von einer breiten Nutzergruppe in Anspruch genommen wird, von jedem einzelnen Nutzer jedoch nur selten.

Kriterium: Verbreitung	
Hoch	Das Zahlungsverfahren wird auf absehbare Zeit von sehr vielen Kunden verwendet.
Mittel	Das Zahlungsverfahren wird auf absehbare Zeit nur von einem Teil der Kunden verwendet.
Gering	Das Zahlungsverfahren wird auf absehbare Zeit nur von sehr wenigen Kunden verwendet.

Tabelle 6: Ausprägungen des Kriteriums „Verbreitung“

5.2 Betragsbereich und Kostenstruktur

Anhand der Kriterien dieser Kategorie wird untersucht, ob die Zahlungsverfahren für die in einem Szenario zu zahlenden Beträge geeignet sind (vgl. Abschnitt 3.1.1). Dies ist nur dann der Fall, wenn weder system- oder nutzerbedingte Beschränkungen gegen die Nutzung des Verfahrens für relevante Betragsbereiche sprechen noch in diesen Betragsbereichen unverhältnismäßig hohe transaktionsabhängige Kosten auftreten.

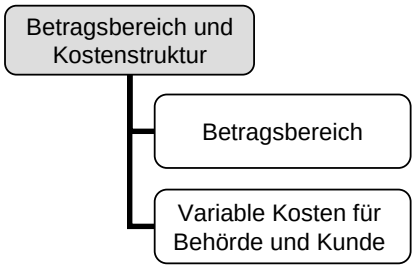


Abbildung 7: Kriterienkategorie "Betragsbereich und Kostenstruktur"

5.2.1 Betragsbereich

Betragsspektrum

Anhand des Kriteriums „Betragsbereich“ wird bewertet, welche Beträge mit dem Zahlungsverfahren grundsätzlich beglichen werden können. Der Betragsbereich kann durch system- oder nutzerabhängige Faktoren begrenzt sein. Ein systemabhängiger Betragsbereich ist beispielsweise bei der Geldkarte gegeben, bei der nur Zahlungen von 0,01 bis 200 Euro möglich sind. Bei Verfahren wie der Überweisung ist die Bereichsuntergrenze auf 0,01 Euro festgelegt, die Obergrenze hängt jedoch von nutzerabhängigen Faktoren ab. Dazu zählen der Kontostand, der eingeräumte Überziehungsrahmen (Kontokorrentkredit) sowie durch den Bankkunden festlegbare Limits für die maximale Betragshöhe einer einmaligen Transaktion.

Kriterium: Betragsbereich	
Von € bis €	Betragshöhe, die aufgrund system- bzw. nutzerbedingter Beschränkungen nicht über- bzw. unterschritten werden kann.

Tabelle 7: Ausprägungen des Kriteriums „Betragsbereich“

5.2.2 Variable Kosten für Behörde und Kunde

Transaktions- oder betrags-abhängige Kosten

Variable Kosten können sich entweder auf die Zahl der Transaktionen oder auf die Höhe der bezahlten Beträge beziehen. Beispielsweise werden im Rahmen einer GeldKarte-Transaktion 0,3% des Umsatzes, mindestens aber 0,01 Euro fällig. Bei Kreditkartenzahlungen ist üblicherweise neben einem betragsabhängigen Di-

sagio[53] bei jeder Autorisierungsanfrage eine betragsunabhängige Gebühr zu zahlen.

Die transaktionsabhängigen Kosten werden im Folgenden für unterschiedliche Betragshöhen dargestellt.

Kriterium: Variable Kosten		
Für den Kunden	Für die Behörde	Kosten pro Transaktion bei einem Betrag von
€	€	0,05 €
€	€	0,50 €
€	€	5,00 €
€	€	50,00 €
€	€	500,00 €
€	€	5.000,00 €
€	€	50.000,00 €

Tabelle 8: Ausprägungen des Kriteriums „Variable Kosten“

5.3 Sicherheitsanforderungen

Unter den Sicherheitsanforderungen werden im Folgenden organisatorische und rechtliche Aspekte berücksichtigt, die dazu geeignet sind, das Eintreten von Schäden aus Kundensicht zu verhindern. Dabei handelt es sich um die Anforderungen Transaktionskontrolle, Stärke des Authentifizierungsmechanismus, Sperrmöglichkeit und maximaler Haftungsbetrag.

Die Vermeidung möglicher Schäden aus Behördensicht wurde bereits beim Kriterium „Zahlungsgarantie“ betrachtet. Sicherheitsanforderungen, die bei der technischen Implementierung des Zahlungsverfahrens zu beachten sind, werden in Abschnitt 5.4.2 dargestellt.

53 Unter einem Disagio versteht man eine Gebühr (Abgeld, Abschlag) z. B. für Kreditkartenzahlungen.

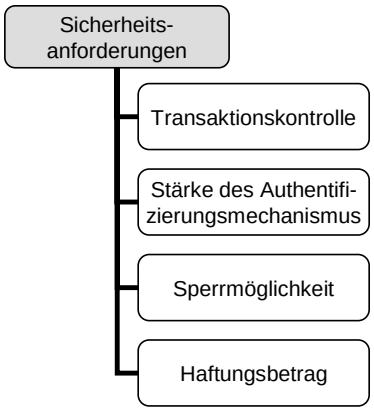


Abbildung 8: Kriterienkategorie „Sicherheitsanforderungen“

5.3.1 Transaktionskontrolle

Zwei Aspekte

Hinsichtlich der bei einem Zahlungsverfahren gebotenen Möglichkeiten zur Transaktionskontrolle sind aus Kundensicht zwei Aspekte von Bedeutung. Der Kunde möchte zum einen sicher sein, dass eine von ihm gewünschte Transaktion erfolgreich initiiert wurde. Zum anderen möchte er kontrollieren können, dass keine unberechtigte Transaktion durchgeführt wurde.

Bestätigung

Bei der Beurteilung der Anforderung „Transaktionskontrolle“ wird deshalb zum einen bewertet, ob der Kunde eine zeitnahe Transaktionsbestätigung erhält. Eine solche Bestätigung ist z. B. wichtig, damit der Kunde weiß, ob die Zahlung bei einem Rechnerabsturz oder einem Abbruch der Verbindung bereits initiiert wurde oder nicht. Dazu könnte dem Kunden die Möglichkeit gegeben werden, den Status jederzeit selbstständig einzusehen oder es könnte z. B. ein telefonischer Support eingerichtet werden.

Nachträglich Kontrolle über durchgeführte Zahlungen

Um unberechtigt durchgeführte Transaktionen erkennen zu können, ist eine Übersicht über die einzelnen durchgeführten Zahlungen erforderlich. Der von Kreditinstituten bereitgestellte Kontoauszug stellt beispielsweise ein Kontrollinstrument dar, wodurch unberechtigt durchgeführte Lastschriften erkannt werden können.

Kriterium: Transaktionskontrolle	
Hoch	Der Kunde erhält sowohl eine zeitnahe Transaktionsbestätigung als auch eine Übersicht der einzelnen getätigten Zahlungen.
Mittel	Der Kunde erhält entweder eine zeitnahe Transaktionsbestätigung oder eine Übersicht der einzelnen getätigten Zahlungen.
Gering	Der Kunde erhält weder eine zeitnahe Transaktionsbestätigung noch eine Übersicht der einzelnen getätigten Zahlungen.

Tabelle 9: Ausprägungen des Kriteriums „Transaktionskontrolle“

5.3.2 Stärke des Authentifizierungsmechanismus

Möglichkeiten der Authentifizierung

Die Stärke des Authentifizierungsmechanismus gibt Hinweise darauf, wie leicht es für einen Dritten sein kann, unberechtigt Zahlungen zu Lasten des Kunden zu initiieren. Grundsätzlich bestehen drei Möglichkeiten, um sich zu authentifizieren: Durch Besitz (z. B. der GeldKarte), Wissen (z. B. der Firstgate-PIN) oder persön-

liche Eigenschaften (bei biometrischen Authentifizierungsmechanismen). Aufgrund der bisher geringen Verbreitung biometrischer Authentifizierungsmechanismen werden im Folgenden nur die Ausprägungen „Besitz“ und „Wissen“ betrachtet.

Qualitätsstufen der Authentifizierung

Bei keiner der beiden grundsätzlichen Authentifizierungsmöglichkeiten „Besitz“ oder „Wissen“ ist es vollkommen ausgeschlossen, dass ein Dritter unberechtigt Zahlungen zu Lasten des Kunden initiieren kann. So kann ein Besitzmerkmal wie eine Karte oder ein Mobiltelefon durch Verlust oder Diebstahl in die Gewalt eines Dritten übergehen. Ein Wissensmerkmal könnte bei unzureichenden (technischen oder organisatorischen) Sicherheitsmaßnahmen z. B. mittels Trojanischer Pferde[54] ausgespäht werden. Zudem besteht die Problematik, dass von den Kunden entweder leicht zu ermittelnde Passwörter verwendet oder sichere Passwörter notiert und für andere Personen zugänglich aufbewahrt werden. Durch die Kombination von Authentifizierungsmechanismen („Zwei-Faktor-Authentifizierung“) lässt sich die Stärke der Authentifizierung steigern.[55]

Kriterium: Stärke des Authentifizierungsmechanismus	
Hoch	Zwei-Faktor-Authentifizierung: Der Authentifizierungsmechanismus beruht sowohl auf Besitz als auch auf Wissen.
Mittel	Ein-Faktor-Authentifizierung: Der Authentifizierungsmechanismus beruht entweder auf Besitz oder auf Wissen.
Gering	Der Authentifizierungsmechanismus beruht auf einem Wissensmerkmal, das nicht ausreichend geheim ist (z. B. Kontonummer und BLZ bei Lastschrift, Kreditkartennummer).

Tabelle 10: Ausprägungen des Kriteriums „Stärke des Authentifizierungsmechanismus“

5.3.3 Sperrmöglichkeit

Sperrmöglichkeit

Eine Möglichkeit zum Schutz vor einer missbräuchlichen Nutzung eines Zahlungsverfahrens ist die Sperre gegen zukünftige Verfügungen zu Lasten des Kunden. Selbst wenn ein Dritter also über die erforderlichen Besitz- bzw. Wissensmerkmale verfügt, sind Schäden für den Kunden in diesem Fall ausgeschlossen. Voraussetzung ist jedoch, dass der Kunde davon erfährt, dass ein Dritter möglicherweise zur Nutzung des Zahlungsverfahrens in der Lage ist, z. B. wenn der Kunde den Verlust der Karte bemerkt oder er bei der Transaktionskontrolle unberechtigte Transaktionen feststellt.

54 „Trojanische Pferde sind Programme, die neben scheinbar nützlichen auch nicht dokumentierte, schädliche Funktionen enthalten und diese unabhängig vom Computer-Anwender und ohne dessen Wissen ausführen. Im Gegensatz zu Computer-Viren können sich Trojanische Pferde jedoch nicht selbständig verbreiten.“ [BSI 2003, S. 1]

55 Weitere Informationen zu Authentisierung und Authentifizierung finden sich im Modul „Authentisierung im E-Government“.

Kriterium: Sperrmöglichkeit	
Ja	Der Kunde kann die zukünftige Nutzung des Zahlungsverfahrens ohne größere Verzögerungen verhindern.
Nein	Die zukünftige Nutzung des Zahlungsverfahrens kann nicht oder nur mit größerer Verzögerung verhindert werden.

Tabelle 11: Ausprägungen des Kriteriums „Sperrmöglichkeit“

5.3.4 Haftungsbetrag

Haftungsbetrag

Mittels des Kriteriums „Haftungsbetrag“ wird bewertet, für welchen Betrag der Kunde maximal aufkommen muss, wenn vor einer eventuellen Sperre unberechtigte Verfügungen zu seinen Lasten vorgenommen wurden[56]. Darüber hinausgehende Beträge werden vom Anbieter des Zahlungsverfahrens dagegen auf Verlangen zurückgebucht.

Der maximale Haftungsbetrag ist bei einigen Zahlungsverfahren als Geldbetrag in Euro festgesetzt. So ist bei der klassischen Kreditkartenzahlung der Haftungsbetrag häufig auf 50 Euro beschränkt[57]. Bei den meisten Verfahren ist er jedoch von anderen Betragsgrößen abhängig, deren Höhe sich je nach Kunde unterscheiden und häufig vom Kunden selbst beeinflusst werden kann. Bei E-Mail-basierten Verfahren hängt der maximale Haftungsbetrag z. B. vom Guthaben auf dem Verrechnungskonto ab. Über die Sicherheit des Zahlungsverfahrens kann in Bezug auf den Haftungsbetrag dann keine eindeutige Aussage getroffen werden, da der Kunde die Entscheidung zwischen Sicherheit und Bequemlichkeit bzw. Kosten der Nutzung selbst trifft. So müsste das Guthaben auf dem Verrechnungskonto aus Sicherheitsaspekten möglichst niedrig gehalten werden, was jedoch häufige Transfers zum Aufladen des Verrechnungskontos zur Folge hätte.

Kriterium: Maximaler Haftungsbetrag	
€	Der Kunde haftet maximal bis zu einem bestimmten Betrag.
Abhängig von	Der Haftungsbetrag ist von einer anderen Betragsgröße abhängig (z.B. Kontostand, Limit).

Tabelle 12: Ausprägungen des Kriteriums „Maximaler Haftungsbetrag“

5.4 Anforderungen an die Integrierbarkeit in den E-Government-Prozess

In der vierten Kriterienkategorie werden schließlich Anforderungen betrachtet, die in hohem Maße von den konkreten Rahmenbedingungen der implementierenden

56 Für durchgeführte Verfügungen seitens des Zahlungsanbieters nach einer erfolgten Sperrung haftet in der Regel der Anbieter selbst.

57 Das kartenherausgebende Institut regelt den Haftungsbetrag in speziellen Bedingungen, die je nach Institut variieren können. Aus missbräuchlichen Verfügungen im Internet, die allein auf Kenntnis der Kreditkartendaten beruhen, entsteht nach den geltenden Regelungen kein Haftungsrisiko für den Karteninhaber.

Behörde abhängig sind. Im Gegensatz zu den vorhergehenden Kriterienkategorien können für diese Anforderungen keine allgemein gültigen Aussagen zu den Zahlungsverfahren getroffen werden. Gleichwohl sind sie bei der Auswahl eines geeigneten Zahlungsverfahrens für ein konkretes Szenario zu berücksichtigen. Im Einzelnen sind dies die Anforderungen, die sich durch den Prozessablauf und die technische Implementierung ergeben. Hinzu kommen die fixen Kosten für die Behörde, die ebenfalls in hohem Maße von behördenindividuellen Faktoren, wie etwa den nötigen Aufwendungen für die Integration des Verfahrens in die Systemlandschaft der Behörde, abhängig sind.

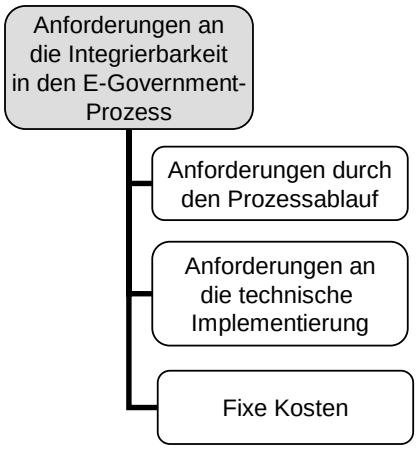


Abbildung 9: Kriterienkategorie "Anforderungen an die Integrierbarkeit in den E-Government-Prozess“

5.4.1 Anforderungen durch den Prozessablauf

Unter den Anforderungen durch den Prozessablauf werden die Anforderungen betrachtet, die sich aus der Abstimmung des konkreten E-Government-Prozesses mit dem Zahlungsablauf des Zahlungsverfahrens ergeben. Wichtig ist dabei vor allem die Frage, zu welchem Zeitpunkt die Zahlung im Prozess erfolgt (vgl. Abschnitt 3.1.4) und wie lange die vollständige Abwicklung der Zahlung dauert. Dabei gilt eine Zahlung dann als vollständig abgewickelt, wenn die Behörde eine Bestätigung über den Eingang der Zahlung erhalten hat und die Zahlung nicht mehr rückgängig gemacht werden kann, d. h. wenn für die Behörde eine Zahlungsgarantie eintritt. Die Anforderungen durch den Prozessablauf können zum Ausschluss von Zahlungsverfahren führen, wenn das Verfahren zwar eine Zahlungsgarantie bietet, die Zahlung bei diesem Verfahren jedoch erst sehr spät im Prozess ausgelöst wird (ein Beispiel hierfür wäre die Zahlung per Nachnahme). Die Anforderungen durch den Prozessablauf sind auch dann nicht erfüllt, wenn der Prozess zur Abwicklung der Zahlung zu lange unterbrochen wird (bei der Überweisung z. B. zwei bis drei Bankarbeitstage). Bei einigen E-Government-Prozessen ist es zudem erforderlich, bei der Bezahlung ein Kassenzeichen zu übermitteln, was nicht bei allen Zahlungsverfahren möglich ist.

5.4.2 Anforderungen an die technische Implementierung

Bei der Ermittlung von Anforderungen an ein Zahlungsverfahren ist zwischen den Eigenschaften des Zahlungsverfahrens selbst und den Anforderungen an die technische Implementierung zu trennen. In den Abschnitten 5.1 bis 5.3 wurden ausschließlich die Eigenschaften der Zahlungsverfahren bewertet. Die meisten Verfahren lassen jedoch Freiheitsgrade bei der Integration zu, sodass sich einige Anforderungen, insbesondere in den Bereichen Sicherheit, Datenschutz und Zukunftsfähigkeit, nicht eindeutig bewerten lassen. Diese Anforderungen werden im Folgenden näher vorgestellt. Zudem werden Empfehlungen für die bestmögliche Erfüllung dieser Anforderungen bei der technischen Implementierung der Zahlungsverfahren gegeben.

Schutzziele der Informations-sicherheit

Im Bereich der Sicherheit sind insbesondere die Schutzziele Vertraulichkeit, Integrität und Authentizität sowie Verfügbarkeit der Systeme von Bedeutung. Vertraulichkeit, Integrität und Authentizität sind dabei wie folgt definiert:

- Vertraulichkeit bedeutet, dass Daten nicht durch Unbefugte eingesehen werden können.
- Integrität der Daten bedeutet, dass diese bei der Übertragung unversehrt bleiben und nicht verändert werden bzw. dass eine Veränderung bemerkt werden kann.
- Unter Authentizität versteht man, dass die Daten tatsächlich von dem vermeintlichen Kommunikationspartner stammen bzw. der Kommunikationspartner derjenige ist, der er vorgibt zu sein.[58]

Zur Erfüllung dieser Sicherheitsanforderungen kann die Kommunikation zwischen Rechnern im Internet durch kryptographische Verfahren abgesichert werden. Solche Verfahren nutzt z. B. „Secure Sockets Layer“ (SSL). Bei der Verwendung des SSL-Protokolls wird die Vertraulichkeit der Daten durch Verschlüsselung und die Integrität der Daten durch sog. „Message Authentication Codes“ (MAC)[59] gewährleistet. Zudem werden bei SSL Server-Zertifikate eingesetzt, anhand derer die Authentizität des Servers überprüft werden kann.

Absicherung von Verbindungen

Eine solche Absicherung der Verbindung zwischen Kunde und Online-Shop sowie der Verbindung zwischen dem Online-Shop und weiteren beteiligten Systemen (ZVP, HKR/ZÜV) wird generell empfohlen, wenn sensible Daten über das Internet übertragen werden.[60] Der Grad der Authentizität der Daten ist zudem

---

58 Zu „Sicherheitsanforderungen bei der elektronischen Kommunikation“ vgl. das Modul „Verschlüsselung und Signatur“ sowie das IT-Grundschutzhandbuch.

59 Der „Message Authentication Code“ wird vom Sender aus der Nachricht und einem geheimen Schlüssel errechnet, der nur dem Sender und dem Empfänger der Nachricht bekannt ist. Der Empfänger erhält die Nachricht und den MAC und kann durch Neuberechnung des MAC überprüfen, ob die Nachricht verändert wurde.

60 Vgl. dazu die Module „Leitfaden für die Einrichtung einer Internetvertriebsplattform (E-Shop)“, „Sicherer Internetauftritt im E-Government“ und „Sichere Client-Server-Architekturen für E-Government“.

vom Authentifizierungsmechanismus des Zahlungsverfahrens abhängig, auf den in Abschnitt 5.3.2 bereits eingegangen wurde.

Verfügbarkeit von Systemen

Ein weiteres Schutzziel im Bereich der Sicherheit ist die Verfügbarkeit der beteiligten Systeme. Sowohl auf Seite der Behörde als auch auf Seite des Anbieters des Zahlungsverfahrens muss die Abwicklung von Zahlungen möglichst jederzeit gewährleistet sein, um die Durchführbarkeit der E-Government-Dienstleistung nicht zu beeinträchtigen. Hinsichtlich der beteiligten Systeme auf Behördenseite sind dazu insbesondere die Empfehlungen des IT-Grundschutzhandbuchs[61] zu beachten. Mit dem Anbieter kann in der Regel in einem so genannten Service-Level-Agreement (SLA) vertraglich eine bestimmte Mindest-Verfügbarkeit vereinbart werden. Bei Nichteinhaltung dieser Mindest-Verfügbarkeit können dann Ansprüche gegen den Anbieter geltend gemacht werden.

Datenschutzrechtliche Anforderungen

Anforderungen im Bereich des Datenschutzes ergeben sich dann, wenn bei der Implementierung des Zahlungsverfahrens die Erhebung, Speicherung oder Verarbeitung personenbezogener Daten (z. B. E-Mail-Adresse, Bankverbindung, Kreditkartennummer, User-ID) in den Systemen der Behörde erforderlich ist. Diese Anforderungen ergeben sich insbesondere aus dem Bundesdatenschutzgesetz (BDSG), dem Teledienstegesetz (TDG), dem Teledienstedatenschutzgesetz (TDDSG) sowie dem Mediendienstestaatsvertrag (MDStV). Eine detaillierte Darstellung der datenschutzrechtlichen Anforderungen sowie der erforderlichen Maßnahmen zur Erfüllung dieser Anforderungen findet sich im Modul „Datenschutzgerechtes E-Government“.

Zukunftsfähigkeit der Implementierung

Schließlich ist auch auf die erforderliche Zukunftsfähigkeit der Implementierung hinzuweisen. Es sollte insbesondere darauf geachtet werden, dass vorhandene Standards sowie Leitlinien eingehalten werden, damit eine möglichst reibungslose Integration in die bestehende Systemumgebung, sowie eine entsprechende Flexibilität bei zukünftigen Entwicklungen und die Möglichkeit zur weiteren Vernetzung gewährleistet sind.

Um dies zu ermöglichen, wurden im Rahmen von BundOnline 2005 relevante Standards und Architekturen für E-Government-Anwendungen (SAGA[62]) festgehalten. SAGA identifiziert erforderliche Standards, Formate und Spezifikationen, legt dafür Konformitätsregeln fest und schreibt diese entsprechend den technologischen Entwicklungen fort. Entscheidungsträgern in der öffentlichen Verwaltung wird damit eine Orientierungshilfe bei der technischen Umsetzung geboten.

5.4.3 Fixe Kosten für die Behörde

Fixe Kosten setzen sich aus einmaligen Kosten für die Inbetriebnahme und wiederkehrenden Kosten für den Betrieb des Zahlungsverfahrens zusammen. Kosten für die Inbetriebnahme können beispielsweise durch Installation oder Anpassung

---

61 Nähere Informationen zum IT-Grundschutzhandbuch finden sich unter http://www.it-grundschutzhandbuch.de/.

62 Weitere Informationen finden sich im Modul „SAGA – Standards und Architekturen für E-Government-Anwendungen“ sowie unter http://www.kbst.bund.de/Anlage304423/SAGA_Version_2.0.pdf.

von Software, durch Erwerb von Hardware oder durch die Integration in die Systemumgebung der Behörde anfallen. Dabei sind sowohl Personalkosten als auch sonstige Kosten zu beachten.

Betriebskosten

Betriebskosten stellen wiederkehrende Kosten zur Aufrechterhaltung der Betriebsbereitschaft dar. Dies können z. B. periodisch anfallende Kosten für die Bereitstellung einer Datenleitung sein.

Die Höhe der fixen Kosten eines Zahlungsverfahrens ist in hohem Maße von den Gegebenheiten der Behörde abhängig. Im Rahmen dieses Moduls können zu den Kosten der Zahlungsverfahren deshalb nur sehr unvollständige Angaben gemacht werden. Zu berücksichtigen sind insbesondere:

- Lizenzkosten,
- Kosten für Payment-Service-Provider[63],
- Kosten für Hard- und Software,
- Zertifikatskosten,
- Installationskosten,
- Integrationskosten,
- Kommunikationskosten,
- Betriebskosten.

63 Der Payment Service Provider realisiert bei Kreditkartenzahlungen die technische Anbindung der Behörde an den Acquirer und verarbeitet die einzelnen Transaktionen.

6 Beschreibung und Bewertung der Zahlungsverfahren

In diesem Abschnitt werden ausgewählte Zahlungsverfahren anhand des Kriterienkatalogs bewertet. Detaillierte Erläuterungen zu den einzelnen Bewertungen finden sich im Anhang des Moduls. Aus jeder der in Abschnitt 2 vorgestellten Kategorien von Zahlungsverfahren wird dabei mindestens ein Verfahren betrachtet. Eine Ausnahme stellen Scheck-basierte Verfahren dar, da derzeit keine elektronische Variante des Schecks existiert. Auch der papiergebundene Scheck hat stark an Bedeutung verloren, zudem können die Ausführungen zur Überweisung vor bzw. nach Lieferung weitgehend auf den Scheck übertragen werden.

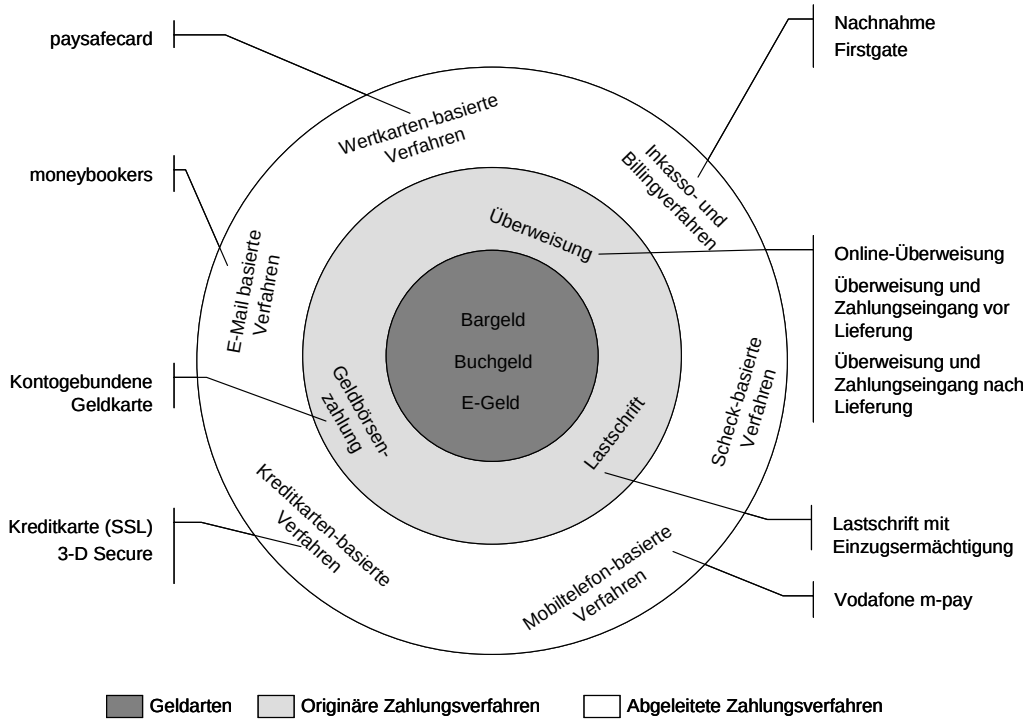


Abbildung 10: Bewertete Zahlungsverfahren

6.1 Bewertung der einzelnen Zahlungsverfahren

Die einzelnen Zahlungsverfahren werden im Folgenden kurz vorgestellt und anhand der in Abschnitt 5 vorgestellten Kriterien beurteilt. Die Bewertung der einzelnen Zahlungsverfahren ist jeweils in einer Tabelle zusammengefasst. Die Beurteilung der Einzelkriterien kann für jedes Zahlungsverfahren dem entsprechenden Abschnitt des Anhangs entnommen werden.

6.1.1 Geldbörsenzahlung

System der GeldKarte

Das GeldKarte-System[64] ist das derzeit in Deutschland am weitesten verbreitete Geldbörsensystem. Es wird von der deutschen Kreditwirtschaft herausgegeben und beruht auf der Speicherung elektronischer Geldeinheiten auf einem Chip. Die GeldKarte-Funktion wird durch die Kreditinstitute zunehmend auf den von ihnen ausgegebenen Kundenkarten (Chipkarten) für den Kunden zur Verfügung gestellt.

GeldKarte-System aus Kundensicht

Um über Geldeinheiten auf dem Chip verfügen zu können, muss die Chipkarte durch den Kunden an einem dafür vorgesehenen Ladeterminal (unter Verwendung der Karten-PIN) geladen werden. Der Ladebetrag wird von dem mit der GeldKarte verbundenen Kundenkonto (kontogebundene GeldKarte) abgebucht und auf dem Chip gutgeschrieben; anschließend steht der geladene Betrag für Zahlungen zur Verfügung. Zur Zahlung im Internet benötigt der Kunde einen geeigneten Kartenleser.

GeldKarte-System aus Behördensicht

Die Behörde benötigt als Gegenstück zur GeldKarte (Chipkarte) des Kunden eine so genannte Händlerkarte. Diese dient als Gegenbuchungsstelle zur GeldKarte des Kunden. Im Rahmen des Bezahlvorgangs führt der Kunde seine GeldKarte in den Kartenleser ein und bestätigt (ohne Eingabe einer PIN) den zu zahlenden Betrag, der ihm im Display des Kartenlesers angezeigt wird. Der Betrag wird sofort vom Guthaben der Kundenkarte abgebucht, die Daten über das Internet übertragen und auf die Händlerkarte aufgebucht. Anschließend reicht die Behörde die auf der Händlerkarte gespeicherten Umsätze bei ihrem Kreditinstitut zur Gutschrift auf dem mit der Händlerkarte verbundenen Konto ein.

---

64 Detaillierte Informationen zum System der GeldKarte sind unter http://www.geldkarte.de/ verfügbar.

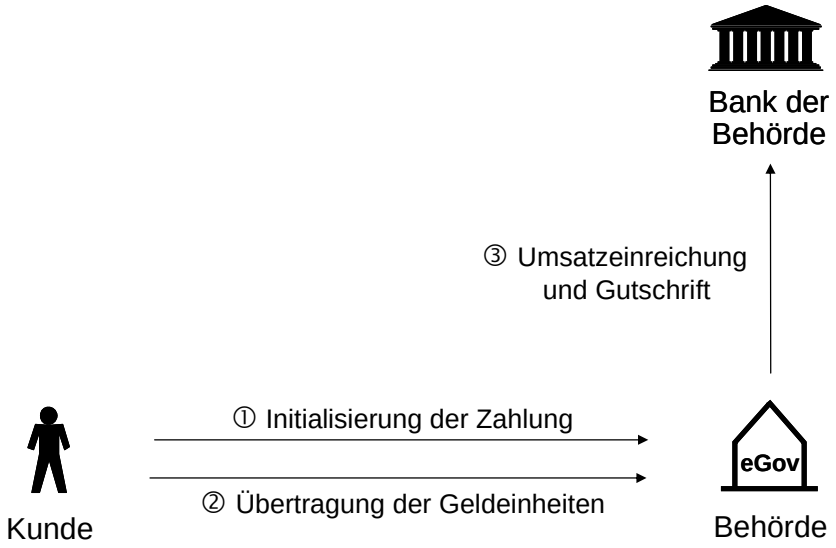


Abbildung 11: Ablauf einer GeldKarte-Zahlung

Zahlungsverfahren: Kontogebundene GeldKarte

Fachspezifische Anforderungen			
Wiederkehrende Zahlung	**nein**		ja
Internationalität	**nein**		ja
Anonymität	nein		**ja**
Zahlungsgarantie	gering	mittel	**hoch**
Verbreitung	**gering**	mittel	hoch
Kostenstruktur			
Betragsbereich	0,01 bis max. 200 Euro (in der Regel nicht mehr als ca. 30 Euro Guthaben)		
Variable Kosten der Behörde bei Betrag von	Prozent		Euro
Umsatz: 0,05 €	**20,0%**		**0,01**
Umsatz: 0,50 €	**2,0%**		**0,01**
Umsatz: 5,00 €	**0,3%**		**0,015**
Umsatz: 50,00 €	**0,3%**		**0,15**
Umsatz: 500,00 €	nicht möglich		
Umsatz: 5.000,00 €	nicht möglich		
Umsatz: 50.000,00 €	nicht möglich		
Fixe Kosten der Behörde in Euro (nur eindeutig zuordenbare Kosten; vgl. Abschnitt 5.4.3)	einmalig		jährlich
Betrag	**0**		**0**
Sicherheit			
Transaktionskontrolle	gering	mittel	**hoch**
Stärke des Authentifizierungsmechanismus	gering	**mittel**	hoch
Sperrmöglichkeit	**nein**		ja
Haftungsbetrag	**Kartenguthaben (max. 200 Euro)**		

Stand: Mai 2005

Tabelle 13: Zusammenfassende Bewertung „Kontogebundene GeldKarte“

6.1.2 Online-Überweisung

Eine Vielzahl von Banken und Sparkassen bieten ihren Privatkunden die Möglichkeit, Bankkonten online über das Internet zu führen. Die durch das Internet-Banking verbreitete Online-Überweisung kann zur Initiierung des Zahlungsauftrags für eine Dienstleistung der Behörde eingesetzt werden. Beispielhaft soll hier auf das von der Postbank angebotene Zahlungsverfahren Postbank Online-Überweisung eingegangen werden. Daneben existieren weitere Anbieter, die ebenfalls die Online-Überweisung zur Verfügung stellen. Eine Auswahl kann Anhang A.12 entnommen werden.

Ablauf der Postbank Online-Überweisung

Bei der Postbank Online-Überweisung wird der Kunde im Rahmen des Bezahlvorgangs auf die Internet-Banking-Webseite der Postbank umgeleitet und es wird ein bereits mit den entsprechenden Überweisungsdaten (Kontoverbindungsdaten des Zahlungsempfängers, Betrag und Verwendungszweck) vorausgefülltes unveränderliches Formular präsentiert. Durch Eingabe seiner PIN und TAN beauftragt der Kunde seine Bank, die Überweisung auszuführen. Damit ist der Vorgang für den Kunden abgeschlossen. Bankenseitig liegt der Überweisungsauftrag elektronisch vor und kann von den Systemen der Bank automatisiert weiterverarbeitet werden. Die Bank übermittelt abschließend an die Behörde eine Bestätigung der Auftragsannahme. Der Zahlungsauftrag wird wie eine gewöhnliche Überweisung behandelt und ist erst vollständig abgewickelt, sobald die Behörde die Gutschrift auf ihrem Konto erhält.

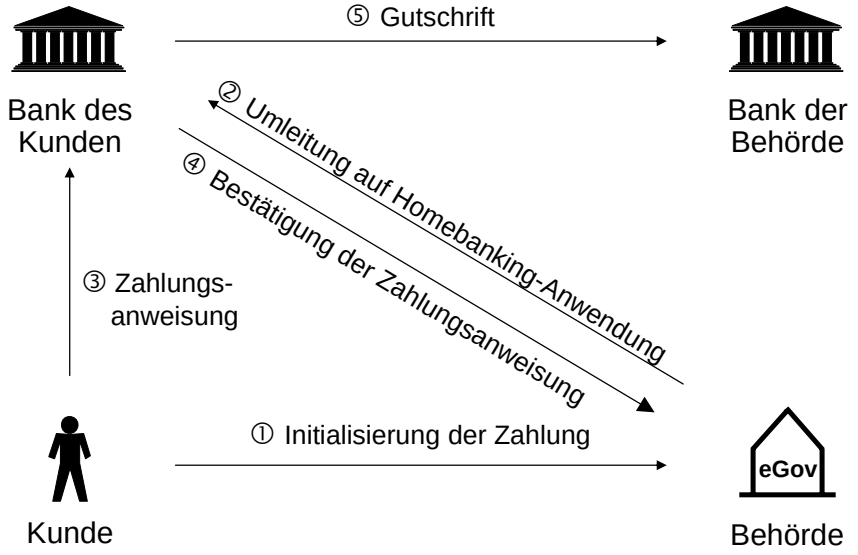


Abbildung 12: Ablauf einer Online-Überweisung

Zahlungsverfahren: Postbank Online-Überweisung

Fachspezifische Anforderungen			
Wiederkehrende Zahlung	**nein**		ja
Internationalität	**nein**		ja
Anonymität	**nein**		ja
Zahlungsgarantie	gering	**mittel**	hoch
Verbreitung	gering	**mittel**	hoch
Kostenstruktur			
Betragsbereich	0,01 Euro bis Verfügungsrahmen		
Variable Kosten der Behörde bei Betrag von	Prozent		Euro
Umsatz 0,05 €	**2%**[65]		**0,001**
Umsatz 0,50 €	**2%**		**0,01**
Umsatz 5,00 €	**2%**		**0,10**
Umsatz 50,00 €	**2%**		**1,00**
Umsatz 500,00 €	**2%**		**10,00**
Umsatz 5.000,00 €	**2%**		**100,00**
Umsatz 50.000,00 €	**2%**		**1.000,00**
Fixe Kosten der Behörde in Euro (nur eindeutig zuordenbare Kosten; vgl. Abschnitt 5.4.3)	einmalig		jährlich
Betrag	**0**		**0**
Sicherheit			
Transaktionskontrolle	gering	mittel	**hoch**
Stärke des Authentifizierungsmechanismus	gering	mittel	**hoch**
Sperrmöglichkeit	nein		**ja**
Haftungsbetrag	**Verfügungsrahmen**		

Stand: Mai 2005

Tabelle 14: Zusammenfassende Bewertung „Postbank Online-Überweisung“

6.1.3 Überweisung (Zahlungseingang vor/nach Lieferung)

Zwei Varianten der Überweisung

Im Rahmen dieser Studie werden bei der Überweisung zwei Varianten unterschieden. Zum einen kann die Behörde mit der Leistungserbringung warten, bis die Überweisung getätigt und das Geld auf dem Konto der Behörde eingegangen ist. Zum anderen kann die Behörde in Vorleistung gehen und die Leistung vor dem Zahlungseingang erbringen.

Da der Zahlungsprozess bei beiden Varianten gleich ist, werden die beiden Varianten im Folgenden zusammen betrachtet. Der Kunde erteilt entweder vor oder nach Leistungserbringung durch die Behörde seiner Bank den Auftrag, den zu zahlenden Betrag an die Behörde zu überweisen. Dazu schließt er mit seiner Bank einen Überweisungsvertrag[66]. Zur Auftragsübermittlung stehen ihm verschiedene Möglichkeiten, wie etwa ein Überweisungsvordruck, die Benutzung von Selbstbedienungsterminals der Bank, die Nutzung von Telefon-Banking oder Internet-Banking zur Verfügung. Vor einer Ausführung des Überweisungsauftrags prüft die Bank die Authentizität des Auftraggebers. Im Falle der papiergebunden Ü-

65 Annahme: Disagio 2%, vgl. Abschnitt A.2.

66 §§ 676a bis 676c BGB regeln den Überweisungsvertrag.

berweisung erfolgt dies durch den Vergleich der Unterschrift mit der bei der Bank hinterlegten Unterschriftsprobe. Bei der Nutzung anderer Zugangswege erfolgt die Überprüfung der Authentizität dadurch, dass die entsprechende PIN bzw. TAN auf Richtigkeit und Gültigkeit überprüft wird. Nach erfolgreicher Überprüfung der Kontodeckung wird eine Übertragung des Geldbetrages an das Kreditinstitut der Behörde veranlasst. Eine Gutschrift auf dem Konto der Behörde ist bei inländischen Überweisungen innerhalb von ein bis drei Bankgeschäftstagen zu erwarten.

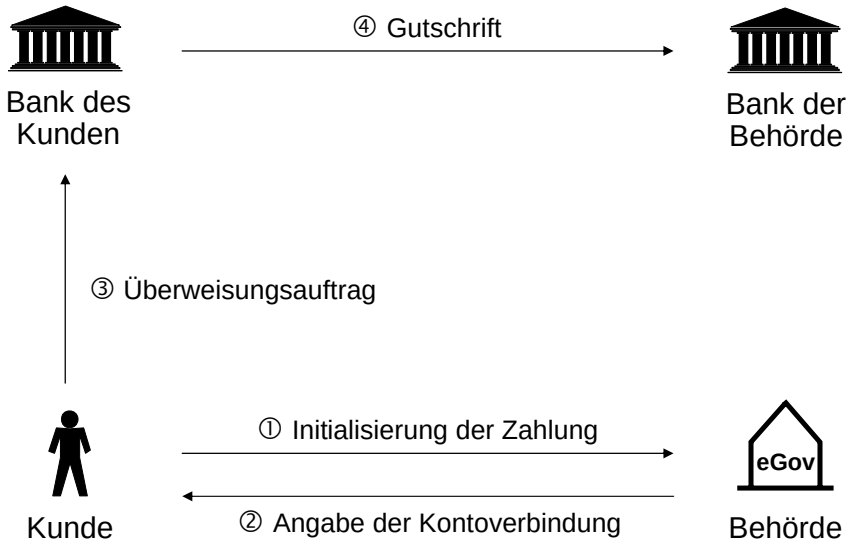


Abbildung 13: Ablauf einer Zahlung mittels Überweisungsauftrag

Zahlungsverfahren: Überweisung und Zahlungseingang vor bzw. nach Lieferung

Fachspezifische Anforderungen			
Wiederkehrende Zahlung	Nein		**ja**
Internationalität	Nein		**ja**
Anonymität	**Nein**		ja
Zahlungsgarantie	**gering** (Überweisung und Zahlungseingang nach Lieferung)	mittel	**hoch** (Überweisung und Zahlungseingang vor Lieferung)
Verbreitung	gering	mittel	**hoch**
Kostenstruktur			
Betragsbereich	0,01 Euro bis Verfügungsrahmen		
Variable Kosten der Behörde bei Betrag von	Prozent		Euro
Umsatz: 0,05 €	abhängig von BpG		**BpG**[67]
Umsatz: 0,50 €	abhängig von BpG		**BpG**
Umsatz: 5,00 €	abhängig von BpG		**BpG**
Umsatz: 50,00 €	abhängig von BpG		**BpG**
Umsatz: 500,00 €	abhängig von BpG		**BpG**
Umsatz: 5.000,00 €	abhängig von BpG		**BpG**
Umsatz: 50.000,00 €	abhängig von BpG		**BpG**
Fixe Kosten der Behörde in Euro (nur eindeutig zuordenbare Kosten; vgl. Abschnitt 5.4.3)	einmalig		jährlich
Betrag	**0**		**0**
Sicherheit			
Transaktionskontrolle	gering	**mittel**	hoch
Stärke des Authentifizierungsmechanismus	gering	**mittel**	hoch
Sperrmöglichkeit	nein		**ja**
Haftungsbetrag	**Verfügungsrahmen**		

Stand: Mai 2005

Tabelle 15: Zusammenfassende Bewertung „Überweisung und Zahlungseingang vor und nach Lieferung“

6.1.4 Lastschrift im Internet

Mittels einer Lastschrift kann die Behörde Beträge zu Lasten des Kunden einziehen lassen. Im Folgenden wird die Annahme getroffen, dass der Behörde hierfür eine rechtskonforme Einzugsermächtigung erteilt worden ist[68]. Diese muss nach den Vorschriften des Lastschriftabkommens [Krepold 2003] in schriftlicher Form oder in elektronischer Form mit qualifizierter elektronischer Signatur vorliegen.

Zahlungsablauf

Um Beträge mittels Lastschrift einzuziehen, schließt die Behörde mit ihrer Bank, der so genannten ersten Inkassostelle, eine schriftliche Inkassovereinbarung. Die Bank nimmt die Lastschrifteinreichung der Behörde entgegen und schreibt dieser

67 Buchungspostengebühr

68 Neben der Lastschrift mit Einzugsermächtigung existiert noch eine weitere Form der Lastschrift, der Abbuchungsauftrag. Sie ist in der Praxis jedoch nur selten zu finden, und wird deshalb nicht weiter betrachtet.

den Betrag auf ihrem Konto gut. Die erste Inkassostelle gibt die Lastschrift über das Bankennetz an die Bank des Kunden weiter und verrechnet den Betrag mit der kontoführenden Bank des Kunden.

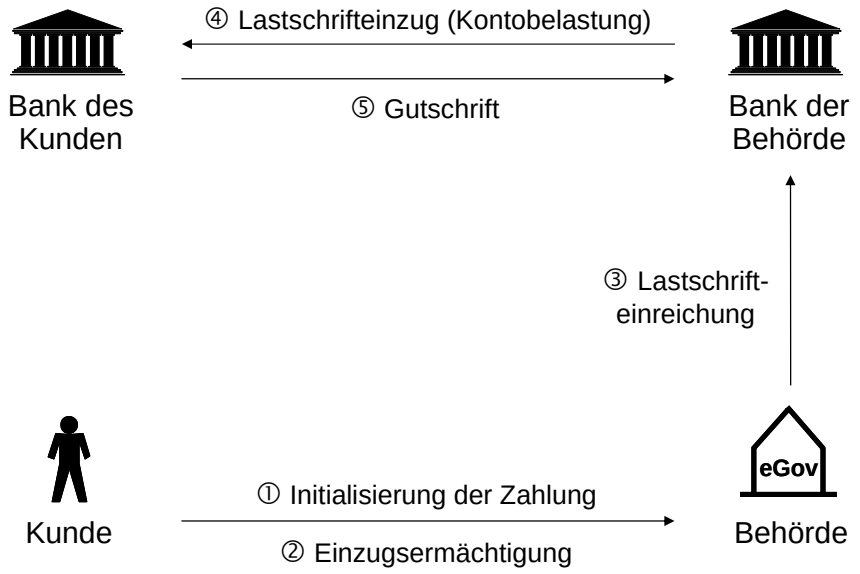


Abbildung 14: Ablauf einer Zahlung mittels Lastschrift

Zahlungsverfahren: Lastschrift (Einzugsermächtigung)

Fachspezifische Anforderungen			
Wiederkehrende Zahlung	nein		**ja**
Internationalität	**nein**		ja
Anonymität	**nein**		ja
Zahlungsgarantie	**gering**	mittel	hoch
Verbreitung	gering	mittel	**hoch**
Kostenstruktur			
Betragsbereich	0,01 Euro bis Verfügungsrahmen		
Variable Kosten der Behörde bei Betrag von	Prozent		Euro
Umsatz 0,05 €	abhängig von BpG		**BpG**
Umsatz 0,50 €	abhängig von BpG		**BpG**
Umsatz 5,00 €	abhängig von BpG		**BpG**
Umsatz 50,00 €	abhängig von BpG		**BpG**
Umsatz 500,00 €	abhängig von BpG		**BpG**
Umsatz 5.000,00 €	abhängig von BpG		**BpG**
Umsatz 50.000,00 €	abhängig von BpG		**BpG**
Fixe Kosten der Behörde in Euro (nur eindeutig zuordenbare Kosten; vgl. Abschnitt 5.4.3)	einmalig		jährlich
Betrag	**0**		**0**
Sicherheit			
Transaktionskontrolle	gering	**mittel**	hoch
Stärke des Authentifizierungsmechanismus	**gering**	mittel	hoch
Sperrmöglichkeit	nein		**ja**
Haftungsbetrag	**0 Euro**		

Stand: Mai 2005

Tabelle 16: Zusammenfassende Bewertung „Lastschrift (Einzugsermächtigung)“

6.1.5 Kreditkartenzahlung (SSL)

Kreditkarten dienen zur bargeldlosen Bezahlung von Waren und Dienstleistungen bei Vertragsunternehmen (Akzeptanzstellen). Der Karteninhaber ist berechtigt, gegen Vorlage der Kreditkarte bei Vertragsunternehmen Leistungen in Anspruch zu nehmen. Eine Auflistung von Kreditkartenunternehmen ist in Abschnitt A.12 des Anhangs dargestellt.

Ablauf einer Kreditkarten-zahlung

Bei einem Einsatz der Kreditkarte im Internet gibt der Karteninhaber die Kreditkartendaten (Kreditkartennummer und Gültigkeitsdatum) in einem Browser-Fenster an und bestätigt die Zahlung. Die Daten werden über eine SSL-Verbindung zur Behörde übertragen, die diese anschließend zur Autorisierung an einen Acquirer weiterleitet. Dem Vertragsunternehmen wird bei einer erfolgreichen Autorisierung eine Autorisierungsnummer mitgeteilt. Die eingereichten Umsätze aus Kreditkartenzahlungen werden in vereinbarten Perioden auf einem Konto des Vertragsunternehmens gutgeschrieben.

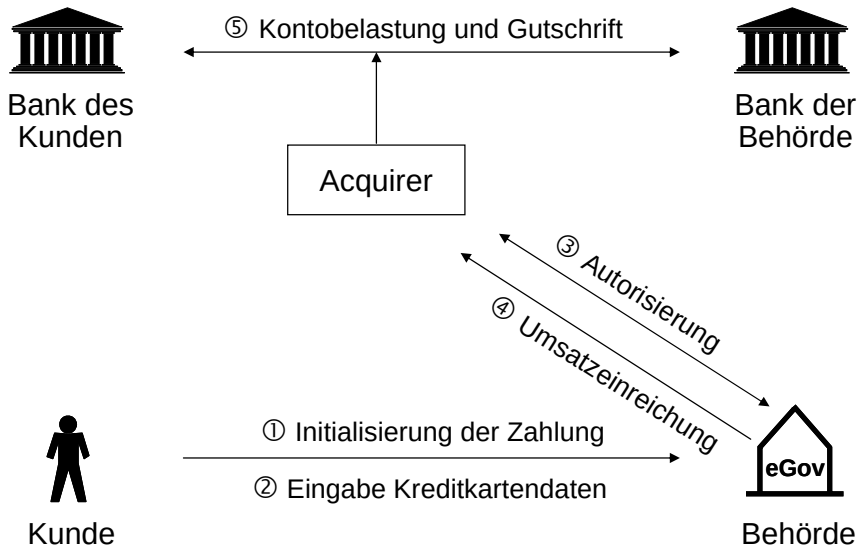


Abbildung 15: Ablauf einer Kreditkartenzahlung (SSL)

Zahlungsverfahren: Kreditkartenzahlung (SSL)

Fachspezifische Anforderungen			
Wiederkehrende Zahlung	nein		**ja**
Internationalität	nein		**ja**
Anonymität	nein		**ja**
Zahlungsgarantie	**gering**	mittel	hoch
Verbreitung	gering	mittel	**hoch**
Kostenstruktur			
Betragsbereich	0,01 Euro bis Verfügungsrahmen		
Variable Kosten der Behörde bei Betrag von	Prozent		Euro
Umsatz: 0,05 €	**1003%**		**0,50**[69]
Umsatz: 0,50 €	**103%**		**0,52**
Umsatz: 5,00 €	**13%**		**0,65**
Umsatz: 50,00 €	**4,0%**		**2,00**
Umsatz: 500,00 €	**3,1%**		**15,50**
Umsatz: 5.000,00 €	**3,0%**		**150,50**
Umsatz: 50.000,00 €	**3,0%**		**1500,50**
Fixe Kosten der Behörde in Euro (nur eindeutig zuordenbare Kosten; vgl. Abschnitt 5.4.3)	einmalig		jährlich
Betrag	**0**		**0**
Sicherheit			
Transaktionskontrolle	gering	**mittel**	hoch
Stärke des Authentifizierungsmechanismus	**gering**	mittel	hoch
Sperrmöglichkeit	nein		**ja**
Haftungsbetrag	**50 Euro**		

Stand: Mai 2005

Tabelle 17: Zusammenfassende Bewertung „Kreditkartenzahlung (SSL)“

6.1.6 Kreditkartenzahlung (3-D Secure)

Bei 3-D Secure handelt es sich um einen von Kreditkartenorganisationen entwickelten Standard zur Abwicklung von sicheren Kreditkartentransaktionen. MasterCard bietet darauf aufbauende Zahlungen unter dem Markennamen „MasterCard SecureCode“, Visa unter dem Markennamen „Verified by Visa“ an. Um das Zahlungsverfahren nutzen zu können, muss es das kartenherausgebende Institut unterstützen und der Kunde muss sich zur Nutzung bei seiner Bank (z. B. im Internet) registrieren, um ein Kennwort zu erhalten[70]. Im Rahmen des Zahlungsvorgangs kann sich der Kunde nun gegenüber der kartenherausgebenden Bank authentifizieren indem er in dem vom Merchant Server Plug-in (MPI)[71] generierten Browser-Fenster sein Kennwort eingibt. Dieses wird anschließend durch das kartenherausgebende Institut überprüft und das Ergebnis wird an das Vertragsunternehmen weitergeleitet. Erfolgreich autorisierte Zahlungen sind garan-

69 Annahme: Disagio 3% zzgl. fixer Transaktionsgebühr von 0,50 Euro, vgl. Abschnitt A.5.

70 Dabei handelt es sich um die in Abschnitt 2.2.2 angesprochene Variante 1 der Authentifizierung.

71 Bei einem „Merchant Server Plug-in“ handelt es sich um eine vom Browser automatisiert aufgerufene Komponente, die von der Bank des Kunden bereitgestellt wird. Diese führt den Kunden durch den Vorgang der Authentifizierung und leitet das Ergebnis an das Vertragsunternehmen weiter.

tiert und das Vertragsunternehmen erhält die eingereichten Umsätze abzüglich eines Disagios auf seinem Konto gutgeschrieben. Kreditkartenanbieter, die Verfahren auf der Basis von 3-D Secure bereitstellen, sind in Anhang A.12 aufgeführt.

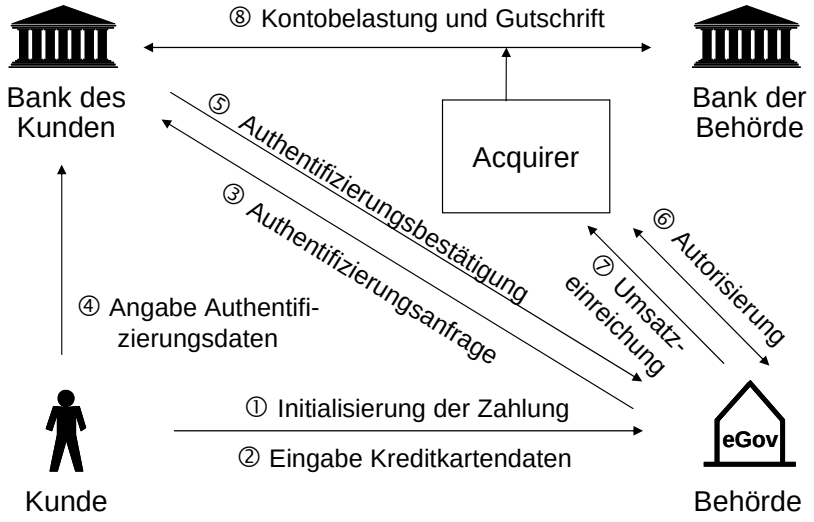


Abbildung 16: Ablauf einer Kreditkartenzahlung (3-D Secure)

Zahlungsverfahren: Kreditkartenzahlung (3-D Secure)

Fachspezifische Anforderungen				
Wiederkehrende Zahlung		**nein**		ja
Internationalität		nein		**ja**
Anonymität		nein		**ja**
Zahlungsgarantie		gering	mittel	**hoch**
Verbreitung		**gering**	mittel	hoch
Kostenstruktur				
Betragsbereich		0,01 Euro bis Verfügungsrahmen		
Variable Kosten der Behörde bei Betrag von		Prozent		Euro
Umsatz	0,05 €	**1003%**		**0,50**[72]
	0,50 €	**103%**		**0,52**
	5,00 €	**13%**		**0,65**
	50,00 €	**4,0%**		**2,00**
	500,00 €	**3,1%**		**15,50**
	5.000,00 €	**3,0%**		**150,50**
	50.000,00 €	**3,0%**		**1500,50**
Fixe Kosten der Behörde in Euro (nur eindeutig zuordenbare Kosten; vgl. Abschnitt 5.4.3)		einmalig		jährlich
Betrag		**0**		**0**
Sicherheit				
Transaktionskontrolle		gering	**mittel**	hoch
Stärke des Authentifizierungsmechanismus		gering	**mittel**	hoch
Sperrmöglichkeit		nein		**ja**
Haftungsbetrag		**50 Euro**		

Stand: Mai 2005

Tabelle 18: Zusammenfassende Bewertung „Kreditkartenzahlung (3-D Secure)“

72 Annahme: Disagio 3% zzgl. fixer Transaktionsgebühr von 0,50 Euro, vgl. Abschnitt A.6.

6.1.7 Wertkarten-basierte Verfahren

Die Bewertung der Wertkarten-basierten Verfahren erfolgt im Weiteren beispielhaft anhand der paysafecard. Weitere Vertreter Wertkarten-basierter Verfahren können Anhang A.12 entnommen werden.

Die paysafecard kann der Kunde an über 7.000 Verkaufsstellen in Deutschland und im Internet erwerben. Die Karte gibt es in zwei Varianten: die rote paysafecard für Jugendliche und die blaue Variante für Erwachsene. Die Karten sind mit Beträgen von 25 Euro, 50 Euro bzw. auch 10 Euro und 100 Euro im Falle der blauen Variante erhältlich. Es ist möglich, bis zu zehn Karten in einem Zahlungsvorgang einzulösen und so etwaige Restguthaben aufzubrauchen. Theoretisch ergibt sich somit ein maximaler Zahlungsbetrag von 1.000 Euro. Es wird jedoch davon ausgegangen, dass der Kunde in der Praxis lediglich eine Karte bei sich führt.

Je nach Händler erhält der Kunde die paysafecard in Scheckkartenformat, als paysafecard-PIN Ausdruck oder beim Online-Kauf den classic paysafecard-PIN. Egal, welche der drei Versionen der Kunde gewählt hat, so hat er einen einzigartigen 16-stelligen PIN-Code, eine Seriennummer, das Produktionsdatum und die Nominale erhalten. Im Scheckkartenformat befindet sich der Code auf der Rückseite der Wertkarte und muss freigerubbelt werden (sie wird deshalb auch Scratch-Card, dt. Rubbelkarte, bezeichnet). Die Karte kann anschließend auf der paysafecard-Webseite durch ein frei wählbares Passwort zusätzlich geschützt werden. Auf der Webseite kann zudem auch das aktuelle Guthaben der Karte und eine Transaktionsübersicht eingesehen werden. Will der Kunde mit der Karte bezahlen, so wählt er im Online-Shop der Behörde das Zahlungsverfahren paysafecard und gibt den auf der paysafecard freigerubbelten Code und gegebenenfalls seine PIN ein. Anschließend wird bei einem paysafecard-Server (unter anderem mit Händlerkennung, Transaktionsnummer, Betrag und Währung) angefragt, ob das Guthaben auf der Karte ausreicht. Ist dies der Fall, wird der Betrag reserviert. Der paysafecard-Server meldet anschließend an den Online-Shop das Ergebnis des Zahlungsvorgangs. Anschließend überweist paysafecard den Zahlungsbetrag abzüglich eines Disagios an die Behörde.

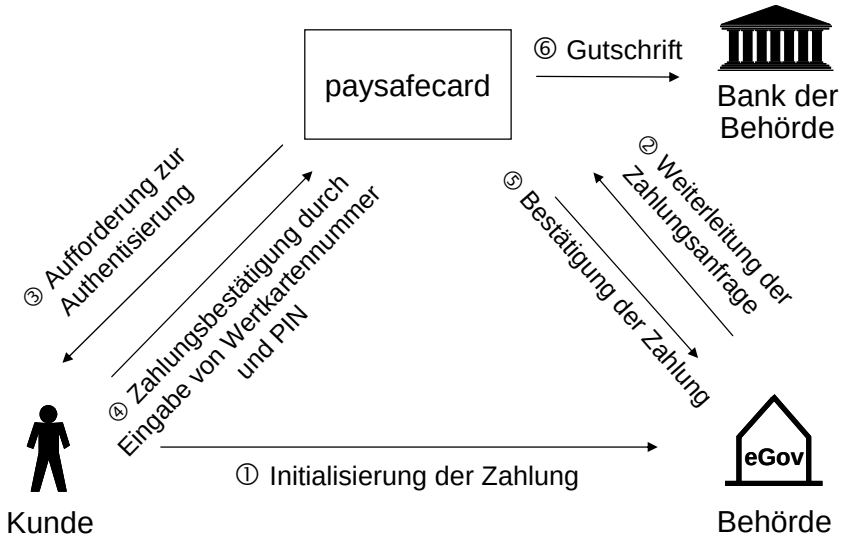


Abbildung 17: Ablauf einer Zahlung mit der paysafecard

Zahlungsverfahren: paysafecard

Fachspezifische Anforderungen			
Wiederkehrende Zahlung	**nein**		ja
Internationalität	nein		**ja**
Anonymität	nein		**ja**
Zahlungsgarantie	gering	mittel	**hoch**
Verbreitung	**gering**	mittel	hoch
Kostenstruktur			
Betragsbereich	0,01 Euro bis 100 Euro		
Variable Kosten der Behörde bei Betrag von	Prozent		Euro
Umsatz 0,05 €	**22%**		**0,01**
Umsatz 0,50 €	**22%**		**0,11**
Umsatz 5,00 €	**22%**		**1,10**
Umsatz 50,00 €	**14%**		**6,96**
Umsatz 500,00 €	nicht möglich		
Umsatz 5.000,00 €	nicht möglich		
Umsatz 50.000,00 €	nicht möglich		
Fixe Kosten der Behörde in Euro (nur eindeutig zuordenbare Kosten; vgl. Abschnitt 5.4.3)	einmalig		jährlich
Betrag	**0**		**0**
Sicherheit			
Transaktionskontrolle	gering	mittel	**hoch**
Stärke des Authentifizierungsmechanismus	gering	mittel	**hoch**
Sperrmöglichkeit	**nein**		ja
Haftungsbetrag	**Kartenguthaben (max. 100 Euro)**		

Stand: Mai 2005

Tabelle 19: Zusammenfassende Bewertung „paysafecard“

6.1.8 E-Mail-basierte Verfahren

Bei E-Mail-basierten Verfahren wird die E-Mail-Adresse des Nutzers zur Identifikation und zur Übertragung von Buchungsinformationen genutzt. Mögliche Anbieter E-Mail-basierter Verfahren sind in Anhang A.12 aufgelistet. Beispielhaft wird nachfolgend auf das Zahlungsverfahren moneybookers näher eingegangen.

Ablauf von moneybookers

Moneybookers wurde von der FSA (Finanz- und Kapitalmarktaufsicht des Vereinigten Königreichs) als „electronic money issuer“ lizenziert und ist damit zur Ausgabe von E-Geld berechtigt. Händlern wird das Verfahren in zwei Varianten angeboten: Beim Basis-Produkt „Email Pay“ registriert sich die Behörde mit ihrer E-Mail-Adresse und muss selbst prüfen, ob das Geld eingegangen ist. Bei der Variante „Merchant Gateway“ wird der Kunde beim Bezahlvorgang auf die Webseite von moneybookers umgeleitet. Der Kunde bestätigt den Zahlungsauftrag und wird wieder zum Online-Shop zurückgeleitet. Anschließend erhält die Behörde eine Bestätigung des Zahlungsvorgangs und kann die Leistung liefern.

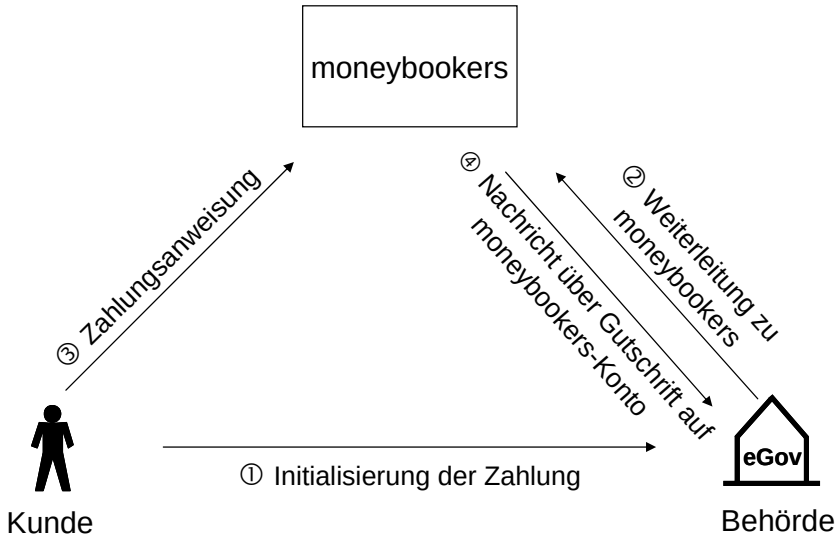


Abbildung 18: Ablauf einer Zahlung mit moneybookers

Zahlungsverfahren: moneybookers

Fachspezifische Anforderungen			
Wiederkehrende Zahlung	nein		**ja**
Internationalität	nein		**ja**
Anonymität	nein		**ja**
Zahlungsgarantie	gering	mittel	**hoch**
Verbreitung	**gering**	mittel	hoch
Kostenstruktur			
Betragsbereich	0,01 Euro bis Verfügungsrahmen		
Variable Kosten des Kunden bei Betrag von	Prozent		Euro
Umsatz 0,05 €	**1,00%**		**0,0005**
Umsatz 0,50 €	**1,00%**		**0,005**
Umsatz 5,00 €	**1,00%**		**0,05**
Umsatz 50,00 €	**1,00%**		**0,50**
Umsatz 500,00 €	**0,10%**		**0,50**
Umsatz 5.000,00 €	**nicht möglich**[73]		
Umsatz 50.000,00 €	**nicht möglich**		
Fixe Kosten der Behörde in Euro (nur eindeutig zuordenbare Kosten; vgl. Abschnitt 5.4.3)	einmalig		jährlich
Betrag	**0**		**0**
Sicherheit			
Transaktionskontrolle	gering	mittel	**hoch**
Stärke des Authentifizierungsmechanismus	gering	**mittel**	hoch
Sperrmöglichkeit	nein		**ja**
Haftungsbetrag	**Guthaben auf Verrechnungskonto**		

Stand: Mai 2005

Anmerkung: Es entstehen ausschließlich für den Sender der Zahlung Kosten in Höhe von 1%, maximal jedoch 0,50 Euro. Für die Behörde entstehen somit keine Kosten.

Tabelle 20: Zusammenfassende Bewertung „moneybookers“

73 Es wird ein maximales Guthaben bei moneybookers von 500 Euro angenommen, vgl. Abschnitt A.8.

6.1.9 Mobiltelefon-basierte Verfahren

Mobiltelefon-basierte Verfahren nutzen das Mobiltelefon zur Übertragung von Buchungsinformationen. Das Mobiltelefon dient dabei gleichzeitig zur Authentifizierung. Im Folgenden sollen die Mobiltelefon-basierten Verfahren am Beispiel des Zahlungsverfahrens Vodafone m-pay bewertet werden. Ähnliche Verfahren werden in Anhang A.12 dargestellt.

Identifizierung über Vodafone D2-Nummer

Mit Vodafone m-pay[74] können Kunden von Vodafone D2 Beträge bis 10 Euro per WAP, im Internet oder per SMS zahlen. Der Kunde identifiziert sich mit seiner Vodafone D2-Nummer. Eine zusätzliche Registrierung ist nicht erforderlich. Für Teilnehmer mit einem Vertrag mit fester Laufzeit gilt ein monatlicher Verfügungsrahmen von 100 Euro. Prepaid- (CallYa-) Kunden steht zur Bezahlung das Guthaben ihres Prepaid- (CallYa-) Kontos (ausgenommen das Startguthaben) zur Verfügung.

Zahlungsablauf im Internet

Zum Bezahlen im Internet wählt der Kunde Vodafone m-pay als Zahlungsart. Nach der Eingabe der Vodafone D2-Nummer, erhält er eine SMS mit einem Bezahl-Code, bestehend aus sechs Ziffern. Dieser ist nur für den aktuellen Bezahlvorgang 30 Minuten lang gültig. Nachdem der Bezahl-Code auf der Website eingegeben wurde, erfolgt eine Bestätigung und das Vodafone-Konto wird um diesen Betrag belastet.

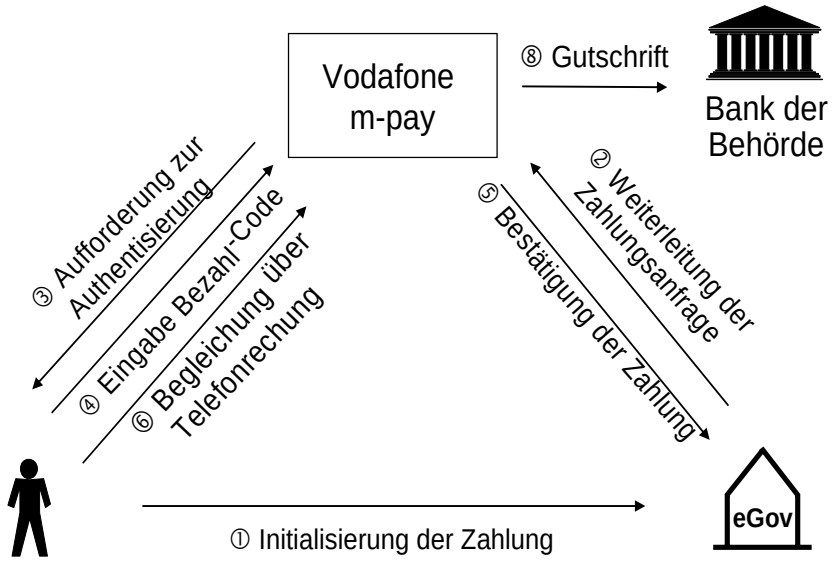


Abbildung 19: Ablauf einer Zahlung mit Vodafone m-pay

74 http://www.vodafone.de/m-pay/

Zahlungsverfahren: Vodafone m-pay

Fachspezifische Anforderungen			
Wiederkehrende Zahlung	nein		**ja**
Internationalität	**nein**		ja
Anonymität	nein		**ja**
Zahlungsgarantie	gering	mittel	**hoch**
Verbreitung	gering	mittel	**hoch**
Kostenstruktur			
Betragsbereich	0,01 bis 10 Euro		
Variable Kosten der Behörde bei Betrag von	Prozent[75]		Euro
Umsatz: 0,05 €	**22,35%**		**0,01**
Umsatz: 0,50 €	**22,35%**		**0,11**
Umsatz: 5,00 €	**22,35%**		**1,12**
Umsatz: 50,00 €	nicht möglich		
Umsatz: 500,00 €	nicht möglich		
Umsatz: 5.000,00 €	nicht möglich		
Umsatz: 50.000,00 €	nicht möglich		
Fixe Kosten der Behörde in Euro (nur eindeutig zuordenbare Kosten; vgl. Abschnitt 5.4.3)	einmalig		jährlich
Betrag	**8.700**		**1.392**
Sicherheit			
Transaktionskontrolle	gering	mittel	**hoch**
Stärke des Authentifizierungsmechanismus	gering	mittel	**hoch**
Sperrmöglichkeit	nein		**ja**
Haftungsbetrag	**max. 10 Euro**		

Stand: Mai 2005

Tabelle 21: Zusammenfassende Bewertung „Vodafone m-pay“

6.1.10 Nachnahme

Zustelldienst als Inkassostelle

Bei der Nachnahme tritt ein Zustelldienst als Inkassostelle auf. Das Verfahren ist nur in Kombination mit einem Brief oder einer Postkarte, bei einigen Zustelldiensten auch nur mit Päckchen oder Paketen möglich. Die Sendung wird dem Kunden erst dann ausgehändigt, wenn dieser den ausstehenden Betrag gegenüber dem Zustelldienst beglichen hat. Im Folgenden soll die Nachnahme am Beispiel der Deutschen Post[76] bzw. DHL[77] dargestellt werden. Neben diesen Unternehmen wird das Verfahren auch von weiteren Zustelldiensten angeboten, die in Anhang A.12 dargestellt sind.

Ablauf einer Nachnahmesendung

Die Behörde erteilt der Post den Auftrag, die Sendung an den Kunden zu überstellen und gibt ein Konto an, auf das der einzuziehende Betrag überwiesen werden soll. Dazu wird in der Regel ein Einlieferungsschein sowie ein Überweisungsträger ausgefüllt und der Sendung beigelegt. Die Sendung kann von der Behörde

75 Vodafone D2 erhält einen Anteil von 22,35% vom Umsatz, mindestens jedoch eine monatliche Vergütung in Höhe von 500 Euro (zzgl. USt.).

76 Näheres dazu unter http://www.post.de/.

77 Näheres dazu unter http://www.dhl.de/.

entweder in einer Postfiliale, Postagentur, bei Zustellern oder Zustelldiensten aufgegeben werden. Verzichtet die Behörde auf den Einlieferungsschein, wäre auch ein Einwurf in einen Briefkasten der Deutschen Post möglich.

Gegen Zahlung des Nachnahme-Betrags durch den Empfänger, seinen Bevollmächtigten oder einen anderen Empfangsberechtigten händigt der Zustelldienst die Sendung aus. Die Zahlung kann bar oder unbar (z. B. durch Einsatz des Lastschriftverfahrens oder einer Kreditkarte) erfolgen. Anschließend übermittelt die Deutsche Post den Nachnahme-Betrag abzüglich des Übermittlungs-Entgelts an das angegebene Konto der Behörde.

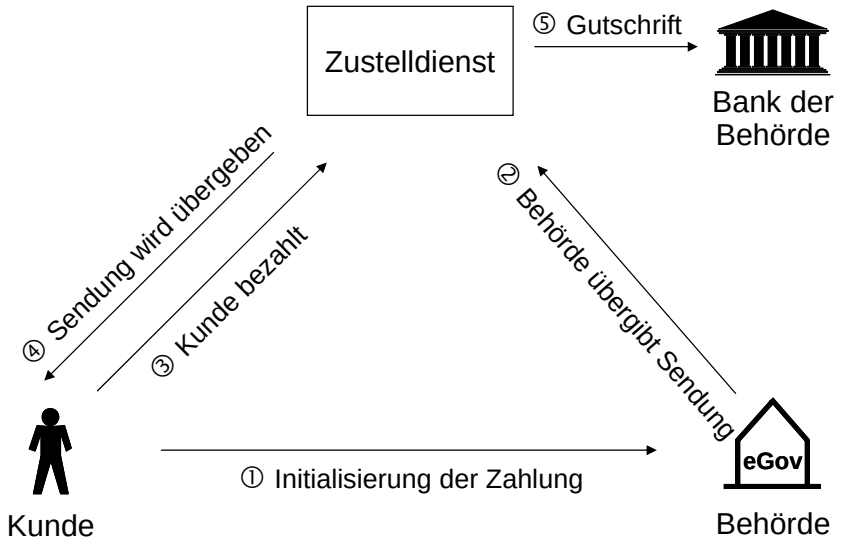


Abbildung 20: Ablauf einer Zahlung per Nachnahme

Zahlungsverfahren: Nachnahmesendung

Fachspezifische Anforderungen			
Wiederkehrende Zahlung	**nein**		ja
Internationalität	nein		**ja**
Anonymität	**nein**		ja
Zahlungsgarantie	gering	mittel	**hoch**
Verbreitung	gering	mittel	**hoch**
Kostenstruktur			
Betragsbereich[78]	0,01 bis 1.600 Euro		
Variable Kosten[79] der Behörde bei Betrag von	Prozent		Euro
Umsatz 0,05 €	**8000%**		**4,00**
Umsatz 0,50 €	**800%**		**4,00**
Umsatz 5,00 €	**80%**		**4,00**
Umsatz 50,00 €	**8%**		**4,00**
Umsatz 500,00 €	**0,8%**		**4,00**
Umsatz 5.000,00 €	nicht möglich		
Umsatz 50.000,00 €	nicht möglich		
Fixe Kosten der Behörde in Euro (nur eindeutig zuordenbare Kosten; vgl. Abschnitt 5.4.3)	einmalig		jährlich
Betrag	**0**		**0**
Sicherheit			
Transaktionskontrolle	gering	**mittel**	hoch
Stärke des Authentifizierungsmechanismus	gering	**mittel**	hoch
Sperrmöglichkeit	**nein**		ja
Haftungsbetrag	**0 Euro**		

Stand: Mai 2005

Tabelle 22: Zusammenfassende Bewertung „Nachnahmesendung“

6.1.11 Billing-Verfahren

Billing-Verfahren ermöglichen die Aufrechnung von (Klein-) Beträgen bis zu einem bestimmten Zeitpunkt oder bis ein bestimmter Mindestgesamtbetrag erreicht wurde. Das Unternehmen Firstgate bietet mit click&buy ein solches Zahlungsverfahren an, das exemplarisch vorgestellt wird[80]. Im Anhang A.12 sind weitere Anbieter von Billing-Verfahren aufgelistet.

Registrierung und Zahlungsausgleich

Zur Nutzung des Zahlungsverfahrens muss sich der Kunde einmalig registrieren. Dazu gibt er seine Anschrift, E-Mail-Adresse und die gewünschte Zahlungsmethode an, mit der Firstgate die Beträge für einen Zahlungsausgleich einziehen soll (derzeit Lastschrift oder Kreditkarte). Nachdem die Daten des Kunden durch Firstgate verifiziert wurden, erhält der Kunde eine PIN, die zur Authentifizierung des Kunden im Bezahlvorgang dient. Bei der Lastschrift-Variante wird die PIN

78 Der Betragsbereich ist bei Briefen und Postkarten auf 1.600 Euro, bei nationalen DHL-Paketen auf 3.500 Euro, bei internationalen DHL-Paketen auf 5.000 Euro beschränkt.

79 Für den Fall Deutsche Post Standardbrief (national und international).

80 Die Ausführungen zu click&buy beziehen sich auf den Standard-Account. Für Großkunden bietet das Unternehmen einen „Professional“-Account, der neben günstigeren Konditionen auch die Abbuchung wiederkehrender Zahlungen ohne Betragsbegrenzung ermöglicht.

durch Angabe im Verwendungszweck einer Abbuchung (hierzu werden die Lastschriftdaten verwendet) mitgeteilt. Als vorläufiger Nutzername dient die E-Mail-Adresse des Nutzers.

Bei einem Zahlungsausgleich mittels Kreditkarte werden die Kreditkartendaten anhand einer Online-Autorisierung überprüft. Anschließend wird die PIN per E-Mail übermittelt. Nutzername sowie Firstgate-PIN kann der Kunde nachträglich ändern. Die Abbuchung vom angegebenen Lastschriftkonto bzw. vom Kreditkartenkonto und die Überweisung des erzielten Umsatzes abzüglich des Disagios an die Behörde erfolgt einmal im Monat[81].

Zahlungsablauf

Die Behörde kann einem Link zu kostenpflichtigen Inhalten einen Preis von 0,05 bis 10 Euro zuweisen. Die Abstufung erfolgt in diesem Bereich in Schritten von 0,01 Euro. Klickt ein Kunde auf einen kostenpflichtigen Link, wird er zu einer Seite von Firstgate weitergeleitet und zur Eingabe seines Firstgate-Benutzernamens und seiner PIN aufgefordert. Nach erfolgreicher Überprüfung dieser Daten durch Firstgate werden dem Kunden Informationen zum Anbieter des abzurufenden Inhaltes und der entsprechende Preis angezeigt. Akzeptiert der Kunde das Angebot, so kann der kostenpflichtige Inhalt bezogen werden.

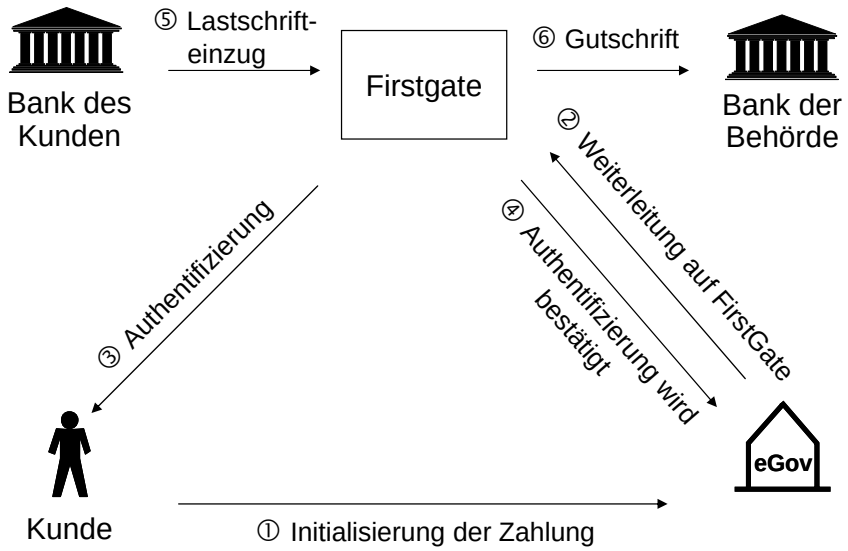


Abbildung 21: Ablauf einer Zahlung mit click&buy

81 Geplant ist, dass Inhalte auch mittels eines vorausbezahlten Kontos nutzbar sind.

Zahlungsverfahren: click&buy

Fachspezifische Anforderungen				
Wiederkehrende Zahlung		**nein**		ja
Internationalität		nein		**ja**
Anonymität		nein		**ja**
Zahlungsgarantie		gering	**mittel**	hoch
Verbreitung		gering	**mittel**	hoch
Kostenstruktur				
Betragsbereich		0,05 bis 10 Euro		
Variable Kosten der Behörde bei Betrag von		Prozent		Euro
Umsatz	0,05 €	**29%**		**0,015**[82]
	0,50 €	**29%**		**0,145**
	5,00 €	**29%**		**1,45**
	50,00 €	nicht möglich		
	500,00 €	nicht möglich		
	5.000,00 €	nicht möglich		
	50.000,00 €	nicht möglich		
Fixe Kosten der Behörde in Euro (nur eindeutig zuordenbare Kosten; vgl. Abschnitt 5.4.3)		einmalig		jährlich
Betrag		**49 Euro**		**60 Euro**
Sicherheit				
Transaktionskontrolle		gering	mittel	**hoch**
Stärke des Authentifizierungsmechanismus		gering	**mittel**	hoch
Sperrmöglichkeit		nein		**ja**
Haftungsbetrag		**nicht begrenzt**		

Stand: Mai 2005

Tabelle 23: Zusammenfassende Bewertung „click&buy“

82 Die hier angebenden Werte beziehen sich auf eine Transaktion bis fünf Euro durch einen Standard-Kunden bei einem monatlichen Umsatz von mehr als 50.000 Euro bis 200.000 Euro durch die Behörde.

6.2 Zusammenfassung

Die folgenden drei Tabellen fassen die Bewertungen der einzelnen Zahlungsverfahren nochmals zusammen. Die Begründungen der einzelnen Bewertung können den entsprechenden Stellen des Anhangs entnommen werden.

Fachspezifische Anforderungen					
Verfahren / Kriterium	**Eignung für wiederkehrende Zahlungen**	**Internationalität**	**Anonymität**	**Zahlungsgarantie zum Zeitpunkt der Leistung**	**Verbreitung**
GeldKarte	nein	nein	ja	hoch	gering
Online-Überweisung (Postbank)	nein	nein	nein	mittel	mittel
Überweisung und Zahlungseingang vor Lieferung	ja	ja	nein	hoch	hoch
Überweisung und Zahlungseingang nach Lieferung	ja	ja	nein	gering	hoch
Lastschrift	ja	nein	nein	gering	hoch
Kreditkarte (SSL)	ja	ja	ja	gering	hoch
Kreditkarte 3-D Secure	nein	ja	ja	hoch	gering
Paysafecard	nein	ja	ja	hoch	gering
moneybookers (Variante "Gateway")	ja	ja	ja	hoch	gering
Vodafone m-pay	ja	nein	ja	hoch	hoch
Nachnahme (Standardbrief)	nein	ja	nein	hoch	hoch
Firstgate click&buy	nein	ja	ja	mittel	mittel

Stand: Mai 2005

Tabelle 24: Bewertungen der Verfahren in der Kategorie „Fachspezifische Anforderungen“

Betragsbereich und Kostenstruktur								
Verfahren / Kriterium	Variable Kosten für Behörde bei einem Betrag von							Fixe Kosten für Behörde (einmalig/jährlich in Euro)
	0,05 Euro	0,50 Euro	5 Euro	50 Euro	500 Euro	5.000 Euro	50.000 Euro	
GeldKarte	0,01	0,01	0,015	0,15				0/0
Online-Überweisung (Postbank)	0,001	0,01	0,10	1,00	10,00	100,00	1.000,00	0/0
Überweisung und Zahlungseingang vor Lieferung	BpG[83]	BpG	BpG	BpG	BpG	BpG	BpG	0/0
Überweisung und Zahlungseingang nach Lieferung	BpG	BpG	BpG	BpG	BpG	BpG	BpG	0/0
Lastschrift	BpG	BpG	BpG	BpG	BpG	BpG	BpG	0/0
Kreditkarte (SSL)	0,50	0,52	0,65	2,00	15,50	150,50	1.500,50	0/0
Kreditkarte 3-D Secure	0,50	0,52	0,65	2,00	15,50	150,50	1.500,50	0/0
paysafecard	0,01	0,11	1,10	6,96				0/0
moneybookers (Variante "Gateway")[84]	0,00	0,00	0,00	0,00	0,00			0/0
Vodafone m-pay	0,01	0,11	1,12					8.700/1.392
Nachnahme (Standardbrief)	4,00	4,00	4,00	4,00	4,00	4,00		0/0
Firstgate click&buy	0,015	0,145	1,45					49/60

Stand: Mai 2005

Tabelle 25: Bewertungen der Verfahren in der Kategorie „Betragsbereich und Kostenstruktur“

83 Buchungspostengebühr

84 Für den Kunden fallen variable Kosten in Höhe von 1% des Betrags, maximal jedoch 0,50 Euro an.

Sicherheit				
Verfahren / Kriterium	**Transaktions-kontrolle**	**Authentifi-zierungs-mechanismus**	**Sperrmöglichkeit**	**Haftungsbetrag**
GeldKarte	hoch	mittel	nein	Kartenguthaben (max. 200 Euro)
Online-Überweisung (Postbank)	hoch	hoch	ja	Verfügungsrahmen
Überweisung und Zahlungseingang vor Liefe-rung	mittel	mittel	ja	Verfügungsrahmen
Überweisung und Zahlungseingang nach Lie-ferung	mittel	mittel	ja	Verfügungsrahmen
Lastschrift	mittel	gering	ja	0 Euro
Kreditkarte (SSL)	mittel	gering	ja	50 Euro
Kreditkarte (3-D Secure)	mittel	mittel	ja	50 Euro
paysafecard	hoch	hoch	nein	Kartenguthaben (max. 100 Euro)
moneybookers (Variante "Gateway")	hoch	mittel	ja	Guthaben auf Ver-rechnungskonto
Vodafone m-pay	hoch	hoch	ja	10 Euro
Nachnahme	mittel	mittel	nein	0 Euro
Firstgate click&buy	hoch	mittel	ja	nicht begrenzt

Stand: Mai 2005

Tabelle 26: Bewertungen der Verfahren in der Kategorie „Sicherheit“

7 Verfahren zur Auswahl geeigneter Zahlungsverfahren

Nachdem die Ausprägungen der in Abschnitt 5 festgelegten Kriterien für die einzelnen Zahlungsverfahren feststehen, müssen im Folgenden die bezüglich der Anforderungen eines Szenarios am besten geeigneten Zahlungsverfahren ausgewählt werden. Dieser Auswahlprozess stellt keine einfache Aufgabe dar, da es häufig nicht genau ein Verfahren gibt, das alle Anforderungen eines Szenarios optimal erfüllt. In diesem Fall ist zu prüfen, ob auf einzelne Anforderungen verzichtet werden soll oder sich durch eine geeignete Kombination verschiedener Verfahren eine bessere Lösung erzielen lässt.

In Abschnitt 7.1 wird die allgemeine Vorgehensweise zur Auswahl geeigneter Zahlungsverfahren beschrieben. Da vermieden werden muss, dass ein Zahlungsverfahren, das in Kombination mit einem anderen Verfahren durchaus sinnvoll wäre, zu schnell ausgeschlossen wird, sind innerhalb des Auswahlprozesses mehrere Schleifen (Rückkopplungen) und Verzweigungen notwendig. Die abstrakte Vorgehensweise wird anschließend an den in Abschnitt 3.2 vorgestellten Beispielszenarien exemplarisch durchgeführt.

7.1 Allgemeine Vorgehensweise

Überblick

Bei der Ermittlung der Anforderungen an ein Zahlungsverfahren wird im Folgenden zunächst untersucht, ob sich das betrachtete Szenario in weitere, elementare Teilszenarien[85] aufspalten lässt. Diese Teilszenarien können sich in ihren Anforderungen durchaus unterscheiden. Auch wenn ein Zahlungsverfahren nicht die Anforderungen des gesamten Szenarios erfüllt, kann es für ein Teilszenario dennoch sehr gut geeignet sein. Nach der Auswahl geeigneter Zahlungsverfahren für die Teilszenarien werden die Ergebnisse wieder zusammengeführt.

Die Bildung und Bewertung der Teilszenarien erfolgt anhand der Kriterien der Kategorie „Fachspezifische Anforderungen“ (vgl. Abschnitt 5.1). Erst nachdem auf diese Weise eine Vorauswahl geeigneter Zahlungsverfahren durchgeführt wurde, folgt eine Betrachtung der transaktionsabhängigen Kosten der verbleibenden Verfahren. Für die abschließende Entscheidung über den Einsatz eines Zahlungsverfahrens werden daraufhin die Kriterien der Kategorie „Sicherheit“ (vgl. Abschnitt 5.3) sowie die Integrierbarkeit des Zahlungsverfahrens in den konkreten Prozess der Behörde herangezogen. Die Vorgehensweise zur Auswahl eines Zahlungsverfahrens ist in Abbildung 22 in einem Prozesskettendiagramm dargestellt und wird im Folgenden detailliert beschrieben.

---

85 Als elementare Teilszenarien werden Szenarien definiert, die bezüglich der Anforderungen in Bezug auf Eignung für wiederkehrende Zahlungen, Internationalität und Anonymität eindeutig sind. Werden z.B. über einen Online-Shop sowohl einmalige als auch wiederkehrende Zahlungen getätigt, werden diese beiden Fälle im Weiteren als zwei getrennte Teilszenarien betrachtet.

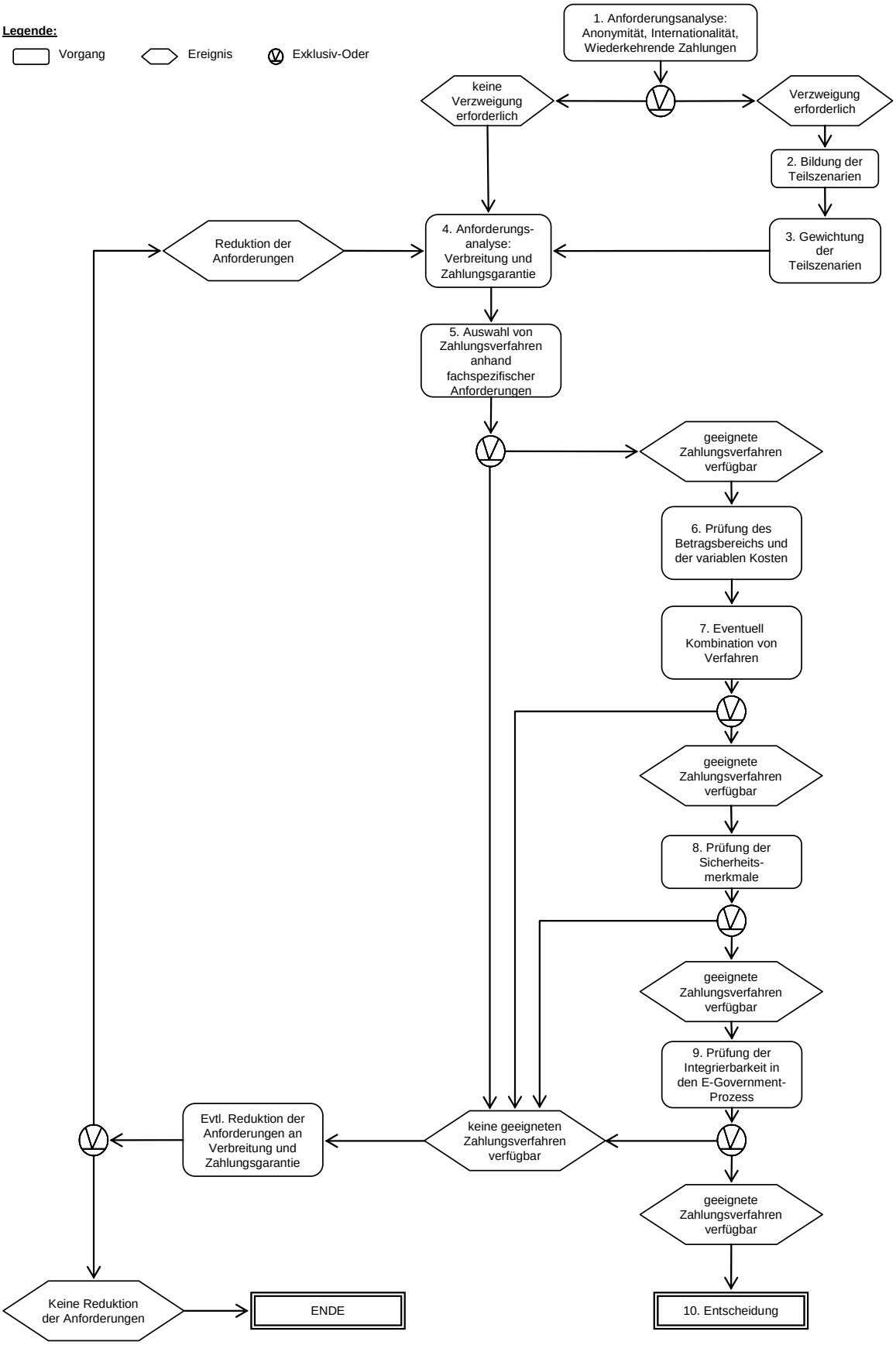


Abbildung 22: Prozesskettendiagramm zur Auswahl eines Zahlungsverfahrens

Schritt 1: Anhand der Kriterien Eignung für wiederkehrende Zahlungen (vgl. Abschnitt 5.1.1), Anonymität (vgl. Abschnitt 5.1.3) und Internationalität (vgl. Abschnitt 5.1.2) wird ermittelt, ob eine Aufspaltung des Szenarios in Teilszenarien erforderlich ist. Die Ermittlung erfolgt anhand von drei Fragen, die jeweils mit „Ja“ oder „Nein“ beantwortet werden können:

Ermittlung der Verzweigungen

- *Soll das Zahlungsverfahren sowohl einmalige Zahlungen als auch periodisch wiederkehrende Abbuchungen ermöglichen?*
- *Ist neben einer personenbezogenen auch eine anonyme Zahlungsmöglichkeit erwünscht?*
- *Soll das Zahlungsverfahren sowohl aus dem Inland als auch aus dem Ausland genutzt werden können?*

Schritt 2: Wurde mindestens eine der Fragen mit „Ja“ beantwortet, so werden nun anhand eines Baumdiagramms die relevanten Teilszenarien ermittelt. Für jede der Fragen aus Schritt 1, die mit „Ja“ beantwortet wurde, wird eine Verzweigungsebene in den Baum eingezeichnet. Aus der Kombination der maximal drei Kriterien mit jeweils zwei Ausprägungen ergeben sich damit maximal acht Teilszenarien (vgl. Abbildung 23). Jedes der Teilszenarien ist bezüglich der Anforderungen an ein Zahlungsverfahren eindeutig. Ein Teilszenario wäre z. B. die periodisch wiederkehrende Bezahlung durch ausländische Nutzer, die jedoch nicht anonym sein müssen.

Bildung der Teilszenarien

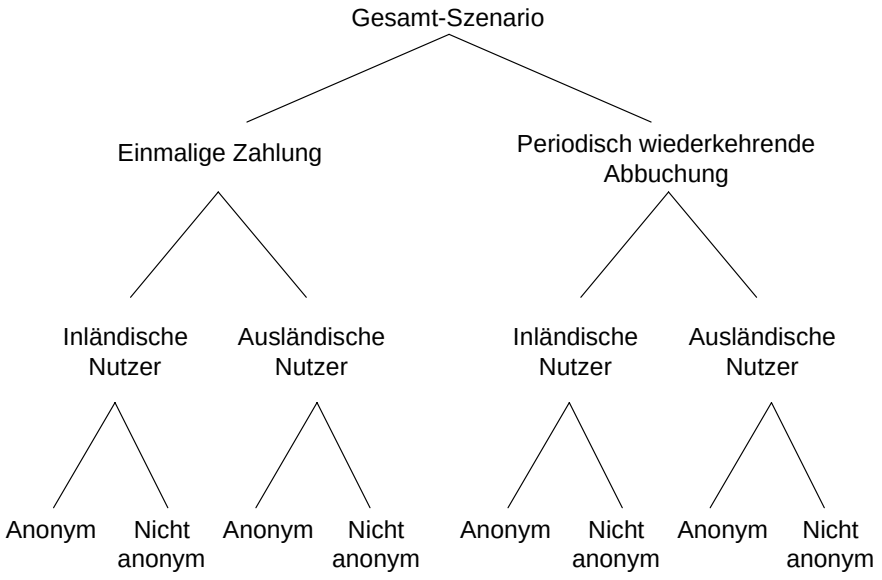


Abbildung 23: Baumdiagramm der Teilszenarien

Schritt 3: Nicht jede der in Schritt 2 ermittelten Möglichkeiten ist allerdings in der Praxis gleichbedeutend. Zur Abschätzung der relativen Bedeutung der Teilszenarien werden die Äste des Baumes daher gewichtet. Die relative Bedeutung eines Teilszenarios kann daraufhin durch Multiplikation der Gewichtungen der einzelnen Äste ermittelt werden.

Gewichtung der Teilszenarien

Schritt 4: Für jedes Teilszenario werden anschließend die Anforderungen an den Umfang der Zahlungsgarantie (vgl. Abschnitt 5.1.4) und die Verbreitung (vgl. Abschnitt 5.1.5) des Verfahrens bestimmt. Diese können sich je nach Teilszenario unterscheiden. Im Fall einer anonymen Zahlung ist die Anforderung an die Zahlungsgarantie in der Regel als hoch einzustufen, bei Zahlungen aus dem Ausland braucht die Verbreitung (in Deutschland) nicht betrachtet werden[86]. Bei ausländischen Nutzern kann die Anforderung an die Zahlungsgarantie auch bei Leistungen der hoheitlichen Verwaltung nicht abgeschwächt werden, da für das Ausland kein sofort vollstreckbarer Titel erlangt werden kann.

Definition der Anforderungen an Zahlungsgarantie und Verbreitung

Schritt 5: Für jedes Teilszenario werden nun anhand von Tabelle 24 Zahlungsverfahren ausgewählt, die die Anforderungen des Teilszenarios hinsichtlich der Kriterien Internationalität, Wiederkehrende Zahlungen, Anonymität, Zahlungsgarantie und Verbreitung mindestens wie gefordert oder besser erfüllen. Wird kein geeignetes Zahlungsverfahren gefunden, sollte in Erwägung gezogen werden, die Anforderungen hinsichtlich Zahlungsgarantie und/oder Verbreitung für das jeweilige Teilszenario zu reduzieren und die Suche zu wiederholen. Ist dies nicht möglich, bleibt die Menge geeigneter Zahlungsverfahren leer, da keines der betrachteten Zahlungsverfahren die fachspezifischen Anforderungen des Teilszenarios erfüllt.

Auswahl von Zahlungsverfahren anhand fachspezifischer Anforderungen

Schritt 6: Für die ausgewählten Zahlungsverfahren wird nun untersucht, ob sie für die zu zahlenden Beträge geeignet sind. Dies ist nur dann der Fall, wenn weder system- oder nutzerbedingte Beschränkungen gegen die Nutzung des Verfahrens für relevante Betragsbereiche sprechen noch in diesen Betragsbereichen unverhältnismäßig hohe transaktionsabhängige Kosten auftreten (wann unverhältnismäßig hohe Kosten vorliegen, liegt im Ermessen des Projektverantwortlichen). Die Eignung der Zahlungsverfahren für bestimmte Betragsbereiche und die dazugehörigen variablen Kosten für die Behörde und den Kunden sind in Tabelle 25 zusammengefasst. Die Kostenwerte in dieser Tabelle müssen bei einigen Zahlungsverfahren eventuell noch um intern auftretende Prozesskosten ergänzt oder je nach Verhandlungsmacht gegenüber dem Zahlungssystemanbieter angepasst werden. Zu prüfen ist auch, ob das Zahlungsverfahren nur von einem oder von mehreren verschiedenen Anbietern, evtl. auch in Verbindung mit einer Zahlungsverkehrsplattform (vgl. Abschnitt 4.2), wie z. B. der Zahlungsverkehrsplattform der Initiative BundOnline 2005, bezogen werden kann.

Berücksichtigung des Betragsbereichs und der variablen Kosten

86 In Abschnitt 5.1.5 wurde als Maß für die Verbreitung ausschließlich die Verbreitung im Inland definiert. Die Verbreitung im Ausland kann in verschiedenen Ländern stark unterschiedlich sein, ein einheitliches Maß für die Verbreitung im Ausland ist schwer zu bestimmen.

Schritt 7: Die Betrachtung der Betragsbereiche kann zu den Ergebnissen führen, dass das Zahlungsverfahren für den gesamten Betragsbereich geeignet, für den gesamten Betragsbereich ungeeignet oder nur für einen Teilbereich geeignet ist. Im letzteren Fall sollte versucht werden, mehrere Zahlungsverfahren so zu kombinieren, dass diese zusammen den gesamten Betragsbereich abdecken[87]. Ist weder ein Zahlungsverfahren allein noch eine Kombination aus Zahlungsverfahren für den gesamten Betragsbereich geeignet, sollte in Erwägung gezogen werden, die Anforderungen hinsichtlich Zahlungsgarantie und/oder Verbreitung zu reduzieren und die Suche nach einem Zahlungsverfahren zu wiederholen.

Eventuell Kombination von Zahlungsverfahren

Schritt 8: Nach der Betrachtung der fachspezifischen Anforderungen und der transaktionsabhängigen Kosten der Verfahren muss überprüft werden, ob die Zahlungsverfahren auch die notwendigen Sicherheitsanforderungen erfüllen. Dabei wird konkret die Frage gestellt, welche Schutzvorkehrungen die Verfahren gegen eine missbräuchliche Verwendung zu Lasten der Kunden bieten (vgl. Abschnitt 5.3). Gerade zur Bezahlung von E-Government-Dienstleistungen sollte der Kunde keine Zahlungsverfahren verwenden müssen, durch deren Nutzung er sich einem signifikanten Risiko aussetzt. Die Sicherheitsanforderungen spielen dagegen bei den weit verbreiteten Verfahren (z. B. Überweisung, Lastschrift, Nachnahme) kaum eine Rolle, da das Risiko für den Kunden nicht erst dadurch entsteht, dass die Behörde die Zahlung mit diesen Verfahren ermöglicht. Sie sind aber insbesondere für neue Zahlungsverfahren kritisch zu betrachten.

Prüfung der Sicherheitsanforderungen

Schritt 9: Für die nun vorliegende Vorauswahl von Zahlungsverfahren, die sich ausschließlich auf die Ausprägungen der Verfahren in den Tabellen 25–27 (Bewertungen der Verfahren in den Kategorien „Fachspezifische Anforderungen“, „Betragsbereich und Kostenstruktur“ und „Sicherheit“) stützt, muss nun im Detail geprüft werden, wie sich diese in den konkreten E-Government-Prozess integrieren lassen (vgl. Abschnitt 5.4). Wichtig ist dabei vor allem die Frage, zu welchem Zeitpunkt die Zahlung im Prozess erfolgt. Davon abhängig ist unter anderem, ob durch das Zahlungsverfahren Verzögerungen oder Medienbrüche im Prozess auftreten und zu welchem Zeitpunkt im Prozess eine Zahlungsgarantie für die Behörde eintritt.
Darüber hinaus muss in Abstimmung mit dem Anbieter des Zahlungsverfahrens im Detail geprüft werden, ob auch Anforderungen an die technische Implementierung für den konkreten Fall der Behörde erfüllt werden können. Dazu zählen z. B. die sichere Übermittlung der Daten, die Möglichkeit zur Vereinbarung von Service-Level-

Integrierbarkeit in den E-Government-Prozess

87 So können z.B. GeldKarte und Kreditkarte kombiniert werden, da der zu zahlende Betrag bei der GeldKarte durch den üblichen Ladebetrag des Kunden auf etwa 50 Euro begrenzt ist, wohingegen die Kreditkartenzahlung bei kleineren Beträgen für die Behörde verhältnismäßig teuer ist.

Agreements, die Erfüllung von Datenschutzbestimmungen durch den Zahlungssystemanbieter und die Unterstützung der relevanten E-Government-Standards.
Für die Auswahl eines oder mehrerer Zahlungsverfahren sind auch die fixen Kosten (einmalig oder periodisch wiederkehrend) in die Betrachtung mit einzubeziehen. Die fixen Kosten sind noch stärker als die variablen Kosten von den Gegebenheiten der Behörde abhängig, im Rahmen dieses Moduls können zu den Kosten der Zahlungsverfahren deshalb nur sehr unvollständige Angaben gemacht werden. Gegebenenfalls können auch an dieser Stelle die Anforderungen an die Verbreitung und die Zahlungsgarantie nochmals variiert werden, um die alternativen Kosten eines Zahlungsverfahrens mit geringerer Verbreitung bzw. einem geringeren Maß an Zahlungsgarantie zu ermitteln.

Entscheidung

Schritt 10: Nach Abschluss der Bewertung der Zahlungsverfahren müssen die für die Teilszenarien geeigneten Verfahren wieder zusammengefasst werden, um zu einer Entscheidung auf Gesamtszenario-Ebene zu gelangen. In den wenigsten Fällen wird es *ein* Zahlungsverfahren geben, das für alle Teilszenarien gleichermaßen geeignet ist. Stattdessen müssen unter Berücksichtigung der Bedeutung der einzelnen Teilszenarien und der Gesamtkosten der Verfahren mehrere Zahlungsverfahren ausgewählt werden. Dadurch lässt sich auch dem Problem einer zu geringen Verbreitung einzelner Zahlungsverfahren begegnen. Soweit möglich sollte für Leistungen, die anonym in Anspruch genommen werden können, unter den angebotenen Zahlungsverfahren auch mindestens ein Verfahren sein, das die anonyme Bezahlung dieser Leistungen erlaubt.

Gestaltung des Online-Angebots

Die Eignung der ausgewählten Zahlungsverfahren für die verschiedenen Teilszenarien muss bei der Gestaltung des Online-Angebots berücksichtigt werden. Durch entsprechende Regelsysteme muss gewährleistet werden, dass bestimmte Zahlungsverfahren in gewissen Teilszenarien nicht angeboten werden.

7.2 Verdeutlichung der Vorgehensweise anhand der Beispielszenarien

Anhand der in Abschnitt 7.1 vorgestellten allgemeinen Vorgehensweise soll im Folgenden eine Entscheidung hinsichtlich der am besten geeigneten Zahlungsverfahren für die in Abschnitt 3.2 vorgestellten Beispielszenarien getroffen werden. Dabei handelt es sich um die Szenarien Elektronischer Mahnantrag, Elektronische Umsatzsteuer-Voranmeldung, PKW-Kauf bei Zollauktion im Internet, Elektronische Handelsregisterauskunft, Elektronisches Begleichen eines Verwarnungsgelds für Falschparken und Online-Zugriff auf kostenpflichtige Statistik-Daten.

Um zu einer Entscheidung zu gelangen, müssen bei den folgenden Analysen teilweise Annahmen getroffen werden. Auch bei sehr ähnlich gelagerten Szenarien einer Behörde dürfen die folgenden Ergebnisse deshalb nicht ohne eine Überprüfung der zugrunde liegenden Annahmen übernommen werden.

7.2.1 Elektronischer Mahnantrag

Mit dem Antrag auf Erlass eines Mahnbescheides (Mahnantrag) wird das Mahnverfahren eingeleitet. Im Mahnantrag muss der Gläubiger Angaben zu seiner Person und zur Person des Schuldners machen sowie den geltend gemachten Anspruch erläutern. Nach Abschluss des zweistufigen Mahnverfahrens erhält der Gläubiger einen Vollstreckungstitel, mit dem er eine Zwangsvollstreckung in das Vermögen des Schuldners erwirken kann.

Schritt 1

Zunächst wird ermittelt, ob für die Auswahl eines Zahlungsverfahrens eine Aufspaltung des Szenarios in Teilszenarien sinnvoll ist:

- *Soll das Zahlungsverfahren sowohl einmalige Zahlungen als auch periodisch wiederkehrende Abbuchungen ermöglichen?*
  Nein. Der Betrag ist für jeden Mahnantrag einzeln in einer Summe zu zahlen.
- *Ist neben einer personenbezogenen auch eine anonyme Zahlungsmöglichkeit erwünscht?*
  Nein. Die Identifikation des Gläubigers ist für das Verfahren ohnehin notwendig.
- *Soll das Zahlungsverfahren sowohl aus dem Inland als auch aus dem Ausland genutzt werden können?*
  Nein. Für Antragsteller mit Sitz im Ausland ist ausschließlich das Amtsgericht Berlin-Schöneberg zuständig. In den übrigen Amtsgerichten werden keine Anträge aus dem Ausland gestellt.

Schritt 2 und 3

Da alle Fragen mit „Nein“ beantwortet wurden, sind keine Verzweigungen notwendig. Es wird ausschließlich das Szenario (Einmalige Zahlung, Inland, nicht anonym) betrachtet.

Schritt 4

Die Zahlungsgarantie muss in diesem Szenario nicht hoch sein, da im hoheitlichen Bereich eine vereinfachte Vollstreckung möglich ist (vgl. Abschnitt 3.1.6). Da jedoch der Antragsteller nicht authentifiziert ist[88], sollte das Zahlungsverfahren bezüglich der Zahlungsgarantie mindestens mit „mittel“ bewertet sein. Ein nur „mittel“ verbreitetes Zahlungsverfahren dürfte für den elektronischen Mahnantrag ausreichen, da das Verfahren an sich relativ komplex ist und für den „Erstmahner“ damit zwangsläufig ein gewisser Einarbeitungsaufwand verbunden ist. Ein unter Umständen erforderlicher zusätzlicher Registrierungsaufwand für das Zahlungsverfahren stellt deshalb keine zusätzlich Hürde für die Nutzung des Online-Angebots dar.

Schritt 5

Für die genannten Anforderungen sind mehrere Zahlungsverfahren verfügbar. Im Einzelnen sind dies die Online-Überweisung, die Überweisung vor Lieferung, die Nachnahme, Vodafone m-pay und click&buy (vgl. Tabelle 27).

---

88 Der Antragsteller identifiziert sich gegenüber der Behörde, d. h. er gibt einen Namen an. Er ist jedoch nicht authentifiziert, da die Behörde nicht überprüft, ob der angegebene Name auch der tatsächliche Name des Antragstellers ist.

Teilszenario	Rel. Bedeutung	Verbreitung	Zahlungsgarantie	Verfahren
Einmalige Zahlung, Inland, nicht anonym	100%	Mittel	Mittel	Online-Überweisung, Überweisung vor Lieferung, Nachnahme, Vodafone m-pay, click&buy

Tabelle 27: Ergebnisse von Schritt 5 für das Szenario "Elektronischer Mahnantrag"

Schritt 6 und 7

Der relevante Betragsbereich richtet sich nach der Gerichtskostentabelle und beginnt bei 18,00 Euro [AGM 2004, S. 83]. Mit Ausnahme von click&buy und Vodafone m-pay, die nur Beträge bis 10 Euro zulassen, sind die Verfahren für den gesamten Betragsbereich geeignet. Die Zahlungsverfahren Vodafone m-pay und click&buy werden daher nicht weiter betrachtet. Abbildung 24 zeigt die transaktionsabhängigen Kosten der verbleibenden Verfahren. Aus der Abbildung wird ersichtlich, dass bei geringen Beträgen die Kosten der Nachnahme, bei höheren Beträgen die Kosten der Online-Überweisung sehr hoch sind. Es empfiehlt sich daher, die Online-Überweisung nur bis zu einem bestimmten Höchstbetrag und die Zahlung per Nachnahme erst ab einem Mindestbetrag zuzulassen. Diese Verfahren sollten daher nur mit mindestens einem der beiden anderen Verfahren kombiniert angeboten werden.

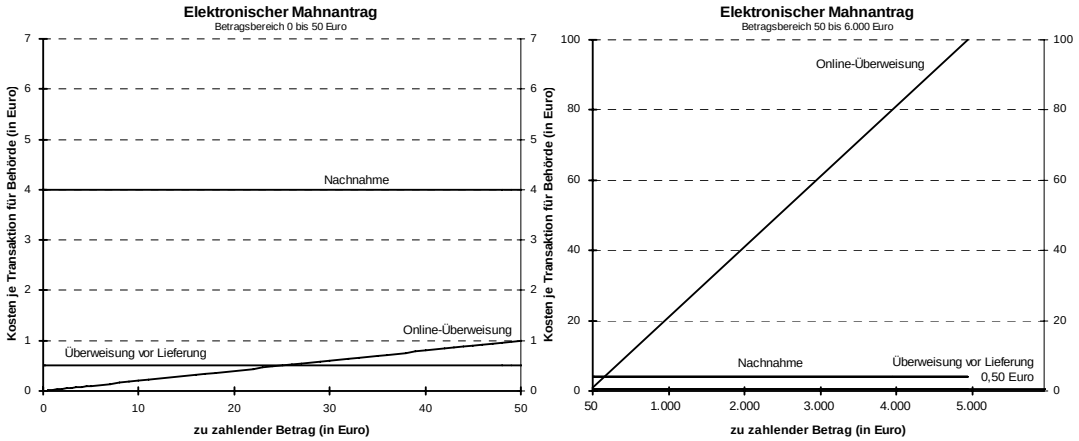


Abbildung 24: Kostenverläufe der Zahlungsverfahren für den elektronischen Mahnantrag[89]

Schritt 8

Nach der Analyse des Betragsbereichs und der transaktionsabhängigen Kosten werden die Sicherheitsanforderungen betrachtet. Den Ausgangspunkt dafür bilden die Sicherheitsanforderungen aus Kundensicht in Tabelle 26, d. h. welche Schutzvorkehrungen die Verfahren gegen eine missbräuchliche Verwendung zu Lasten der Kunden bieten. Zur Bezahlung von E-Government-Dienstleistungen sollte der Kunde keine Zahlungsverfahren verwenden müssen, durch deren Nutzung er sich

89 Annahmen:
- Überweisung vor Lieferung: Es fallen Buchungspostengebühren von 0,50 Euro an.
- Online-Überweisung: Es fällt ein Disagio von 2% an.
- Nachnahme: Es fallen 4 Euro Nachnahmeentgelt und 2 Euro Übermittlungsentgelt an.

einem signifikanten Risiko aussetzt. Die betrachteten Verfahren sind in dieser Hinsicht unbedenklich. Bei der Überweisung und der Nachnahme ist ein Missbrauch zu Lasten des Kunden zwar grundsätzlich möglich, dies jedoch unabhängig davon, ob die Verfahren zur Bezahlung von E-Government-Leistungen eingesetzt werden.

Schritt 9

Für die verbleibenden Verfahren Online-Überweisung, Überweisung vor Lieferung und Nachnahme wird nun die Integrierbarkeit in den konkreten Prozess der Behörde betrachtet. Dabei zeigt sich, dass die Nachnahme für den Fall des elektronischen Mahnantrags nur wenig geeignet ist. Zwar wird der Vollstreckungstitel dem Gläubiger postalisch zugestellt, weshalb eine Bezahlung per Nachnahme grundsätzlich sehr gut geeignet wäre. Bei Nichtannahme der Urkunde wären jedoch alle Leistungen der Behörde bereits erbracht, u. a. auch die Zustellung des Vollstreckungsbescheids an den Schuldner.

Dieses Beispiel zeigt, dass die Nachnahme in jedem Szenario erst dann ausgeschlossen werden kann, wenn feststeht, zu welchem Zeitpunkt im Prozess eine Zahlungsgarantie erforderlich ist und wann Medienbrüche auftreten. Das Vorgehensmodell folgt jedoch der Logik, zunächst durch einfach zu beantwortende Fragen möglichst viele Verfahren auszuschließen und erst dann die Eignung der verbleibenden Verfahren bezüglich aufwändiger zu ermittelnder Anforderungen zu überprüfen, die eine detaillierte Betrachtung des Prozessablaufs erfordern. Die Nachnahme ist auch nicht nur ausschließlich dann anwendbar, wenn physische Güter versandt werden. So kann auch ein Zugangscode für die Nutzung eines elektronischen Angebots auf dem Postweg versandt werden. Der Kunde erhält diesen Zugangscode in diesem Fall nur, wenn er die entsprechende Nachnahmegebühr entrichtet hat.

Bei der Überweisung vor Lieferung tritt das Problem auf, dass es notwendigerweise zu einem Prozessbruch kommt. Bezüglich der Anforderungen an die technische Implementierung wird angenommen, dass diese von den Verfahren erfüllt werden können, die fixen Kosten dürften für diese Verfahren verhältnismäßig gering sein.

Schritt 10

Die Online-Überweisung erfüllt die fachspezifischen Anforderungen und ermöglicht zudem eine Bezahlung der Leistung ohne Prozessbruch. Die transaktionsabhängigen Kosten des Verfahrens sind jedoch gerade für höhere Beträge vergleichsweise hoch. Es bietet sich daher an, die Bezahlung per Online-Überweisung nur bis zu einem Höchstbetrag zuzulassen und ergänzend das Verfahren Überweisung vor Lieferung anzubieten, das zudem weit verbreitet ist. Die Nachnahme sollte für die Bezahlung des elektronischen Mahnantrags nicht angeboten werden, da der Zahlungszeitpunkt für diesen Prozess zu spät stattfindet.

7.2.2 Elektronische Umsatzsteuer-Voranmeldung

Die Umsatzsteuer-Voranmeldung muss von selbstständigen Unternehmern, abhängig von der Steuerhöhe des Vorjahres, monatlich oder vierteljährlich erfolgen. Der Unternehmer ermittelt dabei selbst, ob eine Umsatzsteuer-Vorauszahlung fällig ist. Ist dies der Fall, ist die Zahlung spätestens zehn Tage nach Ablauf des betreffenden Monats bzw. Vierteljahres zu leisten.

Zunächst wird ermittelt, ob für die Auswahl eines Zahlungsverfahrens eine Aufspaltung des Szenarios in Teilszenarien sinnvoll ist: **Schritt 1**

- *Soll das Zahlungsverfahren sowohl einmalige Zahlungen als auch periodisch wiederkehrende Abbuchungen ermöglichen?*
  Nein. Der Betrag wird vom steuerpflichtigen Unternehmer jeweils neu berechnet, die Zahlungen müssen deshalb auch einzeln ausgelöst werden.
- *Ist neben einer personenbezogenen auch eine anonyme Zahlungsmöglichkeit erwünscht?*
  Nein. Die Identität des Steuerpflichtigen steht ohnehin fest.
- *Soll das Zahlungsverfahren sowohl aus dem Inland als auch aus dem Ausland genutzt werden können?*
  Nein. Ähnlich wie beim elektronischen Mahnverfahren wurden für die Besteuerung ausländischer Unternehmer zentrale Zuständigkeiten geschaffen. Für den Großteil der Finanzämter ist dieser Fall daher nicht relevant.

Da alle Fragen mit „Nein“ beantwortet wurden, sind keine Verzweigungen notwendig. Es wird ausschließlich das Szenario (Einmalige Zahlung, Inland, nicht anonym) betrachtet. **Schritt 2 und 3**

Die Anforderung an die Zahlungsgarantie ist für dieses Szenario nur „gering“, da die Besteuerung dem hoheitlichen Bereich zuzuordnen ist und, im Gegensatz zum elektronischen Mahnantrag, die Person des Steuerpflichtigen eindeutig feststeht. Bezüglich der Verbreitung reicht die Anforderung „mittel“ aus, da eventuelle Mehraufwände für die Registrierung durch regelmäßige Effizienzsteigerungen bei Umsatzsteuer-Vorauszahlungen ausgeglichen werden. Eventuell würde sogar die Anforderung „gering“ ausreichen, es soll jedoch zunächst versucht werden, ein geeignetes Verfahren mit mittlerer Verbreitung zu finden. **Schritt 4**

Aufgrund der vergleichsweise niedrigen Anforderungen bezüglich der Zahlungsgarantie und Verbreitung stehen acht Zahlungsverfahren zur Auswahl, die diese Anforderungen erfüllen: Die Überweisung vor bzw. nach Lieferung, die Lastschrift, die Kreditkarte, die Online-Überweisung, die Nachnahme, Vodafone m-pay und click&buy (vgl. Tabelle 28). **Schritt 5**

Teilszenario	Rel. Bedeutung	Verbreitung	Zahlungsgarantie	Verfahren
Einmalige Zahlung, Inland, nicht anonym	100%	Mittel	Gering	Online-Überweisung, Überweisung vor und nach Lieferung, Lastschrift, Kreditkarte, Nachnahme, click&buy

Tabelle 28: Ergebnisse von Schritt 5 für das Szenario "Umsatzsteuer-Voranmeldung"

Das Betragsspektrum ist beim Szenario „Elektronische Umsatzsteuer-Voranmeldung“ nicht begrenzt, es reicht von wenigen Cents bis zu mehreren tausend Euro. Vodafone m-pay und click&buy erlauben jedoch nur die Bezahlung von Beträgen bis zehn Euro, die Nachnahme ist auf Beträge bis 5.000 Euro beschränkt. Bei der Kreditkarte liegt die Grenze beim individuellen Transaktionsli- **Schritt 6**

mit des Kunden, häufig beträgt dieses ebenfalls 5.000 Euro. Den Verlauf der Kostenkurven in den unterschiedlichen Betragsbereichen zeigt Abbildung 25.

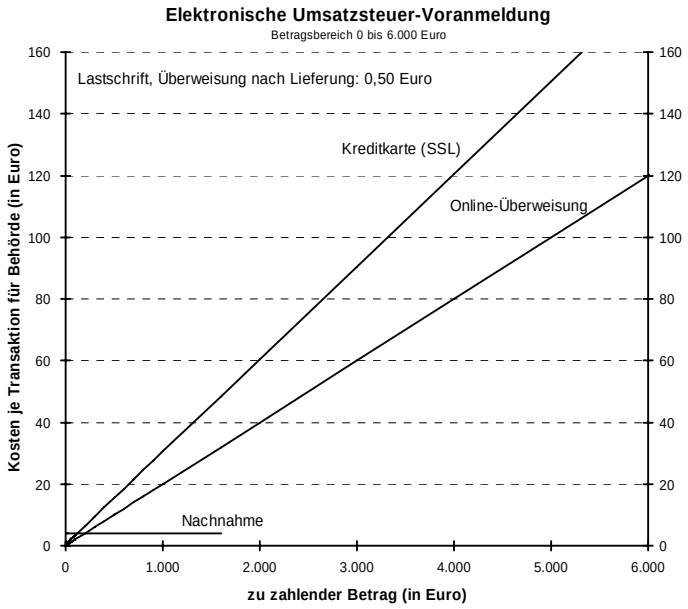


Abbildung 25: Kostenverläufe der Zahlungsverfahren für die elektronische Umsatzsteuer-Voranmeldung[90]

Schritt 7

Da nicht alle Verfahren das gesamte Betragsspektrum abdecken und sich die Kostenkurven schneiden, sollte an dieser Stelle die Kombination von Verfahren in Erwägung gezogen werden. Nachnahme und Kreditkarte beispielsweise können wohl nur in Kombination mit der Überweisung, Lastschrift oder Online-Überweisung angeboten werden, um auch die Bezahlung von Beträgen über 5.000 Euro zu ermöglichen. Zugleich zeigt die Betrachtung der Kostenkurven, dass die Zahlung per Kreditkarte und Online-Überweisung für höhere Beträge mit hohen Gebühren verbunden ist, während die Kosten bei der Überweisung und der Lastschrift sehr gering sind. Vodafone m-pay und click&buy könnten eventuell mit der Nachnahme kombiniert werden, aufgrund der geringen Relevanz des Betragsbereichs bis 10 Euro sollen diese Verfahren jedoch zunächst ganz aus der Betrachtung ausgeschlossen werden.

Schritt 8 und 9

Die Berücksichtigung von Sicherheitsaspekten aus Kundensicht ist bei den betrachteten Zahlungsverfahren unproblematisch, da es sich ausschließlich um allgemein akzeptierte Verfahren handelt. Bei der Betrachtung der Frage, wie diese Zahlungsverfahren in den konkreten Prozess der Behörde integriert werden können, scheidet zunächst die Überweisung vor Lieferung aus, da es sich bei der Umsatzsteuer um eine Zahlung ohne direkte Gegenleistung handelt. Auch die Last-

90 Annahmen:
- Lastschrift, Überweisung nach Lieferung: Es fallen Buchungspostengebühren von 0,50 Euro an.
- Nachnahme: Es fallen 2 Euro Nachnahmeentgelt und 2 Euro Übermittlungsentgelt an.
- Online-Überweisung: Es fällt ein Disagio von 2% an.
- Kreditkarte (SSL): Es fallen transaktionsbezogene Fixkosten in Höhe von 0,50 Euro und 3% Disagio bzgl. Umsatzes an.

schrift und die Nachnahme werden nicht weiter berücksichtigt, da die Prozesse sehr umständlich wären und sich keine erkennbaren Vorteile gegenüber der Überweisung nach Lieferung ergeben. Die Online-Überweisung und die Kreditkarte weisen den Vorteil auf, dass eine Bezahlung ohne Prozessbruch unmittelbar nach Ermittlung der Umsatzsteuerschuld möglich ist. Bezüglich der Anforderungen an die technische Implementierung wird angenommen, dass diese von den verbleibenden Verfahren erfüllt werden können, die fixen Kosten für die Überweisung, Kreditkarte und Online-Überweisung dürften verhältnismäßig gering sein.

Schritt 10

Von den verbleibenden Verfahren ist die Überweisung für die Behörde das kostengünstigste und sollte daher in jedem Fall angeboten werden. Eine sinnvolle Ergänzung stellen die Online-Überweisung und/oder die Kreditkarte dar, die eine bequeme Bezahlung ohne Prozessbruch erlauben. Aufgrund der hohen Kosten für höhere Beträge sollte das Angebot dieser Verfahren jedoch auf einen Höchstbetrag beschränkt werden.

7.2.3 PKW-Kauf bei Zollauktion im Internet

Über die Versteigerungsplattform des Zolls[91] wurden im dritten Quartal des Jahres 2003 über 400 ausgesonderte PKW der Bundes-, Landes- und Kommunalverwaltungen versteigert. Um an der Auktion teilnehmen zu können, muss sich der Kunde zuerst registrieren und bekommt anschließend ein Passwort per E-Mail zugesandt. Nach Erteilung des Zuschlags muss der PKW innerhalb von vier Wochen unter Vorlage des Personalausweises und eines Ausdrucks der E-Mail über den Zuschlag abgeholt werden, ansonsten wird der PKW erneut versteigert.

Schritt 1

Zunächst wird ermittelt, ob für die Auswahl eines Zahlungsverfahrens eine Aufspaltung des Szenarios in Teilszenarien sinnvoll ist:

- *Soll das Zahlungsverfahren sowohl einmalige Zahlungen als auch periodisch wiederkehrende Abbuchungen ermöglichen?*
  Nein. Der Betrag ist im Falle des Zuschlags in einer Summe zu zahlen.
- *Ist neben einer personenbezogenen auch eine anonyme Zahlungsmöglichkeit erwünscht?*
  Nein. Der Abholer des PKW muss sich ohnehin als Meistbietender ausweisen.
- *Soll das Zahlungsverfahren sowohl aus dem Inland als auch aus dem Ausland genutzt werden können?*
  Ja. Im Interesse hoher Versteigerungserlöse ist eine möglichst große Nutzerzahl erwünscht.

Schritt 2 und 3

Da die dritte Frage mit „Ja“ beantwortet wurde, sind je nach Inanspruchnahme der Leistung durch inländische oder ausländische Nutzer zwei Teilszenarien zu unterscheiden. Im Folgenden wird davon ausgegangen, dass die Nutzung der Zoll-Auktion zu 90% durch Kunden aus dem Inland erfolgt.

Schritt 4

Für die beiden Teilszenarien werden nun die Anforderungen an die Zahlungsgarantie und die Verbreitung festgelegt. Die Zahlungsgarantie sollte möglichst be-

91 Siehe dazu http://www.zoll-d.de/auktion/.

reits zum Zeitpunkt der Zuschlagserteilung „hoch“ sein, um den Aufwand für eine erneute Versteigerung mit einem evtl. geringeren Erlös zu verhindern, falls der PKW nicht abgeholt wird. Spätestens zum Zeitpunkt der Übergabe des PKW muss die Zahlungsgarantie in jedem Fall „hoch“ sein. Auch die Verbreitung in Deutschland sollte „hoch“ sein, um eine möglichst große Nutzerzahl zu erreichen.

Schritt 5

Anhand von Tabelle 24 werden anschließend die Zahlungsverfahren ausgewählt, die die bis jetzt ermittelten Anforderungen der Teilszenarien erfüllen. Dies sind für bei ausländischen Nutzern die Überweisung vor Lieferung, die Nachnahme und Vodafone m-pay, bei ausländischen Nutzern kommen neben der Überweisung vor Lieferung und der Nachnahme noch 3-D Secure, die paysafecard und moneybookers in Frage (vgl. Tabelle 29).

Teilszenario	Rel. Bedeutung	Verbreitung	Zahlungsgarantie	Verfahren
Einmalige Zahlung, Inland, nicht anonym	90%	Hoch	Hoch	Überweisung vor Lieferung, Nachnahme, Vodafone m-pay
Einmalige Zahlung, Ausland, nicht anonym	10%	nicht relevant	Hoch	Überweisung vor Lieferung, Nachnahme, 3-D Secure, paysafecard, moneybookers

Tabelle 29: Ergebnisse von Schritt 5 für das Szenario "PKW-Kauf bei Zollauktion"

Schritt 6 und 7

Für diese Verfahren wird nun überprüft, ob sie für den betrachteten Betragsbereich geeignet sind. Bei der Versteigerung eines PKW dürfte der Versteigerungserlös in der überwiegenden Zahl der Fälle über 500 Euro liegen. Für diesen Betragsbereich sind Vodafone m-pay, die paysafecard und moneybookers nicht mehr geeignet, die Nachnahme ist nur für Beträge bis 5.000 Euro möglich. Evtl. ist daher die Betrachtung der Kombination der Nachnahme mit der Überweisung vor Lieferung oder 3-D Secure erforderlich, die beide das gesamte Betragsspektrum abdecken. Die Kostenverläufe der verbleibenden Verfahren sind in Abbildung 26 dargestellt.

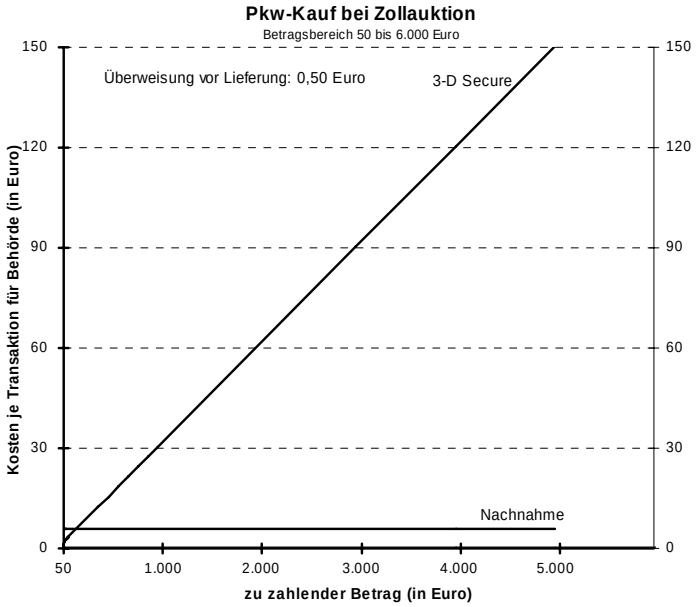


Abbildung 26: Kostenverläufe der Zahlungsverfahren für den PKW-Kauf bei der Zollauktion[92]

Schritt 8

Bezüglich der Sicherheit aus Kundensicht sind die betrachteten Verfahren unbedenklich. Bei der Überweisung und der Nachnahme ist ein Missbrauch zu Lasten des Kunden zwar grundsätzlich möglich, dies jedoch unabhängig davon, ob die Verfahren zur Bezahlung von E-Government-Leistungen eingesetzt werden.

Schritt 9

Für die verbleibenden Verfahren Überweisung vor Lieferung, 3-D Secure und Nachnahme wird nun die Art der Integration in den konkreten E-Government-Prozess der Behörde betrachtet. Bei der Nachnahme wäre die Möglichkeit der Zustellung des Kfz-Briefs und Kfz-Scheins mit den Schlüsseln und einer Beschreibung des Standorts zu prüfen. Gegen die Nachnahme sprechen jedoch auch der eingeschränkte Betragsbereich und der späte Zahlungszeitpunkt, weshalb diese Variante nicht weiter in Erwägung gezogen wird. Der Prozessbruch bei der Überweisung vor Lieferung spielt in diesem Szenario keine Rolle, da es aufgrund der Notwendigkeit der Abholung des PKW ohnehin zu einer Prozessunterbrechung kommt. Ein Nachteil der Überweisung vor Lieferung ist jedoch, dass die Zahlungsgarantie im Vergleich zu 3-D Secure erst später im Prozess eintritt[93]. Bezüglich der Anforderungen an die technische Implementierung wird angenommen, dass diese von den beiden Verfahren erfüllt werden können.

Schritt 10

Da 3-D Secure die Anforderung an die Verbreitung im Teilszenario (Einmalige Zahlung, Inland, nicht anonym) nicht erfüllt, ist zunächst die Überweisung vor Lieferung anzubieten. Es sollte jedoch in Erwägung gezogen werden, 3-D Secure

---

92 Annahmen:
- Überweisung vor Lieferung: Es fallen Buchungspostengebühren von 0,50 Euro an.
- 3-D Secure: Es fallen transaktionsbezogene Fixkosten in Höhe von 0,50 Euro und 3% Disagio bzgl. Umsatzes an.
- Nachnahme: Es fallen 4 Euro Nachnahmeentgelt und 2 Euro Übermittlungsentgelt an.

93 Dies gilt unter der Annahme, dass der Kunde die Zahlung bei 3-D Secure unmittelbar nach Erteilung des Zuschlags vornehmen muss. Evtl. könnte die Zahlung auch bereits bei Abgabe des Gebots vorautorisiert werden.

als alternatives Zahlungsverfahren zu implementieren, da die Zahlung per Kreditkarte von den Nutzern häufig als sehr bequem empfunden wird und die Zahlungsgarantie für die Behörde bereits früher eintritt. Aufgrund der hohen Kosten der Kreditkartenzahlung für höhere Beträge sollte jedoch ein Höchstbetrag festgelegt werden.

7.2.4 Elektronische Handelsregisterauskunft

Spätestens ab dem 01.01.2007 muss das Handelsregister vollständig elektronisch geführt werden[94]; ein Großteil der Handelsregistereintragungen liegt bereits heute in elektronischer Form vor. Dadurch eröffnet sich die Möglichkeit, Handelsregisterauskünfte auch zeit- und ortsunabhängig über das Internet abzurufen. Von Notaren, Rechtsanwälten und Kreditinstituten wird diese Möglichkeit bereits heute häufig genutzt, die anfallenden Gebühren werden dabei per Lastschrift eingezogen. Für gelegentliche Nutzer sollte der Abruf von Informationen jedoch auch ohne vorherige Registrierung möglich sein. Im Folgenden wird daher ein geeignetes Zahlungsverfahren für die elektronische Handelsregisterauskunft durch gelegentliche Nutzer ausgewählt.

Schritt 1

Zunächst wird ermittelt, ob für die Auswahl eines Zahlungsverfahrens eine Aufspaltung des Szenarios in Teilszenarien sinnvoll ist:

- *Soll das Zahlungsverfahren sowohl einmalige Zahlungen als auch periodisch wiederkehrende Abbuchungen ermöglichen?*
  Nein. Die Gebühr richtet sich nach der Anzahl der Abrufe.
- *Ist neben einer personenbezogenen auch eine anonyme Zahlungsmöglichkeit erwünscht?*
  Ja. Eine Identifizierung des Kunden ist für dieses Szenario nicht erforderlich.
- *Soll das Zahlungsverfahren sowohl aus dem Inland als auch aus dem Ausland genutzt werden können?*
  Ja. Der Abruf von Handelsregisterauskünften muss aufgrund des Diskriminierungsverbots auch aus anderen Staaten der EU möglich sein.

Schritt 2 und 3

Aus den beiden Verzweigungen im Baumdiagramm ergeben sich vier Teilszenarien. Es wird davon ausgegangen, dass etwa 10% der Nutzer aus dem Ausland stammen. Die Bedeutung anonymer und nicht anonymer Zahlungen wird gleich gewichtet.

Schritt 4

Für die vier Teilszenarien werden nun die Anforderungen an die Zahlungsgarantie und die Verbreitung festgelegt. Die Zahlungsgarantie muss im Szenario (Einmalige Zahlung, Inland, nicht anonym) nicht hoch sein, da im hoheitlichen Bereich eine vereinfachte Vollstreckung möglich ist (vgl. Abschnitt 3.1.6). Da jedoch der

[94] Vgl. Richtlinie 2003/58/EG des Europäischen Parlaments und des Rates vom 15. 07.2003 zur Änderung der Richtlinie 68/151/EWG des Rates in Bezug auf die Offenlegungspflichten von Gesellschaften bestimmter Rechtsformen.

Antragsteller nicht authentifiziert ist[95], sollte das Zahlungsverfahren bezüglich der Zahlungsgarantie mindestens mit „mittel“ bewertet sein. Für die übrigen Teilszenarien ist eine hohe Zahlungsgarantie erforderlich. Da auch bei Gelegenheitsnutzern von einer gewissen Häufigkeit der Nutzung ausgegangen werden kann, dürfte ein „mittel“ verbreitetes Zahlungsverfahren für dieses Szenario ausreichen.

Schritt 5

Für jedes der Teilszenarien werden nun anhand von Tabelle 24 diejenigen Zahlungsverfahren ermittelt, die die Anforderungen des Teilszenarios hinsichtlich der Kriterien Internationalität, Wiederkehrende Zahlungen, Anonymität, Zahlungsgarantie und Verbreitung mindestens oder besser erfüllen.

Teilszenario	Rel. Bedeutung	Verbreitung	Zahlungsgarantie	Verfahren
Einmalige Zahlung, Inland, nicht anonym	45%	Mittel	Mittel	Online-Überweisung, Überweisung vor Lieferung, Nachnahme, click&buy, Vodafone m-pay
Einmalige Zahlung, Inland, anonym	45%	Mittel	Hoch	Vodafone m-pay
Einmalige Zahlung, Ausland, anonym	5%	nicht relevant	Hoch	paysafecard, 3-D Secure, moneybookers
Einmalige Zahlung, Ausland, nicht anonym	5%	nicht relevant	Hoch	Überweisung vor Lieferung, 3-D Secure, paysafecard, moneybookers, Nachnahme

Tabelle 30: Ergebnisse von Schritt 5 für das Szenario „Handelsregisterauskunft“

Schritt 6 und 7

Für gelegentliche Nutzer liegt der zu zahlende Betrag derzeit bei acht Euro je Abruf. Jedes der betrachteten Verfahren lässt die Zahlung dieses Betrags zu. In Abbildung 27 sind die transaktionsabhängigen Kosten der Verfahren für ein Betragsspektrum von 0 bis 50 Euro dargestellt, auch wenn derzeit nur die Kosten für einen Betrag von acht Euro relevant sind. Würde der Betrag für einen Abruf in Zukunft wesentlich erhöht, wären die Gebühren bei der paysafecard wohl deutlich zu hoch, für den Betrag für acht Euro werden sie jedoch noch akzeptiert. Die Nachnahme soll im Folgenden ausgeschlossen werden, da die Gebühren bei 50% des zu zahlenden Betrags liegen.

95 Der Antragsteller identifiziert sich gegenüber der Behörde, d. h. er gibt einen Namen an. Er ist jedoch nicht authentifiziert, da die Behörde nicht überprüft, ob der angegebene Name auch der tatsächliche Name des Antragstellers ist.

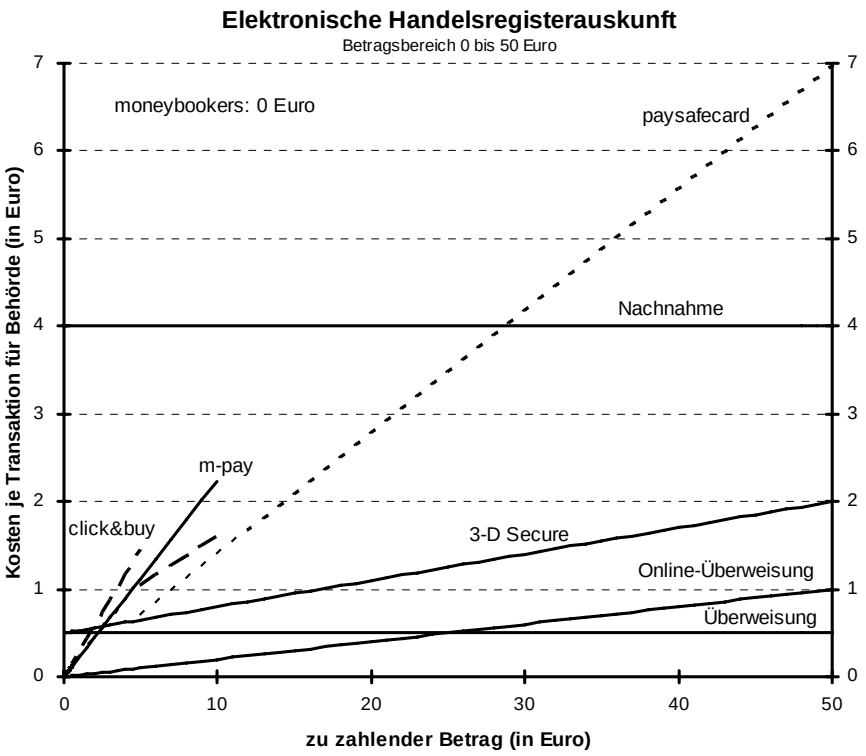


Abbildung 27: Kostenverläufe der Zahlungsverfahren für die elektronische Handelsregisterauskunft[96]

Schritt 8

Nach der Analyse der transaktionsabhängigen Kosten werden die Sicherheitsanforderungen betrachtet. Zur Bezahlung von E-Government-Dienstleistungen sollte der Kunde keine Zahlungsverfahren verwenden müssen, durch deren Nutzung er sich einem signifikanten Risiko aussetzt. Unproblematisch sind in dieser Hinsicht die Überweisung und die Nachnahme, da es sich hierbei um gängige Verfahren handelt. Ein Missbrauchsrisiko entsteht also nicht erst durch die Nutzung einer E-Government-Dienstleistung. Das Zahlungsverfahren click&buy weist bei nicht sorgfältigem Umgang mit der PIN ein gewisses Risiko für den Kunden auf, dass Dritte Verfügungen in unbegrenzter Höhe vornehmen können. Bei der paysafecard besteht das Risiko des Verlusts der Karte und damit wie beim Bargeld auch des verbleibenden Restguthabens.

---

96 Annahmen:

- m-pay: Umsatz > 2.596 Euro je Monat.
- Überweisung: Es fallen Buchungspostengebühren von 0,50 Euro an.
- Online-Überweisung: Es fällt ein Disagio von 2% an.
- 3-D Secure: Es fallen transaktionsbezogene Fixkosten in Höhe von 0,50 Euro und 3% Disagio bzgl. des Umsatzes an.
- Nachnahme: Es fallen 2 Euro Nachnahmeentgelt und 2 Euro Übermittlungsentgelt an.
- paysafecard: Es handelt sich um immaterielle Güter. Das Disagio bis 5 Euro beträgt 19% zzgl. 16% USt., über 5 Euro beträgt das Disagio 12% zzgl. 16% USt. bzgl. des für den Kunden zu zahlenden Betrages.
- click&buy: Es handelt sich um Standardkunden. Die Behörde erzielt ein Forderungsvolumen von über 50.000 bis 250.000 Euro: Bei Tarifierung bis 5 Euro beträgt die Provision 25% zzgl. 16% USt., bei Tarifierung über 5 Euro beträgt die Provision 9,5% zzgl. USt.

Abschließend stellt sich die Frage, wie sich die Verfahren in den konkreten Prozess der Behörde integrieren lassen. Bei der Überweisung vor Lieferung kommt es notwendigerweise zu einem Prozessbruch. Die verbleibenden Verfahren sind für eine Integration in diesen Prozess sehr gut geeignet, die Erfüllung der Anforderungen an die technische Implementierung wird im Folgenden vorausgesetzt. Auch die fixen Kosten werden bei der folgenden Entscheidung nicht berücksichtigt. **Schritt 9**

Vodafone m-pay besticht zwar durch seine im Vergleich zu anderen Verfahren hohe Verbreitung im Inland, ist aber nicht von ausländischen Kunden nutzbar und mit sehr hohen Kosten verbunden. Sowohl die paysafecard als auch 3-D Secure und moneybookers ermöglichen dagegen eine anonyme Zahlung und sind auch aus dem Ausland nutzbar. Bei moneybookers fallen für die Behörde keine transaktionsabhängigen Gebühren an, fraglich ist jedoch, ob der Kunde die transaktionsabhängigen Kosten akzeptiert. Eventuell wäre zu prüfen, ob eine Übernahme der Kosten durch die Behörde gewünscht und organisatorisch möglich wäre. In jedem Fall ist eine Kombination von Verfahren sinnvoll, da keines der Verfahren ohne weiteres von allen Kunden genutzt werden kann. **Schritt 10**

7.2.5 Elektronisches Begleichen eines Verwarnungsgelds für Falschparken

Bei unrechtmäßiger Nutzung eines Parkplatzes wird am Fahrzeug eine Verwarnung mit Zahlungsaufforderung angebracht („Strafzettel“). Dabei wird zunächst nur das amtliche Kennzeichen des Fahrzeugs erfasst. Nur wenn für die entsprechende Verwarnungsnummer innerhalb einer vorgegebenen Frist keine Zahlung eingeht, werden anhand des Kennzeichens Name und Anschrift des Fahrzeughalters ermittelt und es wird ein Bußgeldverfahren eingeleitet.

Zunächst wird ermittelt, ob für die Auswahl eines Zahlungsverfahrens eine Aufspaltung des Szenarios in Teilszenarien sinnvoll ist: **Schritt 1**

- *Soll das Zahlungsverfahren sowohl einmalige Zahlungen als auch periodisch wiederkehrende Abbuchungen ermöglichen?*
  Nein. Der Betrag ist für jede Verwarnung einzeln in einer Summe zu zahlen.
- *Ist neben einer personenbezogenen auch eine anonyme Zahlungsmöglichkeit erwünscht?*
  Ja. Die Identität des Fahrzeughalters wird bis zur Einleitung des Bußgeldverfahrens nicht festgestellt. Die Ordnungswidrigkeit muss zudem nicht notwendigerweise durch den Fahrzeughalter selbst begangen worden sein.
- *Soll das Zahlungsverfahren sowohl aus dem Inland als auch aus dem Ausland genutzt werden können?*
  Ja. Die Ordnungswidrigkeit kann auch von ausländischen Staatsbürgern begangen worden sein, die sich nur vorübergehend in Deutschland aufhalten.

Aus den beiden Verzweigungen im Baumdiagramm ergeben sich vier Teilszenarien. Es wird jedoch davon ausgegangen, dass eine Zahlung aus dem Ausland für nicht mehr als fünf Prozent der Fälle erforderlich ist. Die Bedeutung anonymer und nicht anonymer Zahlungen wird gleich gewichtet. **Schritt 2 und 3**

Für die vier Teilszenarien werden nun die Anforderungen an die Zahlungsgarantie und die Verbreitung festgelegt. Für keines der Teilszenarien ist eine Zahlungsgarantie erforderlich, da die Ordnungswidrigkeit zum Zeitpunkt der Verwarnung bereits erfolgt ist (vgl. Abschnitt 3.1.4). Für deutsche Staatsbürger sollte ein weit verbreitetes Zahlungsverfahren angeboten werden. **Schritt 4**

Da die Anforderung an die Zahlungsgarantie in jedem Teilszenario nur „gering“ ist, werden für nicht anonyme Zahlungen nur wenige der betrachteten Zahlungsverfahren ausgeschlossen. Für das Teilszenario (Einmalige Zahlung, Inland, nicht anonym) erfüllen dagegen nur die Kreditkarte und Vodafone m-pay die Forderung nach einer hohen Verbreitung. Die verbleibenden Zahlungsverfahren sind in Tabelle 31 dargestellt. **Schritt 5**

Teilszenario	Rel. Bedeutung	Verbreitung	Zahlungsgarantie	Verfahren
Einmalige Zahlung, Inland, nicht anonym	47,5%	Hoch	Gering	Überweisung vor Lieferung, Überweisung nach Lieferung, Lastschrift, Kreditkarte, Nachnahme, Vodafone m-pay
Einmalige Zahlung, Inland, anonym	47,5%	Hoch	Gering	Kreditkarte, Vodafone m-pay
Einmalige Zahlung, Ausland, nicht anonym	2,5%	nicht relevant	Gering	Überweisung vor Lieferung, Überweisung nach Lieferung, Kreditkarte, 3-D Secure, paysafecard, moneybookers, Nachnahme, click&buy
Einmalige Zahlung, Ausland, anonym	2,5%	nicht relevant	Gering	paysafecard, 3-D Secure, click&buy, Kreditkarte, moneybookers

Tabelle 31: Ergebnisse von Schritt 5 für das Szenario „Verwarnungsgeld für Falschparken“

Die zu zahlenden Beträge liegen bei Verwarnungsgeldern im Bereich zwischen 5 und 50 Euro. Mit Ausnahme von click&buy und Vodafone m-pay können alle Zahlungsverfahren diesen Betragsbereich abbilden. Diese beiden Verfahren werden daher zunächst nicht weiter betrachtet. **Schritt 6**

Die Kostenverläufe der Verfahren sind in Abbildung 28 dargestellt. In der Abbildung wird deutlich, dass die transaktionsabhängigen Kosten bei der paysafecard und der Nachnahme für diesen Betragsbereich verhältnismäßig hoch sind. Diese Verfahren werden deshalb vorerst aus der Betrachtung ausgeschlossen.

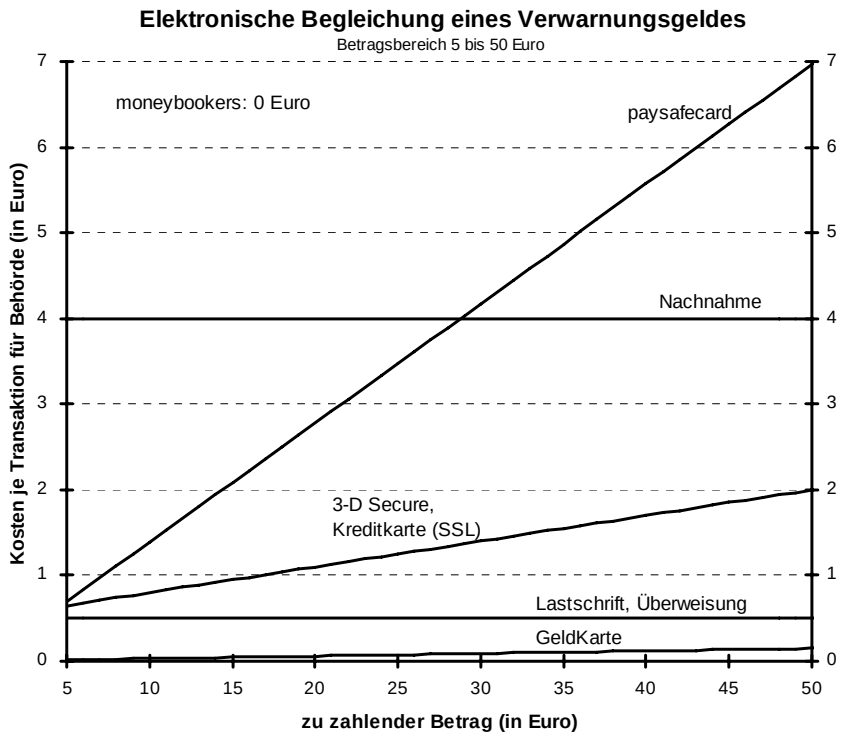


Abbildung 28: Kostenverläufe der Zahlungsverfahren für das elektronische Begleichen eines Verwarnungsgeldes[97]

Schritt 7 und 8

Da genügend Zahlungsverfahren zur Verfügung stehen, kann auf eine Kombination von Verfahren vorerst verzichtet werden. Auch Sicherheitsüberlegungen führen nicht zum Ausschluss von Zahlungsverfahren.

Schritt 9

Abschließend stellt sich die Frage, wie sich die Verfahren in den konkreten Prozess der Behörde integrieren lassen. Dabei zeigt sich, dass die Überweisung vor Lieferung für das elektronische Begleichen eines Verwarnungsgeldes für Falschparken keinen Sinn ergibt, da die Ordnungswidrigkeit bereits erfolgt ist. Auch die Lastschrift wird nicht weiter berücksichtigt, da der Prozess des Bezahlens per Lastschrift sehr umständlich wäre und sich keine erkennbaren Vorteile gegenüber der Zahlung per Überweisung ergeben. Bei der GeldKarte und der Kreditkarte muss ein Weg gefunden werden, beim Bezahlen auch die Verwarnungsnummer zuordnen zu können. Es könnte beispielsweise eine Webseite eingerichtet werden, die nach Eingabe der Verwarnungsnummer die Auslösung der Zahlung ermöglicht.

---

97 Annahmen:
- GeldKarte: Es fallen ausschließlich umsatzabhängige Entgelte an.
- Lastschrift, Überweisung nach Lieferung: Es fallen Buchungspostengebühren von 0,50 Euro an.
- 3-D Secure, Kreditkarte (SSL): Es fallen transaktionsbezogene Fixkosten in Höhe von 0,50 Euro und 3% Disagio bzgl. Umsatzes an.
- Nachnahme: Es fallen 2 Euro Nachnahmeentgelt und 2 Euro Übermittlungsentgelt an.
- paysafecard: Es handelt sich um immaterielle Güter. Das Disagio bis 5 Euro beträgt 19% zzgl. 16% USt., über 5 Euro beträgt das Disagio 12% zzgl. 16% USt. bzgl. des für den Kunden zu zahlenden Betrages.

Die Überweisung ist für das Szenario „Elektronisches Begleichen eines Verwarnungsgeldes für Falschparken“ sehr gut geeignet, da sie ein weit verbreitetes Zahlungsverfahren darstellt und auch aus dem Ausland nutzbar ist. Da mit der Überweisung jedoch keine anonyme Zahlung möglich ist, sollte alternativ zumindest die Zahlung per Kreditkarte möglich sein, ggf. können parallel auch noch weitere Verfahren angeboten werden. **Schritt 10**

7.2.6 Online-Zugriff auf kostenpflichtige Statistik-Daten

In diesem Szenario wird der Vertrieb von Statistik-Daten über das Internet betrachtet, der beispielsweise im Statistik-Shop des Statistischen Bundesamts[98] bereits realisiert ist. Dort können die Datensammlungen in gedruckter Form bestellt oder in elektronischer Form auf den Rechner des Kunden geladen werden. Gegenstand dieses Szenarios ist ausschließlich der Bezug *elektronischer* Daten.

Zunächst wird ermittelt, ob für die Auswahl eines Zahlungsverfahrens eine Aufspaltung des Szenarios in Teilszenarien sinnvoll ist: **Schritt 1**

- *Soll das Zahlungsverfahren sowohl einmalige Zahlungen als auch periodisch wiederkehrende Abbuchungen ermöglichen?*
  Ja. Monatlich erscheinende Berichte könnten als Abonnement regelmäßig per E-Mail zugestellt werden. Beim Großteil der Transaktionen wird es sich jedoch um einmalige Zahlungen handeln.
- *Ist neben einer personenbezogenen auch eine anonyme Zahlungsmöglichkeit erwünscht?*
  Ja. Zumindest bei nicht wiederkehrenden Zahlungen ist der Nutzer anonym, soweit technisch möglich und zumutbar sollte deshalb auch eine anonyme Zahlungsmöglichkeit angeboten werden.
- *Soll das Zahlungsverfahren sowohl aus dem Inland als auch aus dem Ausland genutzt werden können?*
  Ja. Der Bezug elektronischer Statistik-Daten und deren Bezahlung soll z. B. auch ausländischen Unternehmen ermöglicht werden, um über Investitionen in Deutschland entscheiden zu können.

Da jede der drei Fragen mit „Ja“ beantwortet wurde, erfolgt die Ermittlung der Teilszenarien anhand des maximal möglichen Baums mit drei Verzweigungsebenen. Die Kombination der unterschiedlichen Ausprägungen ergibt acht Teilszenarien. **Schritt 2**

Im dritten Schritt werden die Verzweigungen zur Abschätzung der Bedeutung der einzelnen Teilszenarien mit Gewichtungen versehen. Dabei wird angenommen, dass nur etwa 10% der Zahlungstransaktionen periodisch wiederkehrend sind und nur etwa 20% der Zugriffe durch ausländische Nutzer erfolgen. Anonyme und nicht anonyme Zahlungen werden für einmalige Transaktionen gleich gewichtet, für wiederkehrende Zahlungen wird kein anonymes Zahlungsverfahren benötigt. **Schritt 3**

98 Näheres dazu unter http://www-ec.destatis.de/.

Die relative Bedeutung der einzelnen Teilszenarien ergibt sich aus der Multiplikation der Gewichtungen der einzelnen Äste (vgl. Abbildung 29)

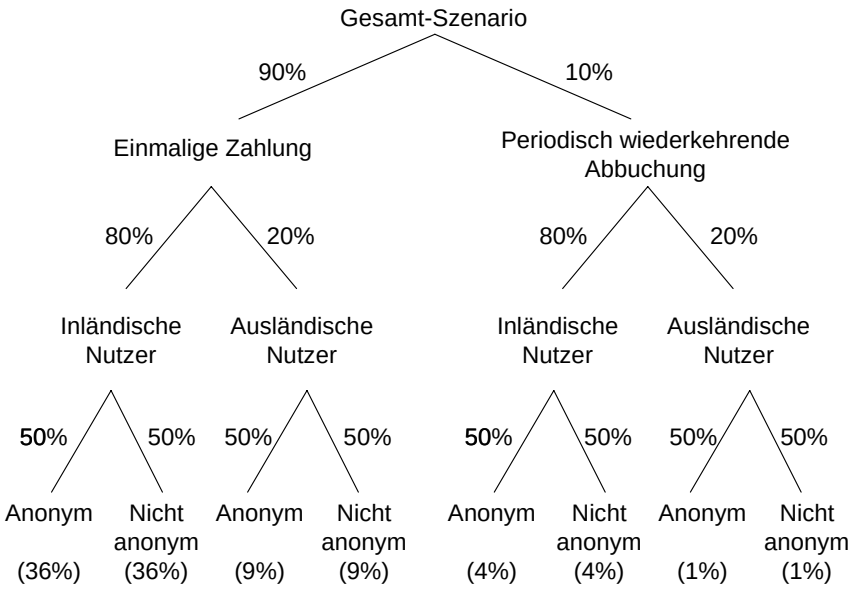


Abbildung 29: Bedeutung der Teilszenarien

Schritt 4

Für die relevanten Teilszenarien werden nun die Anforderungen an die Zahlungsgarantie und die Verbreitung bestimmt. Für das Teilszenario (Wiederkehrende Zahlung, Inland, nicht anonym) wird die Bedeutung der Zahlungsgarantie als „mittel“ eingestuft, da sich der Schaden durch den Ausschluss säumiger Zahler von der weiteren Inanspruchnahme der Dienstleistung weitgehend begrenzen lässt. Für alle anderen Teilszenarien sollte die Zahlungsgarantie „hoch“ sein. Die Anforderung an die Verbreitung in Deutschland wird bei ausländischen Nutzern nicht betrachtet (vgl. Abschnitt 7.1). Bei wiederkehrenden Zahlungen werden inländische Nutzer wohl einen gewissen Initialisierungsaufwand in Kauf nehmen, weshalb ein „mittel“ verbreitetes Zahlungsverfahren vermutlich ausreicht, bei einmaligen Zahlungen sollte die Verbreitung „hoch“ sein.

Schritt 5

Für jedes der Teilszenarien werden nun anhand von Tabelle 24 diejenigen Zahlungsverfahren ermittelt, die die Anforderungen des Teilszenarios hinsichtlich der Kriterien Internationalität, Eignung für wiederkehrende Zahlungen, Anonymität, Zahlungsgarantie und Verbreitung mindestens oder besser erfüllen (Tabelle 32). Dabei zeigt sich, dass bei keinem Zahlungsverfahren wiederkehrende und anonyme Zahlungen durch ausländische Nutzer möglich sind.

Teilszenario	Rel. Bedeutung	Verbreitung	Zahlungsgarantie	Verfahren
Einmalige Zahlung, Inland, anonym	36%	Hoch	Hoch	Vodafone m-pay
Einmalige Zahlung, Inland, nicht anonym	36%	Hoch	Hoch	Vodafone m-pay, Überweisung vor Lieferung, Nachnahme
Einmalige Zahlung, Ausland, anonym	9%	nicht relevant	Hoch	paysafecard, 3-D Secure, moneybookers
Einmalige Zahlung, Ausland, nicht anonym	9%	nicht relevant	Hoch	Überweisung vor Lieferung, 3-D Secure, Nachnahme, paysafecard, moneybookers
Wiederkehrende Zahlung, Inland, nicht anonym	4%	Mittel	Mittel	Überweisung vor Lieferung, Vodafone m-pay
Wiederkehrende Zahlung, Inland, anonym	4%	Mittel	Hoch	Vodafone m-pay
Wiederkehrende Zahlung, Ausland, nicht anonym	1%	nicht relevant	Hoch	Überweisung vor Lieferung, moneybookers
Wiederkehrende Zahlung, Ausland, anonym	1%	nicht relevant	Hoch	

Tabelle 32: Ergebnisse von Schritt 5 für das Szenario "Online-Zugriff auf Statistik-Daten"

Schritt 6

Im Folgenden wird betrachtet, ob die Zahlungsverfahren für den zu zahlenden Betragsbereich geeignet sind und welche transaktionsabhängigen Kosten in den einzelnen Bereichen entstehen. Als relevant wurde für den Online-Zugriff auf kostenpflichtige Statistik-Daten der Bereich von 0,01 bis 50,00 Euro angenommen. Mit Ausnahme von Vodafone m-pay, das nur für Beträge bis 10 Euro geeignet ist, können alle Verfahren aus Schritt 5 den gesamten Betragsbereich abbilden (vgl. Tabelle 25). Die Kostenverläufe der Zahlungsverfahren aus Sicht der Behörde unter den dazugehörigen Annahmen sind in Abbildung 30 dargestellt. Nicht abgebildet sind die Kosten für den Kunden, bei moneybookers sind dies 1% des Betrags.

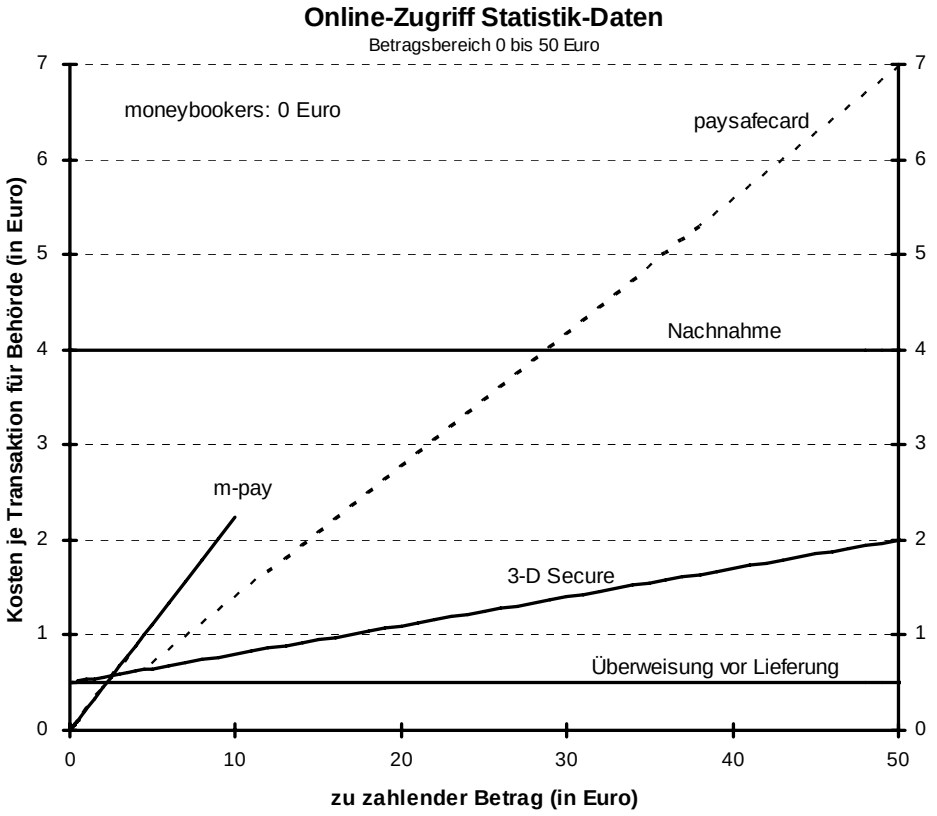


Abbildung 30: Kostenverläufe der Zahlungsverfahren für den Online-Zugriff auf Statistik-Daten[99]

Schritt 7

Bei der Nachnahme sind die Kosten für geringe Beträge unverhältnismäßig hoch. Die Zahlung per Nachnahme sollte daher erst ab einem bestimmten Mindestbestellwert zugelassen werden, was eine Kombination mit anderen Verfahren notwendig macht. Das gleiche gilt für die paysafecard, statt eines Mindestbetrags sollte für die paysafecard jedoch ein Höchstbetrag festgelegt werden.

Schritt 8

Nach der Analyse der transaktionsabhängigen Kosten werden die Sicherheitsanforderungen betrachtet. Zur Bezahlung von E-Government-Dienstleistungen sollte der Kunde keine Zahlungsverfahren verwenden müssen, durch deren Nutzung er sich einem signifikanten Risiko aussetzt. Bei der paysafecard besteht das Risiko des Verlusts der Karte und damit analog zum Bargeld auch des verbleibenden Restguthabens, die verbleibenden Verfahren sind in dieser Hinsicht jedoch unbedenklich.

---

99 Annahmen:
- Vodafone m-pay: Umsatz > 2.596 Euro je Monat.
- Überweisung vor Lieferung: Es fallen Buchungspostengebühren von 0,50 Euro an.
- 3-D Secure: Es fallen transaktionsbezogene Fixkosten in Höhe von 0,50 Euro und 3% Disagio bzgl. des Umsatzes an.
- Nachnahme: Es fallen 2 Euro Nachnahmeentgelt und 2 Euro Übermittlungsentgelt an.
- paysafecard: Es handelt sich um immaterielle Güter. Das Disagio bis 5 Euro beträgt 19% zzgl. 16% USt., über 5 Euro beträgt das Disagio 12% zzgl. 16% USt. bzgl. des für den Kunden zu zahlenden Betrages.
- moneybookers: Es fallen für die Behörde keine transaktionsabhängigen Kosten an.

Schritt 9

Beim Online-Zugriff auf kostenpflichtige Statistik-Daten sollte eine durchgängige Gestaltung des Bestell- und Zahlungsabwicklungsprozesses möglich sein. Diese Anforderung wird jedoch von der Überweisung vor Lieferung und der Nachnahme nicht erfüllt. Bezüglich der Anforderungen an die technische Implementierung wird im Folgenden davon ausgegangen, dass diese durch die verbleibenden Zahlungsverfahren erfüllt werden können.

Schritt 10

Die Ergebnisse der vorangegangenen Schritte müssen nun zu einer Entscheidung zusammengeführt werden. Da für dieses Szenario das Angebot eines anonymen Zahlungsverfahrens wünschenswert wäre, werden zunächst die Verfahren betrachtet, die eine anonyme Bezahlmöglichkeit bieten. Dies ist zunächst das Verfahren Vodafone m-pay, das jedoch nur für eine Betragshöhe bis 10 Euro geeignet ist. Weitere geeignete Verfahren wären die paysafecard, 3-D Secure und moneybookers, die im Gegensatz zu Vodafone m-pay auch aus dem Ausland genutzt werden können. Der Nachteil bei diesen Verfahren ist deren geringe Verbreitung. Ergänzend sollte daher in jedem Fall noch ein verbreitetes Verfahren wie die Überweisung vor Lieferung angeboten werden, auch wenn diese keine anonyme Zahlung ermöglicht und zu einer Unterbrechung im Prozess führt. Mit der Überweisung vor Lieferung sind zudem auch wiederkehrende Zahlungen möglich.

8 Fazit und Ausblick

Bei der Auswahl geeigneter Zahlungsverfahren für die Beispielszenarien wurde deutlich, dass es nicht „das optimale Zahlungsverfahren“ für ein Szenario gibt. Grundsätzlich wäre aus Sicht der Behörde ein für alle Betragshöhen einsetzbares Zahlungsverfahren wünschenswert, das bei den Kunden weit verbreitet ist und gleichzeitig eine hohe Zahlungsgarantie für die Behörde bietet. Von den momentan verfügbaren Verfahren leisten dies nur die Zahlung per Nachnahme und die Überweisung vor Lieferung.

Verbreitete Verfahren mit hoher Zahlungsgarantie ermöglichen keine durchgängigen Prozesse

Diese beiden Zahlungsverfahren weisen jedoch auch gravierende Nachteile auf. So sind bei der Zahlung per Nachnahme die Kosten für die Behörde relativ hoch, für den Kunden ist die persönliche Entgegennahme der Sendung nicht immer möglich bzw. mit Schwierigkeiten verbunden. Zudem ist dieses Verfahren in erster Linie für den Vertrieb physischer Produkte geeignet. Eine Zahlung per Nachnahme wäre zwar z. B. durch Versand eines Zugangscodes auf dem Postweg auch bei digitalen Produkten oder bei Dienstleistungen möglich, allerdings kann die Leistung dann erst nach Zustellung des Zugangscodes genutzt bzw. bezogen werden. Ein derartiger Prozessbruch widerspricht gerade dem Ziel, die Inanspruchnahme von E-Government-Leistungen durchgängig und gleichzeitig einfach und bequem zu gestalten. Auch bei einer Überweisung vor Lieferung kommt es notwendigerweise zu einem Prozessbruch, da die Behörde bis zur Gutschrift des Betrags auf ihrem Konto warten muss, um eine Zahlungsgarantie zu erhalten.

Online-Zahlungsverfahren mit Zahlungsgarantie derzeit kaum verbreitet

Bei der Auswahl eines Zahlungsverfahrens für ein Szenario ist deshalb genau zu differenzieren, in welchen Fällen auch Zahlungsverfahren mit geringerer Verbreitung oder ohne sofortige Zahlungsgarantie in Kauf genommen werden, um eine durchgängige Gestaltung des E-Government-Prozesses zu erreichen. Mit der in diesem Modul entwickelten Methodik ist dies möglich. Beispielsweise kann bei Reduzierung der Anforderung an die Verbreitung eines Verfahrens durch den Einsatz E-Mail-basierter oder Wertkarten-basierter Verfahren, der GeldKarte oder 3-D Secure ein durchgängiger Zahlungsprozess mit sofortiger Zahlungsgarantie für die Behörde erreicht werden.

Ob die Verbreitung dieser Verfahren in Zukunft wesentlich zunimmt, kann nicht beantwortet werden. Nachdem in den vergangenen Jahren viele Internet-Zahlungsverfahren eingestellt wurden, verhalten sich Betreiber von Online-Shops bei der Integration neuer Zahlungsverfahren eher zurückhaltend. Sie warten ab, ob neue Zahlungsverfahren von den Kunden akzeptiert werden. Die Kunden hingegen nehmen neue Zahlungsverfahrens vornehmlich nur dann an, wenn es genügend Akzeptanzstellen gibt. Aufgrund dieses Dilemmas stehen als weit verbreitete Verfahren, die eine Bezahlung ohne Prozessbruch beim Kauf ermöglichen, bis heute nur die klassische Kreditkarte und die Lastschrift zur Verfügung. Diese beiden Verfahren sind dem Kunden bereits vom Bezahlen am Point of Sale bekannt und werden daher auch für den Einsatz im Internet akzeptiert.

Kreditkarte und Lastschrift bieten keine Zahlungsgarantie

Anders als am Point of Sale verzichten die Händler im Internet jedoch bisher auf die Einholung der Unterschrift des Kunden auf einer Einzugsermächtigung. Legt der Kunde bei seiner Bank oder Kreditkartengesellschaft Widerspruch gegen die Abbuchung ein, wird die gerichtliche Geltendmachung der Forderung der Behörde durch das Fehlen des klassischen Urkundenbeweises deutlich erschwert. Die

klassische Kreditkartenzahlung und die Lastschrift bieten für die Behörde daher nur ein sehr geringes Maß an Zahlungsgarantie.

Keines der heute verfügbaren Verfahren bietet damit eine hohe Verbreitung und eine hohe Zahlungsgarantie, und ermöglicht gleichzeitig eine durchgängige Prozessgestaltung (vgl. Abbildung 31). Bei der Kreditkarte und der Lastschrift liegt dies jedoch nur an der fehlenden Unterschrift.

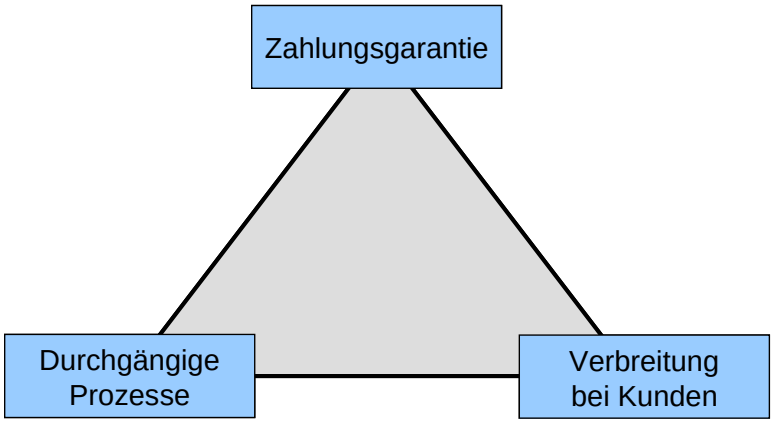


Abbildung 31: "Magisches Dreieck" der Anforderungen an ein Zahlungsverfahren

Mögliche Lösung: Elektronische Signatur

Die Erfüllung aller drei Anforderungen wäre möglich, wenn die handschriftliche Unterschrift auf dem Zahlungsbeleg im Internet durch eine qualifizierte elektronische Signatur ersetzt werden würde, die der handschriftlichen Unterschrift nach europäischem und deutschem Recht weitgehend gleichgestellt ist. Allerdings sind zur Erstellung einer solchen elektronischen Signatur weitere Voraussetzungen auf Seite des Kunden notwendig.

So benötigt der Kunde zum elektronischen Signieren eines Dokuments einen Computer mit Kartenlesegerät sowie eine Signaturkarte (Signaturerstellungseinheit). Im Rahmen der kürzlich von der Bundesregierung vorgestellten JobCard-Initiative sollen bis zum Jahr 2006 alle Arbeitnehmer mit einer solchen Signaturkarte ausgestattet werden. Die Karten können von verschiedenen Anbietern bezogen werden, zwischen denen der Bürger frei wählen kann. So können die Kunden der HypoVereinsbank, der Commerzbank, der Deutschen Bank sowie einiger Genossenschaftsbanken und Sparkassen zukünftig auch ihre Bankkarten als Signaturkarten verwenden.

Kombination von Bankkarte und Signaturkarte ermöglicht neuartige Zahlungsverfahren

Durch die Kombination von Bankkarte und Signaturfunktionalität wird es zukünftig auch möglich sein, im Internet sichere und garantierte Zahlungen abzuwickeln, vergleichbar den heute im stationären Handel gängigen Kartenzahlungen. Wie beim Bezahlen am Point of Sale können die Kontoverbindungsdaten des Kunden vom Kartenlesegerät aus dem Chip ausgelesen werden. Aus den Kontoverbindungsdaten, den Händlerdaten und dem zu zahlenden Betrag wird ein elektronischer Zahlungsbeleg erstellt und angezeigt, den der Kunde durch Eingabe seiner Signatur-PIN unterschreibt. Anschließend werden die Daten zur Prüfung an die Bank weitergeleitet. Bei erfolgreicher Prüfung der Unterschrift und der Kontodeckung kann die Bank unmittelbar eine Zahlungsgarantie aussprechen (vgl. Abbildung 32).

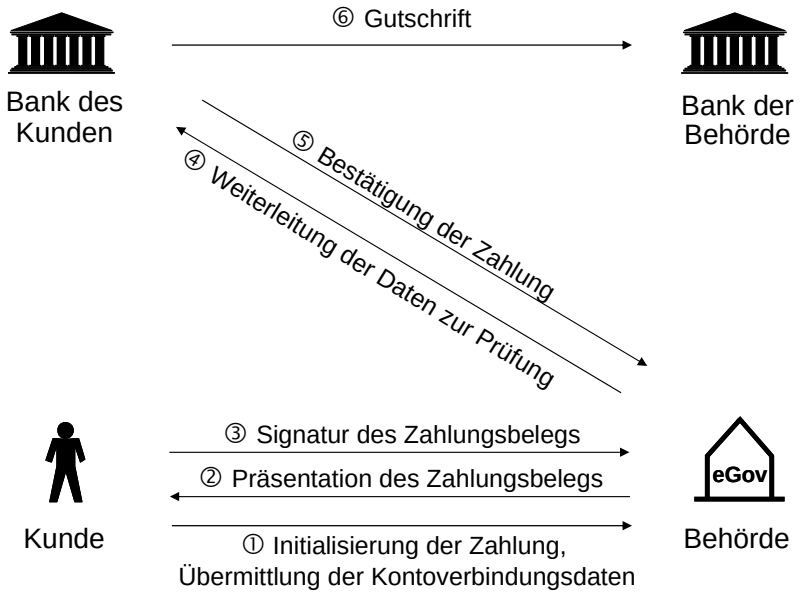


Abbildung 32: Möglicher Ablauf einer Zahlung eines signaturbasierten Verfahrens

Für den Kunden bietet dieses Zahlungsverfahren den Vorteil, dass die Transaktionsdaten durch die Verwendung der elektronischen Signatur vor Veränderungen geschützt sind. Die Zahlung kann zudem nur bei Besitz der Karte und Kenntnis der PIN ausgelöst werden. Etabliert sich das Verfahren bei den Behörden und Händlern, so können Dritte zukünftig nicht mehr allein durch abgehörte oder ausgespähte Informationen wie Konto- oder Kreditkartennummern unberechtigt im Internet einkaufen.

Kombination von Signatur- und Bezahlfunktion für E-Government-Dienstleistungen ideal

Für die Behörde hat ein signaturbasiertes Zahlungsverfahren neben der sofortigen Zahlungsgarantie den Vorteil, dass die elektronische Signatur für die Gestaltung durchgängiger E-Government-Dienstleistungen häufig ohnehin benötigt wird. In einigen Bereichen, z. B. bei kommunalen Dienstleistungen der MEDIA@Komm-Städte, bei der elektronischen Steuererklärung ELSTER oder im elektronischen Rechtsverkehr, ist der Einsatz der elektronischen Signatur bereits heute möglich. Auch bei allen anderen E-Government-Dienstleistungen, in denen heute eine handschriftliche Unterschrift verlangt wird (dies sind insbesondere Antragsverfahren), ist eine elektronische Signatur notwendige Voraussetzung für die Schaffung durchgängiger elektronischer Prozesse. Vor allem für diese Dienstleistungen wäre es ideal, wenn nach der Leistung der Unterschrift auch die Bezahlung der anfallenden Gebühren mit Hilfe der Signaturkarte möglich wäre. Abbildung 33 zeigt einen möglichen Prozessablauf am Beispiel des elektronischen Mahnantrags.

Nach Ausfüllen des Mahnantrags wird dieser mittels der Signaturfunktion auf der Bankkarte unterschrieben. Anschließend erfolgt eine Prüfung des Antrags sowie die Ermittlung der anfallenden Mahngebühren bei der Behörde. In einem weiteren Schritt kann die Bankkarte auch direkt zur Bezahlung der anfallenden Gebühren verwendet werden.

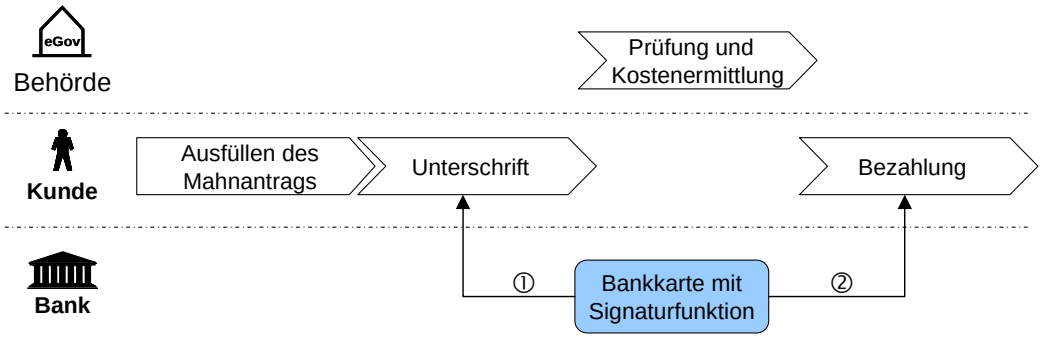


Abbildung 33: Doppelfunktion der Signaturkarte in Antragsverfahren

Ob es in Zukunft ein Zahlungsverfahren geben wird, das die notwendigen Sicherheitsanforderungen aus Behörden- und Kundensicht optimal erfüllt, hängt damit im Wesentlichen davon ab, ob die elektronische Signatur eine ausreichende Verbreitung erlangen wird. Der Weg, den die Bundesregierung mit der Gründung des Signaturbündnisses eingeschlagen hat und der mit der JobCard-Initiative konsequent weitergeführt wird, weist jedoch in jedem Fall in die richtige Richtung.

Anhang

Im Folgenden werden die Bewertungen der Zahlungsverfahren, die in den Abschnitten 6.1.1 bis 6.1.11 dargestellt wurden, näher erläutert (Anhang A.1 bis A.11). In Anhang A.12 findet sich eine Auflistung weiterer Zahlungsverfahren aus den einzelnen Kategorien. Die hier aufgeführten Kosten der einzelnen Verfahren wurden mit größter Sorgfalt ermittelt. Jedoch ist es möglich, dass die tatsächlichen Kosten, bei den einzelnen Anbietern, aufgrund zwischenzeitlicher Änderungen oder aufgrund der individuellen Konditionengestaltung deutlich von den hier genannten abweichen können.

A.1 Geldbörsenzahlung

Aus der Kategorie „Geldbörsenzahlung“ wurde die kontogebundene GeldKarte bewertet.

Fachspezifische Anforderungen:

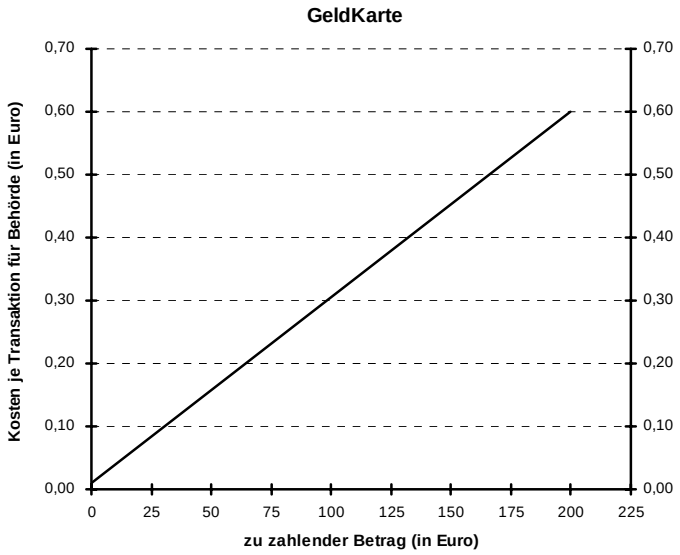
- Wiederkehrende Zahlungen: nein
  Systembedingt ist es nicht möglich, automatisiert ohne aktives Zutun des Inhabers Beträge von der GeldKarte abzubuchen. Wiederkehrende Zahlungen werden somit nicht unterstützt.
- Internationalität: nein
  Um die kontogebundene GeldKarte nutzen zu können, muss der Inhaber ein Konto bei einem deutschen Kreditinstitut besitzen. Kreditinstitute haben sich bei der Eröffnung eines Kontos Gewissheit über die Person und Anschrift des Kontoinhabers zu verschaffen. Dies erfordert in der Regel ein persönliches Erscheinen beim Institut, womit häufig ein hoher Aufwand für den potenziellen Nutzer verbunden ist. Das System eignet sich damit nicht ohne weiteres für einen internationalen Einsatz.
- Anonymität: ja
  Aus den zwischen Behörde und Kunde im Rahmen des Zahlungsvorgangs übermittelten Daten kann kein Personenbezug hergestellt werden. Aus der Sicht der Behörde ist das Zahlungsverfahren anonym.
- Zahlungsgarantie: hoch
  Das System GeldKarte ist derart konzipiert, dass ein unmittelbarer Geldfluss von einer Kundenkarte zu einer Händlerkarte erfolgt. Die Behörde erhält somit eine unmittelbare Verfügungsgewalt über den übertragenen Geldbetrag.
- Verbreitung: gering
  Zur Nutzung der GeldKarte im Internet ist ein Kartenleser der Klasse 3, d. h. ein Kartenleser mit Display und eigener Tastatur, Voraussetzung. Auf absehbare Zeit ist nicht zu erwarten, dass die GeldKarte für Zahlungsvorgänge im Internet eine hohe Verbreitung finden wird, da dies ebenfalls eine hohe Verbreitung von Kartenlesern erfordern würde.[100]

[100] Eine flächendeckende Verbreitung von Kartenlesern der Klasse 3 wird bereits seit mehreren Jahren im Rahmen der Nutzung elektronischer Signaturen erhofft. Eine signifikant zuneh-

Betragsbereich und Kostenstruktur:

Die GeldKarte ermöglicht grundsätzlich Zahlungen von 0,01 bis 200 Euro. Im Jahr 2003 betrug der durchschnittliche Ladebetrag jedoch nur ca. 26 Euro. Beglichen wurden im Schnitt Beträge in Höhe von ca. 2 Euro. Der durchschnittliche Ladebetrag und Bezahlbetrag haben sich seit 1997 kontinuierlich den genannten Werten angenähert und scheinen sich nun auf diesem Niveau einzupendeln.

Für den Kunden entstehen keine transaktionsabhängigen Kosten. Nach der Integration der Händlerkarte in die Systeme der Behörde fallen für jede durchgeführte Transaktion Gebühren in Höhe von 0,3%, mindestens jedoch 0,01 Euro für die Behörde an. Die Transaktionskosten sind nachfolgend dargestellt.



Annahmen: Es werden ausschließlich die Gebühren zur Übertragung der Geldeinheiten von der Kundenkarte auf die Händlerkarte berücksichtigt. Ggf. anfallende Kosten zur Einreichung der Umsätze bei der Bank der Behörde sind in der Abbildung nicht dargestellt.

Abbildung 34: Verlauf der variablen Kosten einer GeldKarte-Transaktion

Sicherheit:

- Transaktionskontrolle: hoch
  Der Kunde muss zur Einleitung der Zahlung den am Kartenleser angezeigten Betrag bestätigen. In der Regel erfolgt eine Anzeige über die erfolgreiche Abwicklung des Zahlungsvorgangs oder im Fehlerfall ein Hinweis auf das Scheitern. Die GeldKarte speichert zudem die letzten 15 Zahlungsvorgänge. Der Nutzer erhält somit eine zeitnahe Transaktionsbestätigung und eine Übersicht bereits getätigter Zahlungen.

- Stärke des Authentifizierungsmechanismus: mittel
  Der Besitzer der GeldKarte kann über den auf dem Chip gespeicherten Geldbetrag verfügen. Die Eingabe einer PIN oder eine Prüfung weiterer Merkmale

mende Nachfrage nach Kartenlesern konnte allerdings bis Ende 2003 nicht verzeichnet werden.

im Rahmen des Zahlungsvorgangs wird nicht verlangt. Das Kriterium ist somit als mittel einzustufen.

- Sperrmöglichkeit: nein
  Die GeldKarte wurde in der Absicht entworfen, eine möglichst nahe Funktionsäquivalenz zu Bargeld zu schaffen. Wie bei Bargeld ist es nicht möglich, die GeldKarte gegen Verfügungen zu sperren.
- Haftungsbetrag: Kartenguthaben (max. 200 Euro)
  Da die GeldKarte weder gesperrt noch bereits durchgeführten Transaktionen widersprochen werden kann, ist der Schaden, den der Kunde maximal erleiden könnte, auf das aktuell verfügbare Kartenguthaben beschränkt. Dieses kann systembedingt maximal 200 Euro betragen.

A.2 Online-Überweisung

Aus der Kategorie „Online-Überweisung“ wurde die Postbank Online-Überweisung bewertet.

Fachspezifische Anforderungen:

- Wiederkehrende Zahlungen: nein
  Da jede Zahlungsanweisung vom Kunden durch Eingabe von PIN und TAN aktiv eingeleitet werden muss, sind wiederkehrende Zahlungen derzeit nicht möglich.
- Internationalität: nein
  Bei der Online-Überweisung handelt es sich um ein System, das derzeit nur von Kunden der Postbank genutzt werden kann. Der Aufwand, das Zahlungsverfahren auch aus dem Ausland zu nutzen, ist dadurch sehr hoch.
- Anonymität: nein
  Es handelt sich bei der Abwicklung des Vorgangs um einen gewöhnlichen Überweisungsauftrag. Der Empfänger sieht bei der Gutschrift den Namen des Auftraggebers.
- Zahlungsgarantie: mittel
  Bisher wird lediglich die Einreichung des Auftrags durch die Bank des Kunden bestätigt. Die Übertragung des Betrages auf das Empfängerkonto, könnte im Rahmen der endgültigen Verarbeitung bei der Bank des Kunden mangels Deckung nicht ausgeführt werden. Zudem kann der Kunde die Überweisung auch bei erfolgreicher Ausführung solange widerrufen, bis sie auf dem Konto des Empfängers gutgeschrieben ist.
- Verbreitung: mittel
  Derzeit kann das Zahlungsverfahren ausschließlich von Postbank-Kunden genutzt werden. Die Postbank plant jedoch, das Bezahlen mit PIN und TAN auch Kunden anderer Banken zu ermöglichen.[101] Da der Großteil der Internet-Nutzer auch Online-Banking verwendet, wird die voraussichtliche Verbreitung auf „mittel“ geschätzt.

[101] Vgl. dazu http://www.fun.de/deutsch/service/broschueren/download/postbankltur.pdf.

Betragsbereich und Kostenstruktur:

Der Betragsbereich wird grundsätzlich nur durch den Verfügungsrahmen auf dem Konto des Kunden begrenzt. Zu beachten ist jedoch, dass die Kunden bei einigen Banken auch Höchstgrenzen für Online-Verfügungen über das Konto festlegen können.

Für den Kunden fallen keine Transaktionskosten an. Die Behörde hat ein umsatzabhängiges Entgelt zu tragen. Eindeutige Aussagen zur Höhe des Entgelts können derzeit nicht getroffen werden. Im Folgenden wird angenommen, dass sich der Disagiosatz für die Online-Überweisung zwischen den üblichen Disagiosätzen für Maestro-Zahlungen (ca. 1%) und Kreditkartenzahlungen (ab ca. 2%) bewegt.

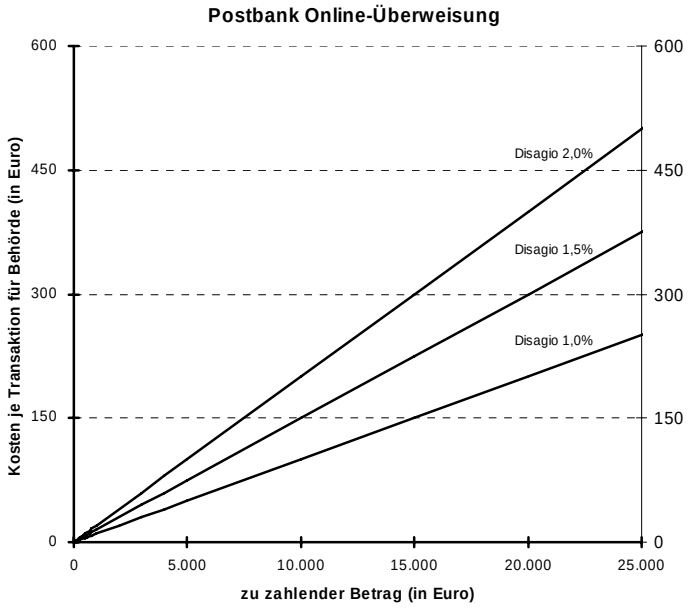


Abbildung 35: Verlauf der variablen Kosten einer Online-Überweisung

Sicherheit:

- Transaktionskontrolle: hoch
  Der Kunde erhält eine zeitnahe Bestätigung, dass der Auftrag von der Postbank entgegengenommen wurde. Nach vollständiger Abwicklung des Zahlungsauftrags kann die Überweisung über den Kontoauszug eingesehen werden.

- Stärke des Authentifizierungsmechanismus: hoch
  Zur Authentifizierung und Zahlungsbestätigung muss der Kunde sowohl seine PIN als auch eine TAN eingeben. Bei der PIN handelt es sich um ein rein wissensbasiertes Merkmal, worüber keine Aufzeichnungen existieren sollten. Die TAN hingegen werden dem Kunden auf einer TAN-Liste physisch zur Verfügung gestellt.[102]

[102] Weitere Informationen zur Authentifizierung, insbesondere durch PIN und TAN, sind im Modul „Authentisierung im E-Government“ verfügbar.

- Sperrmöglichkeit: ja
  Das Online-Konto kann entweder vollständig gegen jegliche Verfügung oder nur gegen Online-Verfügungen gesperrt werden.
- Haftungsbetrag: Verfügungsrahmen
  Werden missbräuchlich Verfügungen über das Konto mittels Online-Überweisungen durchgeführt, so hat der Kunde dafür einzustehen, da nur er die PIN wissen kann und in Besitz der TAN-Liste ist. Transaktionen über den Verfügungsrahmen hinaus sind nicht möglich und bestimmen damit den maximalen Haftungsbetrag.

A.3 Überweisung vor bzw. nach Lieferung

Fachspezifische Anforderungen:

- Wiederkehrende Zahlungen: ja
  Wiederkehrende Überweisungen (Dauerüberweisungen) sind aufgrund eines vom Kunden erteilten Daueraufträgs zu bestimmten, regelmäßig wiederkehrenden Terminen an den selben Zahlungsempfänger in gleich bleibender Höhe möglich.
- Internationalität: ja
  Überweisungen sind generell auch aus dem Ausland möglich. Dazu ist die Angabe internationaler Kennzeichen, wie z. B. der „International Bank Account Number“ (IBAN) oder des „SWIFT[103]-Bank Identifier Code“ (SWIFT-BIC), notwendig, die eine Verarbeitung erleichtern und beschleunigen.
- Anonymität: nein
  Die Behörde erhält von der Bank Angaben zur Person des Überweisenden. Dadurch ist eine anonyme Zahlung nicht möglich.
- Zahlungsgaratie: gering (Zahlung nach Lieferung) / hoch (Zahlung vor Lieferung)
  Beim Kriterium Zahlungsgarantie sind die beiden Varianten der Überweisung zu unterscheiden. Entscheidend für die Zahlungsgarantie beim Zahlungsverfahren Überweisung ist, ob die Zahlung dem Kreditinstitut der Behörde zur endgültigen Gutschrift auf dem Konto der Behörde zur Verfügung gestellt worden ist. Ab diesem Zeitpunkt kann der Kunde den Überweisungsvertrag nicht mehr kündigen. Auf nationaler Ebene kann dies bis zu drei Banktagen dauern. Bei der Leistungserbringung vor Zahlungseingang ist die Zahlungsgarantie somit gering, da ein Kunde die Überweisung widerrufen bzw. gar nicht initiieren könnte. Bei der Leistungserbringung nach Zahlungseingang und unwiderruflicher Gutschrift ist die Zahlungsgarantie hoch, da ein Kunde den Überweisungsvertrag dann nicht mehr kündigen kann.

[103] Die "Society for Worldwide Interbank Financial Telecommunication" (S.W.I.F.T.) ist eine Gesellschaft, die ein internationales Datenübertragungsnetz für Finanznachrichten zwischen ihren Mitgliedern betreibt. Mitglieder und Träger der Gesellschaft sind vorwiegend Kreditinstitute.

- Verbreitung: hoch
  Da in Deutschland nahezu jede Person ein Bankkonto besitzt und dadurch Überweisungen in Auftrag geben kann, ist die Verbreitung als hoch einzustufen.

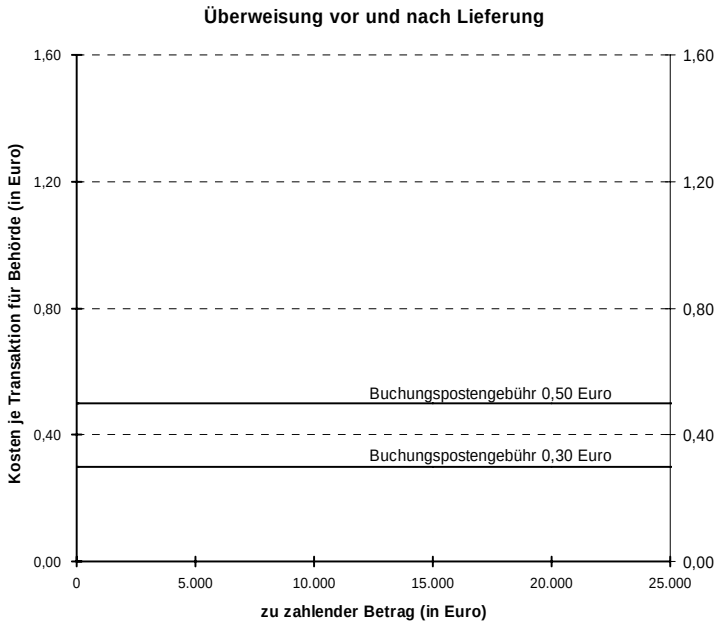
Betragsbereich und Kostenstruktur:

Der Betragsbereich bei der Überweisung beginnt bei 0,01 Euro und ist nach oben nur durch den Verfügungsrahmen des Kunden begrenzt.

Für den Kunden können Überweisungsgebühren in Form einer Buchungspostengebühr anfallen. Häufig werden jedoch pauschal bepreiste Kontoführungsmodelle gewählt, wodurch keine zusätzlichen transaktionsabhängigen Kosten anfallen.

Fix(Zusatz-)kosten fallen für die Behörde bei bestehenden Kontoverbindungen nicht an.

Von der Behörde sind jedoch in der Regel Gebühren je Buchungsposten zu zahlen. Die Höhe dieser transaktionsabhängigen Gebühr ist in den meisten Fällen jedoch verhandelbar. Im Folgenden wird die Annahme getroffen, dass die Gebühren entweder 0,30 oder 0,50 Euro je Buchungsposten betragen.



Annahme: Es fallen Buchungspostengebühren in der angegebenen Höhe an. Weitere Kosten, z. B. für die Rechnungsstellung oder die Zahlungsüberwachung, werden nicht betrachtet.

Abbildung 36: Verlauf der variablen Kosten einer Überweisung vor und nach Lieferung

Sicherheit:

- Transaktionskontrolle: mittel
  Der Kunde erhält bei der Überweisung keine sofortige Bestätigung der Zahlungsausführung, evtl. erhält er eine Bestätigung der Annahme des Auftrags. Er kann die Zahlungen jedoch aufgrund der Buchungsposten auf seinem Kontoauszug nachvollziehen.

- Stärke des Authentifizierungsmechanismus: mittel
  Je nach eingesetztem Verfahren kann sich das Niveau zwischen mittel (Ein-Faktor-Authentifzierung, z. B. händische Unterschrift) und hoch (Zwei-Faktor-Authentifzierung, z. B. PIN und TAN) bewegen. Für den Schutz des Kunden vor missbräuchlichen Verfügungen ist jedoch das geringere Sicherheitsniveau ausschlaggebend.
- Sperrmöglichkeit: ja
  Der Kunde kann sein Konto gegen Verfügungen sperren lassen.
- Haftungsbetrag: Verfügungsrahmen
  Verfügungen sind nur bis zur Höhe des Verfügungsrahmens des Kontos möglich.

A.4 Lastschrift (Einzugsermächtigung)

Fachspezifische Anforderungen:

- Wiederkehrende Zahlungen: ja
  Das Lastschriftverfahren eignet sich nach einmaliger Erteilung einer Einzugsermächtigung für wiederkehrende Zahlungen, da Beträge ohne aktives Zutun des Kunden von dessen Konto eingezogen werden können.
- Internationalität: nein
  Um das Lastschriftverfahren nutzen zu können, muss der Kunde ein Konto bei einem deutschen Kreditinstitut besitzen.[104]
- Anonymität: nein
  Der Name des Kunden muss auf der Einzugsermächtigung und auf dem Lastschriftbeleg angegeben werden und erscheint auch auf dem Kontoauszug des Zahlungsempfängers.
- Zahlungsgarantie: gering
  Der Kunde kann innerhalb von sechs Wochen nach Belastung seines Kontos der Abbuchung widersprechen. Eine Angabe von Gründen ist nicht notwendig.[105]
- Verbreitung: hoch
  Das Verfahren ist in der Praxis sowohl auf Kunden- als auch auf Behördenseite weit verbreitet und akzeptiert.

---

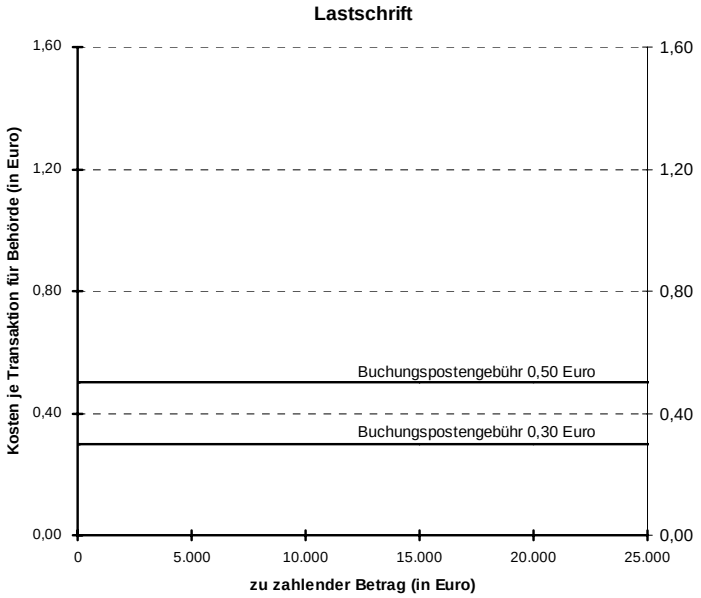
104 Es existieren derzeit jedoch Bestrebungen auf europäischer Ebene ein EU-weites Lastschriftverfahren einzuführen. Weitere Informationen finden sich dazu unter http://europa.eu.int/-comm/internal_market/payments/directdebit/index_de.htm#studies.

105 Über die Frist von sechs Wochen hinaus, die im Lastschriftabkommen geregelt ist, hat der für Bankrecht zuständige XI. Zivilsenat des Bundesgerichtshofs (BGH) wie folgt entschieden: Ein Widerspruch gegen Kontobelastungen aufgrund Einzugsermächtigungslastschriften ist ohne Einhaltung einer bestimmten Frist bis zur Genehmigung der Belastungen durch den Kontoinhaber zulässig. Vergleiche dazu BGH, Urteil vom 06. 06.2000, Aktenzeichen: XI ZR 258/99.

Betragsbereich und Kostenstruktur:

Der Betragsbereich ist bei der Lastschrift nicht begrenzt. Gegebenenfalls kann der Kunde noch nach Erteilung der Einzugsermächtigung für ausreichende Deckung des Kontos sorgen.

Das Lastschriftverfahren verursacht für den Kunden keine direkten Kosten. Für die Behörde fallen keine fixen Kosten an, in der Regel jedoch variable Kosten in Höhe der Buchungspostengebühr.



Annahme: Es fallen Buchungspostengebühren in der angegebenen Höhe an.

Abbildung 37: Verlauf der variablen Kosten einer Lastschrift

Sicherheit:

- Transaktionskontrolle: mittel
  Der Kunde erhält im Rahmen der Lastschrifteinreichung keine zeitnahe Transaktionsbestätigung. Auf dem Kontoauszug erhält der Kunde Kenntnis über bereits von seinem Konto abgebuchte Lastschriften.
- Stärke des Authentifizierungsmechanismus: gering
  Die Behörde kann die Unterschrift des Kunden nur prüfen, wenn die Unterschrift bei der Behörde vor Ort erbracht wird. Da dies in der Regel nicht der Fall ist, wird die Stärke des Authentifizierungsmechanismus als gering bewertet.
- Sperrmöglichkeit: ja
  Der Kunde kann sein Konto gegen Verfügungen sperren lassen.
- Haftungsbetrag: 0 Euro
  Da Lastschriften innerhalb der von seiner Bank vorgegebenen Frist jederzeit widersprochen werden kann, muss der Kunde nicht für unberechtigte Verfügungen haften.

A.5 Kreditkartenzahlung (SSL)

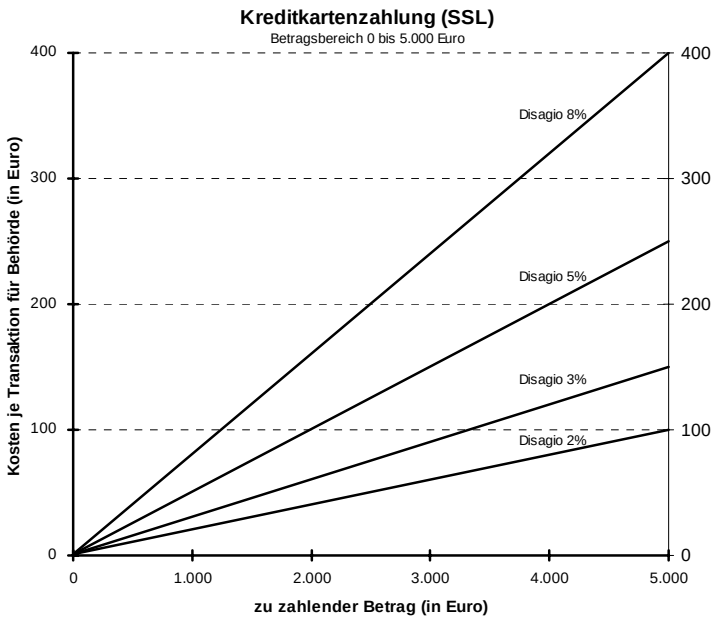
Fachspezifische Anforderungen:

- Wiederkehrende Zahlungen: ja
  Der Händler kann die Kreditkartendaten des Kunden auch wiederholt zum Einzug von Zahlungen verwenden.
- Internationalität: ja
  Kreditkarten werden von den Kreditkartengesellschaften weltweit vermarktet. Kreditkartenzahlungen können jederzeit ohne zusätzlichen Aufwand von jedem Karteninhaber durchgeführt werden.
- Anonymität: ja
  Die Behörde benötigt für die Autorisierung der Zahlung nur die Kreditkartennummer und das Gültigkeitsdatum der Karte, der Name des Karteninhabers ist für die Autorisierung in der Regel nicht notwendig. Kreditkartenzahlungen können damit so gestaltet werden, dass auch eine pseudonyme Bezahlung möglich ist.
- Zahlungsgarantie: gering
  Der Kunde kann jederzeit abstreiten, die Zahlung ausgelöst zu haben. Die Kreditkartenunternehmen verlangen für eine Zahlungsgarantie den Beweis einer rechtsverbindlichen Willenserklärung (z. B. eine handschriftliche Unterschrift oder eine qualifizierte elektronische Signatur) durch den Kunden. Bei einer Kreditkartzahlung über SSL, die ohne diesen Beleg initiiert wird, kann der mit der Zahlung belastete Karteninhaber die Zahlungsauslösung jederzeit, d. h. auch noch Monate nach der Transaktion, glaubhaft abstreiten.
- Verbreitung: hoch
  Ein sehr hoher Anteil der Kunden besitzt eine Kreditkarte. In Deutschland sind derzeit ca. 22 Millionen Kreditkarten im Umlauf [Source 2004].

Betragsbereich und Kostenstruktur:

Der Betragsbereich ist bei Kreditkartenzahlungen grundsätzlich nicht begrenzt. Zu beachten ist jedoch das individuelle Verfügungslimit des Karteninhabers.

Für den Kunden entstehen keine transaktionsabhängigen Kosten. Hat die Behörde die Kreditkartenzahlung mittels einer SSL-Verbindung in ihre Systeme integriert, so fallen in der Regel zusätzlich noch eine fixe Transaktionsgebühr zur Datenübermittlung und ein Disagio bzgl. des Zahlungsbetrags an.



Annahmen: Die Behörde übermittelt Kreditkartendaten zur Autorisierung unter Einbeziehung eines Netzbetreibers an einen Acquirer weiter. Es entstehen dadurch eine fixe Transaktionsgebühr in Höhe von 0,50 Euro (brutto) und ein Disagio. Die Kurven geben unterschiedliche Disagiosätze wieder.

Abbildung 38: Verlauf der variablen Kosten einer Kreditkartenzahlung (SSL)

Sicherheit:

- Transaktionskontrolle: mittel
  Der Kunde erhält eine monatliche Kreditkartenabrechnung als Übersicht aller eingereichten Belastungen. Eine zeitnahe Transaktionsbestätigung erfolgt bei Zahlungen im Internet dagegen in der Regel nicht.

- Stärke des Authentifizierungsmechanismus: gering
  Bei Kreditkartenzahlungen wird die Authentifizierung an Hand der auf der Kreditkarte aufgebrachten Daten (Kreditkartennummer und Gültigkeitsdatum) durchgeführt. Diese sind für Dritte mit geringem Aufwand zugänglich[106] und somit als nicht ausreichend geheim einzustufen.

- Sperrmöglichkeit: ja
  Um Schäden für den Kunden vorzubeugen, werden von den Kreditkartenorganisationen Telefonleitungen geschaltet, die jederzeit eine unmittelbare Sperre der Kreditkarte ermöglichen.

- Haftungsbetrag: 50 Euro
  Bei Verlust der Karte haftet der Kunde in der Regel mit einem maximalen Betrag von 50 Euro, wenn Verfügungen am Point of Sale vorgenommen werden und die Karte nicht gesperrt wurde. In Einzelfällen werden mit dem Kunden auch andere Haftungsbeträge vereinbart.

106 Beispielsweise können die Daten von Belegen aus vergangenen Kreditkartenzahlungen abgelesen werden.

A.6 Kreditkartenzahlung (3-D Secure)

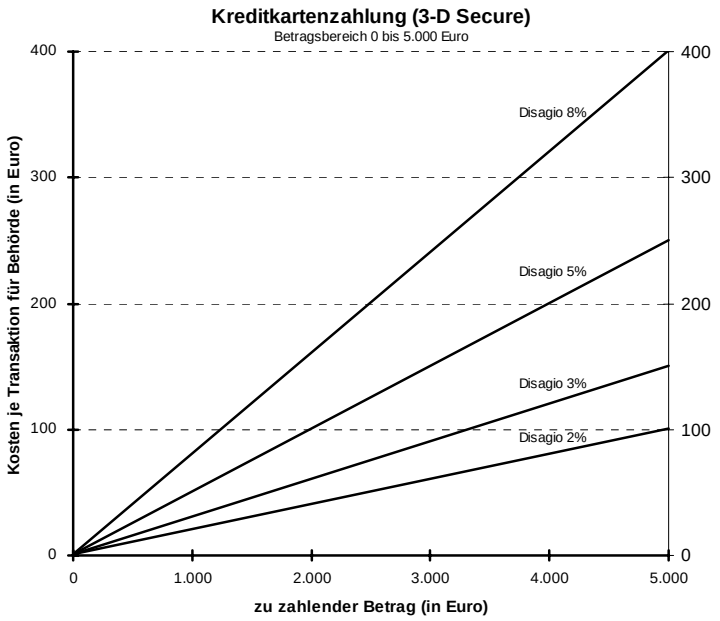
Fachspezifische Anforderungen:

- Wiederkehrende Zahlungen: nein
  Der Kunde muss die Zahlungen einzeln durch Eingabe seines Kennworts freigeben. Ohne Eingabe des Kennworts durch den Kunden erhält der Händler keine Zahlungsgarantie.
- Internationalität: ja
  Kreditkartenzahlungen über 3-D Secure unterscheiden sich hinsichtlich der Eignung für eine internationale Nutzung nicht von einer Kreditkartenzahlung über SSL. Sie können jederzeit ortsunabhängig über das Internet initiiert werden.
- Anonymität: ja
  Die Behörde benötigt für die Autorisierung der Zahlung nur die Kreditkartennummer und das Gültigkeitsdatum der Karte, der Name des Karteninhabers ist für die Autorisierung in der Regel nicht notwendig. Zur Authentifizierung des Karteninhabers wird nur die PIN benötigt. Kreditkartenzahlungen können damit so gestaltet werden, dass auch eine pseudonyme Bezahlung möglich ist.
- Zahlungsgarantie: hoch
  Die Behörde erhält bei Einsatz von 3-D Secure in der Regel eine sofortige Zahlungsgarantie.
- Verbreitung: gering
  Derzeit existieren in Deutschland kaum Vertragsunternehmen, die 3-D Secure zur Zahlung einsetzen. Die Vertragsunternehmen sind auch zukünftig nicht verpflichtet, auf 3-D Secure basierende Zahlungsmöglichkeiten anzubieten.

Betragsbereich und Kostenstruktur:

Der Betragsbereich ist bei Kreditkartenzahlungen grundsätzlich nicht begrenzt. Zu beachten ist jedoch das individuelle Verfügungslimit des Karteninhabers.

Für Kunden entstehen im Rahmen der Transaktion keine Kosten. Hat das Vertragsunternehmen die 3-D Secure Kreditkartenzahlung in ihr System integriert, so fallen in der Regel zusätzlich noch eine fixe Transaktionsgebühr zur Datenübermittlung und ein Disagio bzgl. des Zahlungsbetrags an.



Annahmen: Die Behörde übermittelt Kreditkartendaten zur Autorisierung unter Einbeziehung eines Netzbetreibers an einen Acquirer weiter. Es entsteht dadurch eine fixe Transaktionsgebühr in Höhe von 0,50 Euro (brutto) und ein Disagio. Die Kurven geben unterschiedliche Disagiosätze wieder.

Abbildung 39: Verlauf der variablen Kosten einer Kreditkartenzahlung (3-D Secure)

Sicherheit:

- Transaktionskontrolle: mittel
  Der Kunde erhält eine monatliche Kreditkartenabrechnung als Übersicht aller eingereichten Belastungen. Eine zeitnahe Transaktionsbestätigung erfolgt bei Zahlungen im Internet dagegen in der Regel nicht. Auch das Merchant Server Plug-in (MPI) führt nicht zu einer erhöhten Transaktionskontrolle, da dieses lediglich den Status der Authentifizierung meldet. Rückschlüsse auf erfolgreich eingereichte Autorisierungen können daraus nicht gezogen werden.
- Stärke des Authentifizierungsmechanismus: mittel
  Das Merchant Server Plug-in (MPI) führt eine wissensbasierte Authentifizierung durch.
- Sperrmöglichkeit: ja
  Um Schäden des Kunden vorzubeugen, werden von den Kreditkartenorganisationen Telefonleitungen geschaltet, die jederzeit eine unmittelbare Sperre der Kreditkarte ermöglichen.
- Haftungsbetrag: 50 Euro
  Der Kunde haftet aus missbräuchlichen Verfügungen in der Regel mit einem maximalen Betrag von 50 Euro. In Einzelfällen werden mit dem Kunden auch andere Haftungsbeträge vereinbart.

A.7 Wertkarten-basierte Verfahren

Aus der Kategorie „Wertkarten-basierte Verfahren“ wurde die paysafecard bewertet.

Fachspezifische Anforderungen:

- Wiederkehrende Zahlungen: nein
  Systembedingt ist es nicht möglich, ohne aktives Zutun des Kunden automatisiert Beträge abzubuchen.
- Internationalität: ja
  Kunden aus dem Ausland können die paysafecard über das Internet beziehen.[107] Für den Einsatz der paysafecard sind keine weiteren Voraussetzungen notwendig.
- Anonymität: ja
  Die Kunden können die Karten auch durch Barzahlung erwerben. Die Behörde erhält während des Zahlungsprozesses keine kundenbezogenen Daten.
- Zahlungsgarantie: hoch
  Der Zahlungssystemanbieter garantiert für die Übermittlung der eingereichten Zahlungen an die Behörde.
- Verbreitung: gering
  Die Verbreitung der paysafecard wird als gering eingestuft. Indikatoren dafür sind die derzeit vergleichsweise geringe Nutzerzahl sowie die geringe Zahl an Akzeptanzstellen.

Betragsbereich und Kostenstruktur:

Zahlungen sind mit der paysafecard im Bereich von 0,01 bis 100 Euro möglich. Zwar können bei einer Transaktion bis zu zehn Karten verwendet werden, aus Praktikabilitätsgründen erscheint jedoch die Begrenzung des Betragsbereichs auf 100 Euro sinnvoll.

- Fixe Kosten entstehen für die Behörde mit Ausnahme der Implementierungskosten nicht.
- Variable Kosten für den Kunden fallen nicht an.
- Die Behörde muss bei materiellen Gütern 5,5 Prozent Provision zuzüglich gesetzlich vorgeschriebener Umsatzsteuer aus der Summe des vom Kunden zu zahlenden Betrags plus Versandkosten an paysafecard zahlen. Bei immateriellen Leistungen muss die Behörde bei Transaktionen bis fünf Euro 19 Prozent Provision zahlen. Bei immateriellen Gütern über fünf Euro sind 12 Prozent fällig. Beide Fälle werden noch mit der gesetzlich vorgeschriebenen Umsatzsteuer belegt.

[107] Mögliche Online-Bezugsquellen finden sich auf http://www.paysafecard.de/.

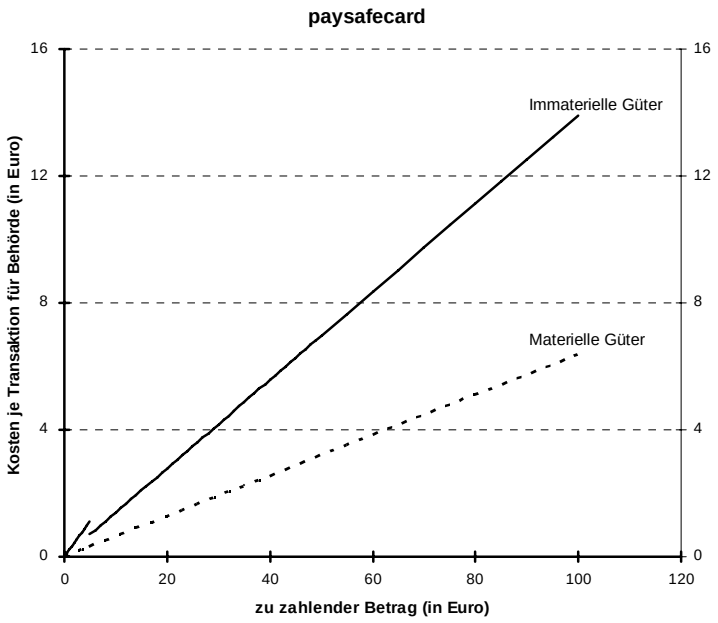


Abbildung 40: Verlauf der variablen Kosten bei der paysafecard

Sicherheit:

- Transaktionskontrolle: hoch
  Der Kunde erhält nach jeder Zahlung eine Ausführungsbestätigung. Das Guthaben der Karte und bereits getätigte Buchungen können auf der paysafecard-Webseite eingesehen werden.
- Stärke des Authentifizierungsmechanismus: hoch
  Zur Nutzung der paysafecard ist es notwendig, im Besitz des 16-stelligen Codes auf der Karte (Besitzmerkmal) zu sein, und das persönliche Passwort (Wissensmerkmal) zu kennen.
- Sperrmöglichkeit: nein
  Die Sperrung der paysafecard ist nicht möglich.
- Haftungsbetrag: Kartenguthaben (max. 100 Euro)
  Da die paysafecard nicht gesperrt werden kann, ist der Schaden, den der Kunde maximal erleiden könnte, auf das aktuell verfügbare Kartenguthaben beschränkt. Dieses kann systembedingt maximal 100 Euro betragen.

A.8 E-Mail-basierte Verfahren

Aus der Kategorie „E-Mail-basierte Verfahren“ wurde moneybookers bewertet.

Fachspezifische Anforderungen:

- Wiederkehrende Zahlungen: ja
  Termin- und Daueraufträge können eingerichtet werden. moneybookers sorgt anschließend selbstständig für die Ausführung.
- Internationalität: ja
  Zahlungen können an jeden Inhaber einer E-Mail-Adresse erfolgen. Ist der Empfänger noch nicht bei moneybookers angemeldet, muss er sich jedoch registrieren, um die Zahlung annehmen zu können.
- Anonymität: ja
  Der Behörde wird ausschließlich die E-Mail-Adresse des Kunden mitgeteilt. Somit ist eine pseudonyme Nutzung des Dienstes möglich.
- Zahlungsgarantie: hoch
  Nach Initiierung der Zahlungstransaktion durch den Kunden wird dem Zahlungsempfänger der Betrag sofort auf seinem moneybookers-Konto gutgeschrieben. Der Empfänger kann unmittelbar über das elektronische Geld verfügen.
- Verbreitung: gering
  In Deutschland sind bisher nur verhältnismäßig wenige Nutzer bei moneybookers registriert. Hinderlich für eine hohe Verbreitung könnte sein, dass es sich bei moneybookers um kein nationales E-Geld-Institut handelt.

Betragsbereich und Kostenstruktur:

Grundsätzlich könnten mit moneybookers auch Beträge in Höhe von mehreren Tausend Euro beglichen werden. Geht man jedoch von vergleichbaren Zahlungsverfahren aus, die ebenfalls auf Guthabenbasis aufbauen, so erscheint ein verfügbares Guthaben von 500 Euro je Nutzer als angemessen, was in der Praxis den Betragsbereich auf 500 Euro einschränken würde. Es ist nicht zu erwarten, dass Nutzer im Vorhinein wesentlich höhere Beträge bei moneybookers vorhalten werden.

Es entstehen ausschließlich für den Sender der Zahlung, somit den Kunden der Behörde, Kosten in Höhe von 1%, maximal jedoch 0,50 Euro. Aus Sicht der Behörde entstehen somit für den Empfang von Geldeinheiten keine Kosten. Zu berücksichtigen ist allerdings, dass die Geldeinheiten auf einem Verrechnungskonto von moneybookers vorgehalten werden. Für die Übertragung von Geldeinheiten vom Verrechungskonto bei moneybookers auf ein Konto der Behörde sind jedoch Gebühren an moneybookers zu entrichten.

Sicherheit:

- Transaktionskontrolle: hoch
  Der Kunde kann unmittelbar im Anschluss an die Transaktion in seinem persönlichen Bereich eine Übersicht der getätigten Zahlungen einsehen.
- Stärke des Authentifizierungsmechanismus: mittel
  Zur Auslösung einer Zahlungstransaktion durch moneybookers ist ein Passwort erforderlich.

- Sperrmöglichkeit: ja
  Das moneybookers Konto kann gesperrt werden.
- Haftungsbetrag: Guthaben auf Verrechnungskonto
  Der Kunde haftet mit seinem gesamten Guthaben auf dem Verrechnungskonto.

A.9 Mobiltelefon-basierte Verfahren

Aus der Kategorie „Mobiltelefon-basierte Verfahren“ wurde Vodafone m-pay bewertet.

Fachspezifische Anforderungen:

- Wiederkehrende Zahlungen: ja
  Mit Vodafone m-pay können regelmäßige Zahlungen automatisch vom Vodafone-Konto abgebucht werden.
- Internationalität: Nein
  Vodafone m-pay steht derzeit nur Kunden der in Deutschland ansässigen Vodafone D2 zur Verfügung.
- Anonymität: ja
  Der Kunde übermittelt bei der Zahlung nur die Rufnummer seines Mobiltelefons. Er tritt damit gegenüber der Behörde nur unter einem Pseudonym auf.
- Zahlungsgarantie: hoch
  Mit der Autorisierung der Transaktion übernimmt Vodafone D2 das Zahlungsausfallrisiko.
- Verbreitung: hoch
  Das Unternehmen verfügt nach eigenen Angaben derzeit über 26 Millionen Kunden. Die Verbreitung des Zahlungsverfahrens wird daher als hoch eingestuft.

Betragsbereich und Kostenstruktur:

Zahlungen mit Vodafone m-pay sind nur bis zu einem Betrag von 10 Euro möglich.

- Für den Kunden entstehen bei der Nutzung keine Gebühren.
- Die Behörde trägt eine einmalige Anbindungsgebühr in Höhe von 7.500 Euro (zzgl. USt.) sowie einen monatlichen Basispreis in Höhe von 100 Euro (zzgl. USt.).
- Vom monatlichen Umsatz muss die Behörde einen Anteil von 22,35 % (mindestens 500 Euro (zzgl. USt.)) abführen.

Annahmen: Die Behörde setzt mehr als 2.596 Euro im Monat um.

Abbildung 41: Verlauf der variablen Kosten bei Vodafone m-pay

Sicherheit:

- Transaktionskontrolle: hoch
  Der Kunde erhält einen Überblick über getätigte Transaktionen auf seiner Mobilfunkrechnung (ausgenommen Prepaid- (CallYa-) Kunden).
- Stärke des Authentifizierungsmechanismus: hoch
  Die Identifizierung erfolgt anhand der Vodafone-SIM[108]-Karte. Zur Nutzung von Vodafone m-pay ist es notwendig, im Besitz einer registrierten SIM-Karte (Besitzmerkmal) zu sein und die PIN zu kennen (Wissensmerkmal).
- Sperrmöglichkeit: ja
  Eine Sperrung ist möglich.
- Haftungsbetrag: 10 Euro
  Werden vor einer Sperre missbräuchliche Verfügungen getätigt, so haftet der Kunde nur bis zu einer Summe von 10 Euro.

108 Abkürzung für Subscriber Identification Module: Teilnehmeridentifizierungsmodul auf Basis einer Chipkarte für Mobiltelefone.

A.10 Nachnahme

Aus der Kategorie „Nachnahme“ wurde der Standardbrief der Deutschen Post sowie das DHL-Paket bewertet.

Fachspezifische Anforderungen:

- Wiederkehrende Zahlungen: nein
  Die Zahlung muss jedes Mal erneut durch den Kunden ausgelöst werden.
- Internationalität: ja
  Nachnahmesendungen ins Ausland sind grundsätzlich möglich. Damit kann das Zahlungsverfahren auch international eingesetzt werden.
- Anonymität: nein
  Um das Zahlungsverfahren nutzen zu können, muss der Kunde gegenüber der Behörde seine Adresse bekannt geben. Ansonsten ist eine Zustellung nicht möglich. Das Verfahren ist für eine anonyme Nutzung nicht geeignet.
- Zahlungsgarantie: hoch
  Da der Kunde die Leistung erst erhält, nachdem diese gegenüber dem Zustelldienst bezahlt wurde, ist die Zahlungsgarantie als hoch einzustufen. Im Fall der Nichtannahme durch den Kunden wird die Lieferung an die Behörde zurückgesandt. Zu beachten ist jedoch, dass die Zahlungsgarantie keine Kosten für individuell erstellte Leistungen abdeckt.
- Verbreitung: hoch
  Zur Nutzung des Verfahrens sind auf Kundenseite keine Voraussetzungen notwendig.

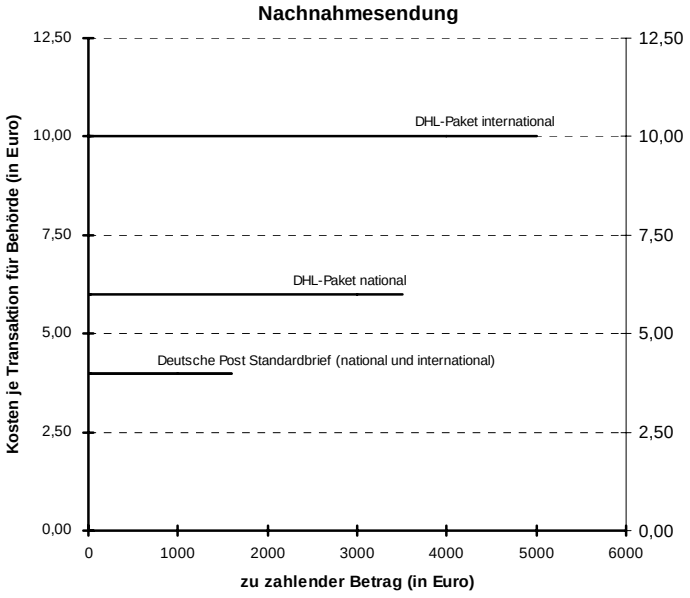
Betragsbereich und Kostenstruktur:

Der Betragsbereich bei der Nachnahme beginnt bei 0,01 Euro und ist auf einen Paketwert von 5.000 Euro[109] begrenzt. Die Kostenstruktur des Verfahrens ist im kleinpreisigen Bereich jedoch unrentabel.

- Fixe Kosten fallen bei der Nachnahme für die Behörde nicht an.
- Variable Kosten für den Kunden fallen nicht an.
- Unabhängig vom Betragsvolumen muss die Behörde bei einer Nachnahmesendung durch die Deutsche Post ein Nachnahme-Entgelt und eine Geldübermittlungsgebühr entrichten. Das Nachnahme-Entgelt ist von der Behörde zu leisten, auch wenn der Kunde die Annahme verweigert. Die Geldübermittlungsgebühr fällt nur an, wenn die Deutsche Post den vom Kunden erhaltenen Betrag an die Behörde übermittelt, wobei die Gebühr vom eingezogenen Nachnahmebetrag abgezogen wird. Bei der Nachnahme fallen bei einem Standardbrief (national und international) zwei Euro Nachnahme-Entgelt und zwei Euro Übermittlungsgebühr, in der Summe somit vier Euro an variablen Kosten für die Behörde an. Bei Versand eines DHL-Pakets im Inland belaufen

[109] Der Betragsbereich ist bei Briefen und Postkarten auf 1.600 Euro, bei nationalen DHL-Paketen auf 3.500 Euro, bei internationalen DHL-Paketen auf 5.000 Euro beschränkt. Vgl. u. a. http://www.deutschepost.de/dpag?check=yes&lang=de_DE&xmlFile=1386#/.

sich die Kosten auf sechs Euro: vier Euro Nachnahme-Entgelt und zwei Euro Übermittlungsgebühr. Wird ein Paket durch die Deutsche Post ins Ausland versandt, erhöht sich die Übermittlungsgebühr auf sechs Euro und somit die Gesamtkosten auf zehn Euro.



Annahmen: Der Kunde nimmt die Sendung an.

Abbildung 42: Verlauf der variablen Kosten einer Nachnahmesendung

Sicherheit:

- Transaktionskontrolle: mittel
  Der Kunde erhält eine Bestätigung des an den Zustelldienst bezahlten Betrages. Eine Übersicht über getätigte Zahlungen fehlt jedoch. Somit wird die Transaktionskontrolle mit mittel bewertet.
- Stärke des Authentifizierungsmechanismus: mittel
  Die Zustellung einer Nachnahmesendung erfolgt durch Aushändigung an den Empfänger, einen Empfangsbevollmächtigten oder einen Ersatzempfänger gegen Begleichung des Nachnahmebetrags. Der Authentifizierungsmechanismus ist als mittel einzustufen.
- Sperrmöglichkeit: nein
  Eine grundsätzliche Sperrung des Nachnahme-Verfahrens ist systembedingt nicht möglich. Es kann jedoch die Annahme der Sendung verweigert werden.
- Haftungsbetrag: 0 Euro
  Für den Empfänger entsteht keine Haftung, da er die Annahme der Sendung verweigern kann. Sollte der Empfänger eine Sendung annehmen, die nicht den erwarteten Inhalt darstellt, so kann er anderweitige Ansprüche gegen den Absender geltend machen.

A.11 Billing-Verfahren

Aus der Kategorie „Billing-Verfahren“ wurde Firstgate click&buy bewertet.

Fachspezifische Anforderungen:

- Wiederkehrende Zahlungen: nein
  Mit click&buy ist es nicht möglicht, ohne aktives Zutun des Kunden wiederkehrende Zahlungen ausführen zu lassen, da jeder Zahlungsvorgang vom Kunden durch Eingabe seines Benutzernamens und seiner PIN ausgelöst werden muss.
- Internationalität: ja
  click&buy kann in mehreren Ländern zum Bezahlen von Web-Inhalten genutzt werden. Die Nutzerdaten können dabei international verwendet werden. Eine erneute Registrierung in einem anderen Land ist nicht notwendig.
- Anonymität: ja
  Der Behörde werden die erzielten Umsätze in aggregierter Form monatlich von Firstgate überwiesen. Der Kunde bleibt somit gegenüber der Behörde anonym.[110]
- Zahlungsgarantie: mittel
  Firstgate garantiert nicht für die Zahlungsfähigkeit des Kunden. Das Risiko, dass dieser nicht zahlen kann, trägt die Behörde.
- Verbreitung: mittel
  Anfang 2004 waren etwa 2,5 Millionen Nutzer bei Firstgate registriert. 2.500 Anbieter unterstützen das Zahlungsverfahren. Die Verbreitung wird mit mittel bewertet.

Betragsbereich und Kostenstruktur

Die Behörde kann Preise von 0,05 bis maximal 10 Euro je Produkt/Dienstleistung festsetzen. Die Abstufung erfolgt in diesem Bereich in Schritten von 0,01 Euro.

- Es fällt für die Behörde ein einmaliges Anmeldeentgelt in Höhe von 49 Euro an. Zusätzlich sind Aufwendungen für die Integration des Verfahrens in den Internet-Auftritt der Behörde zu beachten. Weitere einmalige Fixkosten entstehen in der Regel nicht.
- Neben den einmaligen Fixkosten fallen monatliche Bereitstellungskosten in Höhe von fünf Euro an.
- Variable Kosten entstehen ausschließlich für die Behörde. Es wird zwischen unterschiedlichen Forderungsvolumina je Monat unterschieden. Je nach Forderungsvolumen werden unterschiedliche Provisionssätze zwischen 9,5% und 38% zzgl. USt. fällig. Weiterhin wird differenziert, ob eine Tarifierung bis fünf Euro oder über fünf Euro erfolgt. Bei einer Tarifierung über fünf Euro ist

[110] Bei Reklamation leitet Firstgate die Kundendaten an die Behörde weiter, damit diese die Probleme mit dem Kunden klären kann. Für diesen Fall erklärt der Kunde sich im Rahmen der Registrierung mit einer Weitergabe der personenbezogenen Daten einverstanden.

der Provisionssatz geringer, es fallen jedoch zusätzliche Kosten in Höhe von 0,50 Euro je Transaktion an.

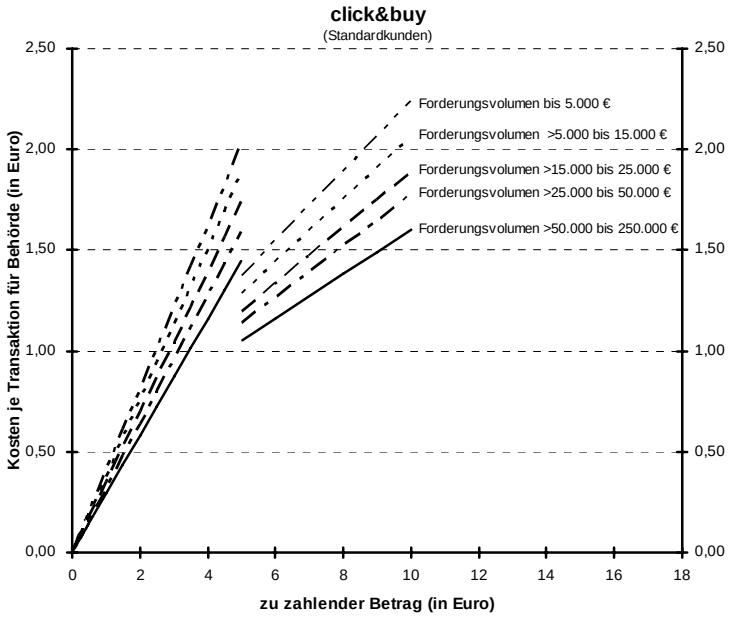


Abbildung 43: Verlauf der variablen Kosten bei click&buy

Sicherheit

- Transaktionskontrolle: hoch
  Nachdem der Kunde eine Transaktion durchgeführt hat, erhält er innerhalb weniger Minuten eine Transaktionsbestätigung per E-Mail. Die getätigten Umsätze kann er auf der Firstgate-Webseite im Service-Bereich einsehen.
- Stärke des Authentifizierungsmechanismus: mittel
  Die Authentifizierung erfolgt mittels einer vom Benutzer gewählten PIN. Die Stärke des Authentifizierungsmechanismus wird daher als mittel eingestuft.
- Sperrmöglichkeit: ja
  Ein Sperrung des Zahlungsverfahrens ist durch Zusendung einer E-Mail an Firstgate möglich.
- Haftungsbetrag: nicht begrenzt
  Eine grundsätzliche Haftungsbeschränkung des Kunden für die getätigten Transaktionen vor einer Sperrung gibt es nicht. Der Kunde haftet vollständig für den auftretenden Schaden.

A.12 Übersicht über in Deutschland verfügbare Zahlungsverfahren

Verfahren	Erläuterung	Anbieter	Internet-Adresse
Geldbörse			
GeldKarte	Angebot der GeldKarte-Funktionalität auf vielen Bankkundenkarten mit Chip.	Kreditwirtschaft	http://www.geldkarte.de/
Überweisung			
Atos Origin Online-Überweisung	Eingabe der Internet-Banking-Daten (PIN und TAN) und damit Autorisierung der Zahlung durch den Kunden über ein Applet; Bank des Kunden erhält Überweisungsdaten zur Ausführung.	Atos Origin	http://www.atosorigin.de/
ECObanking	Eingabe der Internet-Banking-Daten (PIN und TAN) und damit Autorisierung der Zahlung durch den Kunden über ein Applet; Bank des Kunden erhält Überweisungsdaten zur Ausführung.	liberECO payment solutions	http://www.libereco.de/
fun HomePay	Kunde vereinbart mit seiner Bank die Nutzung des Online-Überweisungsverfahren als Zahlungsverfahren; Kunde wird vom Händler auf die Internet-Banking-Seite seiner Bank umgeleitet, wo er ein vorausgefülltes Überweisungsformular per HBCI, PIN/TAN oder elektronischer Signatur autorisiert.	Fun Communications	http://www.fun.de/
Pago Online-Überweisung	Eingabe der Internet-Banking-Daten (PIN und TAN) und damit Autorisierung der Zahlung durch den Kunden über ein Applet; Bank des Kunden erhält Überweisungsdaten zur Ausführung.	Pago eTransaction Services	http://www.pago.de/
PaylikeCash	Eingabe der Internet-Banking-Daten (PIN und TAN) und damit Autorisierung der Zahlung durch den Kunden über einen Webclient; Bank des Kunden erhält Überweisungsdaten zur Ausführung.	Elaxy	http://www.elaxy.de/
Postbank Online-Überweisung	Kunde und Behörde müssen ein Konto bei der Postbank besitzen. Kunde wird auf Internet-Banking-Seite der Postbank umgeleitet, wo er ein vorausgefülltes Überweisungsformular durch PIN/TAN autorisiert.	Postbank	http://www.postbank.de/
Überweisung vor/nach Lieferung	Der Kunde überweist den Betrag vor oder nach Lieferung von Ware/Dienstleistung auf ein Konto der Behörde.	Kreditwirtschaft	http://www.zka.de/[111]

[111] Im Zentralen Kreditausschuss (ZKA) sind die fünf Spitzenverbände der deutschen Kreditwirtschaft (Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e.V., Bundesverband deutscher Banken e.V., Bundesverband Öffentlicher Banken Deutschlands e.V., Deutscher Sparkassen- und Giroverband e.V. und Verband deutscher Hypothekenbanken e.V.) zusammengeschlossen.

Verfahren	Erläuterung	Anbieter	Internet-Adresse
Lastschrift			
Bei der Lastschrift handelt es sich um ein von der Kreditwirtschaft angebotenes Zahlungsverfahren.		Kreditwirtschaft	http://www.zka.de/
Scheck			
Der Scheck ist ein von der Kreditwirtschaft angebotenes Zahlungsverfahren. Eine elektronische Variante ist derzeit nicht verfügbar.		Kreditwirtschaft	http://www.zka.de/
Kreditkarten-basierte Zahlungsverfahren			
American Express Card	Neben der Zahlung durch Angabe der Kreditkartendaten im Browser ermöglicht American Express auch die Abfrage von Kartenprüfnummern (CSC).	American Express International	http://www.americanexpress.com/
MasterCard	Neben der Zahlung durch Angabe der Kreditkartendaten im Browser ermöglicht MasterCard auch die Abfrage von Kartenprüfnummern (CVC bzw. CVC2). Das 3-D-Secure-Verfahren wird unter dem Markennamen „MasterCard SecureCode“ angeboten.	MasterCard International	http://www.mastercard.de/
Visa Karte	Neben der Zahlung durch Angabe der Kreditkartendaten im Browser ermöglicht Visa auch die Abfrage von Kartenprüfnummern (CVV bzw. CVV2). Das 3-D-Secure-Verfahren wird unter dem Markennamen „Verified by Visa“ angeboten.	Visa International	http://www.visa.de/
Wertkarten-basierte Zahlungsverfahren			
paysafecard	Guthabenkarte mit optionalem Zugriffschutz durch PIN. Bezug der Karte im Handel oder im Internet möglich.	paysafecard.com Wertkarten	http://www.paysafecard.com/
T-Pay Micro-Money	Die Guthabenkarte ist eine von fünf Bezahlvarianten im Produktportfolio T-Pay der Deutschen Telekom. Bezug der Karte im Handel oder im Internet möglich.	Deutsche Telekom, Deutsche Telekom Card-Service	http://www.micromoney.de/
E-Mail-basierte Zahlungsverfahren			
Anypay	Übertragung von Werteinheiten durch Nachricht per E-Mail. Zahlungsausgleich per Kreditkarte.	Globyte Internet	http://www.anypay.de/
money-bookers	Übertragung von Geldeinheiten durch Nachricht per E-Mail. Zahlungsausgleich per Kreditkarte oder Überweisung.	moneybookers	http://www.moneybookers.com/
PayPal	Übertragung von Geldeinheiten durch Nachricht per E-Mail. Zahlungsausgleich über Kreditkarte.	PayPal (Europe)	http://www.paypal.de/
WEB.Cent	Übertragung von Werteinheiten durch Nachricht per E-Mail. Zahlungsausgleich per Lastschrift, Kreditkarte oder Überweisung.	WEB.DE	http://www.web.de/

Verfahren	Erläuterung	Anbieter	Internet-Adresse
Mobiltelefon-basierte Zahlungsverfahren			
allPAY	Nach Eingabe seiner Mobiltelefonnummer erhält der Kunde eine SMS mit einem Bezahlcode (PIN), den er im Browser-Fenster eingibt. Der Zahlungsausgleich erfolgt über die Mobilfunkrechnung.	allPAY	http://www.allpay.info/
fun PhotoPay	Kunde fotografiert mit seinem Kamera-Mobiltelefon einen Strichcode der auf einem Bildschirm angezeigt wird, ab. Die auf dem Mobiltelefon installierte Software fun PhotoPay überträgt die Zahlungsdaten zur Verrechnung an einen Zahlungsdienstleister. Der Zahlungsausgleich erfolgt per Kreditkarte, Lastschrift oder Online-Überweisung.	Fun Communications	http://www.fun.de/
Geldhandy	Zur Nutzung muss sich der Kunde registrieren und erhält optional eine PIN zugesandt, die die Bezahlvorgänge zusätzlich absichert. Um zu bezahlen gibt der Kunde einen Code in das Browser-Fenster ein, den er durch Wahl einer kostenlosen Rufnummer erhält. Der Zahlungsausgleich erfolgt monatlich über einen Einzug der Rechnungssumme.	IN MEDIAS RES	http://www.geldhandy.info/
Handypay	Nach Eingabe seiner Mobiltelefonnummer erhält der Kunde eine SMS mit einem Bezahlcode (PIN), den er im Browser-Fenster eingibt. Der Zahlungsausgleich erfolgt über die Mobilfunkrechnung.	Enterpayment	http://www.handypay.de/
Street Cash	Street Cash sendet eine SMS mit Zahlungsinformationen an die Mobiltelefonnummer des Kunden, die er mit Eingabe seiner PIN bestätigt. Der Zahlungsausgleich erfolgt über Kreditkarte oder per Lastschrift.	Inatec solutions	http://www.streetcash.de/
Vodafone m-pay	Vodafone-Kunden können Beträge bis 10 Euro begleichen. Dazu muss der Kunde einen per SMS übermittelten Code als Zahlungsbestätigung in einem Browser-Fenster eingeben. Der Kunde wird vorher über seine Vodafone D2-Nummer identifiziert. Der Zahlungsausgleich erfolgt über die Mobilfunkrechnung.	Vodafone	http://www.vodafone.de/m-pay/
Inkasso- und Billingverfahren			
Bill4net	Der Kunde kann kostenpflichtige Downloads durch Wahl einer Service-Rufnummer begleichen. Der Zahlungsausgleich erfolgt über die Telefonrechnung.	Pgmedia IN-Systems	http://www.bill4net.de/
click&buy	Der Kunde klickt auf einen kostenpflichtigen Link. Anschließend bestätigt er durch Eingabe von Benutzername und PIN den kostenpflichtigen Abruf. Der Zahlungsausgleich erfolgt über Kreditkarte oder Lastschrift.	FIRSTGATE	http://www.firstgate.de/
Click2Pay	Der Kunde klickt auf einen kostenpflichtigen Link. Anschließend bestätigt er durch Eingabe von Benutzername und PIN den kostenpflichtigen Abruf. Der Zahlungsausgleich erfolgt über Kreditkarte oder Lastschrift.	Click2Pay	http://www.click2pay.de/

Verfahren	Erläuterung	Anbieter	Internet-Adresse
Voice Dialer	Um in einen kostenpflichtigen Bereich zu gelangen, wählt der Kunde eine angezeigte Servicerufnummer. Anschließend wird der Zugang freigeschaltet und er kann in dem Bereich solange verweilen, bis er auflegt. Der Zahlungsausgleich erfolgt über die Telefonrechnung.	MoreCon AG More Connections i.G.	http://www.morecon.de/
Internet-Dialer	Eine installierte Dialer-Software trennt beim Klicken auf den kostenpflichtigen Link die bestehende Internet-Verbindung und wählt sich mit einer Service-Rufnummer wieder ein. Anschließend werden dem Kunden die kostenpflichtigen Seiten angezeigt. Der Zahlungsausgleich erfolgt über die Telefonrechnung.	MoreCon AG More Connections i.G.	http://www.morecon.de/
iclear	Nach der Anmeldung kann der Kunde mit Benutzernamen und Passwort einkaufen. Bei Rücksendungen oder Falschsendungen erhält der Kunde sein Geld zurück.	EuroCoin Iclear	http://www.iclear.de/
infin-Micro-Payment	Der Kunde kann kostenpflichtige Downloads durch Wahl einer Service-Rufnummer begleichen. Der Zahlungsausgleich erfolgt über die Telefonrechnung.	infin – Ingenieurge-sellschaft für Informations-technologien	http://www.infin.de/
IN-micropay	Der Kunde wählt die im Browser-Fenster angezeigte Rufnummer. Anschließend gibt er die ihm per Telefon mitgeteilte PIN in das Browser-Fenster ein und der Inhalt wird freigeschaltet. Der Zahlungsausgleich erfolgt über die Telefonrechnung.	IN-telegence	http://www.in-micropay.de/
INwebcall	Der Kunde wählt die im Browser-Fenster angezeigte Rufnummer und gibt die ebenfalls angezeigte PIN ein. Anschließend wird der Inhalt solange freigeschaltet, bis der Kunde wieder auflegt. Der Zahlungsausgleich erfolgt über die Telefonrechnung.	IN-telegence	http://www.in-micropay.de/
Nachnahme	Gegen Begleichung des Zahlungsbetrages wird dem Kunden die Ware übergeben. Anschließend leitet der Zustelldienst den Inkassobetrag an die Behörde weiter.	Deutsche Post, DHL, UPS, DPD, GLS , TNT, Hermes	http://www.deutschepost.de/ http://www.dhl.de/ http://www.ups.de/ http://www.dpd.de/ http://www.gls-germany.com/ http://www.tnt.de/ http://www.hermes-vs.de/
PayBest	Durch Anruf einer Service-Rufnummer erhält der Kunde eine Gutscheinnummer im Wert von 2,50 Euro angesagt. Zum Bezahlen trägt der Kunde diese Nummer in eine dafür vorgesehenes Eingabefeld ein. Der Zahlungsausgleich erfolgt über die Telefonrechnung.	4FriendsOnly.-com Internet Technologies	http://www.paybest.de/
PurePay	Ein Browser-Plug-in stellt dem Kunden abhängig von seiner Systemumgebung unterschiedliche Bezahlvarianten zur Verfügung. Das Entgelt wird durch Anwahl einer Servicerufnummer geleistet und über die Telefonrechnung eingezogen.	ALBIS Zahlungs-dienste	http://www.albis-zahlungsdienste.de/
T-Pay Pay by Call	Durch Anwahl einer Servicerufnummer begleicht der Kunde den Zahlungsbetrag. Der Zahlungsausgleich erfolgt über die Telefonrechnung.	Deutsche Telekom	http://www.telekom.de/t-pay/

Stand: Mai 2005

Literaturverzeichnis

[AGM 2004]
Koordinierungsstelle für das automatisierte gerichtliche Mahnverfahren (AGM): Die maschinelle Bearbeitung der gerichtlichen Mahnverfahren. http://www.mahnverfahren.nrw.de/service/brosch/brosch.pdf, 01.07.2004. Abruf am 28.04.2005.

[BdB 2003]
Bundesverband deutscher Banken (BdB): Fast 30 Millionen Online-Konten in Deutschland. http://www.bdb.de/index.asp?channel=111010&art=766&ttyp=1&tid=996, 16.07.2003. Abruf am 12.01.2004.

[BfF 2002]
Bundesamt für Finanzen: Feinkonzept ePayment Geschäftsprozesse. Bonn 2003.

[BMF 2002]
Bundesministerium der Finanzen: Das System der Öffentlichen Haushalte. http://www.bundesfinanzministerium.de/Anlage11509/Das-System-der-Oeffentlichen-Haushalte.pdf, 2002. Abruf am 08.01.2003.

[BSI 2003]
Bundesamt für Sicherheit in der Informationstechnik: Trojanische Pferde – Definition und Wirkungsweise. Bonn 2003.

[HDE 2005]
Hauptverband des Deutschen Einzelhandels (HDE): E-Business: Mehrheit der Branche erwartet steigende Umsätze**.** http://www.einzelhandel.de/servlet/PB/menu/1044106/index.html, 09.03.2005. Abruf am 04.04.2005.

[Justizregister Bayern 2005]
Justizregister Bayern: RegisSTAR. https://handelsregister.justizregister.bayern.de/introtext.htm, 2005. Abruf am 06.04.2005.

[KBSt 2001]
Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung im Bundesministerium des Innern: Zertifizierung nach dem Konzept „Papierarmes Büro (Domea-Konzept)“. http://www.kbst.bund.de/Anlage300444/Band+53+-"Beschreibung+des+Zertifizierungsverfahrens+und+Anforderungskatalog+-1.2"++(1,+2+MB).pdf, Dezember 2001. Abruf am 20.01.2004.

[Krepold 2003]
Krepold, Hans-Michael: Lastschriftverkehr. In: Hellner, Thorwald; Schröter, Jürgen; Steuer, Stephan; Weber, Ahrend (Hrsg.): Bankrecht und Bankpraxis. Köln 2003, RZ 6/300-6/509.

[Rankl/Effing 2002]
Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten. München u. a. 2002.

[Schieb 2004]
Schieb, Jörg: Das Ende des Plastikgeldes naht. In: Handelsblatt Nr. 4 vom 07.01.2004, S. 15.

[Source 2004]
Source: 22 Millionen Kreditkarten in Deutschland. In: Source Informationsdienst Nr. 1 vom 15. Januar 2004, S. 1–2.

[StMJ 2002]
Bayerisches Staatsministerium der Justiz (StMJ): Justizminister Dr. Manfred Weiß: Bayern setzt im Mahnverfahren auf das Internet. http://www2.justiz.bayern.de/_presse/PM/2002/-03052002.htm, 03.05.2002. Abruf am 02.03.2004.

[Werner 2003]
Werner, Stefan: Die ec-Karte. In: Hellner, Thorwald; Schröter, Jürgen; Steuer, Stephan; Weber, Ahrend (Hrsg.): Bankrecht und Bankpraxis. Köln 2003, RZ 6/1300-6/1820.

[Zahlungssicherheit 2005]
Zahlungssicherheit.de: Glossar – L: Liability Shift/Haftungsumkehr. https://www.kartensicherheit.de/ww/de/pub/glossar/glossar___l.php, Abruf am 12.04.2005

[ZKA 2004]
Zentralen Kreditausschuss: Kreditwirtschaft stellt POZ-Verfahren Ende 2006 ein. Pressemitteilung vom 15.10.2004. http://www.zentraler-kreditausschuss.de/index.php?theme=pressemitteilungen_f.htm&id=51&year=2004, Abruf am 08.04.2005

Autorendarstellung

Markus Breitschaft, Dipl. Wirtsch.-Inf., absolvierte eine Ausbildung zum Luftwaffenoffizier. Anschließend studierte er Wirtschaftsinformatik an der Universität Regensburg mit den Schwerpunkten Bankinformatik, Kryptographie, Systemtheorie und Finanzierung. Seit Abschluss seiner Tätigkeit als Consultant für Informationstechnologie bei der Pallassoft, arbeitet er als wissenschaftlicher Mitarbeiter am ibi research an der Universität Regensburg. Im Rahmen des Kompetenzzentrums E-Business & E-Government beschäftigt er sich mit der Erforschung der Potenziale von Chipkarten und elektronischer Signaturen, Zahlungssystemen im E-Business und E-Government sowie mit der Modellierung und Optimierung von Prozessen.
Kontakt: markus.breitschaft@ibi.de

Thomas Krabichler, Dipl.-Kfm., absolvierte von 1996-1998 eine Ausbildung zum Bankkaufmann. Im Jahr 2002 schloss er das Studium der Betriebswirtschaftslehre mit den Schwerpunkten Wirtschaftsinformatik, Marketing sowie Finanzierung und Bankbetriebslehre an der Universität Eichstätt-Ingolstadt ab. Am ibi research beschäftigte er sich zunächst mit Strukturen europäischer Bankenmärkte, bevor er im Rahmen des Kompetenzzentrums E-Business & E-Government u. a. für das „ibi-Benchmarking Firmenkundenportale“ verantwortlich war. Den aktuellen Forschungsschwerpunkt von Herrn Krabichler bilden Strategien und Geschäftsmodelle zur Einführung und Verbreitung multifunktionaler Chipkarten.
Kontakt: thomas.krabichler@ibi.de

Dr. Ernst Stahl, Dipl.-Kfm., ist seit dem Abschluss seines Studium der Betriebswirtschaftslehre wissenschaftlicher Mitarbeiter am ibi research an der Universität Regensburg. Neben konzeptioneller und wissenschaftlicher Arbeit im Forschungsprojekt „Modellbank“ ist Ernst Stahl Mitautor zahlreicher Artikel in den Themenschwerpunkten „Electronic Banking“ und „Electronic Commerce“ sowie Mitverfasser der Studien "Status quo und Entwicklung des Direct Banking in Deutschland" und „Einsatz von SB-Internet-Terminals in Banken und Sparkassen". Forschungsschwerpunkte sind die Analyse und Bewertung strategischer Positionierungsmöglichkeiten von Finanzdienstleister im Electronic Business.
Seit 2003 leitet Ernst Stahl das Kompetenzzentrum E-Business & E-Government, indem auch dieses Modul des E-Government-Handbuches entstanden ist.
Kontakt: ernst.stahl@ibi.de

Georg Wittmann, Dipl.-Kfm., studierte Betriebswirtschaftslehre an der Universität Regensburg mit den Schwerpunkten Bankinformatik, Finanzierung, Statistik und Finanzwissenschaften. Während seines Studiums war er mehrere Jahre bei Consors Discount-Broker in Nürnberg tätig. Seit Abschluss seines Studiums ist Georg Wittmann wissenschaftlicher Mitarbeiter am ibi research an der Universität Regensburg. Seit 2003 ist er Mitarbeiter des Kompetenzzentrums E-Business & E-Government. Dort sind seine Forschungsschwerpunkte Marketing im Firmenkundengeschäft, E-Government, E-Payment und Electronic Banking sowie insbesondere Modelle zur Einführung und Verbreitung multifunktionaler Chipkarten.
Kontakt: georg.wittmann@ibi.de

Über das ibi

research

an der Universität
Regensburg

Das ibi ist eine Einrichtung zur anwendungsorientierten Forschung und Umsetzung der Forschungsergebnisse in die Finanzwirtschaft.

Ausgangspunkt ist das 1993 gegründete Institut für Bankinformatik und Bankstrategie an der Universität Regensburg. Dieses Institut wurde 2003 in ibi research an der Universität Regensburg umbenannt. Seit diesem Zeitpunkt ist ihm das Institut für Bankinnovation GmbH zur wirtschaftlichen Umsetzung der Foschungsergebnisse zur Seite gestellt. Beide Institute sind über einen gemeinsamen Beirat verbunden.

Gemäß Satzung fließen die Ergebnisse der gemeinnützigen Gesellschaft ibi research unmittelbar in die Lehre der Universität ein. Umgekehrt stützen sich die Arbeiten im ibi research auf die Forschung des Lehrstuhls für Wirtschafsinformatik II, insbesondere Bankinformatik, an der Universität Regensburg.

Die Gesellschafter von ibi research verstehen sich als Paten für eine dauerhafte Kooperation zwischen Universität und Praxis.

Kontakt

ibi research an der Universität Regensburg GmbH
Schloss Thurn und Taxis
Emmeramsplatz 5

93047 Regensburg

Telefon +49 (0)9 41 9 43 – 19 01
Telefax +49 (0)9 41 9 43 – 18 88
http://www.ibi.de
info@ibi.de