

Zahlungsverfahren im Internet

Auswertung der Präsentationsveranstaltung am 21. Februar 2001 und Bewertung der Verfahren aus datenschutzrechtlicher Sicht

0 Einleitung

Mit der stetig steigenden Zahl der Internet-Nutzer in Deutschland und der zunehmenden Verlagerung zahlreicher Geschäftsprozesse in das Internet stellt sich für die Verbraucher immer mehr die Frage, inwieweit sie das Internet nicht nur als Informationsmedium, sondern auch als Mittel nutzen können, um ihren Bedarf an Waren und Dienstleistungen aller Art zu befriedigen. Ob solche Möglichkeiten in Anspruch genommen werden, hängt in entscheidendem Maße davon ab, inwieweit auch eine Bezahlung über das Internet möglich ist.

Die im Offline-Bereich bisher gängigen Möglichkeiten des bargeldlosen Zahlens lassen sich nur teilweise ins Internet übertragen. Vor allem aber fehlt es an der Akzeptanz der Verbraucher, denen ganz überwiegend eine Zahlung über das Internet nicht sicher genug ist. So besteht angesichts der Risiken für Integrität und Authentizität der Daten im Internet nur eine geringe Neigung der Verbraucher, etwa die Kreditkartendaten über das Internet zu übertragen.

Viele Verbraucher befürchten zudem, dass bei der Zahlung im Internet eine Vielzahl von personenbezogenen Daten entsteht, die von den am Zahlungsvorgängen beteiligten Stellen zu allen möglichen Zwecken - beispielsweise zur Erstellung umfassender Kundenprofile - verarbeitet wird. Das Misstrauen, das Schicksal einmal ins Netz gegebener personenbezogener Daten nicht mehr kontrollieren zu können, ist weit verbreitet. Dadurch sinkt die Akzeptanz noch weiter.

Auf der anderen Seite zeigt sich ein erhebliches wirtschaftspolitisches Interesse, den Verbrauchern akzeptable, sichere und dennoch einfach zu handhabende Zahlungslösungen für das Internet anzubieten. Der Gesetzgeber hat mit der Novellierung des Bundesdatenschutzgesetzes (BDSG) einen entscheidenden Schritt dazu getan, indem er in § 3a BDSG nunmehr ausdrücklich die Daten verarbeitenden Stellen dazu verpflichtet, ihre Verarbeitung personenbezogener Daten an dem Ziel von Datensparsamkeit und Datenvermeidung auszurichten. Insbesondere soll dieses Ziel durch Anonymisierung und Pseudonymisierung erreicht werden. Die gleiche Verpflichtung besteht bereits seit 1997 gemäß § 4 Abs. 1 TDDSG, § 13 Abs. 1 MDStV für die Anbieter von Multimedia-Diensten auf der Ebene der Verarbeitung personenbezogener Daten, die bei der Inanspruchnahme solcher Dienste entstehen können. Damit stellt auch der Gesetzgeber klar, dass der beste Datenschutz dort herrscht, wo personenbezogene Daten gar nicht erst entstehen.

Das Angebot von Zahlungslösungen im Internet ist aber nicht nur für die "Business to Consumer (B2C)"-Beziehung, also für die Abwicklung von Prozessen des elektronischen Geschäftsverkehrs (e-Commerce), von Bedeutung. Vielmehr ist eine derzeit sehr dynamische Entwicklung auch in der elektronischen Verwaltung (e-Government) zu beobachten, die dazu führt, dass auch hier über die Zahlung staatlicher Abgaben jeglicher Art über das Internet nachgedacht werden muss. Zahlungsverfahren im Internet beschränken sich daher nicht nur auf die Geschäftswelt, sondern werden auch in den Bereichen "Business to Administration (B2A)" als auch "Consumer to Administration (C2A)" zunehmend Anwendung finden.

Um einen Überblick zu gewinnen, inwieweit die auf dem Markt befindlichen oder geplanten Zahlungsverfahren im Internet den datenschutzrechtlichen Forderungen Rechnung tragen, haben der Berliner Beauftragte für Datenschutz und Akteneinsicht, Herr Prof. Dr. Hansjürgen Garstka, als Vorsitzender der Arbeitsgruppe "Teledienste/Mediendienste" des Düsseldorfer Kreises der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern, Herr Dr. Werner Kessel, als Vorsitzender des Arbeitskreises Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie Herr Dr. Alexander Dix als Vorsitzender des Arbeitskreises Medien dieser Konferenz am 21. Februar 2001 im Berliner Rathaus Schöneberg eine Reihe von Anbietern dazu eingeladen, ihre Lösungen für die Zahlung von Waren und Dienstleistungen im Internet vorzustellen.

Auf der Präsentationsveranstaltung am 21. Februar 2001 im Berliner Rathaus Schöneberg wurden insgesamt 7 Verfahren vorgestellt, die auf unterschiedlichen Ebenen das Bezahlen Internet ermöglichen oder zumindest unterstützen sollen.

Dabei hat sich gezeigt, dass alle sieben Anbieter ein hohes Interesse an Fragen des Datenschutzes und der Datensicherheit haben, da diese Merkmale auch von Anbieterseite als entscheidend für die Akzeptanz empfunden werden. Datenschutz und Datensicherheit werden also weniger als Behinderung sondern vielmehr als Marktvorteil begriffen. Bei allen vorgestellten Verfahren sind unterschiedliche Möglichkeiten der anonymen oder pseudonymen Nutzung vorgesehen, die in der folgenden Bewertung genauer beleuchtet werden sollen.

Dabei wird unter 1. zunächst die Wirkungsweise und der Ansatz der einzelnen Verfahren vorgestellt, bevor unter 2. die einzelnen Verfahren aus datenschutzrechtlicher Sicht betrachtet werden.

1 Die auf der Veranstaltung vorgestellten Verfahren

1.1 SET

SET steht für *Secure Electronic Transaction* und wird von der Gesellschaft für Zahlungssysteme mbH (GZS) angeboten. SET ist selbst kein Zahlungsverfahren im Internet. Bei SET handelt es sich vielmehr um ein Protokoll, das Visa, Mastercard und einige Technologiefirmen 1997 definiert haben.

Voraussetzung für die Anwendung von SET ist, dass der Kunde über eine Kreditkarte verfügt. Auf der Basis von SET können somit grundsätzlich alle Zahlungsverfahren im Internet eingesetzt werden, die über die Zahlungsfunktion einer Kreditkarte realisiert werden.

Um SET anwenden zu können, sind die folgenden Schritte erforderlich:

Der Karteninhaber muss zunächst bei seiner Karten ausgebenden Bank ein SET-Zertifikat beantragen. Ihm wird daraufhin die SET-Wallet-Software von der Bank zur Verfügung gestellt. Der Kunde hat auch die Möglichkeit, die Wallet-Software aus dem Internet herunterzuladen. Nach Benachrichtigung durch die Bank kann der Kunde von einer Zertifizierungsinstanz, dem Trust-Center, das beantragte Zertifikat herunterladen. Der Kunde kann nunmehr die gewünschten Artikel in dem von ihm gesuchten Internetshop auswählen und diese mit der SET-Wallet bezahlen.

1.2 DASIT

Die Abkürzung DASIT steht für *Datenschutz in Telediensten*. DASIT ist eine vom Bundesministerium für Wirtschaft geförderte Pilotanwendung für ein Zahlungssystem im Internet. Träger des Projekts sind die Deutsche Genossenschaftsbank als Konsortialführerin, die Projektgruppe Verfassungsverträgliche Technikgestaltung der Universität Gesamthochschule Kassel sowie als Verantwortliche für die technische Umsetzung die Fa. GMD Forschungszentrum Informationstechnik GmbH. Das Projekt hat eine Laufzeit von Oktober 1998 bis Dezember 2001. Mit dem Verfahren DASIT soll demonstriert werden, dass eine insbesondere an den Grundsätzen von Datenvermeidung und Datensparsamkeit ausgerichtete Bezahlung im Internet möglich ist.

DASIT stellt aus Sicht des Kunden zwei Szenarien zur Verfügung. Zum einen ist es möglich, DASIT in einer sog. vollidentifizierten Variante zu nutzen. Zum anderen hat der Kunde auch die Möglichkeit, DASIT pseudonym anzuwenden. Als Protokoll wurde im Rahmen des Feldversuchs SET eingesetzt (s. 1.1).

1.3 Wire Card

Die Wire Card AG ist ein bankunabhängiger Anbieter für Zahlungsdienstleistungen im Bereich des elektronischen Geschäftsverkehrs. Das Unternehmen bietet Händler orientierte Lösungen an und integriert dabei verschiedene Zahlungskonzepte, wie z. B. das Internet, mobile Plattformen, aber auch die elektronische Bezahlung vor Ort (Point of Sale).

Abhängig von Zahlungsoptionen und Kommunikationsplattformen bietet Wire Card für die Händler unterschiedliche Systeme an, wie beispielsweise "Wire Card Secure Online Payment (SOP)", "Wire Card Batch" oder "Wire Card Escrow Banking". Die Funktionsweisen dieser einzelnen Lösungen sind sehr unterschiedlich, so dass eine Darstellung im einzelnen in diesem Rahmen nicht möglich ist.

1.4 Paybox

Das von der Fa. Paybox.Net AG angebotene Verfahren Paybox basiert auf der Nutzung der Mobilkommunikation. Es ist mit jedem Mobiltelefon in jedem Netz ohne spezifische Technik und ohne zusätzliche Software nutzbar. Paybox unterstützt dabei auch neue Standards, wie WAP GPRS und wird auch in Zukunft UMTS unterstützen.

Zur Funktionsweise von Paybox: Kauft eine Kunde via Internet bei einem Internet-Händler ein, so startet der Händler eine Transaktionsanfrage via Internet bei Paybox. Daraufhin führt Paybox eine Autorisierungsanfrage über GSM beim Kunden durch. Der Kunde muss diese Anfrage mittels PIN bestätigen. Anschließend vergibt Paybox eine Autorisierungsnummer, die mit SSL über das Internet an den Händler übermittelt wird. Gleichzeitig überträgt Paybox die Transaktion an eine X.400 Postbox der Deutschen Bank. Die Deutsche Bank veranlasst beim Kunden die Lastschrift und eine entsprechende Gutschrift beim Händler.

1.5 paysafecard

Die paysafecard ist eine Wertkarte zum Bezahlen im Internet. Zwischen dem Web-Shop-Betreiber und der Wertkarten paysafecard.com Wertkarten AG werden keine personenbezo-

genen Daten ausgetauscht. Der Nutzer der paysafecard kann Zahlungsvorgänge im Internet anonym abwickeln. Es fallen keine Transaktionskosten und Kontoführungsgebühren für den Kunden an. Die paysafecard ist in Deutschland ein Produkt der Commerzbank AG.

In Österreich sind derzeit ca. 100 Akzeptanzstellen unter Vertrag. In Deutschland ist die Markteinführung im Mai 2001 geplant. Der Kunde hat dann die Möglichkeit, an einer der Vertriebsstellen (etwa Commerzbank Shops, Bertelsmann Club, Lotto Toto Annahmestellen, Tankstellen, usw.) Karten im Wert von 50, 100 oder 200 DM zu erwerben. Durch Nutzung mehrerer Karten können Beträge bis zu 2000 DM bezahlt werden. Die paysafecard ist beliebig übertragbar und für Jugendliche unter 18 Jahren wird eine spezielle Karte, die sogenannte <18 paysafecard, angeboten, mit der nur jugendfreie Produkte bzw. Dienstleistungen erworben bzw. in Anspruch genommen werden können.

1.6 infin-MicroPayment

Beim Zahlungsverfahren infin-MicroPayment wird auf der WebSite des Händlers eine 0190-Telefonnummer angezeigt, über die der Kunde eine Transaktionsnummer (TAN) erhält. Nach Eintragung dieser TAN in das im Browser angezeigte Eingabefeld stehen die gewünschten Informationen zum Download bereit. Das Inkasso erfolgt durch die Telekom. Auf der Telefonrechnung erscheint der Betrag (0,50 bis 5,00 DM) sowie eine vom Händler definierte Textinformation. Mit diesem Zahlungsverfahren können nur virtuelle Produkte (z. B. Downloads) bezahlt werden. Der Kunde bleibt gegenüber dem Händler anonym.

1.7 XPressPay

Das Bezahlverfahren XPressPay setzt die Installation von Software auf dem PC des Kunden voraus. Möchte der Kunde ein kostenpflichtiges Internet-Angebot nutzen, so beendet der Client nach einer Bestätigungsanfrage automatisch die bestehende Internetverbindung und baut eine speziell tarifierte Verbindung zum X-PressPay-Inkasso-Server auf. Dieser überträgt dann den modifizierte Call-Record automatisch zum Inkasso-Unternehmen (hier: Telekom). Nach erfolgreichem Abschluss des Bezahlvorgangs wird die ursprüngliche Internetverbindung wieder hergestellt und die Downloadberechtigung dem Contentgeber übermittelt. Als letzter Schritt wird der Content zum Kunden übertragen. Das Verfahren kann zur Abrechnung beliebig hoher Beträge eingesetzt werden.

Auf der Telefonrechnung des Kunden erscheinen alle Einzelbeträge. Eine summarische Auflistung ist möglich, wird aber derzeit nicht unterstützt. Der Name und die Anschrift des Kunden wird nur bei Zahlungsverzug von der Telekom an die Gesellschaft für Online-Zahlungssysteme mbH übermittelt.

2. Datenschutzrechtliche Bewertung

Eine ausführliche datenschutzrechtliche Bewertung der bei der Veranstaltung vorgestellten Verfahren kann nach einer jeweils einstündigen Präsentation nicht vorgenommen werden. Es soll jedoch versucht werden, anhand bestimmter Kriterien Vorteile und Schwachstellen aus datenschutzrechtlicher Sicht anzusprechen. Ein Vergleich der einzelnen Verfahren untereinander ist ebenfalls kaum möglich, da den vorgestellten Lösungen ganz unterschiedliche Ansätze von der reinen Software-Lösung bis zum integrierten Zahlungsverfahren zugrunde liegen.

Die Verfahren sollen zunächst daraufhin untersucht werden, inwieweit sie sich an dem in § 3a BDSG vorgegebenen Ziel von Datenvermeidung und Datensparsamkeit ausrichten. Aufgrund der unterschiedlichen Aufgaben beim Zahlungsvorgang soll dabei differenziert werden zwischen dem Emittenten, d. h. dem Kreditinstitut bzw. dem Anbieter einerseits sowie dem Händler andererseits (s. 2.1).

Unter 2.2 sollen Aspekte der Datensicherheit betrachtet werden. Dabei geht es vor allem um die Datensicherheit bei der Übertragung personenbezogener Daten über das Internet, d. h. insbesondere auch um Fragen der Verschlüsselung personenbezogener Daten.

Schließlich sollen die Verfahren aus der Sicht des Kunden betrachtet werden. Dabei wird unter 2.3 insbesondere dazu Stellung genommen, inwieweit die Zahlungsvorgänge für den Kunden transparent und nachvollziehbar sind.

2.1 Datenvermeidung und Datensparsamkeit

Wie bereits angedeutet, verpflichtet § 3a BDSG die Anwender von Datenverarbeitungssystemen dazu, sich bei deren Gestaltung und Auswahl an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten (Datenvermeidung und Datensparsamkeit). In § 3a Satz 2 BDSG sind dabei schon die wichtigsten Beispiele genannt, mit denen dieses Ziel erreicht werden kann. Danach ist vor allem von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen.

Für die Anwendung von Zahlungslösungen im Internet kommt dem Gesichtspunkt von Anonymisierung und Pseudonymisierung entscheidende Bedeutung zu. Dabei sind hinsichtlich der Anonymität bzw. Pseudonymität des Kunden zwei Seiten zu betrachten. Zum einen ist zu untersuchen, ob der Kunde gegenüber dem Anbieter bzw. dem Emittenten anonym bzw. pseudonym agieren kann. Auf der anderen Seite ist zu prüfen, ob der Kunde beim Einkauf im Internet - ähnlich wie bei den üblichen Bar-Geschäften des täglichen Lebens - anonym bzw. pseudonym gegenüber dem Händler auftreten kann. Zu den Verfahren im Einzelnen:

2.1.1 SET

Im Rahmen der Anwendung von SET ist eine anonyme oder pseudonyme Nutzung gegenüber dem Emittenten nicht möglich und auch nicht vorgesehen. Da die Abrechnung im Rahmen von SET auf der Ausgabe einer Kreditkarte beruht, führt das kartenemittierende Kreditinstitut alle Bestandsdaten, die im Rahmen einer "normalen" Ausgabe einer Kreditkarte verarbeitet werden. Es handelt sich dabei beispielsweise um Daten wie Name, Anschrift, Telefonnummer, Bankverbindung, Kreditrahmen usw. Unter Umständen werden diese Daten bei einem vom Institut beauftragten Dienstleister, dem sog. Prozessor (z. B. der GZS), gespeichert.

Im Rahmen der Abrechnung erhält der Emittent die ebenfalls üblicherweise bei einem Kreditkartenkauf anfallenden Daten über einzelne Transaktionen. Dabei handelt es sich im Wesentlichen um Kartenummer, Verfalldatum, Transaktionsdatum, Währung, Betrag und einen Branchencode. Wie auch bei der Offline-Bezahlung mit einer Kreditkarte erhält das emittierende Kreditinstitut allerdings keine Detailinformationen über den Kauf selbst, insbesondere darüber nicht, welche Artikel im Einzelnen gekauft wurden. Angesichts des mit SET verfolgten Ansatzes, auch bei der Zahlung im Internet ein Kreditkartenbasiertes Modell anzubieten, das der Kreditkartenbezahlung außerhalb des Internets weitgehend entspricht, ist es hier systemimmanent, dass eine Anonymität bzw. Pseudonymität gegenüber der emittierenden Bank

nicht möglich und auch nicht vorgesehen ist.

Gegenüber dem Händler erlaubt SET als Protokoll durchaus zumindest eine pseudonyme Bezahlung. Ob diese tatsächlich angeboten wird, hängt nicht von SET oder der GZS ab, sondern vielmehr vom Design des Internet-Shops. Regelmäßig sollte aber eine pseudonyme Bezahlung gegenüber dem Händler möglich sein. Für die Abrechnung ist es aus Sicht des Händlers in jedem Falle ausreichend, wenn er die Transaktionsnummer als einziges Datum erhält. Diese kann vom Händler nicht ohne Weiteres einer Person zugeordnet werden; dies wäre vielmehr nur mit Hilfe der emittierenden Bank möglich. Weitere Kartendaten des Kunden sind für den Abrechnungsvorgang im SET-Protokoll nicht erforderlich. Insofern kann von einer starken Pseudonymität gegenüber dem Händler ausgegangen werden. Dies ist unter dem Gesichtspunkt von § 3a BDSG positiv zu bewerten.

Zum Zwecke der Ausstellung des Zertifikats durch das Trust-Center werden durch das kartenemittierende Kreditinstitut außerdem Bestandsdaten an das Trust-Center übermittelt. Dabei handelt es sich um Name, Kartenummer und Authentifizierungsdaten des Kunden. Transaktionsdaten erhält das Trust-Center selbstverständlich nicht.

Im Ergebnis ist festzustellen, dass der Grundsatz von Datenvermeidung und Datensparsamkeit zumindest in der Beziehung zwischen Händler und Kunden bei Nutzung des SET-Protokolls in positiver Weise berücksichtigt werden kann.

2.1.2 DASIT

Mit dem Projekt DASIT wird ausdrücklich das Ziel verfolgt, eine an den Zielen von Datenvermeidung und Datensparsamkeit ausgerichtete Variante der Bezahlung von Waren und Dienstleistungen im Internet zu entwickeln.

Bei DASIT wird bereits auf der Ebene der Bestandsdaten die Möglichkeit geboten, zwischen einer vollidentifizierten Variante und einer pseudonymen Variante zu wählen. Wünscht der Kunde die Vollidentifizierung, so werden Name, Anschrift, e-mail-Adresse und Telefonnummer obligatorisch verarbeitet. Für die Nutzung zu Marketing-Zwecken können außerdem optional Alter und Interessengebiete angegeben werden.

Bei der pseudonymen Variante werden keine Bestandsdaten erhoben. Optional ist auch hier zu Marketing-Zwecken die Angabe von Alter und Interessengebiet möglich. Das Pseudonym gibt sich der Nutzer selbst und lässt dieses bei einer Zertifizierungsstelle registrieren. Das Zertifikat über das Pseudonym ist mit keinem weiteren Datum verknüpft, das einen Bezug zur Identität des Nutzers herstellt.

Auch bei der pseudonymen Nutzung werden allerdings zum Zwecke der Lieferung der Ware personenbezogene Daten durch den Emittenten erhoben. Dabei handelt es sich um Name und Lieferanschrift. Diese Daten werden an den Transportunternehmer weitergegeben.

Bei Nutzung der pseudonymen Variante kann der Kunde auch gegenüber dem Händler pseudonym auftreten. Der Händler erhält dabei nur Informationen über den Warenkorbinhalt sowie die Transaktionsnummer (TAN). Eine Zuordnung dieser Information zur Person des Kunden ist durch den Händler nahezu ausgeschlossen. Der Händler kann bestenfalls den Bezug zum Pseudonym, das sich der Nutzer selbst gegeben hat, herstellen.

Als weitere Stellen sind bei DASIT der Zertifizierer, der Prozessor sowie das Transportunternehmen beteiligt. Die Zertifizierungsinstanz ist nicht in den eigentlichen Zahlungsvorgang involviert. Sie erhält bei der vollidentifizierten Variante Name und Anschrift, bei der pseudonymen Variante zusätzlich die Zuordnung des Pseudonyms. Beim Prozessor, z. B. der GZS, werden sog. Zahlungsinformationen verarbeitet. Das sind Daten darüber, wer bei welchem Händler zu welchem Preis eingekauft hat. Bei der pseudonymen Variante verarbeitet der Prozessor diese Daten nur unter dem Pseudonym. Das Transportunternehmen erhält - wie oben angedeutet - Name und Anschrift des Kunden sowie im Falle der pseudonymen Variante die Transaktionsnummer.

Hierbei wird der Grundsatz von Datenvermeidung und Datensparsamkeit weitgehend berücksichtigt. Angesichts der Zielstellung des Projektes DASIT wäre es wünschenswert gewesen, auch eine gegenüber dem Emittenten anonyme bzw. pseudonyme Auslieferung der gekauften Ware zu ermöglichen.

Im Ergebnis ist auf der Grundlage von DASIT eine pseudonyme Nutzung, die sowohl aus Sicht des Händlers als auch des Emittenten einer anonymen Nutzung sehr nahe kommt, möglich. Dies ist aus datenschutzrechtlicher Sicht deutlich positiv zu bewerten.

2.1.3 Wire Card

Bei Wire Card hat der Kunde im Regelfall gegenüber dem Zahlungsdienstleister keine Möglichkeit, anonym aufzutreten. Im Einzelnen hängt dies allerdings von dem zugrunde liegenden Zahlungsmittel ab. So besteht z. B. bei einem Prepaid Zahlungsmittel wie der PaysafeCard durchaus die Möglichkeit, dass der Kunde auch gegenüber dem Zahlungsdienstleister anonym bleibt.

Da es sich bei Wire Card um einen bankunabhängigen Händler orientierten Anbieter handelt, werden bei Wire Card selbst keine Bestandsdaten verarbeitet. Wire Card verarbeitet dementsprechend lediglich Transaktionsdaten. Welche Transaktionsdaten im einzelnen gespeichert werden, ist wiederum abhängig von dem zugrunde liegenden Zahlungsmittel. Erfolgt die Abrechnung beispielsweise über ein Kreditkartenkonto, so werden - ähnlich wie bei SET - die bei einer Kreditkartenbezahlung üblichen Transaktionsdaten durch den Zahlungsdienstleister verarbeitet. Dazu gehören Kreditkartennummer, Gültigkeitsdatum, Name, Betrag und Händler. Diese Daten dienen ausschließlich der Abwicklung der Transaktion und werden acht Jahre bei Wire Card gespeichert.

Ob ein Kunde gegenüber dem Händler anonym auftreten kann, hängt wiederum vom gewählten Zahlungsmittel ab. Bei Prepaid besteht auch hier diese Möglichkeit. Eine gegenüber dem Händler pseudonyme Zahlung ist bei der am häufigsten gewählten Variante der Bezahlung über Kreditkarte im Regelfall möglich. Beim Händler werden in diesem Falle lediglich eine Transaktionsnummer, die auf vier Stellen gekürzte Kreditkartennummer und die Mitteilung über die erfolgte Zahlung gespeichert.

Als weitere Stellen, die im Rahmen der Nutzung von Wire Card personenbezogene Daten verarbeiten, kommen vor allen Dingen Dienstleister in Betracht, die ein Scoring des Kunden durchführen. Dabei besteht in der Regel jedoch kein direkter Zusammenhang zu konkreten Zahlungsvorgängen.

Insgesamt ist auch das Verfahren Wire Card unter dem Blickwinkel von Datenvermeidung und Datensparsamkeit überwiegend positiv zu beurteilen. Während die Verarbeitung personenbe-

zogener Daten durch den Zahlungsdienstleister weitgehend unabhängig von Wire Card stattfindet, bietet Wire Card gegenüber dem Händler die Möglichkeit der pseudonymen Bezahlung. Angesichts der Struktur der Pseudonyme kann davon ausgegangen werden, dass der Händler einen Personenbezug mit vernünftigen Aufwand nicht herstellen kann.

2.1.4 Paybox

Beim Verfahren Paybox ist eine Anonymität gegenüber dem Emittenten nicht möglich. Im Regelfall werden als Bestandsdaten Namen, Adresse, Kontoverbindung, Berufsstand und Telefonnummer des Mobiltelefons gespeichert. Darüber hinaus vergibt Paybox eine PIN und setzt ein persönliches Limit fest. Nach Wahl des Kunden ist es allerdings unter Nutzung der sog. Alias-Funktionalität möglich, pseudonym gegenüber dem Emittenten zu agieren. Der Kunde kann sich dabei sein eigenes Pseudonym aussuchen. Eine Wiederherstellung des Personenbezugs ist in der Paybox-Datenbank möglich. Zunächst erfolgt eine Verknüpfung mit der Handynummer und in einem weiteren Schritt deren Verknüpfung mit der Anschrift des Kunden.

Um insbesondere das persönliche Limit festsetzen zu können, übermittelt Paybox Adresse, Geburtsdatum und Berufsstand zum Zwecke des Scoring an die Fa. Creditreform.

Im Rahmen des einzelnen Zahlungsvorgangs wird eine Reihe von Transaktionsdaten verarbeitet. Es handelt sich dabei um Händler-ID, Kunden-ID, Kaufbetrag, Kaufdatum, Authorisationsnummer und Händlernauftragsnummer. Aus der Kunden-ID ist für die sonst am Zahlungsvorgang beteiligten Stellen (außer Paybox) die Herstellung eines direkten Personenbezuges nicht möglich. Die Verarbeitung dieser Daten dient der Abwicklung des Zahlungsvorgangs. Nach Abwicklung des Zahlungsvorganges werden keine Daten mit direktem Personenbezug bei Paybox gespeichert. Im Übrigen wird durch Paybox das Verfügungslimit ständig fortgeschrieben. Da jede Transaktion als Lastschrift auf den Konsumenten gezogen wird, werden keine Salden gebildet.

Gegenüber dem Händler ist bei Paybox auf Wunsch des Kunden eine pseudonyme Bezahlung möglich. Beim Händler wird lediglich die Authorisationsnummer gespeichert. Eine Herstellung des Personenbezugs wäre für den Händler nur mit großem Aufwand möglich. Dieser hängt zum einen davon ab, wie intelligent sich der Kunde sein Pseudonym gewählt hat. Im Übrigen wäre die Herstellung des Personenbezugs nur durch einen Zugriff auf die Paybox-Datenbank möglich, den der Händler selbstverständlich nicht hat.

Neben der bereits genannten Fa. Creditreform ist - wie unter 1.4 beschrieben - die Deutsche Bank als Prozessor am Zahlungsvorgang beteiligt. Sie hat die Aufgabe, die Transaktionen in Gutschriften und Lastschriften umzuwandeln. Zu diesem Zwecke erhält die Deutsche Bank bei jeder Transaktion die Kunden-ID, den Kaufbetrag, das Kaufdatum sowie die Händler-ID. Aufgrund der Tatsache, dass die Bezahlung über eine Lastschrift des Kundenkontos erfolgt, ist auch gegenüber der Deutschen Bank keine Anonymität gewährleistet.

Zusammenfassend ist festzustellen, dass das Verfahren Paybox die Verpflichtung zu Datenvermeidung und Datensparsamkeit gut erfüllt. So ist aufgrund der Funktionsweise von Paybox zwar eine Anonymität gegenüber dem Emittenten nicht möglich; gegenüber dem Händler kann jedoch weitgehend Pseudonymität auf Kundenwunsch erreicht werden.

2.1.5 *paysafecard*

Bei der *paysafecard* handelt es sich um eine Prepaid-Karte. Es werden keine personenbezogenen Daten erhoben und verarbeitet. Der Kunde hat dadurch die Möglichkeit, im Internet anonym zu bezahlen.

2.1.6 *infin-MicroPayment*

Wählt der Kunde die auf der Web-Site des Händlers angezeigte 0190-Nummer, wird die Telefonnummer des Kunden und der zu zahlende Betrag bei der DTAG zu Abrechnungszwecken gespeichert. Der Anruf des Kunden wird zum Emittenten weiter geroutet, allerdings ohne die Rufnummer des Kunden zu übertragen. Die Zuordnung des Rechnungsbetrages zum Kunden nimmt die DTAG vor. Der Emittent bekommt von der DTAG einen Gesamtbetrag über alle Abrufe ausgeschüttet, den er dann entsprechend seiner Daten über Betrag und Produkt auf die einzelnen Anbieter verteilt.

Aufgrund der erhobenen und gespeicherten Daten ist der Kunde gegenüber dem Händler und dem Emittenten anonym. Die DTAG kennt zwar den Namen und die Telefonnummer des Kunden, hat aber keine Informationen über die vom Kunden erworbenen Produkte. Auf dem Einzelbindungsnachweis der DTAG erscheint derzeit lediglich der Name des Händlers, wodurch unter Umständen ein Bezug zu den erworbenen Produkten hergestellt werden kann.

Es ist festzustellen, dass beim Verfahren *infin-MicroPayment* die Prinzipien der Datenvermeidung und der Datensparsamkeit gut umgesetzt werden.

2.1.7 *XpressPay*

Bei diesem Verfahren liegen die nutzerrelevanten Daten ausschließlich bei der Telefongesellschaft und werden zur Abrechnung der Leistungen benötigt. Der Händler erhält keine personenbezogenen Daten. Bei Zahlungsverzug erhält *XpressPay* von der Telefongesellschaft die Nutzer-Daten für weiteres Inkasso. Auf dem Einzelbindungsnachweis der Telefongesellschaft werden die Namen der Händler und die Beträge aufgelistet.

Die Anonymität der Kunden gegenüber dem Emittenten und den Händlern ist sichergestellt. Das Verfahren ist daher unter dem Gesichtspunkt von Datenvermeidung und Datensparsamkeit positiv zu bewerten.

2.2 Aspekte der Datensicherheit

Die folgenden Ausführungen zu Fragen der Datensicherheit bei den einzelnen Zahlungsverfahren haben lediglich eine eingeschränkte Aussagekraft, da sie auf von unserer Seite nicht überprüfbaren Angaben der Anbieter beruhen. Im Einzelnen:

2.2.1 *SET*

Bei der Datenübertragung werden im Rahmen von SET grundsätzlich symmetrische und asymmetrische hybride kryptografische Verschlüsselungsverfahren eingesetzt (RSA 1024 bit, DES, SHA-1 Hashing mit 160 bit). Zudem wird jede Nachricht mit einer digitalen Signatur nach

dem X.509-Standard versehen. Insofern ist eine starke Authentizität zwischen Käufer und Verkäufer gegeben. Eine Schwachstelle liegt in der Offline-Eingabe der Kreditkartennummer am Kunden-PC. Das Protokoll SET sieht als Möglichkeit auch die Einbeziehung von Chipkarten zur Authentifizierung des Karteninhabers vor. Diese Möglichkeit befindet sich allerdings in Deutschland noch nicht im praktischen Einsatz.

Die die Zertifikate vergebenden Trust-Center werden von den Kreditkartenunternehmen Visa und MasterCard einem Audit zu Aspekten der Datensicherheit unterzogen. Bei erfolgreichem Audit wird durch Visa und MasterCard das Schlüsselmanagement, die Firewall-Technologie, die Systemsicherheit sowie die Gebäudesicherheit zertifiziert.

Soweit Aspekte der Datensicherheit von SET abhängig sind, kann insgesamt ein hohes Datensicherheitsniveau festgestellt werden.

2.2.2 DASIT

Bei der Nutzung von DASIT kommen folgende Elemente der Datensicherheit zum Einsatz:

- SSL-Verschlüsselung zwischen Browser des Nutzers und dem DASIT-Server,
- zwischen dem DASIT-Server und dem Mail-System XML erfolgt eine http-Übertragung,
- zwischen Transporteur und Nutzer erfolgt beim pseudonymem Einkauf eine Verschlüsselung mit SSL.

Soweit als Protokoll SET genutzt wird, wird auf die Ausführungen zu 2.2.1 verwiesen.

Damit kann, wie bei SET, festgestellt werden, dass bei der Nutzung von DASIT ein hohes Niveau der Datensicherheit gewährleistet ist.

2.2.3 Wire Card

Im Verfahren Wire Card kommen beim Emittenten ebenfalls zahlreiche Sicherheitsfunktionen zum Einsatz. Der Schutz der bei Wire Card gespeicherten Daten gegen unberechtigten Zugriff erfolgt durch den Einsatz mehrstufiger Firewalls, einer Zugangskontrolle, durch weitgehende Verwendung des Vier-Augen-Prinzips, durch die Verwendung von Alarmmechanismen und nicht zuletzt durch den Einsatz starker Verschlüsselungsverfahren. Für den Administrator besteht kein Vollzugriff auf die gesamten gespeicherten Daten.

Der Schutz der Vertraulichkeit beim Händler, bei zwischengeschalteten Stellen sowie beim Kunden hängt nicht von Wire Card ab. Bei der Übertragung der Transaktionsdaten zwischen Kunden und Wire Card sowie zwischen Händler und Wire Card werden starke Verschlüsselungsverfahren (Blowfish 2048 Bit RSA) eingesetzt. Für den Fall, dass ein Browser mit diesen Verschlüsselungsverfahren nicht kompatibel ist, erfolgt zunächst eine Verschlüsselung mit SSL 128 Bit, funktioniert auch dies nicht, dann mit 40 Bit. In diesen Fällen erfolgt eine vorherige Warnung des Kunden.

Die Schlüssel werden nach dem Zufallsprinzip generiert und durch ein Workflow-System automatisch verwaltet. Bei der Entwicklung der Kryptografie-Software wird nach einem mehrstufigen Vier-Augen-Prinzip vorgegangen.

Die Integrität der Daten wird durch MD 5 (Hash) abgesichert. Bei Verletzungen der Integrität erfolgt ein sofortiger Verbindungsabbruch und eine interne Alarmierung. Die Integrität der Daten wird beim Händler durch Verwendung einer digitalen Signatur nach dem X.509-Standard sichergestellt.

Die Authentizität zwischen Händler und Emittent wird durch den Einsatz von Zertifikaten geprüft.

Eine Zertifizierung des Verfahrens ist bisher nicht erfolgt.

Zusammenfassend ist aufgrund den uns vorliegenden Informationen bei Wire Card von einem hohen Niveau der Datensicherheit auszugehen.

2.2.4 Paybox

Die Paybox-Datenbank ist in einem Hochsicherheitstrakt der Fa. Lufthansa Systems untergebracht. Die Vertraulichkeit der Daten wird durch eine doppelte Firewall der Lufthansa Systems, einer nach einem Rollenkonzept vorgenommenen Verteilung der Zugriffsrechte, einer physischen Zugangskontrolle zu den Arbeitsplätzen und einem passwortgeschützten Zugang zur Datenbank abgesichert.

Die Datenübermittlung an die Deutsche Bank erfolgt über eine X.400 Postbox nach den Sicherheitsanforderungen der Deutschen Bank. Die Datenübertragung zwischen Händler und Paybox findet über einen SSL-Tunnel unter Verwendung eines authentifizierten Zertifikats statt.

Als Verschlüsselungsverfahren kommen 128 Bit SSL, 3 DES IPsec sowie GSM-interne Verfahren zum Einsatz.

Die Integrität der Daten würde durch Übertragungsprotokolle und Prüfsummen gesichert. In der Kommunikation mit den Händlern werden Zertifikate eingesetzt. Eine Prüfung der Authentizität erfolgt zwischen dem Händler und dem Payboxsystem. Als Authentifizierungsmechanismus kommen SSL-Zertifikate zum Einsatz, wobei eine gegenseitige Authentifizierung erfolgt.

Der Nachweis über durchgeführte Transaktionen wird dadurch geführt, dass der Kunde jede Transaktion mit seiner PIN bestätigen muss und per SMS und e-mail informiert wird.

Das Datensicherheitsniveau bei Paybox wird insgesamt als gut eingeschätzt.

2.2.5 paysafecard

Auf der paysafecard befindet sich ein PIN-Code, der vor dem ersten Gebrauch der Karte freigerubbelt werden muss. Der Kartenbesitzer kann den PIN-Code mit einem Passwort schützen, sodass ein Missbrauch bei Verlust der Karte ausgeschlossen ist. Beim Bezahlen im Web-Shop gibt der Kunde den PIN-Code ein, wodurch der zu bezahlende Betrag von seinem virtuellen Konto abgebucht wird. Nach dreimaliger Falscheingabe der PIN wird die IP-Adresse des Kunden für eine bestimmte Zeit gesperrt.

Der Kunde hat jederzeit die Möglichkeit, sich über den noch zur Verfügung stehenden Karten-

betrag auf der Web-Site des Emittenten zu informieren. Die Kommunikation zwischen dem Kunden und **paysafecard.com** erfolgt verschlüsselt. Zur Verschlüsselung der übertragenen Daten wird das Sicherheitsprotokoll SSL¹ in der Version 2 (40 Bit oder 128 Bit) eingesetzt. Es erfolgt eine Server-Authentifizierung. Der Datenaustausch zwischen **paysafecard.com** und dem Web-Shop erfolgt ebenfalls verschlüsselt. Hier kommt SSLv3 zum Einsatz. Die erforderlichen Zertifikate zur Client- und Server-Authentifizierung werden von Versign oder dem Emittenten erzeugt.

Aufgrund der realisierten technischen Maßnahmen wird die Datensicherheit als sehr gut eingeschätzt.

2.2.6 infin-MicroPayment

Die einzelnen Transaktionen können über den benutzten Telefonanschluss eindeutig dem Kunden zugeordnet werden. Die Übertragung der TAN vom Kunden zum Emittenten erfolgt unverschlüsselt. Durch einmalige Verwendung von Transaktionsnummern kann ein Missbrauch weitestgehend ausgeschlossen werden. Die TAN's bleiben in der TAN-Datenbank des Emittenten für einen gewissen Zeitraum gespeichert, so dass der Kunde bei Verbindungsunterbrechungen oder anderen Fehlern die TAN auch noch zu einem späteren Zeitpunkt benutzen kann.

Die Datensicherheit des Verfahren wird insgesamt als gut eingeschätzt.

2.2.7 XpressPay

In der zu installierenden Software ist eine Verschlüsselungskomponente enthalten, die mit einer Schlüssellänge von 4000 Bit arbeitet. Das implementierte Verschlüsselungsverfahren ist nicht bekannt. Die Verbindung zum XpressPay-Server erfolgt über eine Direktverbindung, wodurch eine hohe Performance und eine maximale Sicherheit erreicht wird. Angriffe Dritter können nahezu ausgeschlossen werden.

Das Datensicherheitsniveau bei *XpressPay* wird insgesamt als gut eingeschätzt.

2.3 Transparenz und Handhabbarkeit für den Kunden

Der Kunde kann seine Datenschutzrechte nur dann in Anspruch nehmen, wenn die Zahlungsverfahren im Internet aus seiner Sicht transparent sind und er nachvollziehen kann, welche Datenverarbeitungsschritte innerhalb des Verfahrens erfolgen. Im Übrigen hängt die Akzeptanz der Verfahren entscheidend nicht nur von der Transparenz ab, sondern auch davon, ob die Handhabung des jeweiligen Verfahrens einfach ist.

2.3.1 SET

Bei SET kann der Kunde seine Zahlungen nachvollziehen. Dafür steht ihm in der SET-Wallet eine Transaktionshistorie zur Verfügung. Darüber hinaus kann der Kunde auch Informationen

¹ Secure Socket Layer

über einzelne Transaktionen erhalten.

Die Akzeptanz von SET ist bisher allerdings vor allem deshalb nicht besonders hoch, da SET sowohl für die Händler als auch für die Karteninhaber ein relativ kompliziertes Verfahren ist. Dies könnte sich in Zukunft möglicherweise dann ändern, wenn ein zentrales System unter der Bezeichnung 3D-SET eingeführt wird, mit dem eine Zentralisierung der Systeme und der Verantwortung bei den Händlerbanken und Kartenemittenten erfolgen soll.

2.3.2 DASIT

Wie bereits angesprochen, ist DASIT grundsätzlich unabhängig von einem konkreten Zahlungssystem. Ob also eine Transparenz für den Kunden insoweit gegeben ist, als er seine Zahlungen generell und im Einzelfall nachvollziehen kann, hängt vom verwendeten Zahlungssystem ab. Bei dem im Feldversuch eingesetzten SET wird auf die Ausführungen zu 2.3.1 Bezug genommen.

2.3.3 Wire Card

Da die Abrechnung im Regelfall über die Kreditkarte vorgenommen wird, kann der Kunde seine Zahlungen auch im Einzelfall über die Kreditkartenabrechnung nachvollziehen. Der Kunde kann darüber hinaus jede Transaktion unter Zuhilfenahme der Transaktions-ID nachprüfen. Er erhält allerdings keine Auskunft über Daten, die unter seinem Pseudonym gespeichert sind.

Die Kunden werden bei Wire Card regelmäßig über das Sicherheitsniveau und die verwendeten Sicherheitsmaßnahmen des Zahlungssystems unterrichtet. Dies gilt natürlich nur insoweit, wie Wire Card in dem Prozess eingebunden ist.

Wie hoch die Akzeptanz und wie einfach die Handhabung ist, kann aufgrund der vorliegenden Erkenntnisse nicht sicher eingeschätzt werden. Insofern ist eine Bewertung in diesem Punkt nicht möglich.

2.3.4 Paybox

Bei Paybox kann der Kunde über das Paybox-Extranet mit Eingabe seiner PIN alle Transaktionen nachvollziehen. Seine letzte Transaktion kann jeweils telefonisch überprüft werden. Als Beweismittel steht dem Kunden zum einen die Lastschrift zur Verfügung. Zum anderen erhält der Kunde bei einer korrekten oder abgebrochenen Transaktion jeweils eine SMS oder e-mail.

Die Handhabung von Paybox stellt den Nutzer aus unserer Sicht vor keine hohen Anforderungen. Die einzelnen Schritte bei der Bezahlung mit Paybox sind gut nachvollziehbar.

2.3.5 paysafecard

Auf der Web-Site von **paysafecard.com** kann sich der Kunde umfassend über das Verfahren informieren. Auch hat der Kunde jederzeit die Möglichkeit, den noch zur Verfügung stehenden Kartenbetrag auf der Web-Site des Emittenten einzusehen. Für Webshop-Betreiber wird ein

API² kostenlos zur Verfügung gestellt. Die Funktionen des API sind ausführlich dokumentiert.

Das Zahlungsverfahren kann vom Kunden leicht nachvollzogen werden. Die Transparenz und Handhabbarkeit des Verfahrens kann daher als sehr gut eingeschätzt werden.

2.3.6 infin-MicroPayment

Auch bei diesem Verfahren hat der Kunde die Möglichkeit, sich auf der Web-Site des Anbieters über den Bezahlvorgang zu informieren. Der Kunde kann die einzelnen Transaktionen durch den Einzelverbindungs nachweis der DTAG nachvollziehen. Die Handhabung des Verfahrens wird bei Verwendung analoger Telefonanschlüsse erschwert, da der Kunde die aktuelle Internet-Session beenden muss, bevor er die 0190-Nummer wählen kann. Nach Erhalt der TAN muss eine neue Verbindung zum Internet aufgebaut werden.

Das Verfahren ist für die Kunden transparent und jedenfalls bei Nutzung eines ISDN-Anschlusses gut handhabbar. Bei analogen Anschlüssen sind Einschränkungen hinzunehmen.

2.3.7 XpressPay

Auf dem Einzelverbindungs nachweis der Telefongesellschaft können die einzelnen Transaktionen nachvollzogen werden. Die getätigten Transaktionen werden auf dem lokalen System des Kunden gespeichert und können mit Hilfe des Browsers offline eingesehen werden. Dadurch hat der Kunde die Möglichkeit, die durchgeführten Transaktionen zu überprüfen.

Die vor der ersten Benutzung zu installierende Software ermöglicht eine einfache Bedienung. Als unter Umständen problematisch ist die automatische Unterbrechung der Internetverbindung anzusehen. Ein beispielsweise im Hintergrund laufender Download könnte undefiniert abgebrochen werden.

Sven Hermerschmidt

² Application programmers interface